Wireless Communications and Mobile Computing

Security and Intelligence of the Internet of Things for 5G and B5G Networks

Lead Guest Editor: Muhammad Asghar Khan
Guest Editors: Mohammed H. Alsharif and Rosdiadee Nordin

Security and Intelligence of the Internet of Things for 5G and B5G Networks

Wireless Communications and Mobile Computing

Security and Intelligence of the Internet of Things for 5G and B5G Networks

Lead Guest Editor: Muhammad Asghar Khan
Guest Editors: Mohammed H. Alsharif and Rosdiadee Nordin

Chief Editor

Associate Editors

Academic Editors

Contents

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4851364, 14 pages
https://doi.org/10.1155/2022/4851364

Research Article

Evolutionary Heuristic Computing Paradigm for 2D-DOA Estimation along Circular Array

Fiaz Hussain Shah,[1] Muhammad Asif Zahoor Raja,[2] Fadi Al-Turjman,[3] Fawad Zaman,[4] and Xiaodong Yang[1]

[1]*School of Electronic Engineering, Xidian University, Xi'an 710071, China*
[2]*Department of Electrical and Computer Engineering, COMSATS University Islamabad, Attock Campus, Attock 43600, Pakistan*
[3]*Artificial Intelligence Engineering Department, Research Centre for AI and IoT, Near East University, 99138 Nicosia, Mersin 10, Turkey*
[4]*Department of Electrical & Electronic Engineering, Imperial College London, UK*

Correspondence should be addressed to Xiaodong Yang; xdyang@xidian.edu.cn

Received 3 October 2021; Revised 21 November 2021; Accepted 6 April 2022; Published 30 April 2022

Academic Editor: Muhammad Asghar Khan

Direction of arrival (DOA) estimation problem has growing interest for the researcher investigating in system identification models arising in the field of digital signal processing, mobile communication, controls, and beamforming. In the presented work, evolutionary heuristic computing paradigm is presented for 2D-DOA estimation of plane waves impinging on uniform circular array. Performance metric of mean squared error is utilized as construction of a fitness function for the system, and the optimization strength of three methodologies, genetic algorithms (GAs), Pattern Search (PS), and integration of GAs with PS (GA-PS) is exploited for 2D-DOA estimation based on elevation as well as azimuth angles. Consistent precision, convergence, stability, and robustness of integrated heuristics of GA-PS are endorsed through outcomes of statistical observations.

1. Introduction

The use of different antenna structural arrays has growing interest in researchers due to remarkable performance in the domain of direction-of-arrival (DOA) parameter estimation, beamforming, radars, sonars, and seismology. Researchers proposed different DOA estimation procedures including MUSIC [1, 2], ESPRIT [3, 4] spatial smoothing methods [5, 6], subspace smoothing procedures [7], and temporal smoothing approach [8] for uniform linear array (ULA). The two-dimensional (2D) DOA (2D-DOA) estimation one preferred to used two-dimensional arrays based on L-shaped array [9, 10], nested array [11–13], coprime array [14, 15], uniform rectangle array (URA) [16, 17], uniform circular array (UCA) [18, 19], virtual uniform-linear-like array (VULA) [20], and visual array VT-MUSIC algorithm [21]. The transformation procedure also exploited for two-dimensional DOA (2D-DOA) estimation algorithms with relatively low computational requirement including UCA-RB-MUSIC [22], UCA-ESPRIT [23], UCA rank reduction [24], and root-MUSIC approach [25]. Beside these deterministic techniques for 1D and 2D DOA estimation, the stochastic procedures are also adopted for these global search based optimization problems [26–29]. All the existing procedures adopted for system identification of DOA models motivate

authors to investigate stochastic optimization mechanism by exploitation of evolutionary heuristics for joint estimation of two-dimensional DOA parameters impinging on circular structural array of far field sources.

The stochastic optimization mechanism by exploitation of artificial intelligence techniques has been implemented extensively to address constrained and unconstrained optimization model associated with a variety of linear/nonlinear systems [30–33]. Few prevailing recent applications include Hammerstein nonlinear control autoregressive systems, active noise control system, transport model for soft tissues, nonlinear optics, nonlinear Bratu systems, nonlinear fractional Riccati systems, nonlinear Jeffery-Hamel flow, nonlinear prey-predator, nonlinear thin film flow models, nonlinear FalknarSkan system, nonlinear Troesch problem, nonlinear singular Lane-Emden systems, nonlinear Thomas-Fermi model of atom, piezoelectric model, magneto-hydrodynamics, astrophysics, atomic physics, plasma physics, control, signal processing, energy, bioinformatics, economics, and finance (see references [34–36] and citation therein). These are source of incitements for authors to perform exploration and exploitation in evolutionary computational heuristic paradigm reliable treatment of 2-D DOA estimation of plane waves impinging of UCA.

In this paper, stochastic optimization solvers are presented for 2D-DOA estimation impinging on UCA from far field sources. The salient features of the scheme are highlighted as follows:

A novel application of evolutionary computational heuristic paradigm is presented for two-dimensional DOA estimation of far field sources involving uniform circular array by exploitation of global search efficacy of genetic algorithms (GAs), pattern search (PS), and integrated strength of GA-PS algorithms.

The performance of optimization mechanisms is substantiated by effective implementation of uniform circular array-based DOA estimation problem having different degrees of freedom. The results of integrated solver GA-PS are relatively better from standalone counterparts GA and PS for each scenario of the data model for DOA.

Consistent accuracy and convergence of the hybrid optimization scheme GA-PS are endorsed through outcomes of statistical observations for DOA problems with different numbers of decision variables and noise variations.

Organization of remaining of the paper is as follows. The data model for two-dimensional DOA estimation problem with uniform circular array geometry is presented in Section 2. Optimization methodology of all three algorithms is described in Section 3. The results of simulations through enough graphical and numerical illustrations with necessary interpretations are presented in Section 4. While the conclusions and further work are provided in last Section 5.

2. Data Model: 2D-DOA Estimation with UCA

When the data or system model for 2D-DOA estimation of plane waves impinging on UCA is presented here, the

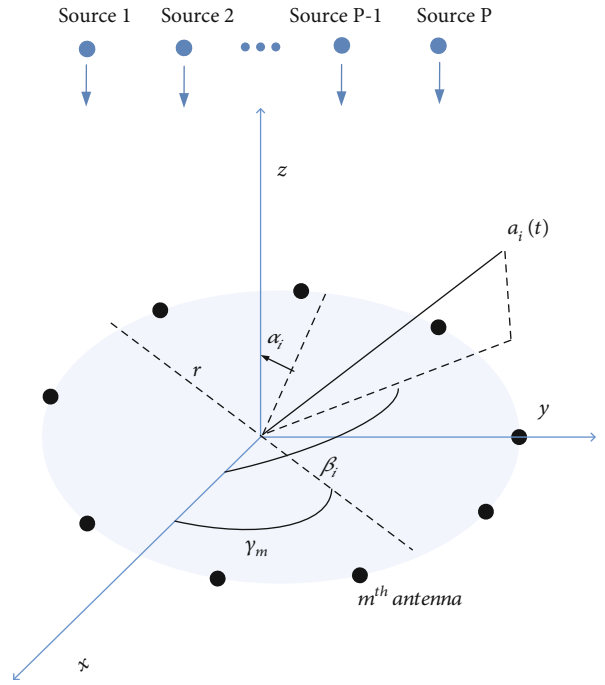


Figure 1: UCA geometry for plane waves.

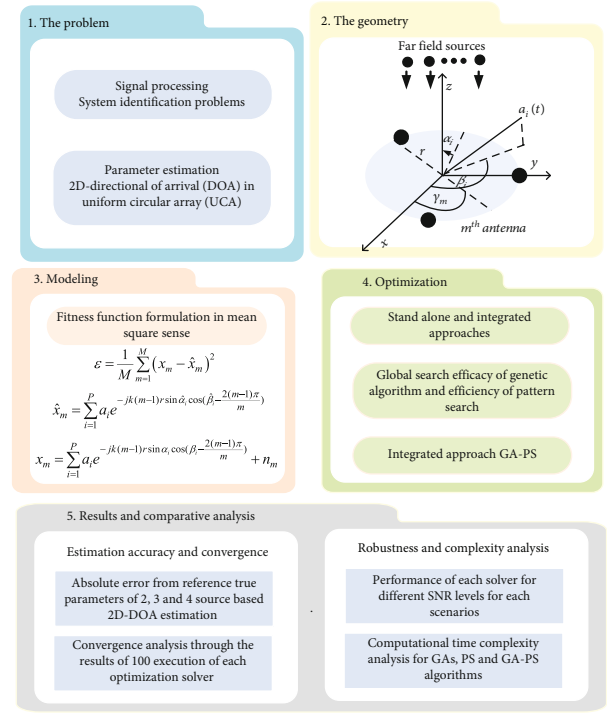


Figure 2: Block structure representation of workflow of the system.

UCA with M antennas have the angle of elevation α between 0 and $\pi/2$ and azimuth β between 0 and 2π for P far field sources, while the angle $\gamma_m = 2\pi m/M$ between mth antenna element for m between 0 and M-1 as shown in Figure 1.

Each electric field signal of m^{th} antenna in UCA from i^{th} sources is written as

$$E(r_m, t) = a_i(t)\mathrm{e}^{j\omega(t-d_i \cdot r_m)}, \quad \text{for } r_m = (x_m, y_m, z_m) = (r\sin(\beta_m), r\cos(\beta_m), 0), \tag{1}$$

where ω denotes the frequency, a_i be the i^{th} amplitude and d_i be i^{th} propagation direction at instance t. The relation for d_i in polar coordinates is given as

$$d_i = \frac{1}{c}(\sin\alpha_i \cos\beta_i, \sin\alpha_i \sin\beta_i, \cos\alpha_i). \tag{2}$$

Then,

$$d_i \cdot r_m = \frac{r}{c}\sin\alpha_i \cos(\beta_i - \gamma_m). \tag{3}$$

Equation (1) becomes

$$\begin{aligned} E(r_m, t) &= a_i(t)e^{j\omega(t-(r/c)\sin\alpha_i \cos(\beta_i-\gamma_n)} \\ &= a_i(t)\mathrm{e}^{j\omega t}\mathrm{e}^{-j(\omega r/c)\sin\alpha_i \cos(\beta_i-\gamma_m)}, \end{aligned} \tag{4}$$

for $A_i(t) = a_i(t)\mathrm{e}^{j\omega t}$ and $k = \omega/c = 2\pi/\lambda$; we get

$$E(r_m, t) = A_i(t)e^{-jkr(m-1)\sin\alpha_i \cos(\beta_i-\gamma_m)}. \tag{5}$$

In case of response, $x_m(t) = E(r_m, t)$ of m^{th} antenna of UCA with noise $n_m(t)$ is given as

$$x_m(t) = \sum_{i=1}^{P} a_i(t)e^{-jk(m-1)r\sin\alpha_i \cos(\beta_i-((2(m-1)\pi)/m))} + n_m(t). \tag{6}$$

The response for single snapshot is given as

$$x_m = \sum_{i=1}^{P} a_i e^{-jk(m-1)r\sin\alpha_i \cos(\beta_i-((2(m-1)\pi)/m))} + n_m. \tag{7}$$

In a matrix form, the response of UCA can be written as follows:

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_M \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ e^{-jkr\sin\alpha_1 \cos(\beta_1-\pi)} & e^{-jkr\sin\alpha_2 \cos(\beta_2-\pi)} & \cdots & e^{-jkr\sin\alpha_p \cos(\beta_p-\pi)} \\ \vdots & \vdots & \vdots & \vdots \\ -jkr(m-1)\sin\alpha_1 \cos\left(\beta_1 - \dfrac{2\pi(m-1)}{m}\right) & e^{-jkr(m-1)\sin\alpha_1 \cos\left(\beta_2-\frac{2\pi(m-1)}{m}\right)} & \cdots & e^{-jkr\sin\alpha_p \cos\left(\beta_p-\frac{2\pi(m-1)}{m}\right)} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_p \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_m \end{bmatrix}. \tag{8}$$

In a vector form, equation (8) is given as

$$\mathbf{x} = \mathbf{A}\mathbf{s} + \mathbf{n}. \tag{9}$$

Here, $\mathbf{s}$ is a steering matrix for the source signals, a matrix $\mathbf{A}$ for amplitude and noise signal is denoted by $\mathbf{n}$.

3. Design Methodology

The design methodology consisted of two parts: a fitness function formulation for 2D-DOA parameter estimation and its optimization with the help of genetic algorithms (GA), pattern search (PS) and integrated approach GA-PS. The generic flow diagram of the proposed methodology is shown in Figure 2.

3.1. Fitness Function of 2D-DOA Estimation of UCA. The fitness function is developed for 2D-DOA estimation of plane waver form P sources impinging on circulate array compose of M antenna elements by the proficiency of approximation theory in mean square error sense as follows:

$$\varepsilon = \frac{1}{M}\sum_{m=1}^{M}(x_m - \widehat{x}_m)^2, \tag{10}$$

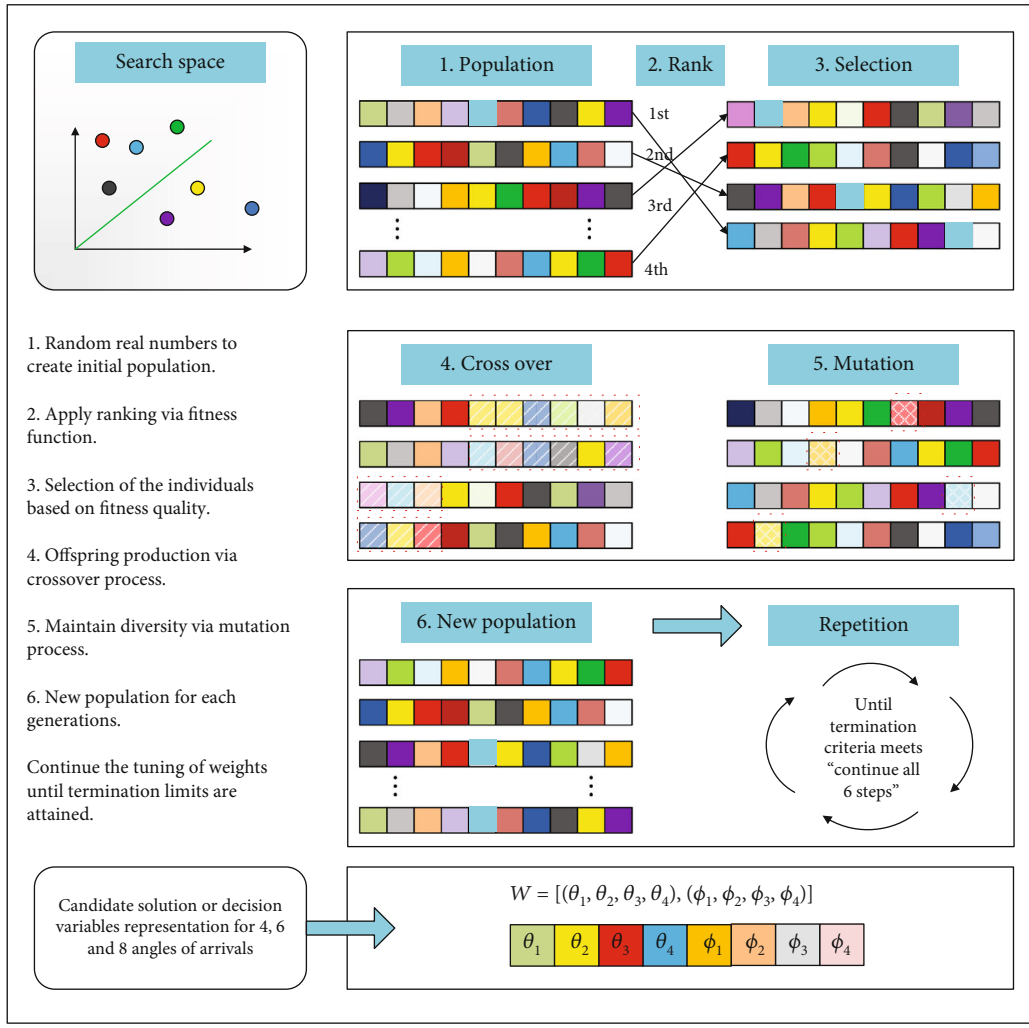


Figure 3: Optimization cycle of genetic algorithms.

where

$$x_m = \sum_{i=1}^{P} a_i e^{-jk(m-1)r \sin \alpha_i \cos (\beta_i - ((2(m-1)\pi)/m))} + n_m,$$
$$\hat{x}_m = \sum_{i=1}^{P} a_i e^{-jk(m-1)r \sin \widehat{\alpha}_i \cos \left(\widehat{\beta}_i - ((2(m-1)\pi)/m)\right)}. \quad (11)$$

Here, x_m is the desired response or signal in case of single snapshot as given equation (7), while $\hat{x}_m$ is an approximate signal of x_m. Now, one has to find the appropriate weights as

$$W = (\alpha_1, \alpha_2, \cdots, \alpha_P, \beta_1, \beta_2, \cdots, \beta_P), \quad (12)$$

such that $\varepsilon \longrightarrow 0$; then accordingly, $\hat{x}_m \longrightarrow x_m$.

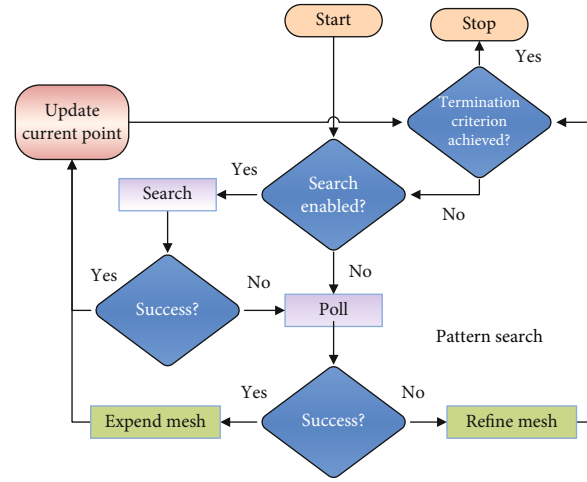


Figure 4: Process flow diagram of PS algorithm.

Table 1: Settings for gas optimization tools.

Index	Set
Individuals in population	360
Total number of generations	1000
Crossover scheme	Heuristic routine
Fraction of crossover	0.2
Function tolerance	10-09
Range initialization	[0-2π]
Selection scheme	Routine of stochastic uniform
Scaling procedure	Ranking
Elitism	2 counts
Mutation scheme	Routine of adaptive feasible
Other	Defaults

Table 2: Settings for PS optimization tools.

Index	Set
Iterations	2000
Penalty	100
Polling scheme	GPS basis on 2 N
Poll ordering	Consecutive
Mesh size	02
Evaluation of fitness	200000
Expansion parameter	2
Contraction parameter	0.5
TolX	0
TolBind	0
TolMesh	10-09

3.2. Optimization of 2D-DOA Parameters. To find the unknown adjustable weights W, 2D-DOA parameter estimation, the standalone optimization strength of GAs, and PS method, as well as hybrid computing heuristics of GA-PS algorithm, are exploited.

GA is developed on mathematical modeling of natural genetic mechanism in human genetic system and the first renewed application introduced by Onnen [37] in early seventies of the last century. GAs work through its fundamental operators of selection, crossover, and mutation for reproduction of the new population of candidate solution at each step increment in generations. The generic workflow of GAs operations is illustrated in Figure 3, while further necessary details of processing blocks can be seen in [38, 39]. Many constrained and unconstrained nonlinear optimization problems are effectively addressed with competency of GAs such as optimization in filter designing [40], life prediction of supercapacitors [41], salesman problem [42], multiaccess edge computing [43], and multiobjective optimization [44].

A pattern search algorithm belongs to the class of derivative free algorithm used broadly by the researchers for viable solution of constrained and unconstrained optimization tasks [45, 46]. The generic workflow diagram of PS by means of process block structures is shown in Figure 4, while broad recent applications of PS in different fields of science and engineering include the design of PID controller [47], automotive safety [48], and health monitoring [49].

In the presented study, standalone and combine strength of both optimization algorithms based on GAs, PS, and GA-PS are used for 2D-DOA estimation of plane waves. The built-in routines are invoked for both GAs and PS methods using the optimization toolbox of MATLAB software with setting of GAs and PS tools as provided in Tables 1 and 2, respectively.

4. Simulations and Results

In this section, results with interpretations are presented for abundant experimentation to test, analyze, and compare the outcomes of GAs PS and GA-PS based on the proposed methodologies. Results are presented throughout in this study based on average of 100 independent trials.

To evaluate the performance of GAs, PS, and their integrated scheme GA-PS, three case studies are taken based on 2, 3, and 4 plane wave sources impinging of UCA as follows:

Case 1. In the said scenario, 2D-DOA estimation problem with $P = 2$ sources and $M = 6$ antenna elements on UCL is taken with settings of elevation α_1 and azimuth β_1 angles as follows:

$$W = (\alpha_1, \alpha_{2,}\beta_1, \beta_2) = \begin{cases} (20^\circ, 70^\circ, 110^\circ, 150^\circ) \text{ degrees}, \\ (0.3491, 1.2217, 1.9199, 2.6180) \text{ radians}, \end{cases} \quad (13)$$

while the values of amplitude are $a = [a_1, a_2] = [1, 3]$. The fitness function for case 1 with $P = 2$ and $M = 6$ is formulated as follows:

$$\varepsilon = \frac{1}{6}\sum_{m=1}^{6}(x_m - \widehat{x}_m)^2,$$

$$x_m = \sum_{i=1}^{2} a_i e^{-jk(m-1)r \sin \alpha_i \cos (\beta_i - ((2(m-1)\pi)/m))} + n_m,$$

$$\widehat{x}_m = \sum_{i=1}^{2} a_i e^{-jk(m-1)r \sin \widehat{\alpha}_i \cos \left(\widehat{\beta}_i - (2(m-1)\pi)/m\right)}. \quad (14)$$

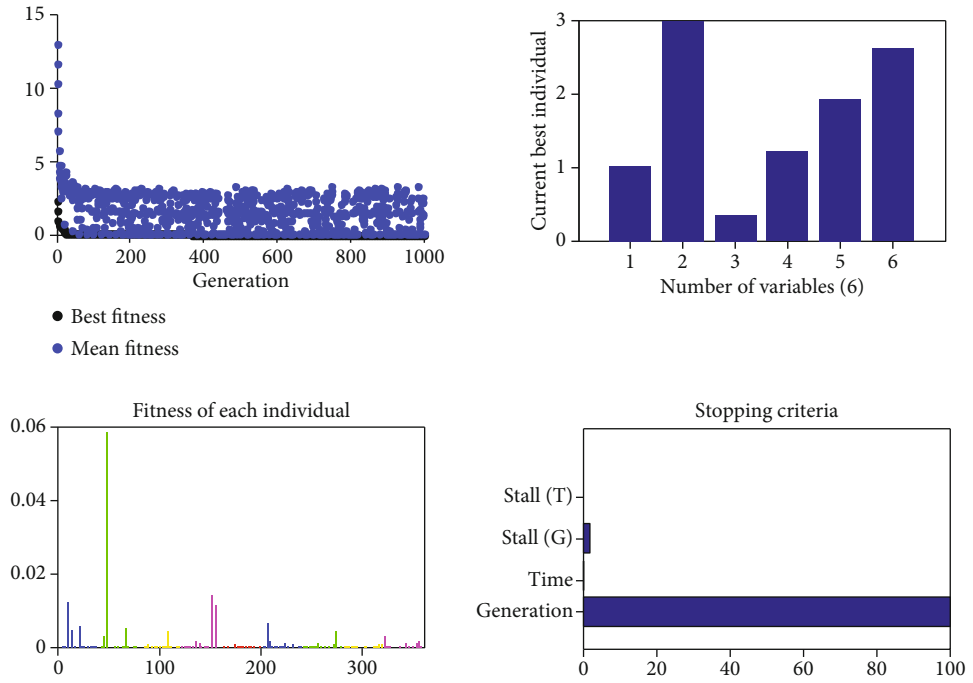


Figure 5: Learning curve with global best individual, fitness of each individual, and stopping conditions of GAs for case 1 of 2D-DOA estimation.

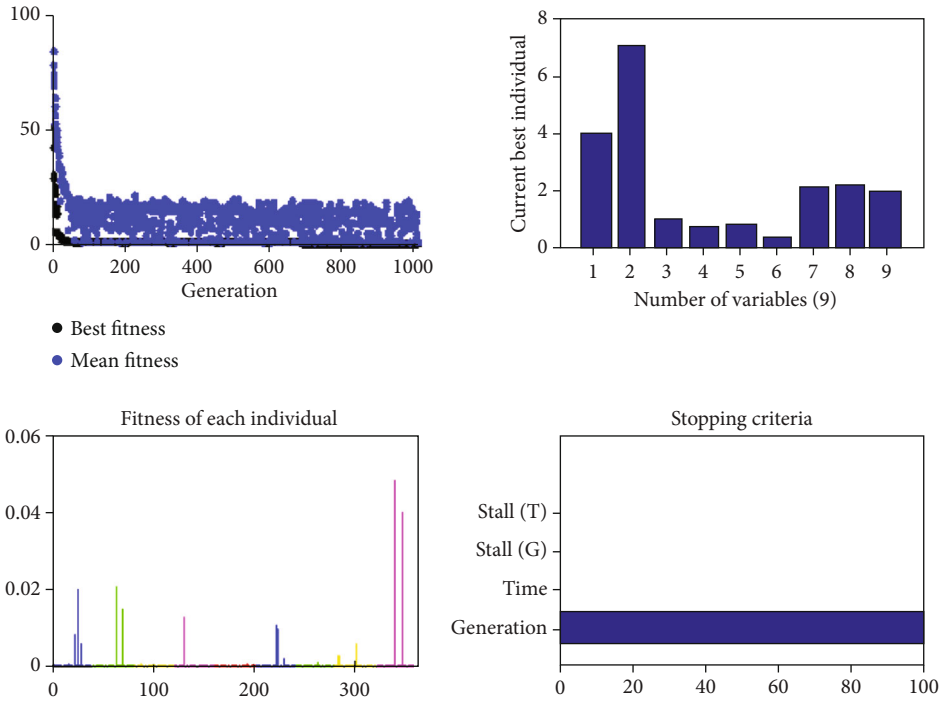


Figure 6: Learning curve with the best global individual, fitness of each individual, and stopping conditions of GAs for case 2 of 2D-DOA estimation.

Table 3: Comparison of results for 2D-DOA model for 2 far field sources.

Index	Desire and Approximated parameters			
	$\alpha 1$	$\alpha 2$	$\beta 1$	$\beta 2$
True (deg)	20.0000	70.0000	110.0000	150.0000
True (rad)	0.3491	1.2217	1.9199	2.6180
GAs (deg)	19.9962	69.9925	109.9964	149.9946
GAs(rad)	0.3490	1.2216	1.9198	2.6179
PS (deg)	19.9905	69.9868	109.9850	149.9889
PS (rad)	0.3489	1.2215	1.9196	2.6178
GA-PS (deg)	20.0020	69.9983	110.0022	150.0004
GA-PS (rad)	0.3491	1.2217	1.9199	2.6180

Table 4: Comparison of results for 2D-DOA model for 3 far field sources.

Index	Parameters					
	$\alpha 1$	$\alpha 2$	$\alpha 3$	$\beta 1$	$\beta 2$	$\beta 3$
True (deg)	20.0000	40.0000	50.0000	110.000	120.000	125.000
True (rad)	0.3491	0.6980	0.8727	1.9190	2.0944	2.1817
GAs (deg)	19.9962	39.9925	49.9791	109.6469	119.9946	124.9850
GAs (rad)	0.3490	0.6980	0.8723	1.9137	2.0943	2.1814
PS (deg)	19.9767	39.9649	49.9475	109.4138	119.9348	124.9290
PS (rad)	0.3488	0.6978	0.8721	1.9104	2.0941	2.1813
GA-PS (deg)	20.0020	39.9925	50.0020	109.9506	120.0003	125.0022
GA-PS (rad)	0.3491	0.6980	0.8727	1.9190	2.0944	2.1817

Table 5: Comparison of results for 2D-DOA model for 4 far field sources.

Index	Desire and Approximated parameters							
	Elevation angle				Azimuth angle			
	$\alpha 1$	$\alpha 2$	$\alpha 1$	$\alpha 2$	$\beta 1$	$\beta 1$	$\beta 1$	$\beta 1$
True (deg)	20.000	54.000	62.000	35.000	105.000	133.000	125.000	166.000
True (rad)	0.3491	0.9424	1.0821	0.6108	1.8325	2.3212	2.1816	2.8972
Gas (deg)	19.939	53.967	61.960	34.996	104.966	132.978	124.979	165.974
Gas (rad)	0.3480	0.9419	1.0814	0.6108	1.8320	2.3209	2.1813	2.8968
PS (deg)	19.933	53.950	61.977	34.996	104.960	132.972	124.968	165.951
PS (rad)	0.3479	0.9416	1.0817	0.6108	1.8319	2.3208	2.1811	2.8964
GA-PS (deg)	19.990	53.978	61.994	34.996	104.983	132.984	124.991	165.986
GA-PS (rad)	0.3489	0.9421	1.0820	0.6108	1.8323	2.3210	2.1815	2.8970

Table 6: Comparative study 2D-DOA model for 2 far field sources.

Index	Noise (dB)	ε	Time	Gens/iter	FC
GAs	Nil	$4.03E-25$	43.12	1000	360360
	30	$3.39E-22$	43.04	1000	360360
	25	$5.61E-19$	43.92	1000	360360
	20	$3.79E-18$	44.14	1000	360360
	15	$6.96E-18$	44.69	1000	360360
	10	$4.19E-17$	45.01	1000	360360
	5	$9.68E-16$	48.50	1000	360360
PS	Nil	$7.26E-21$	3.79	2000	23507
	30	$1.34E-21$	3.80	2000	23507
	25	$4.79E-19$	3.93	2000	23231
	20	$6.26E-18$	3.83	2000	23145
	15	$5.58E-16$	3.85	2000	23468
	10	$4.63E-15$	3.85	2000	23277
	5	$1.89E-14$	3.86	2000	23601
GA-PS	Nil	$1.00E-00$	46.70	3000	383867
	30	$1.00E-34$	46.63	3000	380576
	25	$6.42E-31$	47.53	3000	383591
	20	$1.71E-30$	47.75	3000	381109
	15	$6.23E-28$	48.31	3000	381010
	10	$2.54E-26$	48.64	3000	381359
	5	$1.85E-26$	52.16	3000	381469

Case 2. In this case, 2D-DOA estimation problem with $P = 3$ sources and $M = 9$ antenna elements on UCL is taken with settings of elevation α_1 and azimuth β_1 angles in degree or radian as follows:

$$W = (\alpha_1, \alpha_{2,}\alpha_{3,}\beta_1, \beta_2, \beta_3) = \begin{cases} \begin{pmatrix} 20^\circ, & 40^\circ, & 50^\circ, \\ 110^\circ, & 120^\circ, & 125^\circ \end{pmatrix} \text{degrees}, \\ \begin{pmatrix} 0.3491, 0.6980, 0.8727, \\ 1.9190, 2.0944, 2.1817 \end{pmatrix} \text{radians}, \end{cases} \tag{15}$$

while the values of amplitude are $a = [a_1, a_2, a_3] = [1, 4, 7]$. Using equation (14) for $P = 3$ and $M = 9$, the fitness function for case 2 is constructed.

Case 3. In this scenario, 2D-DOA estimation problem with $P = 4$ sources and $M = 8$ antenna elements on UCL is taken with settings of elevation α and azimuth β angles as follows:

$$W = \begin{pmatrix} \alpha_1, \alpha_{2,}\alpha_{3,} \\ \beta_1, \beta_2, \beta_3 \end{pmatrix} = \begin{cases} \begin{pmatrix} 20^\circ, & 40^\circ, & 50^\circ, \\ 110^\circ, & 120^\circ, & 125^\circ \end{pmatrix} \text{degrees}, \\ \begin{pmatrix} 0.3491, 0.6980, 0.8727, \\ 1.9190, 2.0944, 2.1817 \end{pmatrix} \text{radians}, \end{cases} \tag{16}$$

while the values of amplitude are $a = [a_1, a_2, a_3, a_3] = [1]$. Using equation (7) for $P = 4$ and $M = 8$, the fitness function for case 3 is constructed.

Results are determined for 100 independent trials of the algorithms to pinpoint their performance for two, three, and four far field sources. The optimization characteristics of GAs for 2 and 3 source models in terms of learning curves, best individual, fitness of each individual in the population, and stoppage criteria are shown in Figures 5 and 6 in case of 2 and 3 far-field sources impinging on UCL.

Table 7: Comparative study 2D-DOA model for 3 far field sources.

Index	Noise (dB)	ε	Time	Gens/iter	FC
GAs	Nil	$1E-21$	55.1	1000	360360
	30	$2E-20$	56.4	1000	360360
	25	$3E-19$	56.7	1000	360360
	20	$5E-18$	58.3	1000	360360
	15	$8E-17$	59.4	1000	360360
	10	$9E-16$	60.1	1000	360360
	5	$9E-14$	62.3	1000	360360
PS	Nil	$7.E-15$	5.4	2000	35660
	30	$1E-15$	5.7	2000	35876
	25	$4.E-14$	6.4	2000	35897
	20	$7E-12$	6.7	2000	35876
	15	$4E-10$	6.7	2000	35879
	10	$2E-8$	6.8	2000	35956
	5	$2E-6$	6.9	2000	35989
GA-PS	Nil	$2E-28$	60.20	3000	386246
	30	$2E-28$	61.80	3000	386281
	25	$5E-26$	62.30	3000	386732
	20	$2E-24$	64.10	3000	387149
	15	$6E-24$	65.30	3000	387257
	10	$2E-22$	66.00	3000	387485
	5	$2E-20$	68.40	3000	387681

The results of all three algorithms GAs, PS, and GA-PS against the true parameters of 2, 3 and 4 far-field sources for noiseless environment are presented in Tables 3–5, respectively.

While in case of different noise levels, results of proposed computing paradigm are presented in Tables 6–8 for sources $P = 2$, 3, and 4, respectively. The values of fitness ε and complexity parameters are time consumed, generations/iterations (Gens/iter) executed, and fitness function counts (FCs) by the optimization strategy for finding the decision variables.

One may observe that all three methods attained reasonably well levels of estimation accuracy; however, the results of integrated computing heuristics of GA-PS are more precise than those of GAs and PS standalone solvers. The performance of integrated algorithm GA-PS at the expense of relatively more computations is better than that of standalone schemes. Additionally, the increase in the number of sources and the level of noise variances results are deteriorated for each computing algorithm GAs, PS, and GA-PS, but still, the hybrid GA-PS achieved better reasonable precision than that of standalone counterparts.

The convergence analysis is also conducted for all three optimization solvers GAs, PS and GA-PS for solving 2D-DOA estimation problems are based on 100 trails, and results are presented in Figure 7 and Table 9 for each case study. One may see that percentage convergence of integrated heuristic of GA-PS algorithm is higher from standalone methodologies and performance of each optimization solver degraded with increase in sources from 2 to 4.

The analysis is further conducted with the increase in the number of antenna elements in UCA, i.e., value of M. The results of convergence analysis of 2D-DOA estimation for $P = 2$ and $M = 6$, 8, and 10 in UCL are presented in Table 10 along with achieved fitness level for all three optimization schemes. Accordingly, the results of convergence analysis of 2D-DOA estimation for 3 and 4 far-field sources with different antenna elements in UCA are presented in Tables 11 and 12, respectively. It is seen that rate of convergence for each algorithm increases with the increase in the value of M, but the performance of hybridized approach GA-PS is better from the rest.

Robustness analysis of all three optimization methodologies is conducted for different values of signal to noise (SNR), i.e., 5 dB, 10 dB, 15 dB, 20 dB, 25 dB, and 30Db for 2D-DOA estimation of 2, 3, and 4 sources. The results of robustness analysis each algorithm for different noise variation are presented in Figures 8–10 for sources $P = 2$, 3, and 4, respectively. One may see that for both low and

Table 8: Comparative study 2D-DOA model for 4 far field sources.

Index	Noise (dB)	ε	Time	Gens/iter	FC
GAs	Nil	$6.3e-12$	66.5	1000	360360
	30	$1.2e-09$	66.8	1000	360360
	25	$6.7e-09$	69.8	1000	360360
	20	$8.3e-08$	69.3	1000	360360
	15	$8.9e-08$	71.1	1000	360360
	10	$1.8e-07$	72.3	1000	360360
	5	$1.9e-06$	72.5	1000	360360
PS	Nil	$3.2e-09$	7.2	2000	35660
	30	$2.7e-08$	7.7	2000	35876
	25	$7.3e-08$	7.8	2000	35897
	20	$2.9e-06$	7.9	2000	35876
	15	$1.8e-06$	8.6	2000	35879
	10	$1.9e-04$	8.7	2000	35956
	5	$8.2e-04$	8.9	2000	35989
GA-PS	Nil	$8.3e-16$	73.20	3000	386246
	30	$1.2e-14$	73.60	3000	386281
	25	$8.7e-14$	76.60	3000	386732
	20	$4.3e-12$	76.20	3000	387149
	15	$6.9e-12$	78.20	3000	387257
	10	$1.8e-10$	79.50	3000	387485
	5	$8.9e-09$	80.00	3000	388681

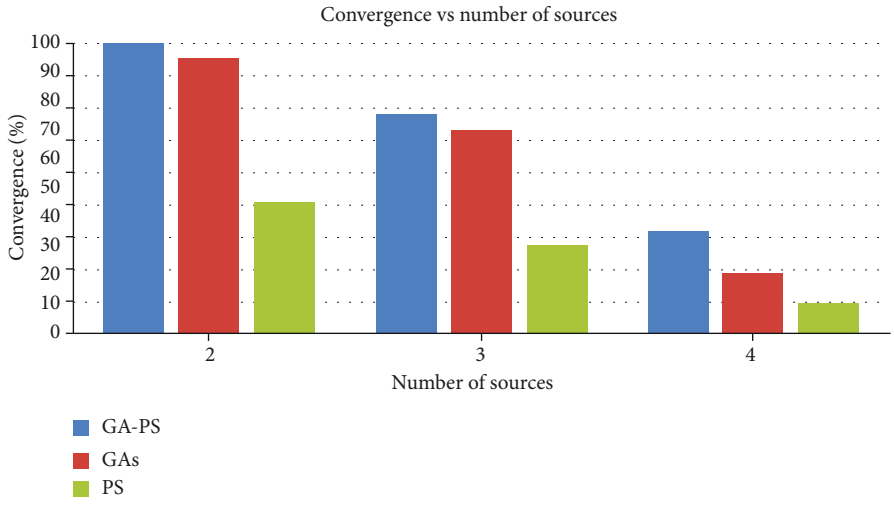


Figure 7: Bar chart illustration of convergence analysis for sources $P = 2$, 3, and 4.

Table 9: Convergence analysis of 2D-DOA estimation for 2, 3, and 4 far field sources with fixed antenna elements in UCL.

Source/antenna	Method	ε	Convergence
2/4	Gas	$1.0E-25$	94%
	PS	$1.0E-21$	44%
	GA-PS	$1.0E-31$	98%
3/6	GAs	$1.0E-21$	69%
	PS	$1.0E-15$	31%
	GA-PS	$1.0E-288$	76%
4/8	GAs	$1.0E-06$	19%
	PS	$1.0E-05$	09%
	GA-PS	$1.0E-17$	36%

Table 10: Convergence analysis of 2D-DOA estimation for 2 far field sources with different antenna elements in UCL.

Antenna UCA	Method	ε	Convergence
6	GAs	$1.0E-25$	95%
	PS	$1.0E-21$	45%
	GA-PS	$1.0E-31$	99%
8	GAs	$1.0E-27$	96%
	PS	$1.0E-22$	52%
	GA-PS	$1.0E-32$	99%
10	GAs	$1.0E-28$	98%
	PS	$1.0E-25$	60%
	GA-PS	$1.0E-00$	100%

Table 11: Convergence analysis of 2D-DOA estimation for 3 far field sources with different antenna elements in UCL.

Antenna UCA	Method	ε	Convergence
9	GAs	$1.0E-21$	69%
	PS	$1.0E-15$	29%
	GA-PS	$1.0E-28$	74%
11	GAs	$1.0E-22$	74%
	PS	$1.0E-16$	39%
	GA-PS	$1.0E-29$	82%
13	GAs	$1.0E-22$	77%
	PS	$1.0E-17$	43%
	GA-PS	$1.0E-30$	85%

Table 12: Convergence analysis of 2D-DOA estimation for 4 far field sources with different antenna elements in UCL.

Antenna UCA	Scheme	ε	Convergence (%)
8	GA	$1.0E-06$	20
	PS	$1.0E-03$	10
	GA-PS	$1.0E-08$	35
10	GA	$1.0E-07$	26
	PS	$1.0E-04$	18
	GA-PS	$1.0E-09$	45
12	GA	$1.0E-07$	30
	PS	$1.0E-05$	25
	GA-PS	$1.0E-10$	55

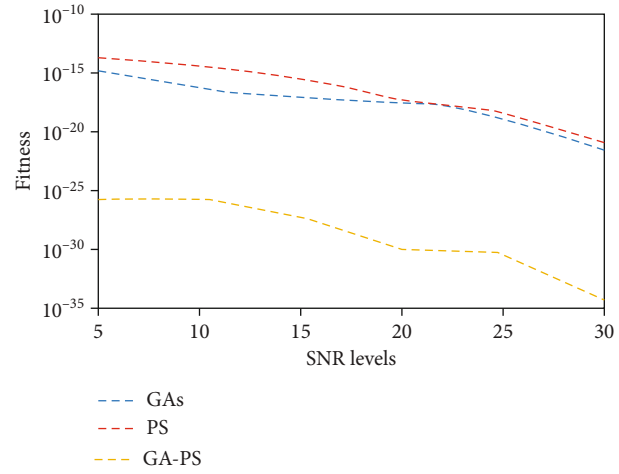


Figure 8: Comparison of fitness for different SNR levels for sources $P = 2$.

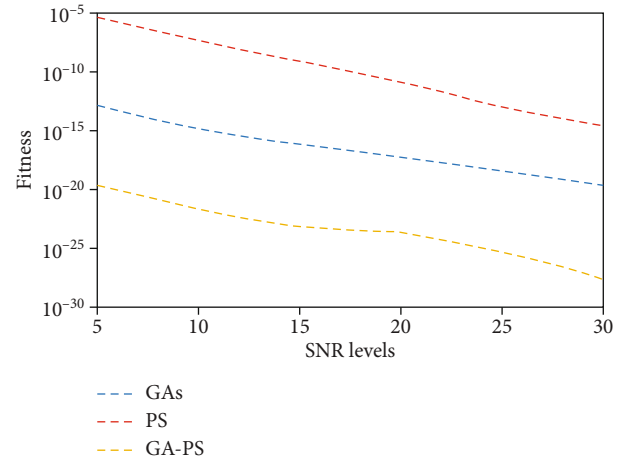


Figure 9: Comparison of fitness for different SNR levels for sources $P = 3$.

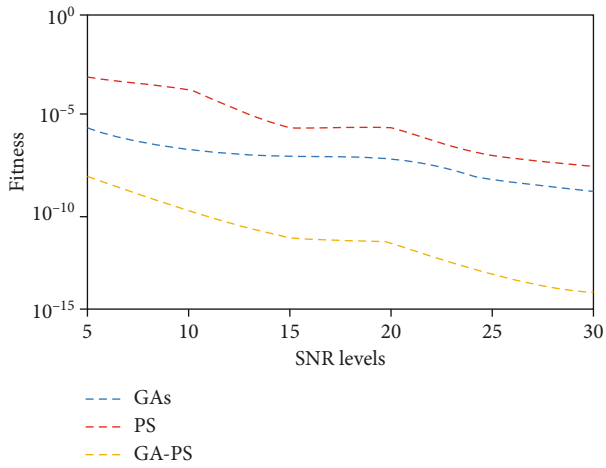


Figure 10: Comparison of fitness for different SNR levels for sources $P = 4$.

Table 13: Performance comparison on statistics for 2 sources based on 2D-DOA estimation.

Index	GAs	PS	GA-PS
Best-fitness	$1.0E-25$	$1.0E-23$	$1.0E-00$
Worst-fitness	$1.0E-21$	$1.0E-17$	$1.0E-28$
Mean-fitness	$1.0E-23$	$1.0E-21$	$1.0E-30$
Minimum-FCs	360360	20545	23147
Maximum-FCs	360360	21324	23986
Mean-FCs	360360	20777	23327
Minimum-time	42.52	3.69	46.10
Maximum-time	44.27	5.01	48.02
Mean-time	43.28	3.91	47.00

Table 14: Performance comparison on statistics for 3 sources based on 2D-DOA estimation.

Index	GAs	PS	GA-PS
Best-fitness	$1.0E-17$	$1.0E-12-12$	$1.0E-31$
Worst-fitness	$1.0E-13$	$1.0E-02$	$1.0E-18$
Mean-fitness	$1.0E-15$	$1.0E-06$	$1.0E-28$
Minimum-FCs	360360	25467	25538
Maximum-FCs	360360	28580	29614
Mean-FCs	360360	26339	26598
Minimum-time	53.09	4.71	58.20
Maximum-time	61.55	6.25	67.62
Mean-time	56.80	5.09	61.88

high values of SNR, the performance of hybridized computing solver GA-PS remains better than that of GAs and PS standalone schemes.

The complexity analysis in terms of minimum-time, maximum-time, mean-time, minimum-FCs, maximum-FCs, and mean-FCs along with the values of best-fitness, worst-fitness and mean-fitness is conducted for 100 executions of each optimization scheme GAs, PS, and GA-PS for all three 2D-DOA scenarios. Results of complexity operators are listed in Tables 13–15 for sources $P = 2$, 3, and 4, respectively. It is seen that computation complexity of PS is superior from GA and GA-PS technique but the performance in terms of accuracy and convergence is better for both GAs and GA-PS methodologies for each case.

Table 15: Performance comparison on statistics for 4 sources based on 2D-DOA estimation.

Index	GAs	PS	GA-PS
Best-fitness	$1.0E-12$	$1.0E-09$	$1.0E-16$
Worst-fitness	$1.0E-04$	$1.0E-01$	$1.0E-05$
Mean-fitness	$1.0E-11$	$1.0E-04$	$1.0E-15$
Minimum-FCs	360360	25347	25538
Maximum-FCs	360360	28720	29614
Mean-FCs	360360	26759	26598
Minimum-time	73.01	9.12	79.11
Maximum-time	69.55	7.51	76.45
Mean-time	72.01	7.83	78.71

5. Conclusion

Novel applications of evolutionary heuristics are effectively presented for 2D-DOA estimation of plane waves impinging on UCL by exploitation of global search efficacy of GAs, efficiency of PS, and integrated optimization strength of GA-PS. The performance of optimization mechanisms is verified by implementation of UCA-based 2D-DOA estimation having different degrees of freedom, i.e., far field sources $P = 2$, 3, and 4. The results of integrated solver GA-PS are relatively better from standalone counterparts GA and PS for each scenario of the data model for DOA. Consistent accuracy, stability, and robustness of the hybrid optimization procedure of GA-PS are established through outcomes of statistical observations for DOA problems with different numbers of decision variables and noise variations but at the cost of relative more computations that that of GAs and PS standalone schemes.

In the future, one may investigate the application of presented computing platform on other circular array structures based on concentric circular array, conic circular array, and coprime circular array for better estimation accuracy of DOA parameters. Moreover, the use of fractional evolutionary/swarming techniques looks promising for the estimation of 2D-DOA parameters more viably.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work was supported in part by the Fundamental Research Funds for the Central Universities (No. JB180205).

References

[1] H. Zhang and H. Zhang, "Research on DOA estimation method of sonar radar target based on MUSIC algorithm," *Journal of Physics: Conference Series*, vol. 1176, no. 3, 2019.

[2] X. Zhang, C. Chen, J. Li, and D. Xu, "Blind DOA and polarization estimation for polarization-sensitive array using dimension reduction MUSIC," *Multidimensional Systems and Signal Processing*, vol. 25, no. 1, pp. 67–82, 2014.

[3] J. Li, X. Zhang, W. Chen, and T. Hu, "Reduced-dimensional ESPRIT for direction finding in monostatic MIMO radar with double parallel uniform linear arrays," *Wireless Personal Communications*, vol. 77, no. 1, pp. 1–19, 2014.

[4] R. Roy and T. Kailath, "ESPRIT-estimation of signal parameters via rotational invariance techniques," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 37, no. 7, pp. 984–995, 1989.

[5] J. Dai and Z. Ye, "Spatial smoothing for direction of arrival estimation of coherent signals in the presence of unknown mutual coupling," *IET Signal Processing*, vol. 5, no. 4, pp. 418–425, 2011.

[6] C. Qi, Y. Wang, Y. Zhang, and Y. Han, "Spatial difference smoothing for DOA estimation of coherent signals," *IEEE Signal Processing Letters*, vol. 12, no. 11, pp. 800–802, 2005.

[7] S. Visuri, H. Oja, and V. Koivunen, "Subspace-based direction-of-arrival estimation using nonparametric statistics," *IEEE Transactions on Signal Processing*, vol. 49, no. 9, pp. 2060–2073, 2001.

[8] D. R. Van Rheeden and S. C. Gupta, "A temporal smoothing approach to direction of arrival estimation of coherent signals in fading channels," in *WCNC. 1999 IEEE Wireless Communications and Networking Conference (Cat. No.99TH8466)*, pp. 286–290, New Orleans, LA, USA, 1999.

[9] N. Xi and L. Liping, "A computationally efficient subspace algorithm for 2-D DOA estimation with L-shaped array," *IEEE Signal Processing Letters*, vol. 21, no. 8, pp. 971–974, 2014.

[10] M. Yang, J. Ding, B. Chen, and X. Yuan, "Coprime L-shaped array connected by a triangular spatially-spread electromagnetic-vector-sensor for two-dimensional direction of arrival estimation," *IET Radar, Sonar & Navigation*, vol. 13, no. 10, pp. 1609–1615, 2019.

[11] G. Qin, Y. D. Zhang, and M. G. Amin, "DOA estimation exploiting moving dilated nested arrays," *IEEE Signal Processing Letters*, vol. 26, no. 3, pp. 490–494, 2019.

[12] F. Chen, J. Dai, N. Hu, and Z. Ye, "Sparse Bayesian learning for off-grid DOA estimation with nested arrays," *Digital Signal Processing*, vol. 82, pp. 187–193, 2018.

[13] Y. Wang, A. Hashemi-Sakhtsari, M. Trinkle, and B. W. H. Ng, "Sparsity-aware DOA estimation of quasi-stationary signals using nested arrays," *Signal Processing*, vol. 144, pp. 87–98, 2018.

[14] F. G. Yan, S. Liu, J. Wang, M. Jin, and Y. Shen, "Fast DOA estimation using co-prime array," *Electronics Letters*, vol. 54, no. 7, pp. 409-410, 2018.

[15] J. Li, D. Jiang, and X. Zhang, "Sparse representation based two-dimensional direction of arrival estimation using co-prime array," *Multidimensional Systems and Signal Processing*, vol. 29, no. 1, pp. 35–47, 2018.

[16] T. Wu, Z. Deng, Y. Li, and Y. Huang, "Two-dimensional DOA estimation for incoherently distributed sources with uniform rectangular arrays," *Sensors*, vol. 18, no. 11, p. 3600, 2018.

[17] D. Su, Y. Jiang, X. Wang, and X. Gao, "Omnidirectional precoding for massive MIMO with uniform rectangular array—-part I: complementary codes-based schemes," *IEEE Transactions on Signal Processing*, vol. 67, no. 18, pp. 4761–4771, 2019.

[18] Q. Li, T. Su, and K. Wu, "Accurate DOA estimation for large-scale uniform circular array using a single snapshot," *IEEE Communications Letters*, vol. 23, no. 2, pp. 302–305, 2019.

[19] J. Xin, G. Liao, Z. Yang, and H. Shen, "Ambiguity resolution for passive 2-D source localization with a uniform circular array," *Sensors*, vol. 18, no. 8, p. 2650, 2018.

[20] R. M. Shubair, A. S. Goian, M. I. AlHajri, and A. R. Kulaib, "A new technique for UCA-based DOA estimation of coherent signals," in *2016 16th Mediterranean Microwave Symposium (MMS),*, pp. 1–3, Abu Dhabi, United Arab, 2016.

[21] D. H. Xu and J. W. Chen, "A novel DOA estimation for uniform circular arrays in correlated environment without interpolation, pp. 650–652, Yonago, Japan, 2006.

[22] C. P. Mathews and M. D. Zoltowski, "Eigenstructure techniques for 2-D angle estimation with uniform circular arrays," *IEEE Transactions on Signal Processing*, vol. 42, no. 9, pp. 2395–2407, 1994.

[23] C. P. Mathews and M. D. Zoltowski, "Performance analysis of the UCA-ESPRIT algorithm for circular ring arrays," *IEEE Transactions on Signal Processing*, vol. 42, no. 9, pp. 2535–2539, 1994.

[24] R. Goossens and H. Rogier, "A hybrid UCA-RARE/Root-MUSIC approach for 2-D direction of arrival estimation in uniform circular arrays in the presence of mutual coupling," *IEEE Transactions on Antennas and Propagation*, vol. 55, no. 3, pp. 841–849, 2007.

[25] G. Jiang, X. Mao, and Y. Liu, "Reducing errors for root-MUSIC-based methods in uniform circular arrays," *IET Signal Processing*, vol. 12, no. 1, pp. 31–36, 2018.

[26] Y. Wang, X. Yang, J. Xie, L. Wang, and B. W. H. Ng, "Sparsity-inducing DOA estimation of coherent signals under the coexistence of mutual coupling and nonuniform noise," *IEEE Access*, vol. 7, pp. 40271–40278, 2019.

[27] J. C. Hung, "Memetic particle swarm optimization scheme for direction-of-arrival estimation in multipath environment," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 6, pp. 3955–3968, 2018.

[28] V. Dakulagi and M. Bakhar, "Smart antenna system for DOA estimation using single snapshot," *Wireless Personal Communications*, vol. 107, no. 1, pp. 81–93, 2019.

[29] A. Sharma and S. Mathur, "Comparative analysis of ML-PSO DOA estimation with conventional techniques in varied multipath channel environment," *Wireless Personal Communications*, vol. 100, no. 3, pp. 803–817, 2018.

[30] P. Lindgren, P. Valter, and R. Prasad, "Retracted article: Advanced business model innovation supported by artificial intelligence, deep learning, multi business model patterns and a multi business model library," *Wireless Personal Communications*, vol. 107, no. 4, pp. 2263–2263, 2019.

[31] B. Sun and Z. Dong, "Comparative study on the academic field of artificial intelligence in China and other countries," *Wireless*

Personal Communications, vol. 102, no. 2, pp. 1879–1890, 2018.

[32] Y. Yue, L. Cao, and Z. Luo, "Hybrid artificial bee colony algorithm for improving the coverage and connectivity of wireless sensor networks," *Wireless Personal Communications*, vol. 108, no. 3, pp. 1719–1732, 2019.

[33] B. G. Prakash, R. Sukumar, and C. Balasubramanian, "A swarm intelligence based clustering technique with scheduling for the amelioration of lifetime in sensor networks," *Wireless Personal Communications*, vol. 103, no. 4, pp. 3189–3207, 2018.

[34] N. I. Chaudhary, S. Zubair, and M. A. Z. Raja, "Design of momentum LMS adaptive strategy for parameter estimation of Hammerstein controlled autoregressive systems," *Neural Computing and Applications*, vol. 30, no. 4, pp. 1133–1143, 2018.

[35] W. U. Khan, Z. Ye, F. Altaf, N. I. Chaudhary, and M. A. Z. Raja, "A novel application of fireworks heuristic paradigms for reliable treatment of nonlinear active noise control," *Applied Acoustics*, vol. 146, pp. 246–260, 2019.

[36] I. Ahmad, H. Ilyas, A. Urooj, M. S. Aslam, M. Shoaib, and M. A. Z. Raja, "Novel applications of intelligent computing paradigms for the analysis of nonlinear reactive transport model of the fluid in soft tissues and microvessels," *Neural Computing and Applications*, vol. 31, no. 12, pp. 9041–9059, 2019.

[37] C. Onnen, R. Babuška, U. Kaymak, J. M. Sousa, H. B. Verbruggen, and R. Isermann, "Genetic algorithms for optimization in predictive control," *Control Engineering Practice*, vol. 5, no. 10, pp. 1363–1372, 1997.

[38] A. Kartci, A. Agambayev, M. Farhat et al., "Synthesis and optimizsssation of fractionassl-order elements using a genetic algorithm," *IEEE Access*, vol. 7, pp. 80233–80246, 2019.

[39] W. Zang, W. Zhang, Z. Wang, D. Jiang, X. Liu, and M. Sun, "A novel double-strand DNA genetic algorithm for multi-objective optimization," *IEEE Access*, vol. 7, pp. 18821–18839, 2019.

[40] S. S. Moghaddasi and N. Faraji, "A hybrid algorithm based on particle filter and genetic algorithm for target tracking," *Expert Systems with Applications*, vol. 147, no. 1, article 113188, 2020.

[41] Y. Zhou, Y. Wang, K. Wang et al., "Hybrid genetic algorithm method for efficient and robust evaluation of remaining useful life of supercapacitors," *Applied Energy*, vol. 260, article 114169, 2020.

[42] A. H. Halim and I. Ismail, "Combinatorial optimization: comparison of heuristic algorithms in travelling salesman problem," *Archives of Computational Methods in Engineering*, vol. 26, no. 2, pp. 367–380, 2019.

[43] L. Tang, B. Tang, L. Kang, and L. Zhang, "A novel task caching and migration strategy in multi-access edge computing based on the genetic algorithm," *Future Internet*, vol. 11, no. 8, p. 181, 2019.

[44] S. Paul and S. Das, "Simultaneous feature selection and weighting—An evolutionary multi-objective optimization approach," *Pattern Recognition Letters*, vol. 65, pp. 51–59, 2015.

[45] K. S. Rajesh, S. S. Dash, and R. Rajagopal, "Hybrid improved firefly-pattern search optimized fuzzy aided PID controller for automatic generation control of power systems with multi-type generations," *Swarm and Evolutionary Computation*, vol. 44, pp. 200–211, 2019.

[46] E. Emary, H. M. Zawbaa, A. E. Hassanien, and B. Parv, "Multi-objective retinal vessel localization using flower pollination search algorithm with pattern search," *Advances in Data Analysis and Classification*, vol. 11, no. 3, pp. 611–627, 2017.

[47] H. Gozde and M. C. Taplamacioglu, "Automatic generation control application with craziness based particle swarm optimization in a thermal power system," *International Journal of Electrical Power & Energy Systems*, vol. 33, pp. 8–16, 2011.

[48] H. Martin, Z. Ma, C. Schmittner et al., "Combined automotive safety and security pattern engineering approach," *Reliability Engineering & System Safety*, vol. 198, article 106773, 2020.

[49] A. Shakya, M. Mishra, D. Maity, and G. Santarsiero, "Structural health monitoring based on the hybrid ant colony algorithm by using Hooke–Jeeves pattern search," *SN Applied Sciences*, vol. 1, no. 7, p. 799, 2019.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2257338, 19 pages
https://doi.org/10.1155/2022/2257338

Research Article

Application Layer-Forward Error Correction Raptor Q Codes in 5G Mobile Networks for Factory of the Future

Athirah Mohd Ramly,[1] **Rosdiadee Nordin**,[2] **and Nor Fadzilah Abdullah**[2]

[1]*Department of Computing and Information System, School of Engineering and Technology, Sunway University, 47500 Subang Jaya, Selangor, Malaysia*
[2]*Department of Electrical, Electronics and System Engineering, Faculty of Engineering & Built Environment, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia*

Correspondence should be addressed to Rosdiadee Nordin; adee@ukm.edu.my

Received 22 December 2021; Revised 11 March 2022; Accepted 26 March 2022; Published 26 April 2022

Academic Editor: Chi-Hua Chen

The future communication requirements for industrial automation will differ significantly from existing technologies. Traffic in Industry 4.0 imposes real-time requirements, requiring ultra-reliable communication (URC) with high reliability and minimal latency. The demand for ultra-high reliability as high as 99.999999 percent and as low as 1 ms end-to-end latency is the major challenge of the NOMA communication system in the factory of the future. The high expectations on reliability and latency need modifications to the radio system's baseband signal processing, medium access control (MAC) layer, and application layer to protect against packet losses. Thus, this paper investigates the utilization of Raptor Q codes, which is a type of Application Layer Forward Error Correction (AL-FEC), by developing an end-to-end system level simulator to evaluate and analyze the performance of the transmission signals based on cross-layer approach; from the physical layer (PHY), MAC layer, and application layer parameters in an indoor factory network setting. The factory is assumed to be operated with various factory robots of different speeds, from static to 10 km/h. The 5G technology relies heavily on flexible network operations. High user density, high user mobility, deployment, and coverage are all qualities that allow for this flexibility. Through extensive simulations, the results showed that the Raptor Q codes are not only able to give good results, i.e., packet reception rate (PRR) = 0.9 of 10 m or 1.8% to 10 m or 3.4% depending on different scenarios, but are also able to meet PRR = 0.9 in the mobility scenario at 10 km/h. Thus, the Raptor Q codes can be seen as a good candidate for obtaining results within a strict range of requirements set by URC communications for the factory of the future replacing RLNC.

1. Introduction

Machine-to-machine (M2M) communication is a fundamental technology for the next-generation (5G) networks, allowing billions of multifunctional devices to interact with one another with little or no human involvement [1]. Furthermore, data packets are expected to include crucial information in several practical and promising 5G applications, such as autonomous driving and public safety systems, and should be sent with ultra-reliability and low latency [2]. The biggest issue with ultra-reliable and low-latency communication (URLLC) is to come up with a coding scheme that can handle ultra-reliable transmission [3]. In the recent decade, researchers have been particularly interested in rateless fountain codes. The first practical implementation of fountain codes was Luby transform (LT) codes [4]. With an average decoding cost of $O(k \log(k))$ operations, it can retrieve the original k information symbols. Researchers in [5] suggested Raptor codes, which combine an LT code with a high code rate precode to reduce decoding complexity further and solve the high error floor in LT codes. Furthermore, the 3rd Generation Partnership Project (3GPP) has already standardized a well-designed systematic Raptor code dubbed R10 code [6] composed of a systematic low-density generator matrix (LDGM)

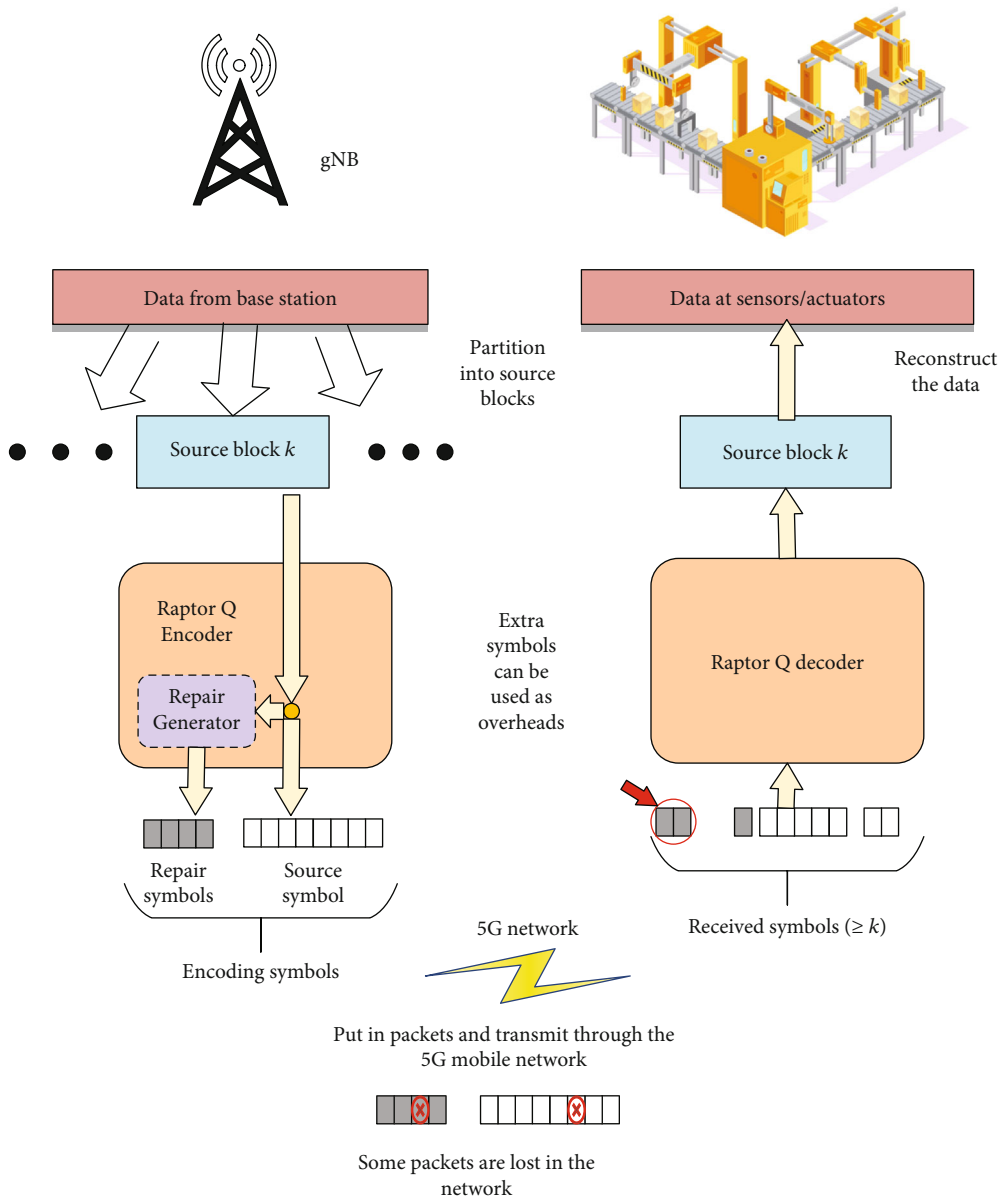


Figure 1: Block illustration of the Raptor Q coding and decoding system.

code as the precode and an inner LT code. With a reasonable code length, R10 code may efficiently disseminate data over a broadcast/multicast network [7]. As a result, rateless codes for the mMTC have the potential to provide excellent reliability [8]. One approach for addressing this problem is to use the most recent rateless codes, such as Raptor Q codes with maximum likelihood (ML) decoding algorithm [9, 10], to enhance coding performance for delivering delay-sensitive applications across future 5G networks. Raptor Q codes are a high-order field F_q extension of Raptor codes that is seen as a promising option to enhance the capacity of R10 codes, providing a compromise between complexity and reliability. The 3GPP has standardized the Application Layer Forward Error Correction (AL-FEC) based on Raptor codes [5] over Multimedia Broadcast and Multicast Services (MBMS) [11] to offer robust and dependable multicast/broadcast services over unreliable channels. Raptor codes were adopted by the 3GPPP because they outperformed previous AL-FEC schemes and because they are implemented in software rather than hardware. Furthermore, the quantity of redundant symbols may be calculated on-the-fly, removing the need for exact channel information prior to data transmission. Because multicast/broadcast transmission is without an ARQ mechanism, the AL-FEC technique sends redundant data together with the original data (packets) to allow the receiver to recover damaged or missing source data by utilizing the redundant ones.

For broadcast and multicast services via wireless networks, AL-FEC protection based on Raptor codes has been widely investigated. These studies investigated the tradeoffs between AL-FEC, physical, and MAC layer parameters

for broadcast services over WLANs [12, 13], Long-Term Evolution (LTE) [14, 15], and Digital Video Broadcasting-Handheld (DVB-H) [16] and found that only a well-designed and optimized system can maximize spectral efficiency and user's QoE. Some research has been conducted into cross-layer optimization frameworks that modify AL-FEC redundancy based on the physical layer modulation and coding schemes (MCSs) used to enable dependable video streaming applications across unreliable wireless channels [17–21]. However, because each multicast user has a different channel condition, multicast video broadcasting to numerous viewers poses extra limitations. As a result, finding system settings that are optimum (offer high quality of experience (QoE)) for each multicast user based on the quality of service (QoS) needs of the applications is difficult.

Hence, the researchers in [22] examined the performance of an AL-FEC protection system in next-generation mobile networks. Findings in [22] demonstrate that the suggested online technique can perform as well as or better than a retransmission-based error recovery technique under certain situations. Meanwhile, researchers in [23] proposed a new AL-FEC application architecture scheme based on Raptor Q codes. Therefore, we investigate the performance improvements that such an error control architecture may bring to NGMN-edge computing integrated systems. The literature has previously looked at industrial applications and their needs for industrial wireless communication systems. In this regard, the work carried out within the German research framework "Reliable Wireless Communication in Industry" should be highlighted. Associated applications were gathered, and their needs merged into three so-called requirement profiles as part of the HiFlecs project [24]. Corresponding needs were gathered from all ZDKI projects and scientifically evaluated by an associated research study [25].

In addition, the whitepaper [26] provided an overview of the use of radio systems in industrial contexts and a summary of the requirements for the various applications. For discrete manufacturing applications, high reliability (PER $\leq 10^{-9}$) and low latency (order of magnitude: 1 ms) are forecasted as stated in [26]. The packet size is intended to be between 20 and 50 bytes. This use case is the most difficult from a communication technology standpoint and is thus taken to be a reference use case in the following without restricting the generality. In terms of industry standardization, the specifications of 3GPP MBMS [11], DVB AL-FEC [27], and IETF FEC framework [28] all contain a common FEC framework to secure streaming service delivery based on AL-FEC. Meanwhile, the researchers in [29] introduced the utilization of fountain codes with very short packets. However, it only investigates the PHY layer without considering the upper layer, such as MAC and APP layer.

Systematic network coding [15–18] is an alternate strategy to reducing computing complexity, which sends the original packets in uncoded form and inserts a limited number of encoded packets into a generation to adjust for network transport inefficiencies. The other key approach to minimize the computational cost of the RLNC is to use sparse coding coefficient rows, which have a relatively modest mandated number of nonzero coding coefficients.

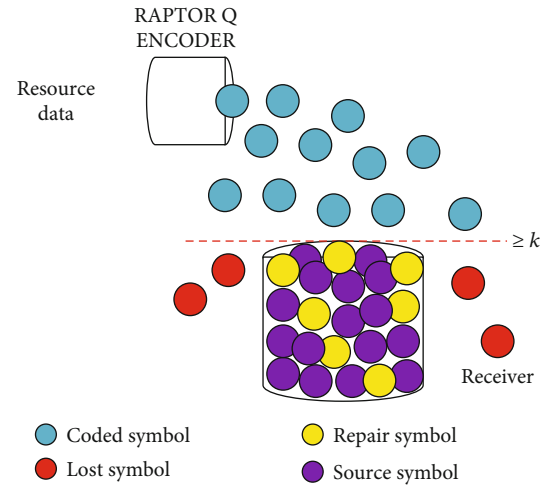


Figure 2: Illustration of symbols in the encoding and decoding system of the Raptor Q codes.

Small Galois fields [19, 20] or novel kinds of network coding [21] have been used in several research investigations to alleviate the computational challenges of network coding. On servers with a high number of graphics processing units (GPUs), the GF (2^8) RLNC can be computed quickly [22–24]. On general-purpose multicore CPUs, computational solutions for GF (2^8) network coding have mostly focused on intelligently splitting the coefficient and data matrices to permit parallel processing [25, 26]. The network coding computations have been substantially accelerated due to these partitioning schemes (and reduced the energy consumption [27, 28]). The matrix block operations can be scheduled according to the dependence structure of the calculations in a DAG [29] to gain some extra performance. Most of the partitioning techniques [25, 26] are suited for progressive RLNC decoding. However, the DAG approach in [29] is confined to nonprogressive decoding of a whole generation of coded packets. Researcher in [29] presented to use the advantages of DAG scheduling to progressive RLNC decoding.

As mentioned in [19, 30–32], the compute-and-forward paradigm, which recodes packets in intermediary network nodes, gives way to RLNC. RLNC can operate on source packet blocks or a sliding window encompassing several source packets [20, 21, 33–36]. DSEP Fulcrum was developed by a researcher in [Nguyen] as a block code that relies on RLNC block coding. However, RLNC comes with high computational complexity. To achieve low computational complexity, a smaller Galois field [37–41] can be considered to minimize RLNC computational complexity at the tradeoff of reduced decoding probability due to the greater probabilities of linearly dependent encoded packets. In addition, the Fulcrum RLNC technique allows for flexible recoding and decoding in either a small Galois field (at the price of collecting more coded packets to compensate for linear dependencies) or a large Galois field (with high complexities) or a mix of the two [42].

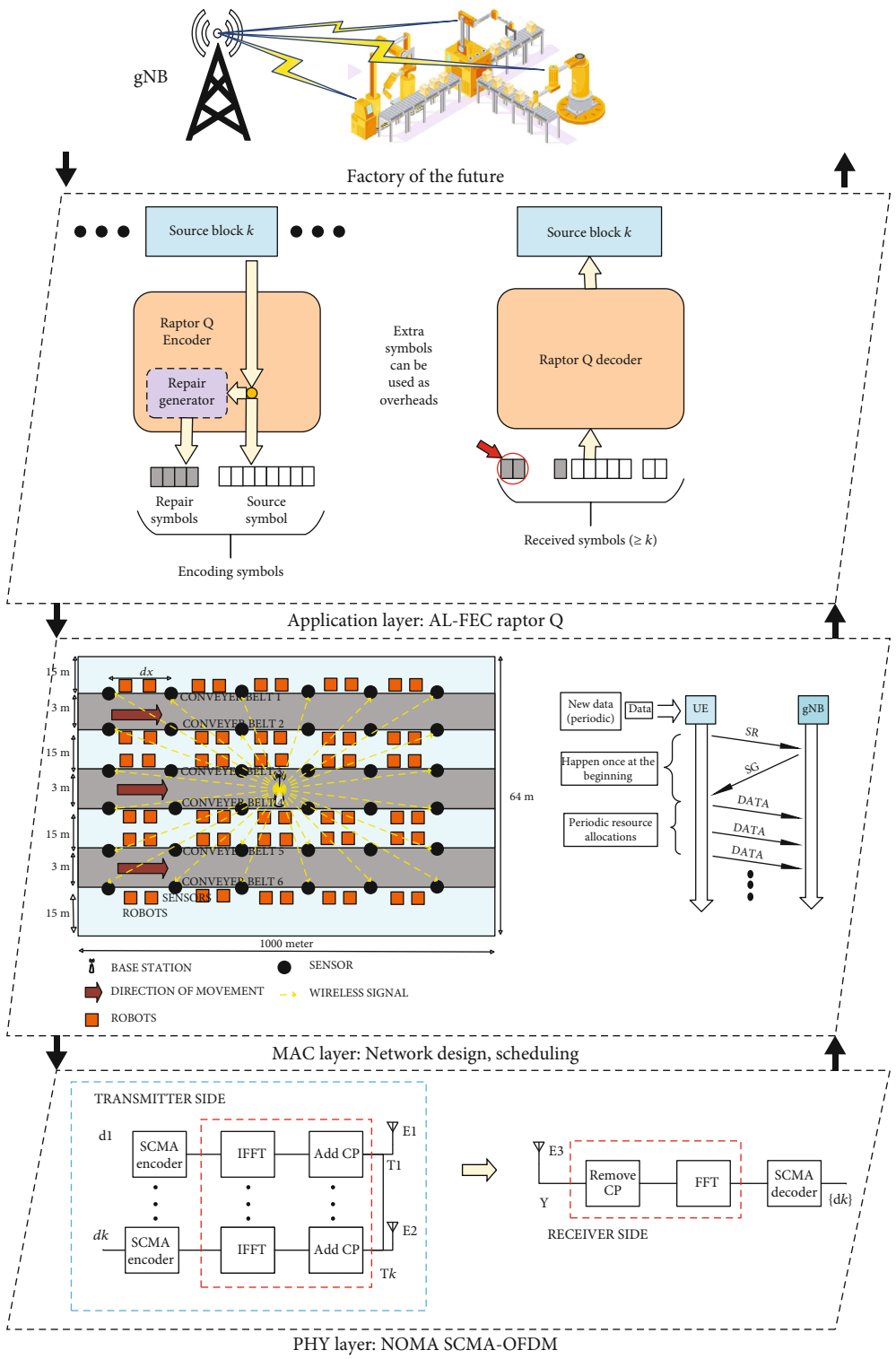


Figure 3: Illustration of the components of the subsystem.

Nonetheless, RLNC also can be replaced with other common rateless coding classes as LT codes [10] or Raptor codes [5]. Raptor codes, in fact, deliver near-optimal performance while requiring substantially less decoding complexity, allowing for longer source blocks. According to [43], Raptor offers codes considerably greater encoding throughput for bigger generation sizes, as investigated in depth in [44], due to a linearly rising asymptotic encoding computational

Table 1: Simulation parameters of the system PHY-MAC-APP [43, 45, 50].

Parameters	Values
PHY layer block	
Radio access mode (modulation)	Sparse code multiple access (SCMA)
SCMA codewords	4
SCMA codebook size	4
SCMA layers	6
SNR	1 : 20
Channel coding (FEC)	Polar
Bandwidth (kHz)	200 (NB-IoT)
Code rate	1/2
Subframe time (ms)	1
Channel model	Rayleigh fading +AWGN
Receiver type	MMSE
Carrier frequency (GHz)	3.5/28
Subcarrier spacing (kHz)	60
Symbol duration (μs)	16.67
Cyclic prefix (μs)	1.17 (normal) 17.84 (extended)
Diversity	Frequency
Subframe (ms)	0.2
Slot (ms)	0.25
Physical channel name	UL
Data rate (kbps)	8.4
Jitter (μs)	100
Delay spread (DS) $\mathrm{lgDS} = \log_{10}(\mathrm{DS/1\ s})$	-1.71 (μ_{lgDS}) 0.18 (σ_{lgDS})
AOD spread (ASD) $\mathrm{lgASD} = \log_{10}(\mathrm{ASD}/1^\circ)$	1.56 (μ_{lgASD}) 0.25 (σ_{lgASD})
AOA spread (ASA) $\mathrm{lgASA} = \log_{10}(\mathrm{ASA}/1^\circ)$	1.66 (μ_{lgASA}) 0.28 (σ_{lgASA})
Shadow fading (SF) [dB]	4.32
K-factor (K) [dB]	7 (μ_K) 8 (σ_K)
MAC layer block	
Numbers of sensors	48
Numbers of robotics/lane	25/50/100
Traffic model	Periodic
BS transmit power (dBm)	30
Noise figure (dB)	9
Payload size (bytes)	50/200/300/500
Speeds (for moving robotics) (km/h)	0(static)/3/7/10
Number of lane	6
Lane width (m)	1
Simulation area size (m)	$1000 \times 64 \times 12$
Queuing model	M/G/1
Rate of arrival	Poisson distributed
Dispatching scheme	First come, first serve
Scheduling	Semi-persistent
APP layer block	
Generation size, T	1024
Total upper layer header, L	23
Source block length, K	20
Code rate, CR	0.5
Base station height (gNB), m	10
FEC	Raptor Q/Repetition/ RLNC

difficulty in n; in contrast, RLNC encoding computational complexity scales asymptotically with $O(n^2)$. It is vital to remember that Raptor does systematic encoding, which means that the n source packets can be delivered in the uncoded form initially as soon as they become accessible from the application, followed by the coded repair symbols.

Although all these previous works used RLNC network coding and FEC codes in the system, none of them focused on the overall performances in terms of packet reception rates (PRR) and the end-to-end (E2E) delay of the system by using the more practical version Raptor codes, which are Raptor Q codes. The emergence of 5G technologies and the Internet of Things (IoT) for Industrial Revolution 4.0 in an indoor smart manufacturing setting is the primary motivation for this research. Smart factory concepts need the use of data from the production line. One way to wirelessly gather machine sensor information in severe manufacturing conditions is an enabler for such applications, and Raptor Q coding has been offered as a tool to develop appropriate network protocols. Hence, this paper presents a cross-layer E2E system performance analysis using Raptor Q codes for an indoor factory of the future. We compare the end-to-end latency and packet reception rate (PRR) of Raptor Q codes encoding and decoding with RLNC network coding for an additional viewpoint on the Raptor Q codes encoding and decoding. More specifically, the main contributions of this paper are presented as follows:

(1) This paper is the extended work from [30] where the authors investigated and designed the PHY-MAC cross-layer model by introducing the NOMA technique at the PHY layer and utilizing semi-persistent scheduling at the MAC layer in an indoor factory scenario. However, the proposed work in [45] had only been investigated until the MAC layer and not entirely investigated until the system/application level of the indoor factory. Hence, this paper focuses on the APP layer performance analysis by introducing Raptor Q codes to improve the overall reliability and end-to-end delay by tackling the packet losses

(2) Adjusting Raptor Q encoding parameters including code rate, symbol size, and the amount of source symbols on the fly to account for time-varying wireless networks and the reliability of Raptor Q codes

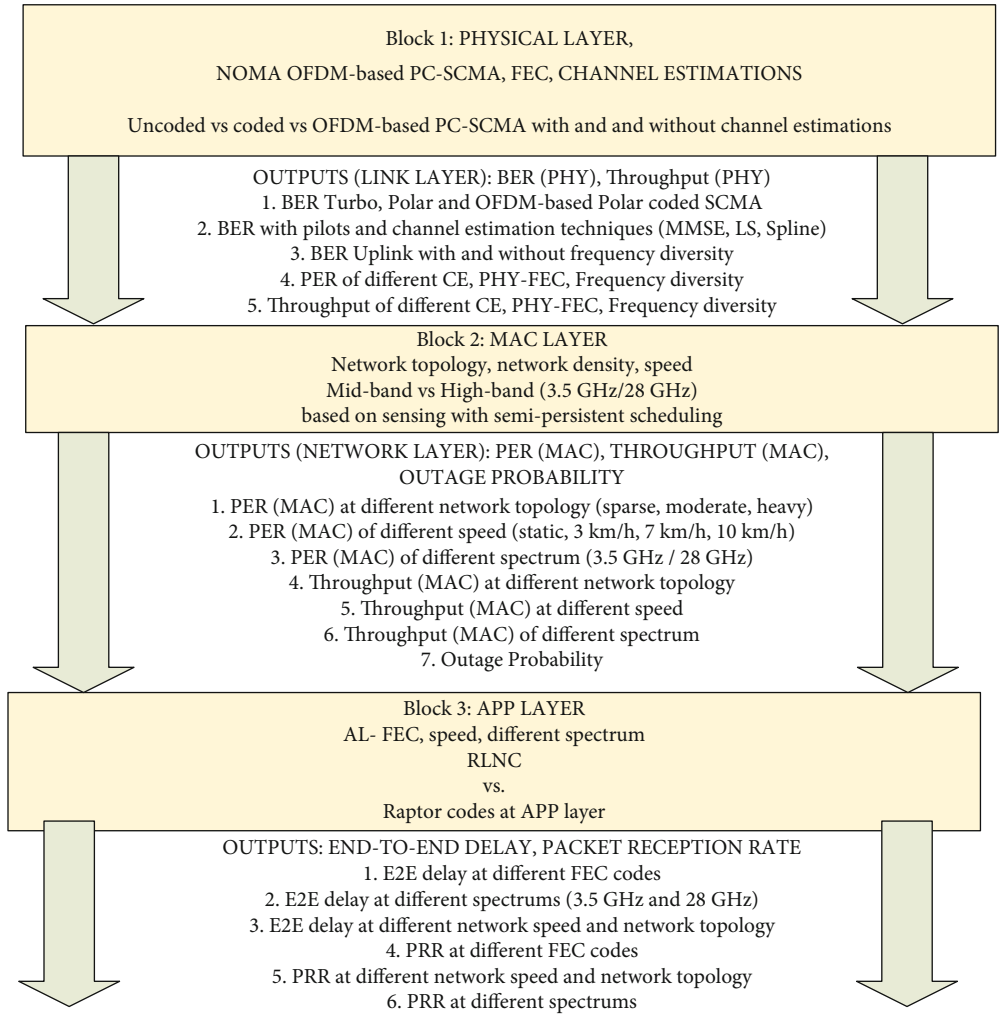


Figure 4: Factory of the future communication model system.

(3) The system model is developed based on cross-layer simulation of potential wireless deployment for future factory automation applications with considered system parameters based on 3GPP TR 38.913 [46] and METIS [47] under different network densities, speeds, and frequency spectrums

(4) An event-based simulator in measuring packet reception rate (PRR) and E2E delay performance is being developed, and the results obtained are analyzed with Repetition codes as the performance comparison. The results could be a valuable insight for the factories of future services [48].

This paper has the following structure. The basic concepts and overview of Raptor Q codes are discussed in Section 2. The PHY-MAC-APP layer simulation system and measurement setup are elaborated in Section 3. Results and discussions are further analyzed in Section 4. Finally, Section 5 presents the conclusion of the paper.

2. Factory Applications and Its Communication System Requirements

The Raptor is a forward error correction (FEC) technique deployed in software that protects against network packet loss at the application layer. A Raptor code is made up of an outer code (precode) Φ and an inner LT code C that are serially concatenated. The precode Φ is a (n, k) block code that uses k source symbols to create n intermediate symbols. The LT code C is then used to create k output symbols by encoding the n intermediate symbols with a $(k\gamma, n, \Omega(x))$ LT encoder, where the inverse of the Raptor code receives code rate CR. The code rate CR is derived as [49]:

$$CR = \frac{1}{\gamma} = \frac{1}{1+\varepsilon}, \tag{1}$$

where $\mathcal{E}$ is the overhead of the Raptor code. Meanwhile, the LT code generator matrix is built using a predetermined

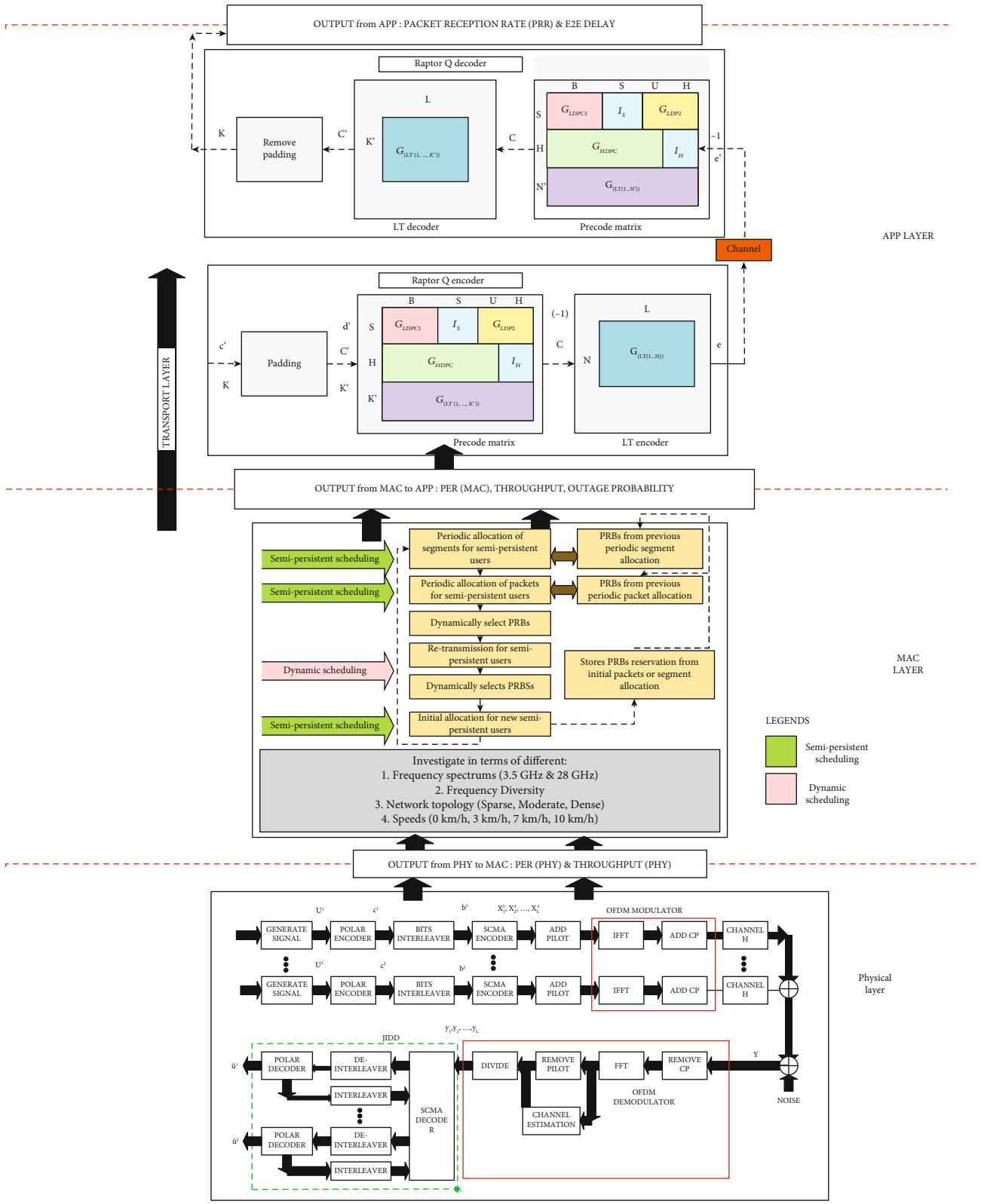


Figure 5: The PHY-MAC-APP system model proposed in this paper.

degree distribution expressed as

$$\Omega(x) = \sum_{d=1}^{d_{\max}} \Omega_d x^d, \tag{2}$$

where each row's degree d follows the probability distribution in (3) and satisfies (4).

$$\Omega_d = (\Omega_1, \Omega_2, \cdots, \Omega_{\max}), \tag{3}$$

$$\Omega(x) = \sum_{d=1}^{d_{\max}} \Omega_d = 1. \tag{4}$$

The Raptor code is denoted as (5), whereas the information symbols and received coded symbols are denoted as

$$\eta = \xi(\gamma, k, \Omega(x), \Phi), \tag{5}$$

$$\boldsymbol{s}_{k\,x\,1} = (s_1, s_2, s_3, \cdots, s_k)^T, \tag{6}$$

$$\boldsymbol{c}_{\gamma k\,x\,1} = \boldsymbol{G}^{LT}_{\gamma k\,x\,n} \boldsymbol{G}^{pre}_{n\,x\,k} \boldsymbol{s}_{k\,x\,1}, \tag{7}$$

where k represents the number of information symbols, γk is the number of received symbols, and n denotes the number of intermediate symbols. The LT generator matrix and the precode generator matrix, respectively, are denoted as $\boldsymbol{G}^{LT}_{\gamma k\,x\,n}$ and $\boldsymbol{G}^{pre}_{n\,x\,k}$. Moreover, the input alphabet of a q-ary Galois Field, $\boldsymbol{G}^{F(q)}$, is expressed as

$$\boldsymbol{G}^{F_q}_{q-1} = \left(0, 1, \alpha, \cdots, \alpha^{q-2}\right), \tag{8}$$

where α is denoted by a primitive element of GF(q) and then the Raptor Q code's nonzero elements are then arbitrarily selected from $\boldsymbol{G}^{F_q}_{q-1}$, where each nonzero entry in $\boldsymbol{G}^{LT}_{\gamma k\,x\,n}$ and $\boldsymbol{G}_{n\,x\,k}$ is sampled separately and uniformly from F_q.

Raptor Q is the most versatile and recent technology in Digital Fountain's Raptor range [10]. At the application layer, the Raptor Q encoder collects incoming Real-time Protocol (RTP)/User Datagram Protocol (UDP) packets to build source blocks, each of which has k source packets (symbols) with T bytes, and then creates N encoded symbols with T bytes from each block. Because the Raptor Q codes are systematic, the original k source symbols are the initial encoding symbols of N encoded symbols, and the remaining R symbols of N symbols are termed as the repair symbols $(N = k + R)$. The $CR = k/N = k/(k + R)$ code rate for Raptors is expressed as (1). Meanwhile, the Raptor Q decoder waits for all UDP packets belonging to a specific source block to arrive at the receiver. When the total number of acquired packets (source and repair symbols) for a particular source block is $k^{'}\,(\mathcal{E} + 1)\,k$ at the decoder, the Raptor Q decoder can decode the block with a high probability where all source packets of the source block are rebuilt and sent to the application layer.

Figure 1 shows a simpler illustration of the concept of signals from the gNB emitted at the application layer in a factory environment. The data sent from gNB is then divided into several source blocks k. This source block is encoded using Raptor Q encoding, which produces a source symbol followed by a repair symbol generated by the repair generator. These encoded symbols are arranged in packets and transmitted over the 5G mobile network. In the network, some transmitted packets are lost due to interference of the surrounding conditions as well as poor or challenging environment. On the sensors/actuators decoding section, the received symbol must be $\geq k$. The redundant repair symbol can be used as an overhead for the source symbol in the Raptor Q decoding process at the sensors/actuators. The source block data on decoding then reconstructs the data. Then, the data is sent to the receiver. In the use of the Raptor Q code, the symbols do not need to be arranged sequentially. Most importantly, sufficient symbols should be received at the receiver, as illustrated in Figure 2.

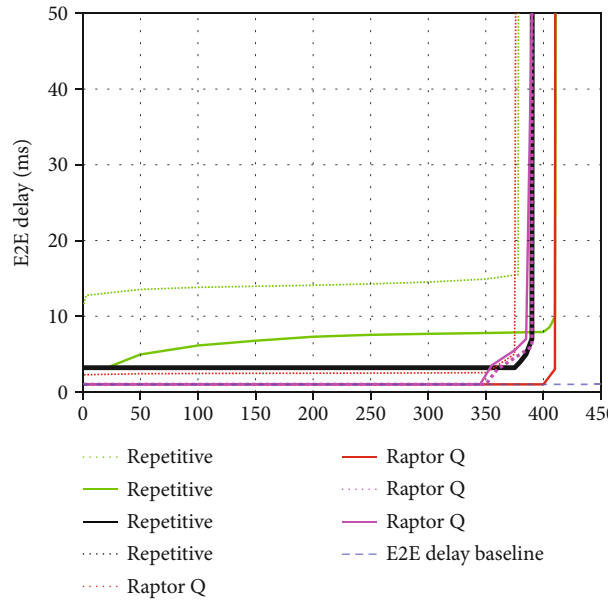


Figure 6: E2E delay in perfect CSI.

3. System Model

An event-based simulator is developed to analyze the end-to-end system performance of a 5G wireless communication system for an indoor factory of the future across different cross-layer system parameters. The simulator has been developed and divided into three subsystems, as shown in Figure 3 to decrease computing complexity and time. The components of the subsystems consist of the following:

(1) *Physical layer:* nonorthogonal multiple access (NOMA)-based OFDM-SCMA [50]. SCMA combines the bit-to-QAM symbol mapping and spreading procedures, and entering bits are immediately mapped to a multidimensional codeword of an SCMA codebook set

(2) *MAC layer:* indoor factory cross-layer design simulator as proposed in work [45] where the results obtained from [45] are to be used and analyzed

further in the APP layer simulator to evaluate overall system performance

(3) *Application layer:* AL-FEC Raptor Q model simulator as proposed in this paper

The indoor factory broadcast concept is based on [48], where it enables a simple, rapid, and large-scale transmission of messages without feedback to the sensors/actuators. It eliminates the need for complicated routing and avoids coverage limitations by reducing reliance on high-cost infrastructure rollout. The objective of this indoor factory broadcast model is to evaluate the latency and reliability of AL-FEC Raptor Q codes and Repetition codes in an indoor factory building (consisting of sparse, moderate, and dense network density) contexts for the same scenario. This indoor factory broadcast model is a MATLAB-based event-based simulator that comprises three distinct components. Meanwhile, RLNC simulation is based on [51] theory and is implemented in our in-house simulator from the PHY layer until the APP layer.

The location of each sensor is examined and assessed using the position, speed, and outputs of the realistic sensor density (v_d) for each beacon period to build an indoor factory simulator, as illustrated in Figure 3. Each sensor's (or actuators) received power P_R is computed based on its distance from the tagged sensor. The SINR (signal-to-interference ratio) is calculated for each sensor based on co-channel interference from a list of sensors with $P_R >$ threshold.

A NOMA OFDM-SCMA simulator is utilized in the physical layer block to compute the BER_{phy}, PER_{phy}, and $throughput_{phy}$ for various SNR (signal-to-noise ratio) values. The computed SINR is transmitted to the (PER_{PHY}) versus SNR curves for each sensor or actuator. The component parameters in the PHY layer are considered in Table 1.

The MAC system model has been explained in our previous work in [45]. To summarize, a cross-layer design for an indoor factory of the future is designed and developed to suit the stringent requirements for URLLC. In work [45], a cross-layer strategy is proposed by utilizing semi-persistent scheduling (SPS) at MAC and code-domain NOMA at PHY to achieve an ultra-reliable communication (URC) for potential 5G mobile network deployment for the factory of the future. By having outputs from [45], results of PER_{mac}, $throughput_{mac}$, and outage probability are critically evaluated and analyzed by varying multiple parameters such as network densities (sparse, moderate, and dense), various speed of sensors/actuators that are realistic to the indoor factory scenarios (static, 3 km/h, 7 km/h, and 10 km/h), and two allocated 5G frequency spectrums, which is mid-band (3.5 GHz) and high band (28 GHz).

The reason for using two different types of spectrums at MAC layer is to investigate the characteristics of the spectrums when it is deployed in an indoor factory. Based on the results in [45], it is shown that the mid-band spectrum outperformed the high band due to the high-band spectrum being highly susceptible to the clutters present in the factory. The traffic model considered in the MAC layer block is periodic since SPS is utilized in the MAC layer; it has the advantage of manipulating the previous knowledge regarding the traffic characteristics. Moreover, the first-come first-serve (FCFS) dispatching scheme is considered, and it is assumed that no items are discarded from the queue. A M/G/1 queuing model is considered, and the rate of arrival is classified as Poisson distributed. In addition to that, general distribution is assumed as a service rate. Table 1 shows the parameters used at the MAC layer block, as stated in [45], whereas Figure 4 shows the factory of the future communication model system.

To increase the reliability of the indoor factory broadcast system model, the AL-FEC model is employed. The FEC block emulates this function in the simulation. A source block (SB) is formed of K source symbols of size $T = (N_{PSDU\,FEC})$ in the FEC block. The physical layer service data unit (PSDU) size for a particular message type is $(N_{PSDU,FEC})$, and FEC is described as

$$\left(N_{PSDU,rep}\right)_{app} = N_{payload} + N_{headers}, \tag{9}$$

$$\left(N_{PSDU,rap}\right)_{app} = \left(\frac{N_{payload}}{k}\right) + N_{headers}. \tag{10}$$

There are three types of FEC schemes introduced in this paper, which are the Repetition codes, RLNC, and Raptor Q codes that are implemented at application layer (APP). Repetition codes are introduced as it is simple and there are no feedback requirements. The complexity of this method is minimal. Repetition codes, on the other hand, have a high latency requirement and inefficient bandwidth usage, making them unsuitable for URLLC applications.

As a result, this paper investigates the systematic Raptor Q codes, and the results obtained are being compared to the Repetition codes and RLNC results. The overall PHY-MAC-APP model system is shown in Figure 5.

At the application layer, the Raptor Q encoder gathers input SB at the transmitter and fragments them to size $K = 8$ to create source symbols of size $T = (N_{PSDU,rap})_{APP}$. K is the length of a source block or the number of source symbols (SSs) that make up a source block (SB) in raptor codes. It also produces R repair symbols, which are specified by the code rate (CR) in (1). The Raptor decoder gathers all the source symbols that correspond to a given source block at the receiver. If the total number of combined received symbols for a particular block of data meets $k' \geq (\mathcal{E} + 1) * k$, where the encoded symbol overhead $\mathcal{E} > 0$, the Raptor decoder successfully decodes all of the source packets. Each transmitted encoded symbol has an ESI (encoded symbol identifier) sequence number that may be used to calculate the average end-to-end delay.

Note that $CR = 1$ denotes the absence of the redundant symbols, whereas $CR = 0.5$ denotes a 50% increase in overhead. Raptor encoding and decoding delays are less than 1 ms, according to measurements in [49], and Raptor chipsets with fast implementation are widely available. As a result, the Raptor processing delay is ignored when calculating the end-to-end delay. In this model, the User Datagram Protocol (UDP) is assumed for low latency and no retransmissions. For successful decoding (PER <1%), the packet reception rate (PRR) results obtained from Equation (11)

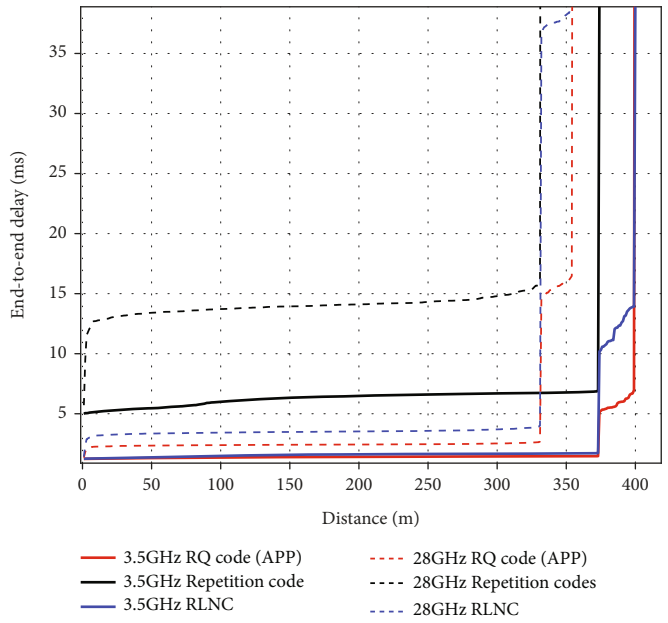


Figure 7: E2E delay with frequency diversity in dense network.

are transmitted to the FEC block, where either Repetition codes overhead $N_r = 4$ or Raptor Q codes overheads $\mathcal{E}$ is chosen depending on the FEC type.

$$\begin{aligned}(\rho(v_d, d)) &= \left(1 - PER_{phy}(s,t)\right), N_{\max} \geq N_{\text{receive}} \\ &= \left(1 - PER_{phy}(s,t)\right) * \left(\frac{N_{\max}}{N_{\text{receive}}}\right), N_{\max} < N_{\text{receive}},\end{aligned} \tag{11}$$

where $N_{\max}$ is the maximum number of sensors/actuators within $r_{\text{sense}} = 100$ m of the transmitter sensor/actuator and N_{receive} is the total number of sensors/actuators that successfully receive the signal among $N_{\max}$; PER_{PHY} is the PHY layer PER calculated in the PHY layer block. In addition, the PRR used in this study is the average PRR of all of the sensors/actuators at a distance of d from the tagged sensor/actuator. For the end-to-end delay computation, the corresponding overhead for the provided FEC type is used. The end-to-end latency is calculated using Equations (12) and (13), with the number of repetitions $N_r = 4$ for Repetition codes and ESI overhead of $ESI_{K+\mathcal{E}} = K/CR$ for Raptor codes.

$$(\tau_{ss}(v_d))_{rep,APP} = N_r * \tau_{MAC}(v_d), \tag{12}$$

$$(\tau_{ss}(v_d))_{\text{raptor}} = \frac{K}{CR} * \tau_{MAC}(v_d). \tag{13}$$

Given the equation $\tau_{MAC}(v_d)$ is expressed as

$$\tau_{MAC}(v_d) = T_s = T_{\text{total}HD}, \tag{14}$$

where $T_{\text{total}HD}$ is the time taken by PHY layer source symbol. It is assumed that a half-duplex $(ksi = 0)$ operation is being used, which corresponds to the full cancellation of the self-interference, and all resources are assumed available $(\delta = 1)$.

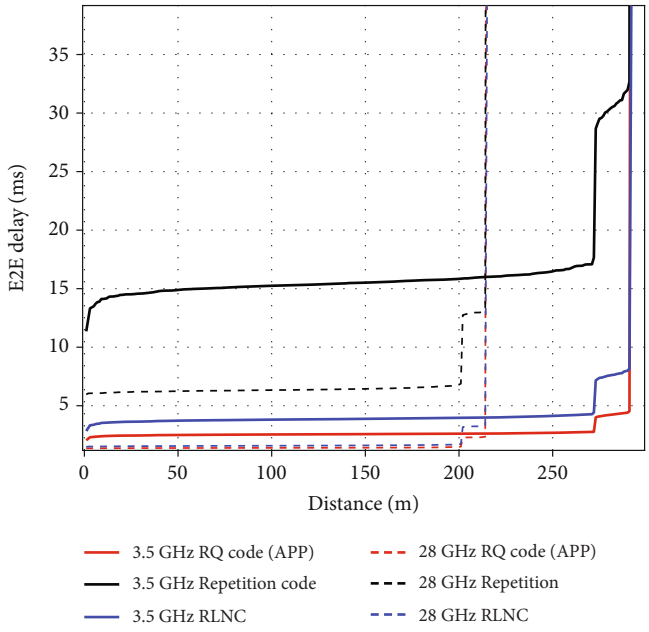


Figure 8: E2E delay without frequency diversity in dense network at stationary.

4. Results and Discussions

In this section, the system performance of factory of the future is developed and investigated in terms of packet reception rate (PRR $(\rho(v_d, d))$) and end-to-end delay in an indoor factory environment. Firstly, the performance of Repetition, RLNC,

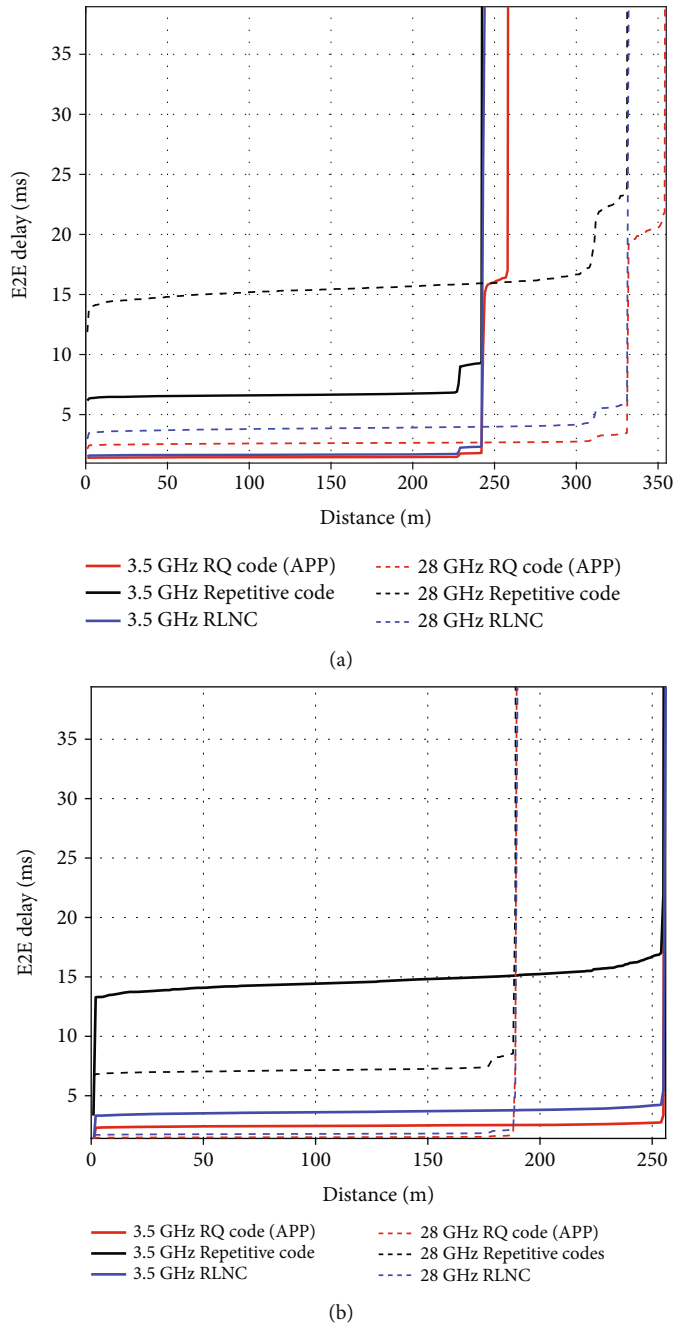


Figure 9: (a) E2E delay at 3 km/h sparse network and (b) E2E delay at 10 km/h.

and Raptor Q codes are being compared in terms of different parameters such as sensor network densities, speeds, and spectrums. Sensor density is calculated as $v_d = 0.025$ sensor/meter for sparse network, $v_d = 0.05$ sensor/meter for moderate network, and $v_d = 0.1$ sensor/meter for dense network as being computed by using Equations (15) and (16). To ensure consistency when comparing both codes, $r_{sense} = R$ is standardized to 100 m, and it is assumed that all resources are available $(\delta = 1)$. Also, half duplex operation $(ksi = 0)$ is used to simulate all the sensors [55].

$$v_d = n \times \frac{N_l}{1000}, \tag{15}$$

$$n = \frac{1000}{6 \times speed}, \tag{16}$$

where N_l indicates number of lanes as per stated in Table 1.

4.1. End-to-End Delay Performance. Based on stringent requirements of URLLC as mentioned in [1], the target

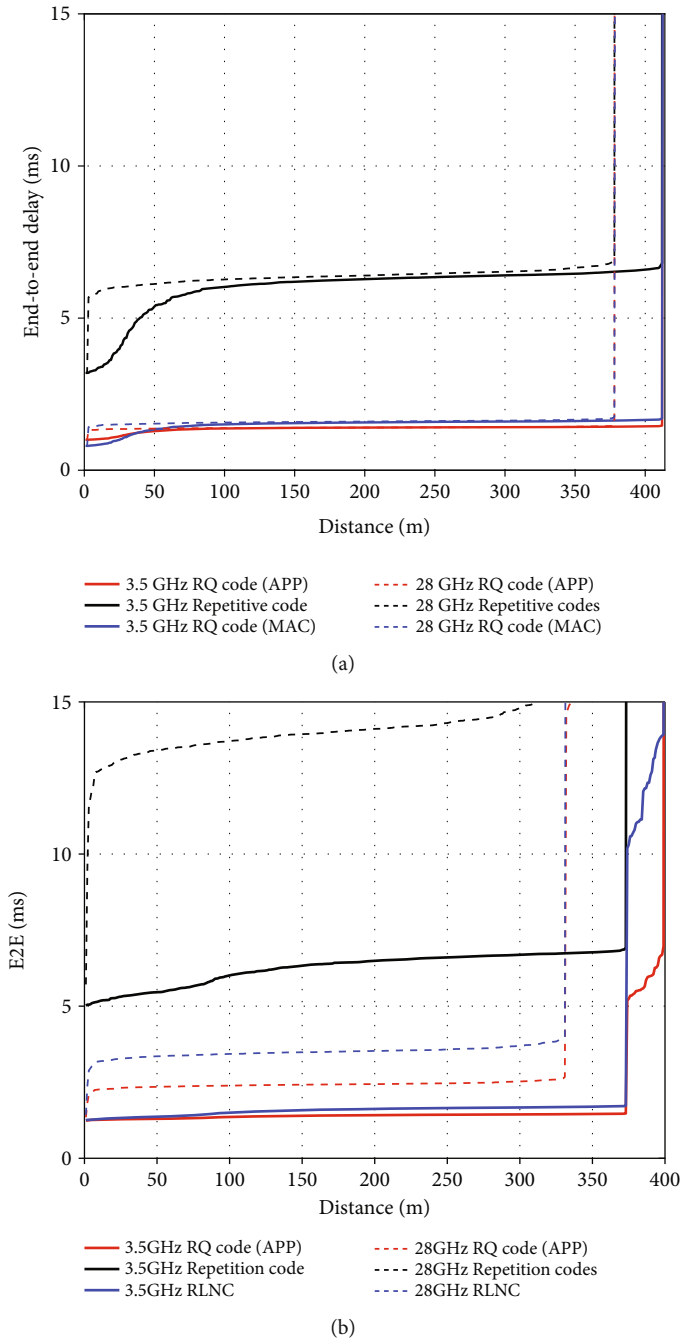


Figure 10: PRR RLNC vs. Raptor Q in moderate scenario at static and 10 km/h.

E2E delay is 1 ms. Figure 6 shows the performance comparison of Repetition and Raptor Q codes in perfect channel state information (CSI). It is shown that AL-FEC Raptor Q for static mid-band with dense network deployment has the results by having an E2E delay of 1 ms for coverage of 400 m. Meanwhile, the same spectrum of 3.5 GHz of Repetition codes has shown the distance coverage of 400 m with larger than 15 ms delay. This shows that it was unable to achieve the target URC E2E delay requirement, which is 1 ms, exceeding a huge delay gap of 7 ms, whereas Raptor Q codes of 28 GHz obtained a distance coverage of 391 m. The performance of the mid-band spectrum gives an improvement of nearly 21 m. The combination of mid-band spectrum and Raptor Q codes at APP provide high tolerance towards packet error channel erasure by extending the coverage. Starting from this point onwards, the performances of source coding are compared between RLNC and Raptor Q and also be considered. Next, the E2E delay results were analyzed at dense network density with frequency diversity, as shown in Figure 7. In this case, the situation is investigated at a speed of 10 km/h. The difference in performance between the mid-band and high band is assessed by

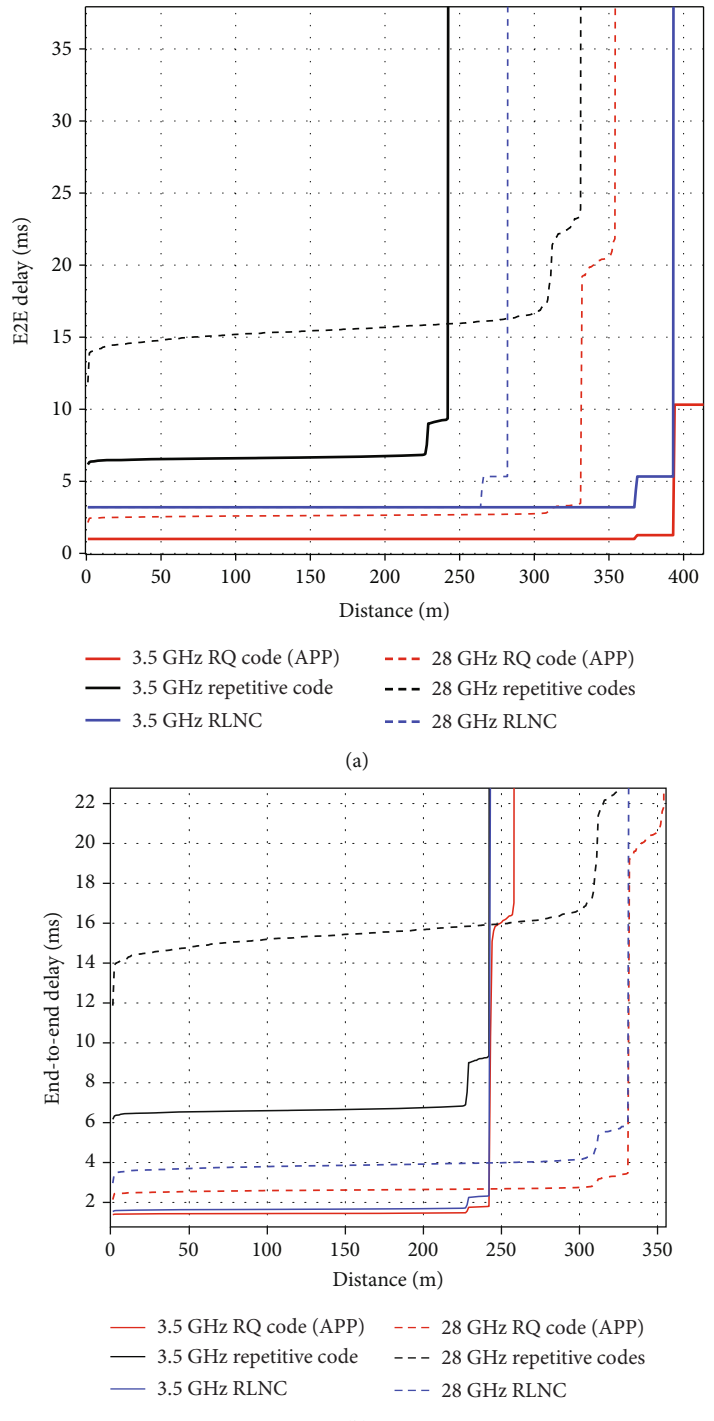


Figure 11: E2E delay in dense network at 3 km/h (b) E2E delay in dense network at 7 km/h.

using RLNC and Raptor Q codes. It can be seen that at 3.5 GHz with dense network density and Raptor Q codes yield the best results compared to the rest. It covers a distance of 375 m at an E2E delay of 1 ms. Meanwhile, the same spectrum of RLNC codes also yields the same distance coverage as Raptor Q. Furthermore, based on the overall performances, it can be seen that the mid-band outperformed the high band. This is because the characteristics of the 3.5 GHz band are more stable and robust towards longer distance coverage during movement, whereas, the high-band signal (28 GHz) is highly susceptible to obstructions and signal interferences.

In addition to that, Figure 8 shows the performance comparison of E2E delay without frequency diversity. The performance of the simulation is assessed similarly in Figures 6 and 7. As predicted, the mid-band with Raptor Q codes at stationary

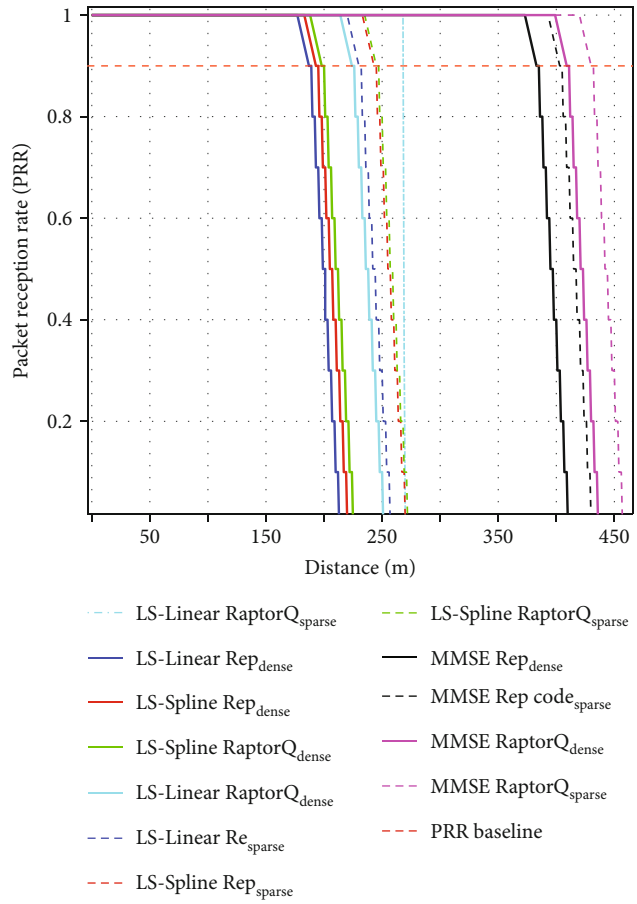


Figure 12: PRR comparison between types of channel estimations.

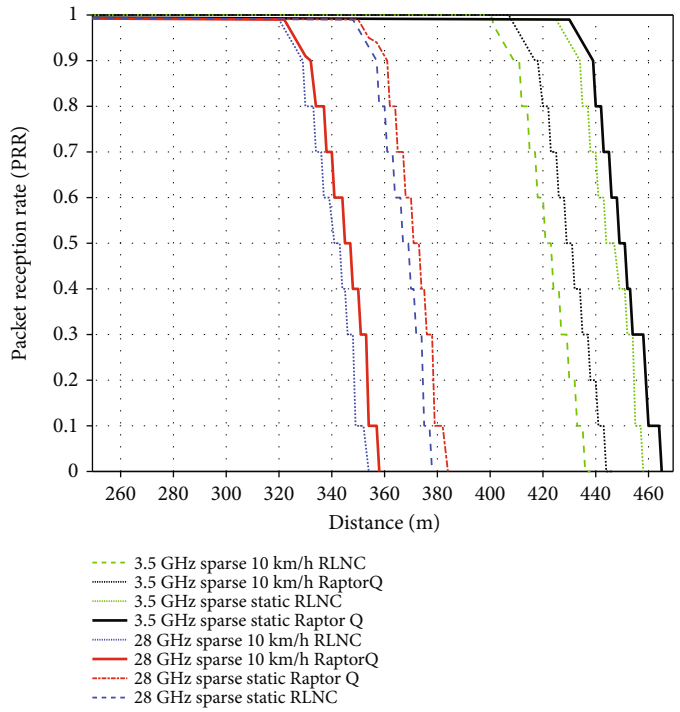


Figure 13: PRR in sparse scenario at static and 10 km/h.

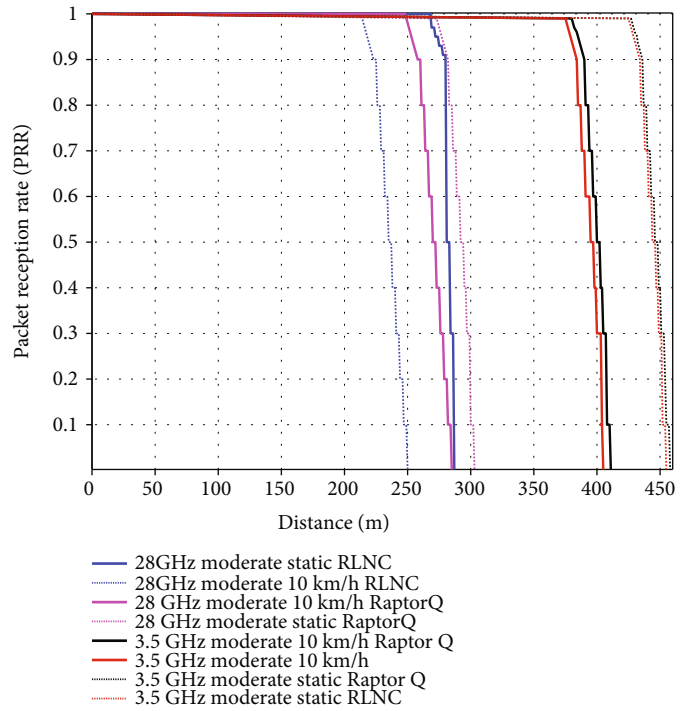


Figure 14: PRR RLNC vs. Raptor Q in moderate scenario at static and 10 km/h.

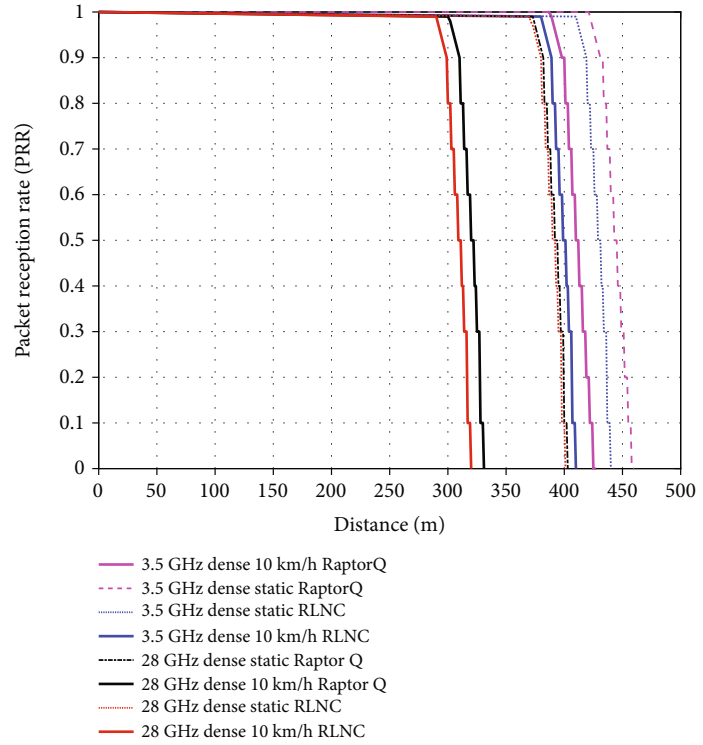


Figure 15: PRR RLNC vs. Raptor Q in dense scenario at static and 10 km/h.

Table 2: Coverage performance between RLNC and Raptor Q codes at 3.5 GHZ for different speeds and network densities.

Distance coverage		Speed			
Targeted PRR = 0.9	Density	Static	3 km/h	7 km/h	10 km/h
	Sparse	426 m	410 m	405 m	402 m
RLNC	Mod.	425 m	409 m	402 m	395 m
	Dense	410 m	405 m	390 m	380 m
	Sparse	430 m	420 m	412 m	407 m
Raptor Q codes	Mod.	427 m	412 m	410 m	399 m
	Dense	422 m	409 m	400 m	387 m
	Sparse	5 m (0.93%)	10 m (2.4%)	7 m (1.7%)	5 m (1.2%)
Improvement (meter)	Mod.	2 m (0.47%)	3 m (0.73%)	8 m (2.0%)	4 m (1%)
	Dense	12 m (2.8%)	4 m (1.0%)	10 m (2.5%)	7 m (1.8%)

Table 3: Coverage performance between RLNC and Raptor Q codes at 28 GHz for different speeds and network densities.

Distance coverage		Speed			
Targeted PRR =0.9	Density	Static	3 km/h	7 km/h	10 km/h
	Sparse	357 m	355 m	340 m	320 m
RLNC	Mod.	280 m	238 m	230 m	250 m
	Dense	370 m	311 m	315 m	300 m
	Sparse	361 m	378 m	370 m	322 m
Raptor Q codes	Mod.	283 m	242 m	233 m	260 m
	Dense	373 m	320 m	322 m	290 m
	Sparse	4 m (1.1%)	23 m (6.0%)	30 m (8.8%)	2 m (0.6%)
Improvement (meter)	Mod.	3 m (0.7%)	4 m (1.7%)	17 m (7.3%)	10 m (3.9%)
	Dense	3 m (0.8%)	9 m (2.8%)	7 m (2.2%)	10 m (3.4%)

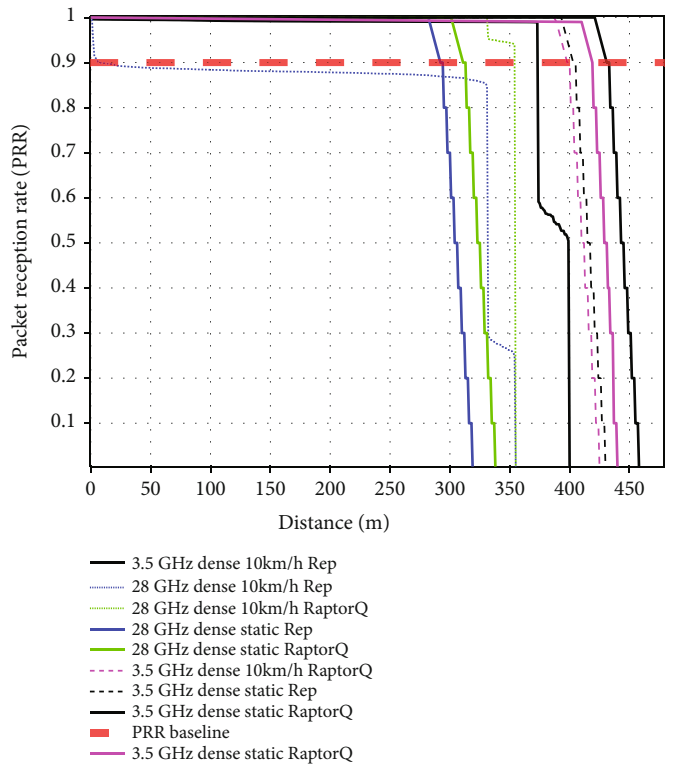


Figure 16: PRR Repetition vs. Raptor Q in dense scenario at static and 10 km/h.

showed the best results, with the distance coverage of 275 m at 1 ms E2E delay. RLNC also yields 275 m coverage; however, the delay is more than 1 ms, where this shows that it was unable to achieve the target URC E2E delay requirement, which is 1 ms. Moreover, the high band with Raptor Q yields a distance coverage of 200 m within acceptable E2E delay. Pursuing this further, Raptor Q codes and RLNC showed an improved distance coverage of 75 m at a stationary position.

Subsequently, the results obtained are analyzed in terms of frequency diversity with the presence of MMSE CE. Figures 9 and 10 are analyzed in different networks at different speeds such as 3 km/h and 10 km/h, respectively. Raptor Q codes with the spectrum of 3.5 GHz, as shown in Figure 9(a) have shown a result, which was 225 m distance coverage at E2E delay of 1 ms, whereas as shown in Figure 9(b), the highest distance coverage by Raptor Q are slightly lower, which was 189 m. There is an increase of 6.4% in the mid-band sparse network at 3 km/h, whereas a 2% increase in high-band sparse at 10 km/h.

In Figure 10(a), static and 10 km/h in moderate scenarios using Raptor Q codes, the distance covered is observed to be 410 m within the targeted 1 ms delay. RLNC, however, is not achieving the URC targeted delay of 1 ms, although it has the same distance coverage as Raptor Q codes. Correspondingly, spectrum 3.5 GHz outperformed spectrum 28 GHz with the distance coverage difference of 100 m at the static condition and 58 m at the speed of 10 km/h. Afterward, Figure 10(b) showed the results of Raptor Q codes and RLNC at 3.5 GHz and 28 GHz spectrums. Raptor Q codes at 3.5 GHz outperformed the Raptor Q codes at 28 GHz by a total distance coverage difference of 75 m. However, at a speed of 10 km/h, only Raptor Q codes with mid-band 5G is achieving the URC-targeted E2E delay. Despite good distance coverage, the rest are not achieving the stringent requirement of URC targeted delay.

Concurrently, the results are being analyzed under a busy and dense network scenario, which is 100 sensors per km per lane. In addition, the results are also being observed at different speeds such as static, 3 km/h and 7 km/h. As expected, the mid-band spectrum outperformed the high-band spectrum in all four scenarios. In a dense network, the transmitted messages are experiencing a high rate of collision with one another which has caused an increase in E2E delay. Raptor Q codes in mid-band managed to achieve results within the targeted E2E delay. In Figures 11(a) and 11(b), at speeds of static and 3 km/h, the coverage area is up to 360 m, whereas the distance coverage is 280 m at speeds of 7 km/h.

4.2. Packet Reception Rate (PRR) Performance. Figure 12 shows the comparison of PRR with different types of CE at the receiver in sparse and dense scenarios. Based on [1], the targeted range for PRR is 0.9. MMSE CE outperformed LS CE by 432 m in distance coverage by implementing Raptor Q codes scheme in sparse networks. Besides, Repetition codes with the MMSE CE scheme also outperformed LS CE by 385 m (dense) and 405 m (sparse), respectively. The rest of the results are observed and analyzed based on MMSE CE at different scenarios, spectrums, AL-FEC, and sensor speed.

As shown in Figure 13, the results show a sparse network condition at speeds of static and 10 km/h, respectively. It is observed that Raptor Q codes at mid-band spectrum at stationary yielded the best result by having a distance of 426 m at $PRR = 0.9$ or 0.93% coverage improvement compared to RLNC, while RLNC of 10 km/h mobility at high band produced the worst results by having a distance of 402 m. This means that the Raptor Q codes scheme showed an improved distance coverage of 5 m or 1.2%.

Consequently, the results are obtained and analyzed in moderate conditions at static and 10 km/h as shown in Figure 14, whereas in Figure 15, the PRR is being analyzed in a dense scenario at static and 10 km/h. In a moderate static network scenario (mid-band), an improvement of 2 m or 0.47% can be observed, whereas at 10 km/h, an improvement of 4 m or 1% can be seen. On the other hand, a coverage improvement of 3 m (0.7%) and 10 m (3.9%) can be observed in the high-band spectrum at static and 10 km/h. Additional repair symbols are sent by Raptor Q codes to compensate for a target PRR's decreased performance. However, the cost associated with the additional repair symbols is relatively high.

Tables 2 and 3 show the summary of the obtained results from Figure 16, Figure 13, and Figure 14. These tables are divided into three categories which are sparse, moderate, and dense network. Based on the overall results in all two tables, it can be observed that the difference in coverage between RLNC and Raptor Q codes at high band is in the dense network at a speed of 10 km/h, which is 10 m or 3.4% improvement. Meanwhile, in mid-band, the improvement of 7 m or 1.8% can be seen. This is because the Raptor Q codes have a high tolerance for packet errors as well as erasure channels. Each packet is believed to have an equal chance of error, and if a mistake occurs, the packet is expected to be "erased." Since the packet transmission at higher layers has the same characteristics as a binary erasure channel (BEC), thus, it is able to offer a good opportunity for the execution of Raptor Q codes.

5. Conclusion

In this paper, the performance of PRR and E2E delay is evaluated and analyzed by using two types of AL-FEC schemes, namely, RLNC and Raptor Q codes, as a comparison. To test the reliability of such codes, performance is tested in various scenarios such as network density, sensor's velocity, and different spectrums (3.5 GHz and 28 GHz) which are studied and analyzed.

Firstly, the delayed performance has shown that the Raptor Q codes are able to meet the strict URC requirement of 1 ms in all types of proposed scenarios (sparse, moderate, and dense). The Raptor Q codes also meet the 1-ms delay target in a static state as well as in a moving state of 3 km/h, 7 km/h, and 10 km/h. In contrast to the RLNC, wherein some scenarios, its performance is not able to meet the pre-determined URC requirements. This clearly shows that the Raptor Q codes are ideal for obtaining low latency times at the APP layer. It is crucial to remember that Raptor Q executes systematic encoding, which means that the n source packets can be delivered in the uncoded form initially when

they become available from the application, followed by the y-coded repair symbols.

Besides that, the results are evaluated at the packet reception rate (PRR). In the attached results, the Raptor Q codes are not only able to give good results (PRR = 0.9) of 1.2% in a high-density static scenario and 1.8% in high density 10 km/h mobility (mid-band), even the Raptor Q codes are also able to meet PRR = 0.9 in the mobility scenario at 10 km/h in dense network with the improvement of 3.4% or 10 m in distance coverage in the 5G high band. Achievable PRR indicates that the communication system is robust and highly reliable in packet delivery in the application layer. Meanwhile, the RLNC cannot meet the requirement of PRR = 0.9 in the dense scenario at a speed of 10 km/h. These results imply that the Raptor Q calculation for low overhead encoding and decoding for all generation sizes, n, will be significantly faster if the implementation has been tuned for the scenario when the number of symbols needed to construct the intermediate block is near to n. Furthermore, Raptor Q decoding performance is significantly greater than RLNC decoding throughput because Raptor Q has a linear asymptotic decoding difficulty, whereas RLNC decoding has an underlying asymptotic computational complexity of $O(n^3)$.

However, this paper only focuses on a specific generation size and symbol size setting for an indoor factory. As future work, it is necessary to introduce a smaller generation size such as 16, 32, and 64 bytes to improve the reliability and E2E delay, as well as to study the effect of reducing the generation size in an industrial setting.

Thus, the Raptor Q codes can be a good candidate for obtaining results within a strict range of requirements set by the URC use case. As a result, RLNC can be replaced with other common classes of rateless codes, such as Raptor Q, for reliable source coding, especially in an indoor factory deployment.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

All authors conceived and design the study. Athirah Mohd Ramly conducted the experiment, analyzed the data, and wrote the paper. All authors contributed to manuscript revisions. All authors approved the final version of the manuscript and agree to be held accountable for the content therein.

Acknowledgments

This work was supported in part by the Center for Research and Instrumentation (CRIM) and the Faculty of Engineering and Built Environment (FKAB), Universiti Kebangsaan Malaysia (UKM), and in part by the Malaysian Ministry of Education and Universiti Kebangsaan Malaysia Research Grant under Grant GUP-2021-023.

References

[1] Huawei, "5G ToB Service Experience Standard Whitepaper," 2021, https://carrier.huawei.com/~/media/CNBGV2/download/products/servies/5g-b2b-service-experience-standard-white-paper-en1.pdf.

[2] S. R. Pokhrel, J. Ding, J. Park, O. -S. Park, and J. Choi, "Towards enabling critical mMTC: a review of URLLC within mMTC," *IEEE Access*, vol. 8, pp. 131796–131813, 2020.

[3] D. Feng, C. She, K. Ying et al., "Toward ultrareliable low-latency communications: typical scenarios, possible solutions, and open issues," *IEEE Vehicular Technology Magazine*, vol. 14, no. 2, pp. 94–102, 2019.

[4] M. Luby, "LT codes," in *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings*, pp. 271–280, Vancouver, BC, Canada, 2002.

[5] A. Shokrollahi, "Raptor codes," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2551–2567, 2006.

[6] M. Luby, A. Shokrollahi, M. Watson, and T. Stockhammer, "Raptor forward error correction scheme for object delivery," *Internet Engineering Task Force (IETF), RFC 5053*, vol. 11, no. 3, pp. 82–89, 2007.

[7] S. Nie, S. Gu, J. Jiao, W. Xiang, and Q. Y. Zhang, "A novel systematic raptor network coding scheme for Mars-to-Earth relay communications," in *2016 IEEE Wireless Communications and Networking Conference*, pp. 1–6, Doha, Qatar, 2016.

[8] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive multiple access based on superposition Raptor codes for cellular M2M communications," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 307–319, 2017.

[9] M. T. Gul, A. Ali, D. K. Singh et al., "Merge-and-forward: a cooperative multimedia transmissions protocol using RaptorQ code," *IET Communications*, vol. 10, no. 15, pp. 1884–1895, 2016.

[10] A. Shokrollahi and M. Luby, "Raptor codes," *Foundations and Trends in Communications and Information Theory*, vol. 6, no. 3-4, pp. 213–322, 2011.

[11] 3GPP, *UMTS; LTE; Multimedia Broadcast/Multicast Service (MBMS)*, Protocols and Codecs, 2015.

[12] M. Samokhina, K. Suwon, K. Moklyuk, S. Choi, K. Seoul, and J. He, "Raptor code-based video multicast over IEEE 802.11 WLAN," in *IEEE APWCS*, Citeseer, 2008.

[13] X. Chen, V. Subramanian, and D. J. Leith, "PHY modulation/rate control for fountain codes in 802.11a/g WLANs," *Physical Communications*, vol. 9, no. 9, pp. 135–144, 2013.

[14] J. Calabuig, J. Monserrat, D. Gozalvez, and D. Gomez-Barquero, "AL-FEC for streaming services in LTE E-MBMS," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, pp. 1–12, 2013.

[15] N. Ma and M. Diao, "CoFi: Coding-assisted file distribution over a wireless LAN," *Symmetry*, vol. 11, no. 1, p. 71, 2019.

[16] J. Heide, M. V. Pedersen, F. H. P. Fitzek, and T. Larsen, "Network coding for mobile devices-systematic binary random rateless codes," in *2009 IEEE International Conference on Communications Workshops*, pp. 1–6, Dresden, Germany, 2009.

[17] Y. Li, S. Blostein, and W.-Y. Chan, "Systematic network coding for two hop lossy transmissions," *EURASIP Journal on Advances in Signal Processing*, vol. 2015, no. 1, 2015.

[18] S. Pandi, F. Gabriel, J. A. Cabrera, S. Wunderlich, M. Reisslein, and F. H. P. Fitzek, "PACE: redundancy engineering in RLNC

for low latency communication," *IEEE Access*, vol. 5, pp. 20477–20493, 2017.

[19] L. Wei and W. Chen, "Compute-and-forward network coding design over multi-source multi-relay channels," *IEEE Transactions on Wireless Communications*, vol. 11, no. 9, pp. 3348–3357, 2012.

[20] D. Malak, E. Ohad, M. Médard, and E. M. Yeh, "Throughput and delay analysis for coded ARQ," in *2019 International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT)*, pp. 1–8, Avignon, France, 2019.

[21] D. Malak, M. Medard, and E. M. Yeh, "Tiny codes for guaranteeable delay," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 4, pp. 809–825, 2019.

[22] M. Kim, K. Park, and W. W. Ro, "Benefits of using parallelized nonprogressive network coding," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 293–305, 2013.

[23] S. Lee and W. W. Ro, "Accelerated network coding with dynamic stream decomposition on graphics processing unit," *The Computer Journal*, vol. 55, no. 1, pp. 21–34, 2012.

[24] H. Shojania, B. Li, and X. Wang, "Nuclei: GPU-accelerated many cores network coding," in *IEEE Infocom*, pp. 459–467, Rio de Janeiro, Brazil, 2009.

[25] S.-M. Choi, K. Lee, and J.-S. Park, "Fast parallel implementation for random network coding on embedded sensor nodes," *International Journal of Distributed Sensor Networks*, vol. 10, no. 2, Article ID 974836, 2014.

[26] K. Park, J.-S. Park, and W. W. Ro, "On improving parallelized network coding with dynamic partitioning," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 11, pp. 1547–1560, 2010.

[27] H. Shin and J.-S. Park, "Energy efficient QoS-aware random network coding on smartphones," *Mobile Networks and Applications*, vol. 22, no. 5, pp. 880–893, 2017.

[28] H. Shin and J.-S. Park, "Reducing energy consumption of RNC based media streaming on smartphones via sampling," *Multimedia Tools and Applications*, vol. 78, no. 20, pp. 28461–28475, 2019.

[29] S. Wunderlich, J. A. Cabrera, F. H. P. Fitzek, and M. Reisslein, "Network coding in heterogeneous multicore IoT nodes with DAG scheduling of parallel matrix block operations," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 917–933, 2017.

[30] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[31] J. He, V. Tervo, X. Zhou et al., "A tutorial on lossy forwarding cooperative relaying," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 66–87, 2019.

[32] M. El Soussi, A. Zaidi, and L. Vandendorpe, "Compute-and-forward on a multiaccess relay channel: Coding and symmetric-rate optimization," *IEEE Transactions on Wireless Communications*, vol. 13, no. 4, pp. 1932–1947, 2014.

[33] F. Gabriel, S. Wunderlich, S. Pandi, F. H. P. Fitzek, and M. Reisslein, "Caterpillar RLNC with feedback (CRLNC-FB): reducing delay in selective repeat ARQ through coding," *IEEE Access*, vol. 6, pp. 44787–44802, 2018.

[34] J. K. Sundararajan, D. Shah, M. Medard, and P. Sadeghi, "Feedback based online network coding," *IEEE Transactions on Information Theory*, vol. 63, no. 10, pp. 6628–6649, 2017.

[35] P. U. Tournoux, E. Lochin, J. Lacan, A. Bouabdallah, and V. Roca, "On-the-Fly erasure coding for real-time video applications," *IEEE Transactions on Multimedia*, vol. 13, no. 4, pp. 797–812, 2011.

[36] S. Wunderlich, F. Gabriel, S. Pandi, F. H. P. Fitzek, and M. Reisslein, "Caterpillar RLNC (CRLNC): a practical finite sliding window RLNC approach," *IEEE Access*, vol. 5, pp. 20183–20197, 2017.

[37] I. Chatzigeorgiou and A. Tassi, "Decoding delay performance of random linear network coding for broadcast," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7050–7060, 2017.

[38] A. Douik and S. Sorour, "Data dissemination using instantly decodable binary codes in fog-radio access networks," *IEEE Transactions on Communications*, vol. 66, no. 5, pp. 2052–2064, 2018.

[39] M. Nistor, D. E. Lucani, T. T. V. Vinhoza, R. A. Costa, and J. Barros, "On the delay distribution of random linear network coding," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 5, pp. 1084–1093, 2011.

[40] J. Qureshi, C. H. Foh, and J. Cai, "Online XOR packet coding: efficient single-hop wireless multicasting with low decoding delay," *Computer Communications*, vol. 39, pp. 65–77, 2014.

[41] H. Tang, Q. T. Sun, Z. Li, X. Yang, and K. Long, "Circular-shift linear network coding," *2017 IEEE International Symposium on Information Theory (ISIT)*, vol. 65, no. 1, pp. 65–80, 2019.

[42] D. E. Lucani, M. V. Pedersen, D. Ruano et al., "Fulcrum: flexible network coding for heterogeneous devices," *IEEE Access*, vol. 6, pp. 77890–77910, 2018.

[43] V. Nguyen, E. Tasdemir, G. T. Nguyen, D. E. Lucani, F. H. P. Fitzek, and M. Reisslein, "DSEP fulcrum: dynamic sparsity and expansion packets for fulcrum network coding," *IEEE Access*, vol. 8, pp. 78293–78314, 2020.

[44] M. Luby, L. Minder, and P. Aggarwal, *Performance of CodornicesRq software package*, International Computer Science Institute, 2019.

[45] A. M. Ramly, N. F. Abdullah, and R. Nordin, "Cross-layer design and performance analysis for ultra-reliable factory of the future based on 5G Mobile networks," *IEEE Access*, vol. 9, pp. 68161–68175, 2021.

[46] METIS II, *METIS II, V.1, Deliverable D2.1., "Performance Evaluation Framework"*, METIS II, 2016.

[47] GPP TS, *Service Requirements for next generation new services and markets*, ETSI, 2018.

[48] M. H. Alsharif, R. Nordin, M. M. Shakir, and A. Mohd Ramly, "Small cells integration with the macro-cell under LTE cellular networks and potential extension for 5G," *Journal of Electrical Engineering and Technology*, vol. 14, no. 6, pp. 2455–2465, 2019.

[49] K. Zhang, Q. Zhang, and J. Jiao, "Bounds on the reliability of RaptorQ codes in the finite-length regime," *IEEE Access*, vol. 5, pp. 24766–24774, 2017.

[50] A. H. Kelechi, M. H. Alsharif, A. M. Ramly, N. F. Abdullah, and R. Nordin, "The four-C framework for high capacity ultra-low latency in 5G networks: a review," *Energies*, vol. 12, no. 18, p. 3449, 2019.

[51] M. V. Pedersen, J. Heide, and F. Fitzek, "Kodo: an open and research oriented network coding library," *Lecture Notes in Computer Science*, vol. 6827, pp. 145–152, 2011.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7356733, 10 pages
https://doi.org/10.1155/2022/7356733

Research Article

Intelligent on Demand Clustering Routing Protocol for Wireless Sensor Networks

Muhammad Amir Khan [1,2] **and Adnan Anwar Awan** [3]

[1]*Department of Computer Science, COMSATS University Islamabad Abbottabad Campus, 22060, Pakistan*
[2]*Department Of Computer Science, IIC University Of Technology, Phnom Penh 121206, Cambodia*
[3]*Department of Electrical and Computer Engineering, COMSATS University Islamabad Abbottabad Campus, 22060, Pakistan*

Correspondence should be addressed to Muhammad Amir Khan; amirkhan@cuiatd.edu.pk

Received 30 December 2021; Accepted 21 February 2022; Published 29 March 2022

Academic Editor: Muhammad Asghar Khan

WSNs have become one of the most widely used approaches in a range of applications, including agriculture, smoke detectors, health care, and factory monitoring. WSN provides a number of benefits, including low cost, compact size, multifunctionality, self-organization, and the ability to be routed via WSN protocols. WSN is being used in more practical applications than ever before. Nonetheless, one of the most critical problems is energy shortage. It limits WSN technology from being fully utilized. Sensors are typically powered by batteries, which have a short lifespan. Even if renewable energy sources (such as solar or piezoelectric devices) are used as additional energy in wireless sensor networks, there is still room for efficient energy consumption. In our research, we identify the shortcomings of the existing LEACH protocol, suggest a novel methodology that improves the LEACH protocol, and compare it to the basic LEACH approach. Our research aims to increase network lifespan by reducing energy consumption, primarily based on limitations of the LEACH and its related algorithms.

1. Introduction

A wireless sensor network comprises low-power, low-cost, and multipurpose wireless sensor nodes that can perform sensing, wireless communication, and computing. These sensor nodes are deployed randomly. These nodes must configure themselves into a wireless network and fulfill a certain task after they have been deployed. Because sensor nodes have finite batteries, power is the most important resource in WSN. In this research, we provide a hierarchical routing protocol based on the LEACH protocol. Environmental monitoring, security and surveillance home intelligence, health care application, military uses, battlefield monitoring, object protection, intelligent guiding, and more applications of the LEACH protocol exist. The main challenge in WSN technology is extending the network's life and minimizing the sensor network's energy consumption. To monitor earthquakes, battlefields, industrial environments, residential monitoring [1], agricultural fields [2], physical atmospheric conditions, and smart houses, wireless sensor nodes are often spread throughout the sensing region. Sensor nodes sense their surroundings, collect data, and transfer it to the base station through a wireless network. Because of the dense deployment of WSN, charging node batteries is problematic. As a result, a primary focus of WSN technology is to reduce sensor node power consumption to extend the network's life. Many clustering-based algorithms have been proposed. Some of them are given in Literature Survey.

Clustering is a method that efficiently regulates network energy consumption by reducing sensor transmission range. The CH controls group communication with the BS in this mode of operation. Sensor nodes do not transfer data to the BS directly; instead, the cluster head gets the data in its

entirety, aggregates it, and passes it to the BS. The related cluster head receives the data from all of the member nodes in the cluster. The cluster head releases TDMA schedule to all the nodes to avoid conflicts. Every node of the cluster handovers its data to the cluster head exclusively according to the stated distribution mechanism. Hence, if there is no time interval, the sensor node will switch off its transceiver. TDMA scheduling favors preserving the energy of sensor nodes, so these member nodes can also last for a long time. Usually, each member node transfers the data to the neighboring cluster head; sensor nodes use the least energy to transfer data. CH performs computations on the collected information and filters out unnecessary bits, which decrease the amount of data that must be provided to the BS. So, the transmission energy of the sensor is considerably lowered. WSN is considered to be a very resource-limited form of the network where energy consumption is one of the key issues. Data are transmitted to the whole network instead of the target point, which is known as flooding. CH is unstable in the LEACH protocol; it is based primarily on round principles, with each round having two phases: setup and steady state. In this research paper, we propose an energy-aware multihop routing protocol based on gateways. The major objective of this study is to minimize sensor node energy consumption by logically dividing the network into various portions.

When it comes to wireless sensor networks, the way power is distributed across sensor nodes determining whether they are homogenous or heterogenous networks. Homogenous protocols include LEACH, HEED, and PEGASIS, while heterogenous protocols include DEEC and SEP [1]. Network structure, reliable routing, topology based, and communication model are the four types of protocols that are used for routing. Based on the distribution of hierarchical routing and flat nodes, the system is divided into two protocols [1, 2]. SNs (sensor nodes) conduct their detecting duties concurrently in a flat network, where all nodes have the same function. There are two types of sensors in a hierarchical network: those that have a lot of energy and those that have a low amount of energy.

Clustering is used in wireless sensor networks to build energy-efficient protocols. LEACH [1] was the first hierarchical routing protocol presented by Heintzelman et al. The first most common protocol is based on the clustering process [1]. SNs are divided into clusters to reduce latency and battery consumption in wireless sensor networks. Clustering is an effective method for organizing wireless sensor networks [1]. In a wireless sensor network, LEACH is an adaptive, self-organizing clustering technique that uses an equal amount of energy load divided among sensor nodes. A cluster head (CH) is a node that acts as a chief, whereas other nodes are known as common nodes. A CH gathers data from the common nodes and forwards it to the BS. The collection of data from numerous nodes, on the other hand, required more energy. CHs are used to assign time slots to each node and prepare them to transfer data using time-division multiplexing (TDMA). To reduce power usage and data redundancy, TDMA is used [2].

In this paper, the following contributions are made:

(1) Suggest direct communication of nodes that are near to base station, to expand the performance of root cluster

(2) Every cluster contains vice cluster head along with the cluster head which reduce the data loss

(3) The proposed approach is powerful and improved version; it reduces the energy consumption of sensor nodes and extends the WSN's lifetime

2. Literature Survey

LEACH protocol was suggested by W. Heinzelman and Balakrishnan for WSN [3]. A LEACH is an algorithm that organizes the network nodes into small clusters and chooses a CH from each cluster. At first, the node senses its destination and then transmits the pertinent message to the CH. Then, the CH transmits the gathered information to the BS. LEACH protocol's main objective is to enhance energy efficiency by employing a random integer to implement a rotation-based CH selection technique. The LEACH procedures are designed to work in many rounds. There are two phases in each round.

A unique LEACH protocol in a heterogeneous network that matched the simulated outcomes to those of the LEACH homogeneous system was introduced in [4]; they simulated the protocol across a 100×100-meter region. Sharma discovered that 10 nodes contain more energy than the other 90, extending the lifespan of the system and improving the performance of the wireless sensor network. Dynamic K value protocol (DK-LEACH) [5] proposes an optimum clustering. Within the unequal energy distribution, this strategy minimizes energy consumption. The same cluster and different cluster distances are both relevant elements in this case.

The authors looked at route cost and feasible connections between sensor nodes and cluster head of each cluster in node-ranked-LEACH (NR-LEACH) [6]. CH selection is heavily influenced by the current weight. However, it can sometimes raise network overhead. In LEACH-VA [7], according to the total energy consumed in a round, the optimum number of CHs is estimated. This method reduces intercluster communication by employing the Voronoi diagram concept, as well as ant colony optimization for efficient routing. With the exception of higher overhead, this technique outperforms existing LEACH protocols.

In [8], the authors presented BRE-LEACH, an updated LEACH protocol that improved the energy consumption cost, network life cycle, and stability period. The BRE-LEACH technique contains three factors: the first one is the distance to the BS, the second is residual energy, and the third is the multihop transmission. The fundamental factor in the cluster head selection technique is residual energy, which is used to avoid low-energy nodes serving as a cluster head since they require additional energy than regular nodes. This technique increases the life of the network. The selection of CH is based on the remaining energy. Clusters, on the other hand, do not have the same number of

nodes. In IB-LEACH protocol, to expand the energy efficiency of the system, clustering is divided into two parts: intracluster and intercluster. The results of the estimation show that using the IB-LEACH protocol extends the network lifespan. However, because of the additional computation required, the traffic load is increased to some level.

The field observation instrument, FOI-LEACH [9], is a more advanced protocol based on LEACH. By selecting the appropriate CH, this strategy prevents the premature mortality of the cluster head and extends the life of the network. To address the hotspot problem, this technique additionally focuses on the distance between the sensors and base station. However, the scalability problem is not taken into account, which makes it unsuitable for smaller sensing fields.

The routing technique for optimization is proposed by [10] on multiconstraints and multiobjective. For estimation of the quality of routing protocol, the link quality, parameter of residual energy, and traffic load are considered performance parameters. It helps in the fast delivery of packets.

SHE is the protocol of real time represented by [11]. In this traffic, packets followed different paths after the formation of clusters. QoS is acquired by aging tag.

Contributing to this is a clustering technique [12] called energy-aware QoS routing protocol. It made prominent throughput, decreases retransmission of excessive packets, improves the delivery ratio of packets, and most important for WSNs reduces end-to-end delay.

The routing protocol called bihop neighborhood information-dependent is presented in [13]. This one paradigm contains both the two-hop velocity concept and energy balancing. Its suitability in real time is shown through QoS parameters. LEACH extension called PEGASIS is presented in [14] for network lifetime improvement by decreasing the distance of transmission between sensor chain techniques modified for lifetime enhancing of the network, but it represented more enhancement than PEGASIS by placing the leader of the cluster near the base station.

DEEC and EDDEEC protocols were developed [15, 16], respectively. In DEEC, the average network energy and node probability function based on initial energy are formulated. The drawback is that it does not notice the energy of network in every round. EDDEEC represented the threshold function based on three nodes, i.e., advanced nodes, a normal node, and super node.

3. Network Model and Assumption

Two models are discussed in the proposed method, i.e., network model and energy dissipated network model used for microsensor formation, the election of CH, circulation of data to BS, and data aggregation. The second model is used for dissipation of energy that occurs due to transmission and reception of sensed data. The proposed method considers the following assumption while applying the network.

(I) After deployment, each node is nonmovable and it is identified by separate ID

(II) Node's capabilities are similar when considering communication and processing, but when talking about battery energy, it is heterogeneous

(III) The property of data aggregation is used in which multiple data is compressed into one packet

(IV) Depending on distance power, control mode is used to operate all node

(V) The nodes' initial energy is heterogeneous and nonchargeable

(VI) A communication link between nodes is symmetric, so consumption of energy of transmission of packets and rate of data from node A to B and B to A is the same

(VII) The central position is assigned to BS and it is free from memory, consumption capability, and energy constraints

(VIII) In-network area nodes are distributed on the elliptical Gaussian distribution model

By considering the effects of the three parameters, i.e., security, energy, and routing, the position of nodes is a complicated issue in the network.

The lifespan of network depends on the installation method. So, nodes that are near to the base station drain their energy of battery much faster than the one which is away from the BS. To solve this problem, a distribution function called 2D Gaussian is used to control the problem of energy hole in WSN.

For network lifespan and energy balancing, the standard deviation plays a vital role in this function. All area, i.e., M $\times$ Mm^2, is occupied by the N nodes. The distribution for this function is given below:

$$F(u, v) = \frac{1}{2\pi\sigma_u\sigma_v} \exp - \left(\frac{(u-u_o)^2}{2\sigma_u^2} + \frac{(v-v_o)^2}{2\sigma_v^2} \right). \quad (1)$$

The $(u_o v_o)$ is used to represent the positional coordinates and σ_u and σ_v represent standard deviation.

3.1. Radio Energy Model. Figure 1 shows energy model. It is up to the distance that both models, i.e., multipath fading and free space model, are included.

The following is the formula for radio energy which is included for transmitting data x (bit) from distance at the rate of bit/s.

$$E_{\mathrm{Tx}}(x, d, r) = E_{\mathrm{Tx-elec}}(x, r)+) = E_{\mathrm{Tx-amp}}(x, d, r)$$
$$= E_{\mathrm{tx-elec}} * \frac{x}{r} + \epsilon_{fs} * \frac{x}{r} * d^2 \text{ for } d < d_o,$$

$$E_{\mathrm{Tx}}(x, d, r) = E_{\mathrm{tx-elec}} * \frac{x}{r} + \epsilon_{\mathrm{mp}} * \frac{x}{r} * d^4 \text{ for } d > d_o,$$

$$E_{\mathrm{Tx}}(x, d, r) E_{\mathrm{Rx-elec}}(x, d, r) = E_{\mathrm{rx-}elec} * \frac{x}{r}. \quad (2)$$

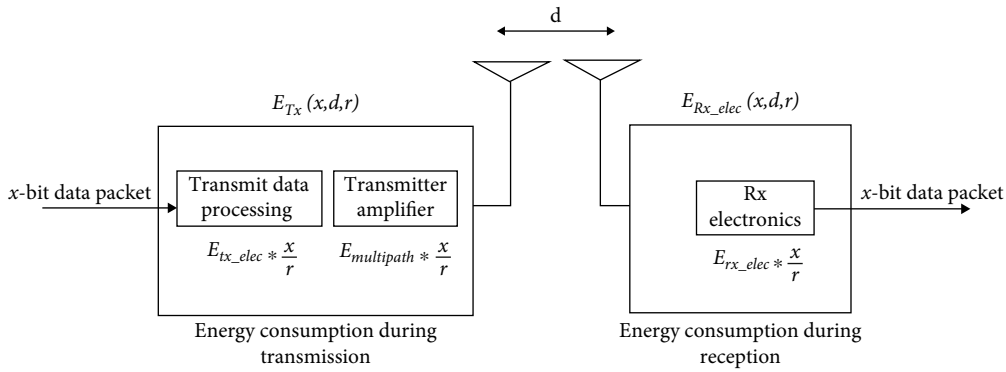


Figure 1: Radio communication model [14].

For transmission of a single packet, $E_{\mathrm{Tx}}(x, d, r)$ represent the total dissipation of energy, $E_{\mathrm{Tx-elec}}(x, r)$ represent electronic digital count, $E_{\mathrm{Tx-amp}}(x, d, r)$ represent the power amplifier energy consumption model designed for free space, $\varepsilon_{\mathrm{mp}}$ is used to represent the multipath model, $E_{\mathrm{Rx-elec}}(x, d, r)$ represent single packet reception for total dissipation of energy, and $E_{\mathrm{rx-elec}}$ represent the dissipation of energy for the receiver circuit.

4. Proposed Protocol

In this research, we present a new hybrid energy-efficient protocol with the goal of reducing energy consumption, extending network stability, increasing network lifetime, and increasing throughput. The suggested method is an improved hybrid EEE-LEACH clustering procedure with round phases for each cycle. Instead of the two stages of the LEACH algorithm, the proposed protocol comprises four phases for each round, as shown below. The steps of algorithms for different cases are given in Table 1.

4.1. First Phase. The proposed approach involves selecting CHs based on the residual energy of nodes to avoid nodes with low energy being scheduled to become CHs and to save energy. Each node chooses a random number Rn ($0 < \mathrm{Rn} < 1$) at the start of each turn, based on the working procedure of LEACH and their upgraded protocols. If the value of R is less than the threshold function defined in equation (3), this node becomes a CH in the current round. However, it reverts to a normal node (NN).

$$T(n) = \begin{cases} P - \dfrac{p}{1 - P * (\mathrm{i} \bmod (1/P))}, & n \in G, \\ 0, & \text{otherwise}, \end{cases} \tag{3}$$

where the ratio of total cluster heads to sensor nodes is denoted with P and indicates the likelihood of each node becoming the cluster head during round 0, G is the set of nodes that will not be elected as a CH in the most recent $1/p$ round, I is the current number of rounds, and mod(•) is the modulus operator. Following the selection of CHs, each CH sets a TDMA scheduled to receive data from cluster members during their assigned time intervals. They then send an announcement message to the network, which includes each CH's ID and coordinates. When NNs get these messages, they generate a distance table to CHs. The NN sends a JOIN demand to the CH with the lowest distance in its table and less than the threshold distance to determine which CH it belongs to. This CH will be the equivalent CH if this CH still has a vacant time slot in the TDMA program and the number of nodes in its cluster is less than Ncl. The NN, on the other hand, sends a second JOIN demand to the next CH with the shortest distance in its table and a distance smaller than the threshold distance and so on. According to the IBRE-LEACH method, the distance between NNs and their CHs should be less than the threshold in order to avoid multipath propagation, which consumes more space than the free space provided in Section 4.5. The Euclidean distance is determined between two devices using the coordinates (X, Y) as indicated in (equation (4)):

$$d = \sqrt{\left[(x2 - x1)^2 + (y2 - y1)^2 \right]}. \tag{4}$$

Furthermore, the suggested technique equalizes the residual energy of CHs in the network by limiting the number of nodes in each cluster. NNs that cannot join any cluster will be ignored once clusters have been created. Abandoned nodes are the name given to these nodes (ANs). These abandoned nodes have the opportunity to route their data to BS, such as NNs and CHs.

4.2. Second Phase. After the CHs and ANs have been fixed, clusters are formed, and all CHs send out an announcement message to all other CHs. Each CH's ID and location are included in this message (or AN). Following that, the proposed protocol selects a root node. This root will be a CH or AN with remaining energy more than or equal to the average current energy of all CHs and ANs and a distance to the BS that is less than or equal to the average distance of all CHs and ANs from the BS.

The root node combines its data with that received from other CHs and ANs before sending it to the BS directly. Its

Table 1: Algorithms.

Algorithm 1 for Setup Phase:
Some Notations used in algorithm:
TN: Total Numbers of nodes
CH: Cluster Head
BS: Base station
N: for every node
R: any random integer

Algorithm 1 case 1
For every N select number between 0 and 1
randomly *If* (R< T (n))
N becomes Cluster Head
N sends its Cluster Head status
Else
N becomes normal node
N receive data sent by CHs
End if
End for
For every (CH)
N selects the CH with min distance from Base Station
N will be member of that cluster
End for
For each (CH)
TDMA Schedule is constructed
End for

Algorithm 1 case 2
Some Notations used in algorithm
node[i].L
node[i].E
Selection of VCH
For node[i] in the same cluster, the node with the most energy after the cluster head is VCH.
node[i].type = 'VCH'
end of for loop

Algorithm 2 Case 1: Transmission directly to the BS (For Steady Phase)
Require: This algorithm is valid for CHs and ANs
D_{CH_BS}: The distance from CH to the BS
$D_{CH—ND}$: The distance from CH to the Next Destination (CH or AN)
$D_{CH—ROOT:}$ The distance from CH to the root
Begin
if $D_{CH\_BS} < D_{CH—ROOT}$ then
if $D_{CH\_BS} < D_{CH—ND}$ then
The CH route its data to the BS directly
end if
end if

Algorithm 2 Case 2: Transmission directly to the Root
Begin
if $D_{CH\_Root} < D_{CH—BS}$ then
if $D_{CH\_Root} < D_{CH—ND}$ then
The CH route its data to the root
end if
end if
Algorithm 2 Case 3: Transmission directly to next destination
Begin
if $D_{CH\_ND} < D_{CH—BS}$ then
if $D_{CH\_ND} < D_{CH—Root}$ then
The CH sends its data to next destination (Cluster)
end if
end if

major goal is to reduce base station overload and ensure that CHs and ANs with low energy and located distant from the base station do not interact directly with it, which wastes a lot of energy.

4.3. Third Phase. Every CH develops its routing table in this phase, which includes distances to all CHs, ANs, the root, and the BS. The same is true for ANs. Every CH and AN knows its next hop using this routing table. As a result of our method, any ANs (which previous routing protocols have abandoned) can route their information to the BS, such as CHs.

4.4. Fourth Phase. During this phase (communication phase), each CH (or AN) can use its routing table to determine the best method for sending its data to the BS, which includes distances to all CHs, ANs, the root, and the BS. The proposed protocol's architecture is depicted in Figure 2.

The workings of our proposed method are depicted in this diagram. Each CH (or AN) creates its own routing table, which includes distances between other CHs, ANs, the root, and the BS. The distances are then ordered from nearest to farthest. The proposed method then offers a set of conditions for selecting the best route for each CH and AN to reach the BS. Consider CH1, which has the closest distance to CH2, then the root, the BS, and so on.

The proposed approach compares dCH2toBS (the distance of the first element in the routing table with the BS) and dCHltoBS (distance between CH1 and the BS). In this case, dcHitoBs is less than dCH2toBs. So, CH2 will not be the next hop of CH1. It then moves on to the next item in its routing table. When it compares dRoot—ToBs (the distance between the root and the BS) to dCHitoBS, it discovers that dCHitoBs is smaller than dRoot—ToBs and the BS is the routing table's third element. As a result, the CH1 decides to send directly to the BS because it is the most efficient path.

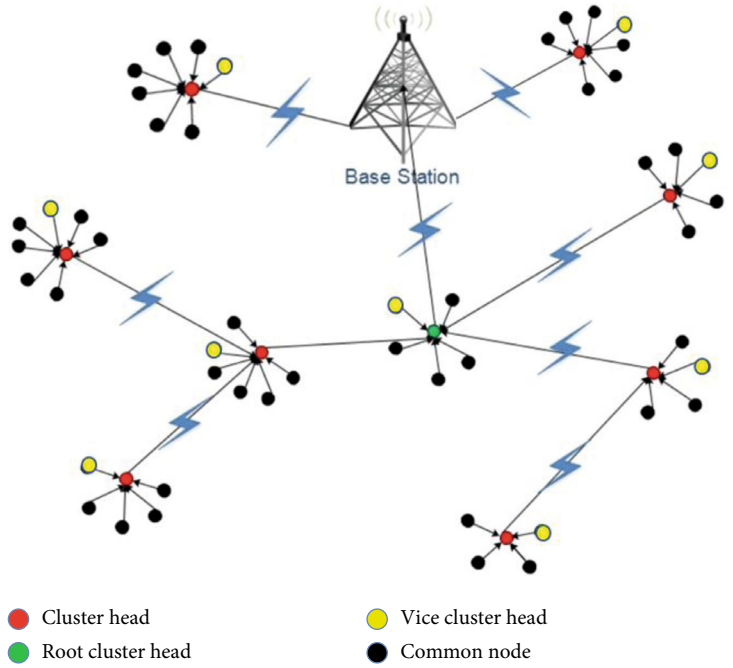


Figure 2: Proposed LEACH architecture.

4.5. Proposed Algorithm

4.6. Simulation Setup. We started by creating a WSN in MATLAB. We have set some default values for each option and initialized them. To make a network with 200 nodes, we specify $N = 200$ and Net size = 200 as the side length of the network's area. If we want to expand the network to 400 nodes, the value of L will be doubled. We must set a chance of nodes being picked as CH in any LEACH. For each round, we set $P = 0.1$ the probability of getting picked as the cluster head. In a network of 200 nodes, $P = 0.1$ suggests that 20 nodes can be CH. For each sensor node in the network, we establish the initial energy. The energy of a node at the start of the simulation is referred to as initial energy. As a result, Ei = 0.5 is assigned as the initial energy value. As a result of conducting the simulation in MATLAB, we now have the following result:

A MATLAB simulation was used to generate the results, which were averaged over 20 trials. The parameters utilized in simulations are summarized in Table 2.

Table 2: Simulation parameters.

Parameter	Value
Total deployment area	100 × 100 m
Location of BS	200, 200 (m)
Cluster head packet size	500 bytes
Total no. of nodes	200
Control packet size	25 bytes
Initial energy of each sensor	0.5 J
Data packet size	100 bytes
No. of rounds	1500

5. Results

The homogeneous network of 200 nodes, spread randomly in 200∗200, is analyzed in our Hybrid-LEACH. The BS coordinates are 150 and 150. The comparison of dead nodes over time in EEE-LEACH, LEACH, and Hybrid-LEACH protocols are illustrated in Figure 3. In comparison to other protocols, our proposed Hybrid-LEACH delivers a better performance in terms of dead nodes over time as seen in the figure. The network lifetime and total energy consumption are depicted in Figure 4. These findings indicate that the suggested technique outperforms the compared protocols in terms of network lifetime. Figure 5 shows how Hybrid-LEACH improves the stability area (number of rounds where all nodes are alive) when compared to LEACH and EEE-LEACH. Energy consumption is the second crucial statistic. Figure 6 depicts the total residual energy in the entire network. The proposed technique uses less energy than LEACH and its upgraded protocol EEE-LEACH, according to the results of this curve. Throughput is the third major statistic considered in this study. Figure 7 shows the number of packets transmitted to the BS for all three protocols. Based on these findings, it is clear that increased amount of packets is transmitted to the BS in Hybrid-LEACH than LEACH and EEE-LEACH.

6. Summary of the Simulations and Results

We tried to compare LEACH and our newly suggested Hybrid-LEACH algorithm after conducting three successive

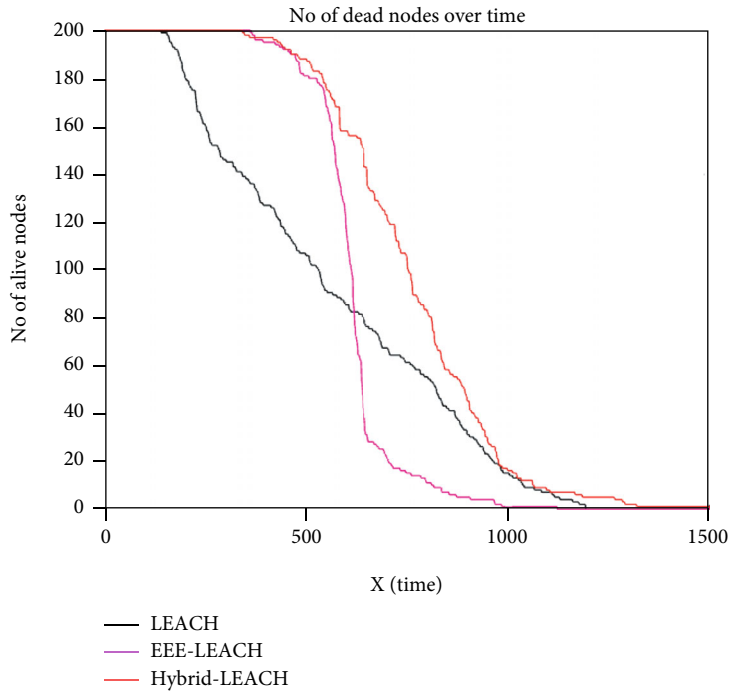


Figure 3: Comparison of number of dead nodes over time in LEACH, EEE-LEACH, and Hybrid-LEACH protocols.

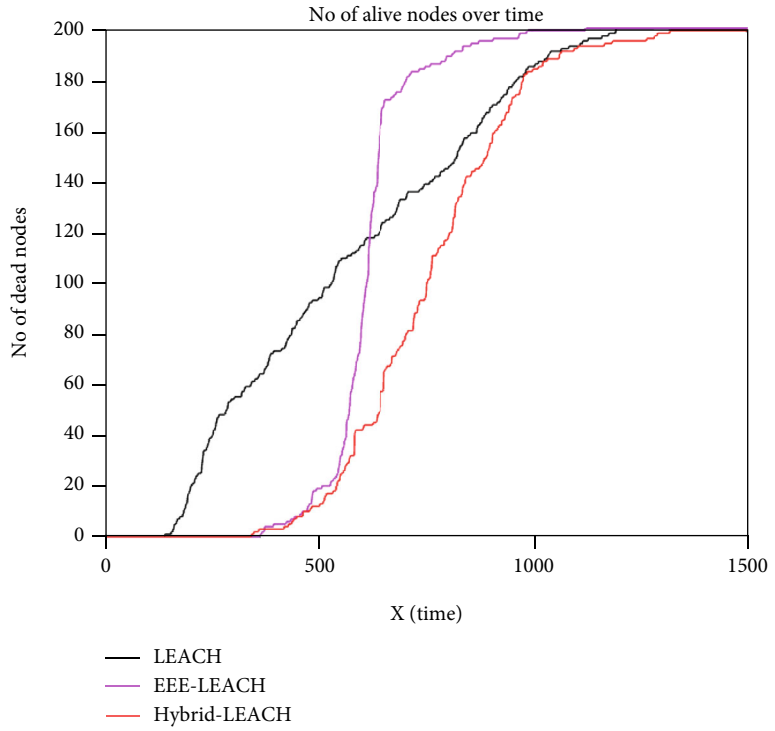


Figure 4: Comparison of number of alive nodes in EEE-LEACH and Hybrid-LEACH protocols.

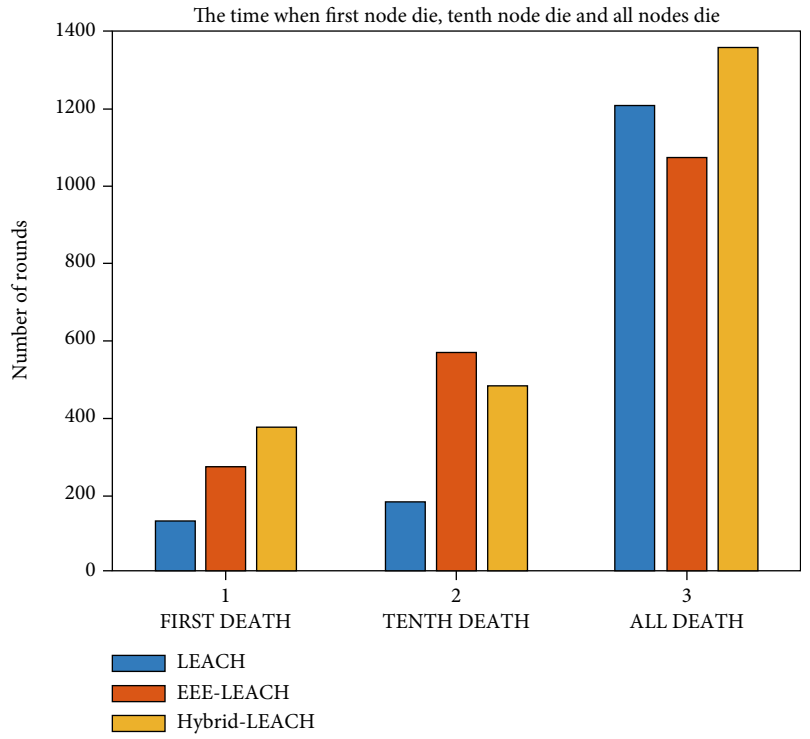


Figure 5: Comparison of the time when the nodes die per round in LEACH, EEE-LEACH, and Hybrid-LEACH protocols.

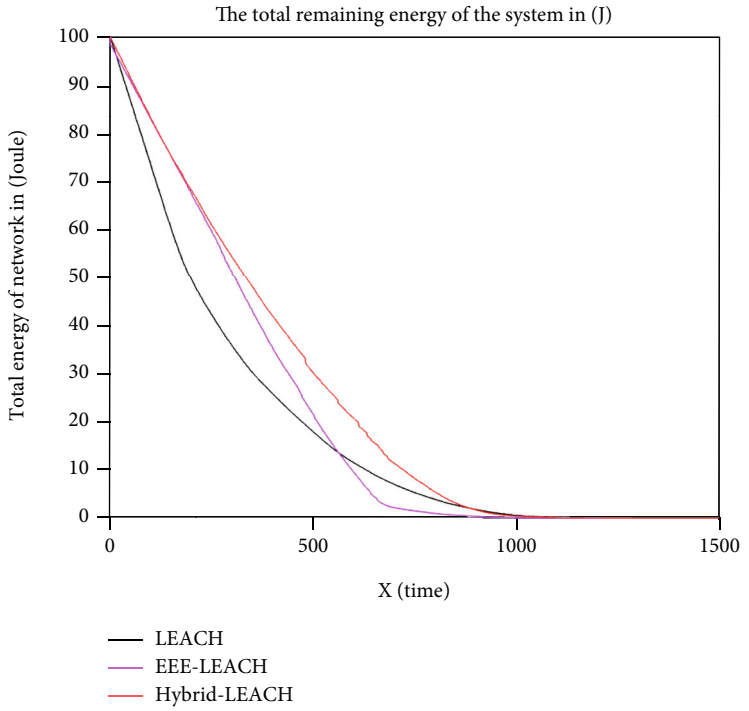


Figure 6: Comparison of total remaining energy over time in LEACH, EEE-LEACH, and Hybrid-LEACH protocols.

simulations in MATLAB with various probabilities and number of nodes. The simulation ends when practically all nodes have died, and all rounds have been completed. Following the completion of the simulation, a three-line graph displaying the simulation results emerges. The sensor nodes' lifetime is represented by one graph, while their energy

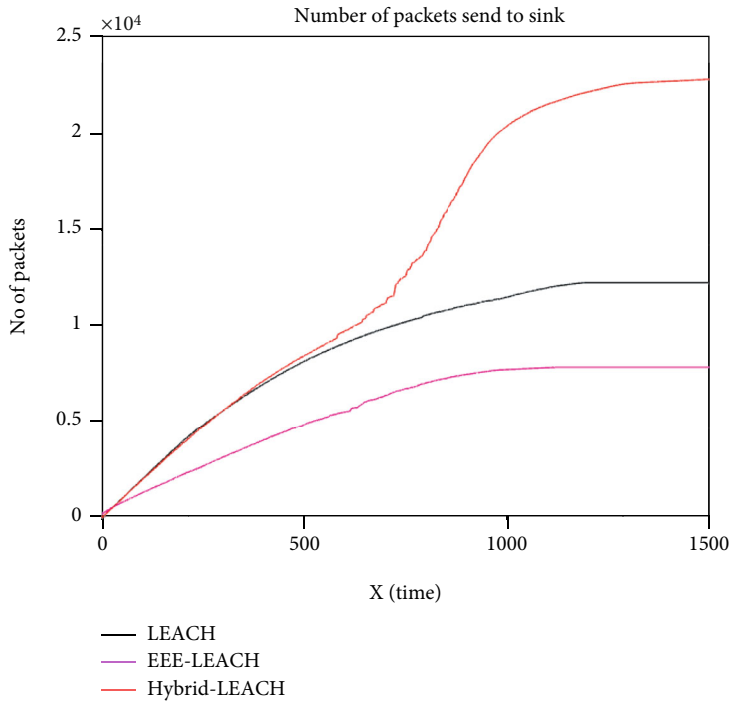


Figure 7: Comparison of number of data packets sent to the sink over time in LEACH, EEE-LEACH, and Hybrid-LEACH protocols.

dissipation is represented by another. Our suggested Hybrid-LEACH offers a superior lifetime enhancement rate and a slower energy dissipation rate than the present LEACH technique, as shown in all three simulations. The Hybrid-LEACH protocol performs better in every simulation in terms of life extension and reduced energy dissipation rate. As a result, the Hybrid-LEACH method can be considered an enhancement to the LEACH protocol.

7. Conclusion

We attempted to compare different forms of LEACH protocols, their implementation, limitations, and obstacles in this study. Many researchers have proposed numerous modified LEACH procedures. We attempted to learn about the difficulties they encountered as well as the method they employed to conduct their investigation. WSN's most used protocol is LEACH. It does, however, have several flaws. As a result, we devised a plan to address a problem with the LEACH protocol. The LEACH protocol's cluster head election mechanism has been updated, and the new altered LEACH is known as Hybrid-LEACH. We discovered that the new modified algorithm achieved our goal and performed better than the existing LEACH protocol after its successful deployment. As a result, our research's goal has been accomplished.

Data Availability

No data were used to support this study. We have conducted the simulations to evaluate the performance of the proposed protocol. However, any query about the research conducted in this paper is highly appreciated and can be asked from the principal author (Muhammad Amir Khan) upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors are thankful to the COMSATS University Islamabad for fully supporting by providing all key resources during the implementation and all afterward phases of this project.

References

[1] C. Puttamadappa and B. D. Parameshachari, "Demand side management of small scale loads in a smart grid using glowworm swarm optimization technique," *Microprocessors and Microsystems*, vol. 71, article 102886, 2019.

[2] S. Prabu, M. Lakshmanan, and V. N. Mohammed, "A multimodal authentication for biometric recognition system using intelligent hybrid fusion techniques," *Journal of medical systems*, vol. 43, no. 8, pp. 1–9, 2019.

[3] S. Shanthi, P. Nayak, and S. Dandu, "Minimization of energy consumption in wireless sensor networks by using a special mobile agent," *Soft Computing and Signal Processing*, vol. 900, pp. 359–368, 2019.

[4] H. Liwen, N. T. Nguyen, W. Tao et al., "Modeling of cloud-based digital twins for smart manufacturing with MT connect," *Procedia Manufacturing*, vol. 26, pp. 1193–1203, 2018.

[5] F. Muzafarov, M. Abdujapparova, K. Davletova, and B. Sa'dullayev, "Development of energy-efficient LEACH protocol for wireless sensor networks," in *2020 International Conference on Information Science and Communications Technologies (ICISCT)*, pp. 1–6, Tashkent, Uzbekistan, 2020.

[6] X. X. Ding, M. Ling, Z. J. Wang, and F. L. Song, "Dk-leach: an optimized cluster structure routing method based on leach in wireless sensor networks," *Wireless Personal Communications*, vol. 96, no. 4, pp. 6369–6379, 2017.

[7] S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, "LA-MHR: learning automata based multilevel heterogeneous routing for opportunistic shared spectrum access to enhance lifetime of WSN," *IEEE Systems Journal*, vol. 13, no. 1, pp. 313–323, 2019.

[8] Z. Hong, L. Yu, and G.-J. Zhang, "Efficient and dynamic clustering scheme for heterogeneous multi-level wireless sensor networks," *Acta Automatica Sinica*, vol. 39, no. 4, pp. 454–460, 2013.

[9] Z. Hong, R. Wang, and X. Li, "A clustering-tree topology control based on the energy forecast for heterogeneous wireless sensor networks," *IEEE/CAA Journal of Automatica Sinica*, vol. 3, no. 1, pp. 68–77, 2016.

[10] A. Moussaoui and A. Boukeream, "A survey of routing protocols based on link-stability in mobile ad hoc networks," *Journal of Network and Computer Applications*, vol. 47, no. 1, pp. 1–10, 2015.

[11] T. Yang, T. Cui, C.-Y. Xu, P. Ciais, and P. Shi, "Development of a new IHA method for impact assessment of climate change on flow regime," *Global and Planetary Change*, vol. 156, no. 9, pp. 68–79, 2017.

[12] X. Wang, T. Yang, M. Wortmann et al., "Analysis of multidimensional hydrological alterations under climate change for four major river basins in different climate zones," *Climatic Change*, vol. 141, no. 3, pp. 483–498, 2017.

[13] T. He, J. A. Stanko, T. F. Abdelzaher, and C. Lu, "A spatiotemporal communication protocol for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 16, no. 10, pp. 995–1006, 2005.

[14] P. Singh and R. Singh, "Energy-efficient QoS-aware intelligent hybrid clustered routing protocol for wireless sensor networks," *Journal of Sensors*, vol. 2019, Article ID 8691878, 12 pages, 2019.

[15] D.-R. Chen, "An energy-efficient QoS routing for wireless sensor networks using self- stabilizing algorithm," *Ad Hoc Networks*, vol. 37, pp. 240–255, 2016.

[16] M. Faheem and V. C. Gungor, "Energy efficient and QoS aware routing protocol for wireless sensor network- based smart grid applications in the context of industry 4.0," *Applied Soft Computing*, vol. 68, no. 7, pp. 910–922, 2018.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8006751, 10 pages
https://doi.org/10.1155/2022/8006751

Research Article

Energy-Efficient Routing Protocol for Next-Generation Application in the Internet of Things and Wireless Sensor Networks

Roopali Dogra,[1] Shalli Rani,[1] Himanshi Babbar,[1] and Daniel Krah[2]

[1]*Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India*
[2]*Tamale Technical University, Ghana*

Correspondence should be addressed to Daniel Krah; dkrah@tatu.edu.gh

Received 17 December 2021; Revised 10 February 2022; Accepted 25 February 2022; Published 22 March 2022

Academic Editor: Muhammad Asghar Khan

Among the key challenges with wireless sensor networks (WSNs) is that most sensor nodes are fueled by energy-constrained batteries, which has a significant impact on the network's efficiency, reliability, and durability. As a result, many clustering approaches have been developed to enhance the energy efficiency of WSNs. Meanwhile, fifth-generation (5G) transmissions necessitate the usage of multiple-input multiple-output (MIMO) multiple antennas in numerous Internet of Things (IoT) applications to furnish increased capacity in a multipath spectrum environment. Instead of a single senor that can facilitate better load balancing utilization, we believe to balance the energy utilization per unit area. The devices in IoT are submerged with various transmission interfaces known as MIMO in 5G networks. With MIMO being more commonly accessible on IoT devices, an effective clustering approach for rapidly evolving IoT systems is both lacking and urgently needed to support a variety of user scenarios. In this paper, we proposed the intelligent MIMO-based 5G balanced energy-efficient protocol which focuses to achieve Quality of Experience (QoE) for transmitting in clusters for IoT networks. The proposed protocol enhances the utilization of energy and lifetime of the network in which it shows 30% less energy utilized in comparison to the existing protocols.

1. Next-Generation Networks (5G): Clustering for IoT-Based Systems

Many services, programs, sensor-embedded digital equipment, and network protocols have been built, and it is still being constructed as the Internet of Things evolved rapidly. The IoT enables genuinely existing things to see, listen, understand, and execute a crucial task by connecting and engaging with each other and sharing essential knowledge while making a decision and doing critical activities. Wireless sensor networks, that provide a continuous layer for the IoT, are critical for 5G telecommunications. A wireless sensor network is composed of a collection of sensor nodes that detect and transfer data to the sink. Every round's sink (or base station) is the endpoint of transmitting data. The primary problems of IoT-based WSNs are increasing the lifetime of the network and reducing energy consumption.

Therefore, one of the primary aspects of 5G wireless communication is massive machine-type communication. Because the current cellular network has wider coverage, a substantial number of deployed equipment, a robust user service management system, etc., Cisco believes that the 3rd Generation Partner Project (3GPP) produced networks would support 80 percent of a total of IoT device connections. The major approach in the upcoming wireless network to conform to the IoT device service well is to improve the present cellular network for service attributes [1]. As a result, the 3GPP organization has already been focusing on IoT network standardization since Release-8 and is much more likely to adopt optimization strategies that have minimal impact on existing networks to facilitate cellular networks to accommodate huge IoT device communication. The transmission data is little, the transmission is rapid, and the battery is tough to replicate with a high number of IoT devices application services

concentrated on the uplink. The key reason for the minimal resource utilization of limited data for IoT devices is collided caused by random access whenever large-scale devices request network connection [2]. The present network has two major flaws that will hinder future widespread IoT access.

(i) Massive IoT device access will occur in a massive number of collisions, particularly with random access congestion, lowering the access success probability and causing a network overload

(ii) IoT devices communicate modest quantities of data, and establishing a data connection with the base station (BS) in Long-Term Evolution (LTE-M) requires more than 25 handshakes, leading to high signaling latency and reduced resource utilization

1.1. IoT-Based WSN's Clustering in 5G. As can be shown, 5G could provide a viable and dependable backhaul infrastructure for a variety of IoT systems. It makes sense to base upcoming protocols for IoT networks on that infrastructure, with QoE monitoring as one of the design principles.

This is becoming the norm because cellular networks with backhaul could provide full connectivity. The communications network usually has three layers, as shown in Figure 1. The devices and sensors in the field make up layer 1 [3]. Telecom companies utilize layer 2 outside of the field, usually in the form of small and medium-sized cells, to assist 3GPP standard communication. Layer 3 is the evolving packet core network (core network), which collects all of the data and information. Layers 2 and 3 are combined to form the backhaul network architecture. In wireless communication, layer 1 is considered as the last hop. All three tiers can benefit from 3GPP communication. Layers 1 and 2 are the only layers where machine-to-machine (M2M) communication is possible. The standard architecture for 3GPP included IoT backhaul is depicted in Figure 1(a). The 3GPP organization, telecom providers, and academia are now working to make 5G a reality by the end of 2021. 5G, as an M2M enabler, offers capabilities like 2–20 Gb/s speed, 0.1-ms latency, and 100 percent coverage and dependability, to support and provide strong QoE for a wide range of applications and utilizations.

In 3GPP for WSN-IoT clustering, the methods used for clustering are essential and can be fruitful for many challenges which can be the managing transmission of data for the numerous sensor nodes, efficiency of energy, decentralized processing, hierarchy in management, etc. [4]. Therefore, to overcome the above challenges or issues, we have applied the clustering methods in WSN-IoT as depicted in Figure 1(b). Clusters are generated at layer 1, and one cluster head (CH) is chosen for each cluster. Each cluster's CH will continue to be responsible for data collection and confusion. First, with clustering in the field, M2M transmission is limited to layer 1. Cross-layer transmission is minimized or avoided, which preserves a huge amount of energy on the devices. Second, the clustering design is advantageous for local data collection and processing. The CH can filter out redundant information, preventing the 3GPP backhaul network from becoming overburdened. Finally, the layer 1 cluster design could be further stratified depending on the network's size, device types, types of application, connectivity, and other factors.

1.2. Main Contributions. To solve the above challenges:

(a) We have proposed the Intelligent Multiple Input Multiple Output-5G based Balanced Energy Efficient (IMIMO-5G based BEE) protocol for intra and interclustering in IoT networking systems

(b) In this protocol, the algorithms are framed for choosing the CH, forming the intra and interclustering for the multihop routing. We have chosen two CH's for the distribution of sensors and energy utilization, and this will increase the lifetime of the network, improve the area of the network by the use of prolonged distance for intercluster transmission

(c) IMIMO-5G-based BEE will firstly allocate the network vertically into intra and interclusters to divide the energy utilization across CHs. The sensors will transmit the data to the CHs and then the data transmitted by the CHs will be sent to the BS (BS)

(d) The clusters that are nearer to the BS have a small radius and by using the clustering and multihop topology, and the nodes interact with one another by transmitting the data from the source to destination to minimize the response time by making the use of Euclidian distance

1.3. Paper Organization. The rest of the paper is organized as Section 2 displays the table showing the literature work of existing authors; Section 3 shows the novelty design of the proposed approach; Section 4 discusses the results and discussion of results which explains the performance evaluation of existing vs. proposed approach; Section 5 concludes the paper.

2. Related Research

Various clustering and nonclustering algorithms are designed to improve the performance of energy consumption, reduce the delay, and increase the lifetime of the network. Below Table 1 displays the existing clustering routing protocol techniques applied by multiple authors.

3. Novel Design

3.1. Clustering Process. The feasible routing for clustering utilizes the k-means algorithm for the formation of clusters, and CHs are chosen based on Euclidean distance and energy of nodes. The attribute value on which the node is authorized to send data to the CH is the rigid threshold communicated by the CH to the appropriate cluster members [13]. When one-third of the nodes have died, and the surviving nodes' leftover energy is inadequate to establish a cluster, the nodes employ the greedy strategy to create a cluster-like multihop routing till the BS is attained. In this phase of networking, n nodes are taken as CHs. In the first round, the leftover node determines the nearest CH using the Euclidean distance, generating n-clusters. The center of each cluster is

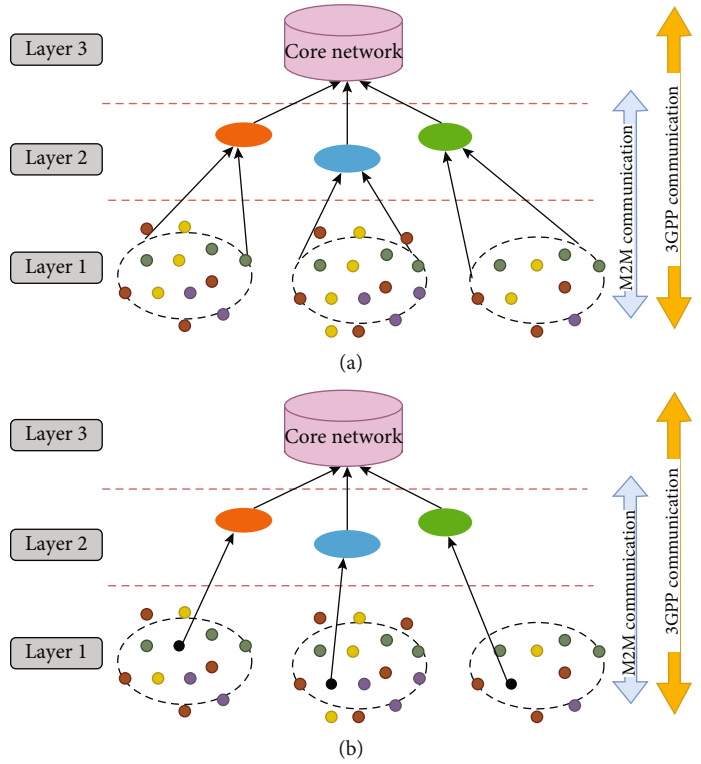


Figure 1: (a) Unclustered WSN-based IoT backhaul. (b) Clustered WSN-based IoT backhaul.

computed in subsequent rounds. The center of m^{th} node, D_j is represented as

$$Dj = \left(\frac{1}{|Q|} \sum_{m \in Q} aj, \frac{1}{|Q|} \sum_{m \in Q} bj \right), \tag{1}$$

where Q denotes the member of the cluster, and a, b denotes the coordinates of the nodes. For the network's gathering of CHs, the algorithm requires not only the distance between the nodes but also their energy. The leftover energy of the nodes is represented by X_j. As a result, the maximal leftover energy and the shortest distance between nodes are used to choose CHs.

$$\text{CH}_{\text{choose}} = \text{maximum}_j \{ \text{minimum}_j \{ g(D_j, X_j) \} \}. \tag{2}$$

A cluster sample is used, with a CH selected at random and a centroid generated to use the centroid formula. At the cluster's core, the centroid is a virtualized node. The preliminary CH is chosen as the node closest to the centroid. Each node is assigned an ID based on its distance from the centroid [14]. The IDs of nodes nearer to the centroid are smaller than those of nodes further away. If the energy of the node containing the next ID number is larger than the threshold, it is selected as the CH. If the value falls below the threshold, the existing CH transfers the cluster member's energy to the BS before terminating the session. BS examines each node to select CH depending on the energy of the nodes. If none of the nodes exceed the threshold's energy, the system creates a data-forwarding loop. The energy of the threshold is computed as

$$X_{ET} = \nu X_{le} \left(\frac{T}{C} - 1 \right) + \nu X_{AD} \left(\frac{T}{C} \right) + \nu X_{le} + \nu \varepsilon_{fs} h^2, \tag{3}$$

where C represents the clusters formed in the area of sensors, as per the time allocated by the CH, the nodes that are nearer to the area will be transmitting the data to the particular CHs.

3.2. Single-Hop and Multihop Topology. WSN might be homogenous or heterogeneous. For most real-time scenarios, a heterogeneous network is preferable to extend the lifespan of the network. Furthermore, there are two kinds of data transmission networks. There are two types of networks: single-hop and multihop.

Single-hop topology: if the cluster-head is one hop distant from the sensor network in clusters, the network is said to be single-hop. It is simple for the cluster head to gather data and transfer it to the base station solely via other cluster heads in single-hop networks. In those other words, the cluster-head performs the time-consuming validation.

Multihop topology: if numerous hops are required to transport data to the cluster-head, the network is said to have been multihop. The operation of obtaining and integrating data for a sensor node in multihop networks is especially costly if next incoming node is not a cluster-head. The gathered information must be authenticated by the sensor node. Signature schemes can be used to offer authenticity.

Table 1: Existing literature survey of clustering routing protocols.

Year/ref	Author name	Technique used	Tools	Parameters	Advantages	Limitations
2014/ [5]	S. Zhang, X. Xu, Y. Wu and L. Lu	MAC mechanism for user-centric scheduling	MATLAB	Delay, reliability	Energy-efficient reduced latency and highly reliable networks	Complexity issues in implementation.
2018/ [6]	M. Elappila, S. Chinara, D. Parhi	Survivable path routing	Network Simulator-2.35	Throughput, end-to-end delay, packet delivery ratio, and remaining energy	Minimizes the network congestion, high packet reception rate decreased end-to-end delay	Mac layer designs with transmission power control schemes
2018/[7]	S. Fu, L. Zhao, Z. Su, X. Jian	Unmanned aerial vehicles (UAV) based relay in WSN	MATLAB-2013b	Power consumption	Maximizes the system performance, decrease the transmitting power	Flightpath selection algorithm for UAV to achieve the best path for data collection
2019/[8]	Y. Zhao, K. Liu, X. Xu, L. Huang	Distributed dynamic cluster head selection and *k*-means	MATLAB	Traffic distribution, throughput, energy consumption	Decreases energy efficiency, uniform density	A large number of devices
2019/[9]	S. Nejakar, P. Benakop	Energy management technique in reactive routing protocol	NSG-2 software	Throughput, packet delivery factor	Improves the network lifetime, increased throughput, reducing energy efficiency	The burden of high power utilization
2019/[10]	T. Behera, S. Mohapatra, M. Khan, A. Gandomi	Efficient cluster head selection scheme	MATLAB	Throughput, average residual energy, number of dead nodes	The optimal number of cluster heads in the network enhances the network lifetime	Realistic scenarios for a WSN-based IoT
2020/[11]	Seyyeddabbasi, F. Kiani	Routing protocol based on ant colony optimization	MATLAB	Energy consumption, network lifetime, remaining energy, buffer size	Finds the optimal path, real-time transfer of data on a large scale of WSN and decentralized IoT	Designed for the generation and analysis of big data
2021/[12]	C. Jothikuamar, V. Deeban, S. Singh	Optimal cluster-based routing and *k*-means	NSG-2 software	Energy dissipation, packet delivery ratio, end-to-end delay	Energy distribution, maximum transmission, prolonged network lifespan	Security mechanism in the implementation

Furthermore, suggested a technique that, at this time, can be deemed the most effective and reliable. The use of these techniques in sensor networks is still a work in progress.

3.3. Energy Model. To constantly monitor the surroundings, we consider a wireless network of S number of IoT smart sensors that can be deployed evenly throughout $N * N$ square space. The associated set of sensor nodes, let us say that l_a is the a^{th} sensor, then, the sensor nodes are represented by $L = \{l_1, l_2, l_3, \cdots \cdots .., \ln\}^{|L|=S} n = 1$.

The presumptions made on the IMIMO-5G-based BEE protocol are explained as

(a) IMIMO-5G is supported by all the sensor nodes

(b) Less amount of data is sent by the sensor nodes and a large amount of data is sent by the CH's

(c) Limited energy

(d) A GPS-capable gadget is not offered with all sensor nodes (i.e., they are assumed a location-unaware)

(e) To develop a decentralized clustering technique that not only extends network lifetime but also ensures network coverage

(f) Based on the length of the receiver, the nodes can adjust the transmit power level

(g) The nodes are expected to be in a fixed position

(h) Every sensor node has different abilities (communication, processing, and battery)

(i) On the access network functionalities, every sensor has its preferences

The wireless system disperses energy to enable the transmitter and amplifier of the transmitter in the case of network transmission and receiving [15]. Furthermore, the wireless

system generates energy to power the receiver circuit. The free space and multipath fading model for the loss of power is p^2 and p^4, respectively. To energize the transmitter, the energy loss is proportional to the distance between both the transmitting and receiving ends. The utilization of power the m-bit message for the distance p is evaluated in equations (4) and (7):

On the transmitting end:

$$A_{TE}(m,p) = A_{TE-elec}(m) + A_{TE-amp}(m,p), \tag{4}$$

$$\text{If } p < p0 \text{ then } mA_{elec} + A\epsilon_{fs}p^2, \tag{5}$$

$$\text{Otherwise, } mA_{elec} + A\epsilon_{bx}p^4. \tag{6}$$

On the receiving end:

$$A_{RE} = A_{RE-elec}(m) = mA_{elec}. \tag{7}$$

3.4. Intelligent MIMO 5G-Based BEE. In the IMIMO-based 5G is required to utilize the latest clustering algorithm through which the IMIMO 5G-based BEE is framed. We presume that almost all IoT devices in the network are MIMO-enabled. When a node is set to CH, MIMO is enabled, allowing it to acquire data from multiple sources via multiple transmission paths [16]. The CHs then will reduce the acquired data and return it directly to the BS. Except for CHs, every sensing node sends a limited amount of data or a video stream (the terminology "Data" defines the limited amount of traffic, including such temperature or humility data, and "Video" defines the massive amount of traffic requiring large bandwidth of the network, such as a video stream). For transmission using the IMIMO-based BEE algorithm, a sensing node will only choose one transmission interface and a CH.

The IMIMO 5G-based BEE comprises of three phases: (a) choosing the CH's, (b) construction of hybrid cluster, (c) collection of data and transmitting, (d) minimizing the consumption of power, (e) improving the Quality of Experience (QoE), and (f) choosing the transmission interfaces. The design of the proposed protocol is shown below. As per the design showcased, the ovals of variable diameter present the unequal architecture of clusters with two different types of transmission topologies, i.e., single-hop and multihop. Besides this, the suboptimal multihop routing paradigm is represented by the routes connecting the CH's. The benefits of the proposed protocol are

(a) It can balance the load

(b) Less overhead for the transmission of data

(c) Fault tolerance is supported

3.4.1. Choosing the CH's. The BS sends a "WELCOME" message to every sensor node in the network domain when the power level reaches a particular threshold. The incoming signal intensity aids each node in calculating its relative distance to the base station (BS), resulting in a combination of clusters of varying sizes [17]. Nodes would quickly calculate their competition radius (CR) after obtaining such a message and submit a report to the BS with anticipated actual remaining energy, revised CR, and the node's ID. In our presented approach MIMO-based 5G, a node's eligibility to be the CH has decided solely if it has more remaining energy than the nodes within its radius. To create unequally sized hybrid clusters, each node must choose its CR. Nodes with more residual energy in MIMO-based 5G will perform larger tasks. As a result, clusters that are farther away from the BS and have more remaining energy employ single-hop topology and have more nodes than clusters closer to the BS that use multihop topology. As the distance between the sensor node and the BS grows, a sensor node with more residual energy must supplement its CR. On the one side, nodes with less residual energy must have a lower CR to avoid dying prematurely. The node CR is evaluated and presented as

$$\text{CR} = \left[\frac{1-\omega\,(p\ \max - p(la, \text{BS})}{p\ \max - p\ \min} - \gamma\left(1 - \frac{A_{\text{remaining}}}{A_{\max}}\right)\right] C_R{}^0, \tag{8}$$

where $p(l_a, \text{BS})$ indicates the distance between l_a, i.e., sensor nodes and BS; ω and γ are the weight of the factors; $C_R{}^0$ shows the highest value of CR; $A_{\text{remaining}}$ is the node's remaining energy; $A_{\max}$ represents the primary node's energy that is same for every node; $p_{\max}$ and $p_{\min}$ are the maximum and minimum distance between the BS and the sensor nodes.

Therefore, once the push notification is received on the BS from the sensors; then, the CH will be selected from among candidate nodes. Later, the matrix is created by BS and then the notification is transmitted to all the sensors on the network. The matrix is represented as

$$\begin{bmatrix} p_{11}^k \cdots \cdots \cdots \cdots \cdots p_{1n}^k \\ \qquad\qquad p_{ab}^k \qquad\qquad \\ p_{n1}^k \cdots \cdots \cdots \cdots \cdots p_{nn}^k \end{bmatrix}. \tag{9}$$

The list of nodes associated with a specific cluster k, as well as the distance between nodes and the ID of CH. In the above matrix, $p^k{}_{ab}$ indicates the distance between node a and node b; k represents the ID of CH. Acquiring the matrix enables each sensor to simply and correctly determine their specific CH as well as the distance to other sensors; as a result, the transmission power can be adjusted following the obtained distance to improve the energy efficiency.

3.4.2. Construction of Hybrid Cluster. The cluster chain creation or network topology structure is influenced by the BS position. Furthermore, it has an impact on the nodes' entire energy utilization. This will have an impact on the network's effectiveness and productivity. To address the abovementioned issues, a multihop construction technique is presented [18]. This approach enables the multihop topology to accommodate the BS's various locations. To avoid aberrant cluster multihop topology, MIMO-based 5G for hybrid clustering uses a projection method to build the chain. Every node in

every cluster project its displacement vector, and all nodes in each cluster are arranged by the vector's primary value.

The value for the principal vector is represented as

If $x_i = 0$, then, PV = $(x_T, 0)$.

If $y_i = 0$, then, PV = $(0, y_T)$.

Else

$$\left(-1, \frac{x_T}{y_T}\right). \tag{10}$$

In which x_T, y_T signify the location of the middle point of the network domain, and x_i, y_i are the x and y notations for else vector are indicated as i which is highlighted in equation (11) and is therefore used to make the connection with the middle point (T) and BS; x_j and y_j show the BS location.

$$I = \left(x_j - x_T, y_j - y_T\right). \tag{11}$$

The procedure for the construction of hybrid clustering is as given below in Figure 2.

When the node projection computation is complete, the BS creates a matrix and sends it to each sensor node. Owing to the increasing magnitude of the projection range, the matrix contains ordered sensor nodes on every cluster. The sorted projection value received allows nodes in each cluster to construct a multihop architecture. Below Figure 3 explains the projection and creation for multihop topology. In cluster domain 3, the sensor nodes vector is l_4 which is evaluated by the BS and it follows a multihop topology. The orange marked line in cluster domain 2 shows the projection value of the sensor node l_4 onto a.

3.4.3. Designing the IMIMO 5G-Based BEE Procedure. Presently, IMIMO-based BEE is built with QoE as the top priority task. However, it will make every effort to cut electricity use. If a node wants to send temperature information back to the BS, for illustration, it can presently interact with one CH using Zigbee and then another CH located further away via Direct-WiFi. Because the throughput values for Zigbee and Direct-WiFi are both sufficient for temperature readings, using Zigbee for transmission can save a lot of energy. If, on either hand, the node needs to send a video stream directly to the BS, and both Direct-WiFi and Zigbee are now accessible, Direct-WiFi will be preferred over Zigbee owing to QoE considerations, even though it consumes more energy. The available transmission interfaces will be classified by their desire. The procedure or algorithm for the classification is as below. If there is a need to transmit the simple data then the transmission interfaces are permitted and in the case of the video stream transmission then only the interfaces with ETI $> x^{ar}$ are permitted. In which ETI signifies the data rate transmitted for the y^{th} network access interface (NAI) and x^{ar} signifies the need for data rate from the application running on node x. Later, the desired interfaces can be classified by dividing the square of the energy utilization.

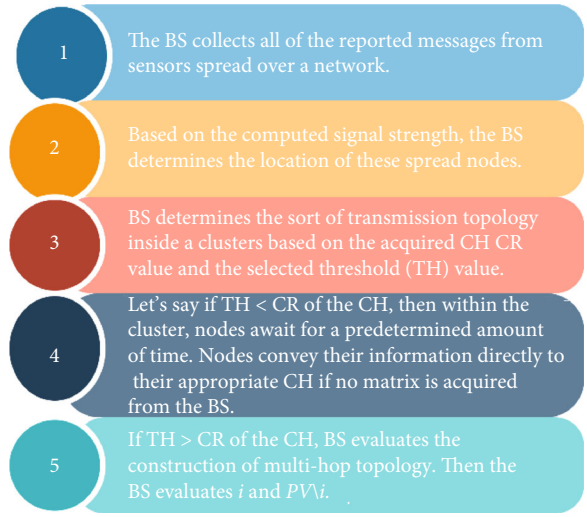


Figure 2: Procedure for the construction of hybrid clustering.

$$\text{Classification}_y = \frac{\left(\text{ETI}_y^{\,r}\right)}{\left(\text{ETI}_y^{\,e}\right)2}. \tag{12}$$

In this, $\text{ETI}_y^{\,e}$ over one unit of the distance transmitted which defines the energy utilized for ETI_y and the classification for interface ETI_y is classification_y.

The following is the QoE for transmission among both node x (Table 2 and link CH via network interface ETI_y:

(i) If $\text{QoE}_{g,h} = 0$, then, by the use of ETI_y the node x cannot connect with CH_h

(ii) If $\text{QoE}_{g,h} ! = 0$, then, $\text{classification}_y/\text{distance}_{x,h}$

In which $\text{distance}_{x,h}$ means the distance between node x and CH_h. We must first normalize the properties of the data transmission interfaces in the ability to execute this method. For illustration, the data rate will be categorized as low (value = 1) or high (value = 2). High (value = 3), medium (value = 2), or low (value = 1) energy utilization will be assessed. In 5G communication, any accessible network connecting interface can be included in this data normalization list.

3.4.4. Algorithm for IMIMO 5G-Based BEE. BEE based on IMIMO 5G presents a CH selection for intracluster transmission by responding to MIMO characteristics. Each sensor will also have a choice for network access interfaces based on its transmission specifications and capabilities. To begin, a node must satisfy its network duties and roles. If it is designed to send video, it must use a high-bandwidth interface [19]. If it is meant to transfer data, on either hand, it may offer a wider choice of network interface options. Furthermore, in comparison to BEE, the nodes should lessen energy utilization and hence increase coverage sensitive longevity yet further. As a result, while QoE is ensured, limited transmission interfaces should indeed be preferred. However, three factors should be considered before the nodes make the final decision: (1) application requirements on the network. (2) Transmission range

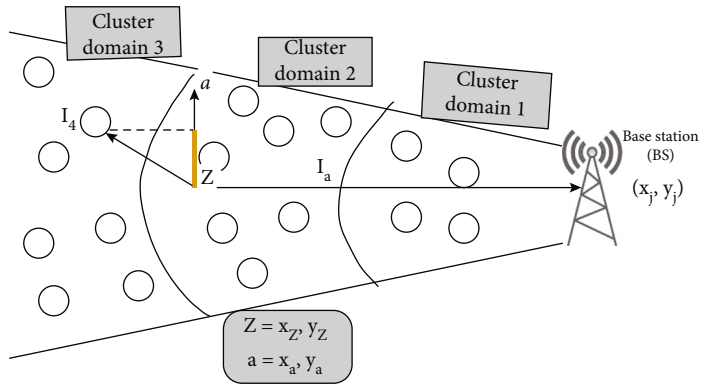


Figure 3: Projection and creation of multihop topology.

Table 2: Transmission interface for node x.

Interface for transmission	CH1	CH2	CH3	…….	CHq
ETI_1	$QoE_{1,1}$	$QoE_{1,2}$	$QoE_{1,3}$	……	$QoE_{1,q}$
ETI_2	$QoE_{2,1}$	$QoE_{2,2}$	$QoE_{2,3}$	……	$QoE_{2,q}$
ETI_3	$QoE_{3,1}$	$QoE_{3,2}$	$QoE_{3,3}$	……	$QoE_{3,q}$
…….	……..	……	……..	……	……..
ETI_4	QoE_z	$QoEz_{,2}$	$QoE_{z,3}$	……	$QoE_{z,q}$

of the access interface. (3) Distance between the nodes and CHs. The node itself can have its preference on the network interfaces even only concerning its characteristics. In this case, we refer to this scenario as a self-concerned approach. However, to select a suitable CH, the context of the CHs also should be considered. For example, considering its interest, a node prefers to use Zigbee to transmit data. However, in its Zigbee communication range, no CHs are available. Therefore, this node has to select the second choice for interfaces, which has a longer communication range. In another case, this node finds a CH in its Zigbee communication range.

4. Simulation Results

The framed approach and the existing algorithms will perform the computations in NS-3 simulator. In this, CR and energy utilization are the main factors. As compared to the existing algorithms, to optimize energy utilization among cluster heads and eliminate hotspot problems created by overloading cluster heads nearer to the BS, our proposed approach divides the network into hierarchical unequal clusters. It utilizes the multihop topology for intra and interclustering transmission and contributes to increasing the lifetime of the network, improving the robustness in the wireless network topology and efficiently balancing the load. Due to the expansion of the network, the size of the network is enlarged. As a result, the suggested energy-efficient routing protocol would work as well as it does when the network expands. The proposed approach should be capable of supporting the flexibility of the wireless topology of the network for this objective.

According to the factors stated above, it is easier to justify the compute the results. This domain is simulated in which the sensing domain of the sensor nodes is distributed equally, and the BS is located outside the WSNs. The duration taken for each sensor node is taken as 35 bytes to the BS. The parameters used in the simulations are recorded as an average of 50 runs for each input of simulations. The coverage for the network is 0-200 m, location of BS is (200, 350) m, several cluster nodes are 200, preliminary energy utilized is 2 Joule, the size of packet broadcasted is 35 bytes, distance between the nodes and CH is 55 m, and the interface used is Zigbee, WiFi, etc. Power utilization is usually the only statistic used when analyzing a clustering algorithm, to the detriment of other factors such as internet connectivity. Instead of counting nodes, coverage sensitivity lifespan has been suggested as a mechanism to assess the lifetime of the network. The dispersion and detection range of the sensors influence network coverage. In the case of network coverage, various sensors in the network are much more significant than the others. Sensors that do not have a substantial effect on the system coverage are permitted to expire earlier than others.

4.1. Iterations of Clustering and Dispersion of CHs. The algorithm overhead is determined or influenced by the number of iterations in the clustering process. Minimizing the number of iterations in every round can lessen the delay in clustering and the number of packets broadcasted. In this Figure 4, the correlation among CR^0 and the number of CHs when the ω and γ are the two different values. If ω and γ are assigned the value to 1 each. Having the value of ω as 0 and γ as 0 produces the minimum number of CHs to increase the CR. With the increase in CHs, the minimization in CR the values of ω and γ reaches 1. In our proposed approach, the value for ω and γ is 1 for each, and CR is given the value of 60. In Figure 5, the battery life is dependent on the total number of nodes in the network. The simulations are executed until and unless the first CH utilizes its battery.

Let us assume, there are 1000 nodes of the entire population, and the application of the approach proposed utilizes and translates into the average 51 yearly link charges for the

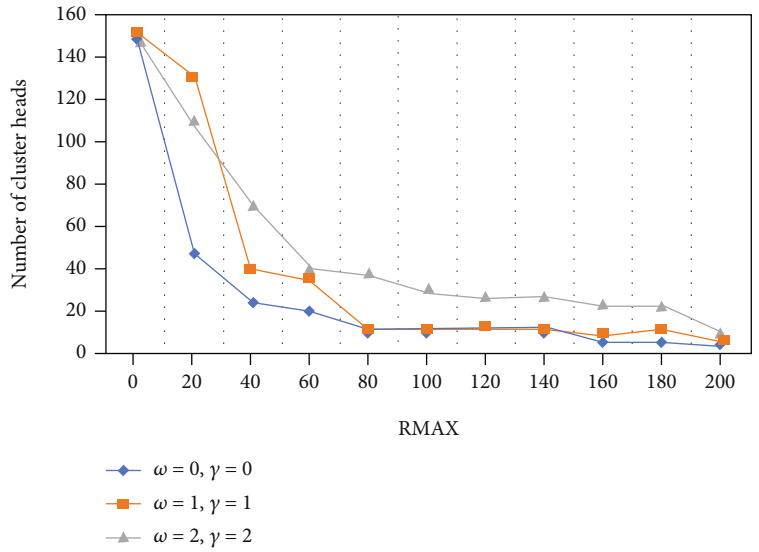


Figure 4: Number of CH's network.

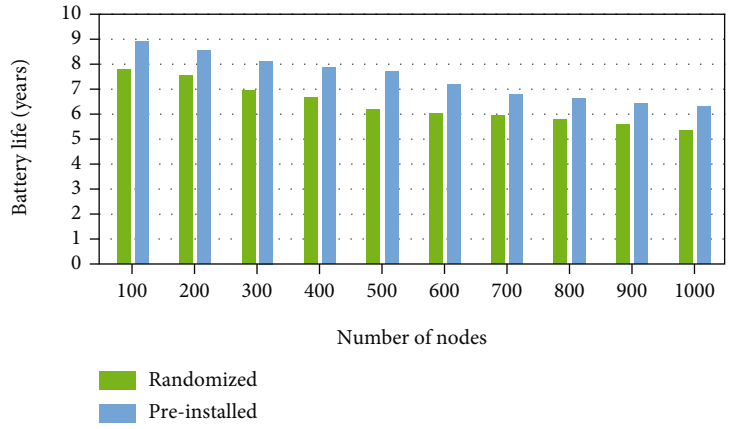


Figure 5: Number of nodes vs. battery life.

Link1 CH and preinstalled setup and 110 yearly charges for the initialized randomized setup. It has been observed that the randomized setup configuration generates a wastage of energy which says that in approximately 91% of the cases, the proposed approach adopts the improvement in the life of the battery.

4.2. Network Area. In both BEE and HEED, the cluster radius is fixed to 50 meters. The sensing radius has been set to 15 meters. To make our issue easier to understand, we divide the network region into 25 m 25 m grids rather than circles. The sensing field is divided into 100 cells in this manner. If a sensor is still active in each cell, we believe that this area can be tracked by the system as shown in Figure 6. A clustering method should be able to cover as many cells as possible to ensure network coverage. Because the sensors are distributed in the network at random, the original coverage with 400 sensors is just 94 cells.

4.3. Interdomain Clustering for IMIMO 5G-Based BEE. Interdomain cluster transmission refers to the interaction between the CHs and the BS. Despite multihop routing, data transmission is extremely difficult to ensure when the network grows in size and the sensors do not enable lengthy transmission. As a result, multihop interdomain cluster transmission must be supported. Moreover, by lowering lengthy transmission between the CHs and the BS, multihop interdomain cluster routing can lessen energy utilization even more. Figure 7 depicts the results of the experiment for IMIMO 5G-based BEE. Delivering packets costs 100 pJ/bit/m^2 in terms of energy. As could be shown, IMIMO 5G-based BEE outperforms BEE in terms of network coverage and entire longevity.

The proposed approach emphasizes the selection of CHs whose objective is to provide the nodes based on IoT for choosing the transmission interfaces and CHs. The analysis of delay is done by separating the entire network into unequal clusters where clusters having the smallest radius which thereby single-hop topology comprises of small chains and the clusters with a huge radius that acquires minimum transmission delay. In the below-given Figure 8, it is shown the CH for the IMIMO 5G has shown the low

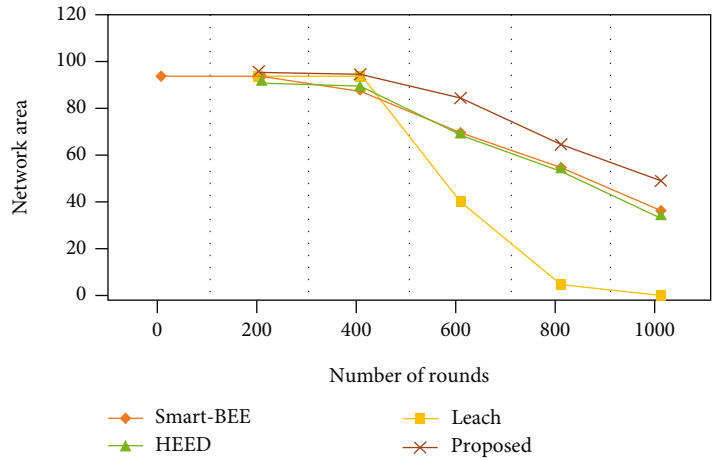


Figure 6: Network coverage area vs. number of rounds.

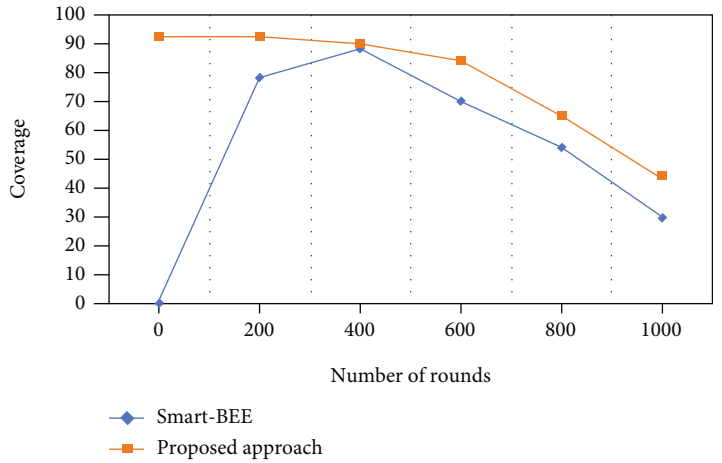


Figure 7: Network sensing coverage between coverage and number of rounds.

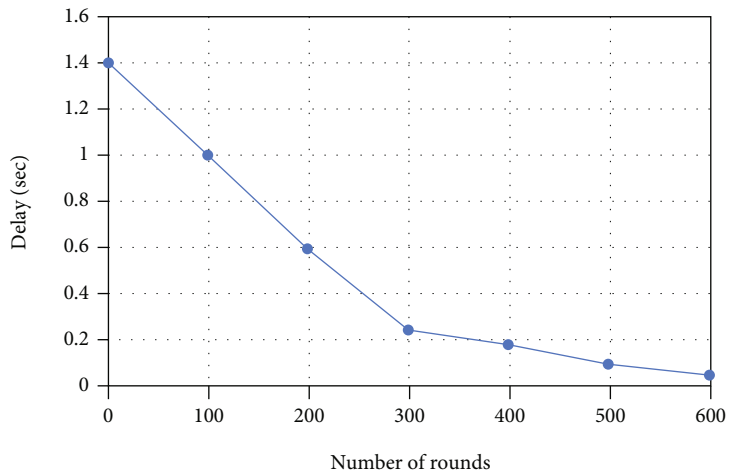


Figure 8: Delay vs. number of rounds.

transmission delay in case of 100 rounds the time took was 1 sec, 400 rounds, it took 0.1 sec, and so on.

5. Conclusion

The purpose of this research is to provide a centralized solution for organizing IoT communication entities into an uneven structure of composite clusters to protect the network from increasing hotspots issues and lengthen the lifespan of the network in the 5G scenario. The proposed protocol, in specific, has distinctive features including multi-hop topology creation, clusters of various communication topologies, balancing energy utilization among cluster heads, conserving energy utilization of nodes in the cluster, and selecting the most appropriate IoT application system transmission interfaces. We have presented the BEE to increase the lifetime of the network which supports the multihop clustering routing protocol. It provides the advanced devices of IoT to choose the transmission interfaces and CHs based on the context of the network. To construct shorter concentric networks, a vector projection approach that determines the BS position was adopted. In contrast, to reduce the strain on the cluster heads and lengthen the network's lifespan, a probabilistic suboptimal and multihop routing method was devised. Lastly, to choose the best transmission interface, a rating system was applied. When compared to state-of-the-art methodologies, quantitative findings demonstrated that an uneven clustering method optimized network survival and balanced energy depletion via cluster heads.

Data Availability

Data is not related to this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] R. E. Mohamed, A. I. Saleh, M. Abdelrazzak, and A. S. Samra, "Survey on wireless sensor network applications and energy efficient routing protocols," *Wireless Personal Communications*, vol. 101, no. 2, pp. 1019–1055, 2018.

[2] H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data-gathering sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 10, pp. 1526–1539, 2009.

[3] C. Iwendi, P. K. R. Maddikunta, T. R. Gadekallu, K. Lakshmanna, A. K. Bashir, and M. J. Piran, "A metaheuristic optimization approach for energy efficiency in the IoT networks," *Software: Practice and Experience*, vol. 51, no. 12, pp. 2558–2571, 2021.

[4] Y. Fathy and P. Barnaghi, "Quality-based and energy-efficient data communication for the internet of things networks," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10318–10331, 2019.

[5] S. Zhang, X. Xu, Y. Wu, and L. Lu, "5G: towards energy-efficient, low-latency and high-reliable communications networks," in *2014 IEEE international conference on communication systems*, vol. 2014, pp. 197–201, Macau, China, Nov 2014.

[6] M. Elappila, S. Chinara, and D. R. Parhi, "Survivable path routing in WSN for IoT applications," *Pervasive and Mobile Computing*, vol. 43, pp. 49–63, 2018.

[7] S. Fu, L. Zhao, Z. Su, and X. Jian, "UAV based relay for wireless sensor networks in 5G systems," *Sensors*, vol. 18, no. 8, article 2413, 2018.

[8] Y. Zhao, K. Liu, X. Xu, H. Yang, and L. Huang, "Distributed dynamic cluster-head selection and clustering for massive IoT access in 5G networks," *Applied Sciences*, vol. 9, no. 1, article 132, 2019.

[9] C. Jothikumar, K. Ramana, V. D. Chakravarthy, S. Singh, and I. H. Ra, "An efficient routing approach to maximize the lifetime of IoT-based wireless sensor networks in 5G and beyond," *Mobile Information Systems*, vol. 2021, 11 pages, 2021.

[10] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand, and A. H. Gandomi, "Residual energy-based cluster-head selection in WSNs for IoT application," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5132–5139, 2019.

[11] A. Seyyedabbasi and F. Kiani, "MAP-ACO: an efficient protocol for multi-agent pathfinding in real-time WSN and decentralized IoT systems," *Microprocessors and Microsystems*, vol. 79, article 103325, 2020.

[12] F. Kiani, E. Amiri, M. Zamani, T. Khodadadi, and A. Abdul Manaf, "Efficient intelligent energy routing protocol in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 3, Article ID 618072, 2015.

[13] J. T. Thirukrishna, S. Karthik, and V. P. Arunachalam, "Revamp energy efficiency in homogeneous wireless sensor networks using optimized radio energy algorithm (OREA) and power-aware distance source routing protocol," *Future Generation Computer Systems*, vol. 81, pp. 331–339, 2018.

[14] X. Liu, "Atypical hierarchical routing protocols for wireless sensor networks: a review," *IEEE Sensors Journal*, vol. 15, no. 10, pp. 5372–5383, 2015.

[15] D. Sharma, S. Singhal, A. Rai, and A. Singh, "Analysis of power consumption in standalone 5G network and enhancement in energy efficiency using a novel routing protocol," *Sustainable Energy, Grids and Networks*, vol. 26, article 100427, 2021.

[16] M. T. Rahama, M. Hossen, and M. M. Rahman, "A routing protocol for improving energy efficiency in wireless sensor networks," in *2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, pp. 1–5, Dhaka, Bangladesh, Sept.2016.

[17] V. Nivedhitha, A. G. Saminathan, and P. Thirumurugan, "DMEERP: a dynamic multi-hop energy efficient routing protocol for WSN," *Microprocessors and Microsystems*, vol. 79, article 103291, 2020.

[18] G. S. Brar, S. Rani, V. Chopra, R. Malhotra, H. Song, and S. H. Ahmed, "Energy efficient direction-based PDORP routing protocol for WSN," *IEEE Access*, vol. 4, pp. 3182–3194, 2016.

[19] K. M. Kumaran and M. Chinnadurai, "A competent ad-hoc sensor routing protocol for energy efficiency in mobile wireless sensor networks," *Wireless Personal Communications*, vol. 116, no. 1, pp. 829–844, 2021.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1738530, 12 pages
https://doi.org/10.1155/2022/1738530

Research Article

Overlapping Coalition Game for Resource Allocation in Many-to-Many D2D Communication

Jihua Sheng[1], **Sihan Liu**[1], **Tiancong Huang**[1] and **Yucheng Wu**[1,2]

[1]*School of Microelectronics and Communication Engineering, Chongqing University, Chongqing, China*
[2]*State Key Laboratory of Power Transmission Equipment & System Security and New Technology, Chongqing University, Chongqing, China*

Correspondence should be addressed to Tiancong Huang; htc@cqu.edu.cn

Received 24 November 2021; Revised 6 January 2022; Accepted 11 January 2022; Published 24 February 2022

Academic Editor: Mohammed H. Alsharif

Device-to-device (D2D) communication is one of the promising technologies for the next-generation cellular network, which uses direct communication between two neighboring devices to obtain a high transmission rate. This paper focuses on wireless resource allocation in a many-to-many D2D communication scenario to maximize the D2D transmission sum rate. Through the model analysis, the objective function is formulated while guaranteeing the minimum transmission rate of both the cellular users (CUs) and the D2D pairs. Based on the candidate sequence, an overlapping coalition game algorithm is proposed to enhance the D2D transmission sum rate. Furthermore, the preference sequence of CUs is adopted in the coalition initialization. According to the interference intensity, a power allocation scheme is designed further to improve the transmission sum rate of the D2D pairs. The simulation results have verified the validity of the proposed algorithm.

1. Introduction

With the rapid development of the Internet of Things (IoT) and cellular technology, the demand for mobile internet access is growing at a tremendous rate in the past decade [1–3]. As one of the critical technologies of 5G [4, 5], device-to-device (D2D) communication can improve the transmission rate of communication networks, enhance the system throughput [6, 7], and reduce the communication delay [8]. D2D communication is a short-distance communication technology that data transmission can be directly carried out between two terminals. D2D communication can be operated as an underlay mode by sharing the cellular spectrum, which significantly improves the performance of network and the user experience [9, 10].

In the hybrid network formed by the cellular users (CUs) and the D2D pairs, the communication quality will be affected. On the one hand, the D2D pairs reusing the cellular spectrum will disturb the communication of CUs. On the other hand, the D2D devices sharing the spectrum will be interfered by the corresponding CUs [11, 12]. Especially, the interferences will be more serious in many-to-many scenario, where one channel resource can be reused by multiple D2D pairs, and a D2D pair can reuse multiple channel resources. The transmission rate of D2D communication will be very small as the existence of serious interferences in a many-to-many scenario, which will restrict the development of D2D communication. Therefore, the methods of reasonable channel allocation and power control are very important in D2D communication research.

This paper mainly focuses on the resource allocation and power control in many-to-many D2D communication, which is different from reported works, such as the random selection [13], cooperative game [14], or matching game with externalities [15] to reuse the channel resources and improve the D2D transmission sum rate. An overlapping coalition game algorithm based on the candidate sequence is proposed to further enhance the D2D transmission sum rate in this work. And the cellular user's preference sequence is adopted to initialize the coalition. Furthermore, a power

control scheme based on interference intensity is designed to improve the utility of the coalition.

The main contributions of this paper are summarized as follows:

(1) In a many-to-many scenario, the system model was analyzed, and the sum transmission rate of D2D pairs with guaranteeing the quality of service (QoS) was formulated as the objective function

(2) An overlapping coalition game algorithm based on the candidate sequence was proposed to guide the channel resource allocation, which could enhance the transmission rate of D2D pairs. Furthermore, the preference sequence was used in the processing of the coalition initialization

(3) A power allocation scheme based on the preference sequence was proposed to allocate the powers of D2D pairs. To ensure the performance requirements of D2D pairs and CUs in the coalition, the coalition utility was used to evaluate whether the power allocation is effective

The rest of this paper is outlined as follows. The related works are described in Section 2. Section 3 provides the system model and the problem formulation. Section 4 provides a detailed description of the resource allocation algorithm and the power control strategy. Simulation results are presented in Section 5. The conclusion is summarized in Section 6. For the sake of convenience, the major symbols used in this paper are listed in Table 1 with their definitions.

2. Related Works

Recent studies concerning resource allocation mainly focused on the following aspects: mode selection [16], resource multiplexing, and power allocation [17] for D2D communication. The D2D communication includes the following scenarios: one-to-one, many-to-one, and many-to-many D2D communication.

(1) One-to-one D2D communication

Resource allocation in one-to-one D2D communication was studied in [18, 19]. In [18], a network-assisted distributed processing architecture was proposed to solve the throughput optimization problem, which included receiving mode selection, verification for relay selection, and transmission power adjustment. It could reduce the burden of centralized processing. A power control and channel allocation scheme for the energy efficiency maximization of D2D pairs through reusing uplink-downlink resources was presented in [19].

(2) Many-to-one D2D communication

For the scenario of multiple channel resources can be multiplexed by one D2D pair, the coalition game with priority sequences was presented to maximize the D2D throughput while guaranteeing the minimum rate of each user in [20]. In [21], a sealed bid single price auction game was introduced to attain the maximum throughput by balancing the interference between D2D users and CUs. In [22], by jointly considering the mode selection and power control strategy, a coalition formation game was proposed to maximize the energy efficiency of all users in the cellular network. In [23], a two-tier resource allocation scheme was discussed to maximize the spectral efficiency with guaranteeing a minimum throughput and its latency requirement. A spectrum resource allocation algorithm based on game theory was proposed to enhance the system sum rate in [24]. However, in [24], the power control strategy was not discussed to improve the system performance.

The resource allocation method which multiple D2D pairs can multiplex a channel resource was investigated in [25–29]. In [25], based on matching theory and coalition game theory, a constrained deferred acceptance algorithm and a coalition formation algorithm were proposed to maximize the system performance with guaranteeing the QoS of all users. In [26], the cooperative D2D communication in an uplink cellular network was investigated, where D2D users acted as relays for cellular users to maximize the total average achievable rate under the outage probability constraint. Channel resource allocation methods based on interference analysis in a multiplexing scenario were studied to improve the system performance in [27, 28]. A distributed resource allocation algorithm based on the interference threshold was introduced to maximize the transmission rate of the D2D pairs in [29]. Only the matching problem between the D2D pairs and the CUs was taken into account in the research works mentioned above, and the performance of the CU was seldom considered during the optimizing process.

(3) Many-to-many D2D communication

Channel multiplexing in a many-to-many D2D communication was studied in [14, 15, 30, 31]. A cooperative game resource allocation algorithm based on the overlapping coalition was proposed to improve the utility of the system, in which the coalition initialization was formed by choosing the most suitable CU to reuse its resources block according to the cross-tier interference strength in [14]. A many-to-many resource allocation algorithm based on externalities was proposed to reach a stable state and improve the performance of the system in [15]. A resource allocation method based on the graph coloring theory was proposed to optimize the spectral efficiency of the system in [30]. An iterative user-subchannel swap algorithm was proposed to maximize the sum rate of LTE and D2D users in [31].

The literature mentioned above showed that the power and the spectrum allocation were considered to optimize the system performance from multiple aspects. The complexity for channel resource allocation of both one-to-one and many-to-one is much lower than that of many-to-many in D2D communication. In this paper, under the condition of guaranteeing the user's QoS, an overlapping coalition formation game is proposed to solve the problem of resource allocation in many-to-many D2D communication.

Table 1: List of major symbols.

Symbol	Description
N	The number of CUs
M	The number of D2D pairs
n_0	Gaussian white noise
$r_{m,n}^D$	The transmission rate of the mth D2D pair sharing
	The nth resource block
r_n^C	The transmission sum rate of the nth CUs
$\xi_{m,n}^D$	The SINR of the mth D2D pair sharing the nth
	Resource block
ξ_n^C	The SINR of the nth CU
p_n^C	The transmit power of nth CUs
p_m^D	The transmit power of D2D pairs
m'	D2D pairs in the same coalition with the mth pair
D_n	A set of all the D2D pairs sharing the same resource
$\chi_{m,n}$	The reusing indicator of CUs
R_C	The transmission sum rate of the all CUs
R_D	The transmission sum rate of the all D2D pairs
$g_{C_{n,m}}$	The path gains from the transmitter of the nth CUs to the mth D2D pair receiver
$g_{D_{m,m}}$	The path gains from the transmitter of the mth D2D pair to D2D pair receiver
$g_{D_{m',m}}$	The path gains from the transmitter of the m'th D2D pair to the mth D2D pair receiver
$g_{D_{n,m,B}}$	The link gain between the mth D2D pair sharing the nth channel resource block and the base station
R_{th}^C	The rate thresholds of CUs
R_{th}^D	The rate thresholds of D2D pairs
$g_{C_{n,B}}$	The path gains of the nth CUs to the base station
$g_{D_{m,B}}$	The path gains of the mth D2D pair to the base station
r_n^C	The transmission rate of CUs
$p_D^{\max}$	The maximum transmit power of D2D pairs
L	The players of all users in the system model
CS	The coalition structure
v	The utility functions
$H(m, S_l)$	Historical information table
p_u	The power interval
k	The path loss constant
$\beta_{n,m}$	The multipath fading parameter from the nth CUs to receiver of the mth D2D pair
$\omega_{n,m}$	The shadow gain from the nth CUs to receiver of the mth D2D pair
$\gamma_{n,m}$	The distance from the nth CUs to the receiver of the mth D2D pair
α	The path loss factor
S_n	A set of the corresponding D2D pairs and the CU that share the nth resource block
$\rho_{(n,m)}$	The interference intensity of the mth D2D pair that reuse the nth cellular user

3. System Model and Problem Formulation

This section provides a detailed description of the system model in many-to-many D2D communication and the optimization problem to maximize the transmission sum rate of D2D pairs is formulated.

In a many-to-many D2D communication scenario, one channel resource can be shared by one CU and multiple D2D pairs, and a D2D pair can reuse multiple channel resources. As shown in Figure 1, CUs and D2D pairs coexist in the cell network, and the network contains N CU and M D2D pair. The set of channel resource blocks contains in the cell is represented as $C = \{1, \cdots, n, \cdots, N\}$. The D2D pair set is $D = \{1, \cdots, m, \cdots, M\}$. The D2D pairs share the uplink of the CUs. For example, the 1st D2D pair (DU1), the 2nd D2D pair (DU2), and the 6th D2D pairs (DU6) in the cell network reuse the spectrum of the 1st CU (CU1). Meanwhile, DU2 can also share the spectrum of CU2.

It is assumed that the base station has the perception function of all complete channel state information (CSI). How the base station obtains the CSI of users is not involved in this study. The mth D2D pair receives the interferences from the corresponding CU and the D2D pairs which share the same channel resource. The transmission rate of the mth D2D pair sharing the nth resource block can be expressed as

$$r_{m,n}^{D} = \log_2\left(1 + \xi_{m,n}^{D}\right),$$
$$\xi_{m,n}^{D} = \frac{p_m^D g_{D_{m,m}}}{n_0 + p_n^C g_{C_{n,m}} + \sum_{m' \in D_n \setminus m} \chi_{m',n} p_{m'}^D g_{D_{m',m}}}. \tag{1}$$

where $\xi_{m,n}^{D}$ is the signal to interference noise ratio (SINR) of the mth D2D pair sharing the nth resource block. p_n^C and p_m^D are the transmit power of the nth CU and the mth D2D pair, respectively. And n_0 is the Gaussian white noise. The symbol of m' represents the m'th D2D pair which shares the same frequency with the mth D2D pair. D_n is a set of all D2D pairs sharing the same channel resource. $g_{C_{n,m}}$, $g_{D_{m,m}}$, and $g_{D_{m',m}}$ are the path gain from the nth CU, the transmitter of the mth D2D pair and the m'th D2D pair to the mth D2D pair receiver, respectively. The parameter $\chi_{m,n}$ is the indicator of reusing the nth resource block. If the nth resource block is reused by the mth D2D pair, $\chi_{m,n} = 1$. Otherwise, $\chi_{m,n} = 0$.

The transmission sum rate of all D2D pairs can be given as

$$R_D = \sum_{n \in C} \sum_{m \in D} r_{m,n}^{D} = \sum_{n \in C} \sum_{m \in D} \log_2\left(1 + \xi_{m,n}^{D}\right). \tag{2}$$

The SINR of the nth CU is expressed as follows:

$$\xi_n^C = \frac{p_n^C g_{C_{n,B}}}{n_0 + \sum_{\mathrm{m} \in D_n} \chi_{\mathrm{m,n}} \mathrm{p_m^D} g_{D_{\mathrm{m},B}}}, \tag{3}$$

where $g_{C_{n,B}}$ and $g_{D_{m,B}}$ are the path gains of the nth CU and the mth D2D pair to the base station, respectively.

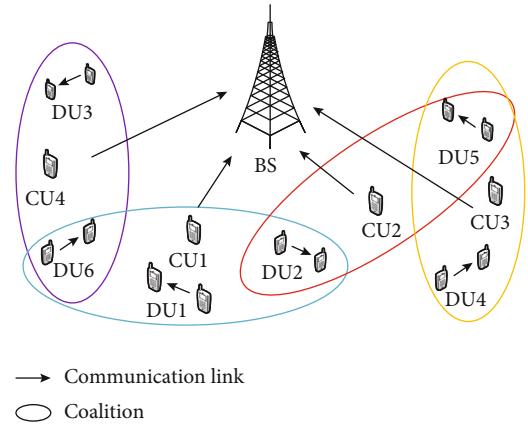


Figure 1: Many-to-many uplink resource reusing system model.

The transmission sum rate of all CUs in the cell can be described as

$$R_C = \sum_{n \in C} r_n^C = \sum_{n \in C} \log_2\left(1 + \xi_n^C\right) = \sum_{n \in C} \log_2\left(1 + \frac{p_n^C g_{C_{n,B}}}{n_0 + \sum_{m \in D_n} \chi_{m,n} p_m^D g_{D_{m,B}}}\right). \tag{4}$$

The objective function is to maximize the transmission rate of all D2D pairs while considering the minimum rate of each user. And it can be described as follows:

$$\max_{\chi_{m,n}, p_m^D} R_D = \sum_{n \in C} \sum_{m \in D} r_{m,n}^{D} = \sum_{n \in C} \sum_{m \in D} \log_2\left(1 + \xi_{m,n}^{D}\right), \tag{5}$$

$$s.t. r_{m,n}^{D} \geq R_{th}^{D} \forall m \in D, \forall n \in C, \tag{6}$$

$$r_n^C \geq R_{th}^C \forall n \in C, \tag{7}$$

$$p_m^D \leq p_D^{\max} \forall m \in D, \tag{8}$$

$$p_n^C \leq p_C^{\max} \forall n \in C, \tag{9}$$

$$\chi_{m,n} \in \{0, 1\} \forall m \in D, \forall n \in C. \tag{10}$$

where R_{th}^D and R_{th}^C are the D2D pairs and CUs' transmission rate threshold values, respectively. The $p_D^{\max}$ and $p_C^{\max}$ are maximum transmit power of the D2D pairs and CUs, respectively. Equation (6) (Equation (7)) represents the transmission rate constraint of the mth D2D pair (the nth CU). Equation (8) (Equation (9)) indicates the transmit power of the mth D2D pair (the nth CU) should be less than or equal to the corresponding maximum value. Equation (10) means whether the mth D2D pair sharing the nth channel resource. Since Equation (5) is a nonlinear equation which involves a binary variables of $\chi_{m,n}$, therefore, the objective function is a mixed-integer nonlinear programming (MINLP) problem.

4. Resource Allocation Algorithm for Optimizing Transmission Rate

This section introduces a resource allocation algorithm based on the overlapping coalition game and power control strategy of all D2D pairs in a many-to-many D2D communication scenario.

4.1. Preference Sequence Coalition Initialization. The definition of the overlapping coalition is given as follows.

Definition 1. In the coalition game $G = (L, v, CS)$, $L = \{1, \cdots, m, \cdots, M\}$ denotes a set of all D2D pairs that share the channel resources. The parameter v represents the utility function. The coalition structure $CS = \{S_1, S_2, \cdots, S_n, \cdots, S_N\}$ denotes a set of S_n, where S_n represents a set of the corresponding D2D pairs and the CU that share the nth resource block. As the D2D pairs can join multiple coalitions, an overlapping coalition structure is formed. It means that $S_i \cap S_j \neq \varnothing$, $i, j \in N, i \neq j$, where S_i and S_j represent the ith and jth coalition in the same coalition structure, respectively.

The utility function of v can be used to evaluate whether the coalition has been improved. The utility function of the mth D2D pair sharing the nth channel resources is defined as

$$v(m, S_n) = \begin{cases} r^D_{m,n}, r^D_{m,n} \geq R^D_{th}, \\ 0, \text{otherwise}. \end{cases} \tag{11}$$

The utility function of the coalition S_n with transmission rate constraints is expressed as

$$v(S_n, CS) = \begin{cases} \sum_{m \in D_n} r^D_{m,n}, r^D_{m,n} \geq R^D_{th}, r^C_n \geq R^C_{th}, \\ 0, \text{otherwise}. \end{cases} \tag{12}$$

The utility function of coalition structure CS is the sum of the utility value of each coalition and it can be expressed as

$$v(CS) = \sum_{n \in C} v(S_n, CS). \tag{13}$$

In the process of coalition initialization, the performance of each CU should be firstly guaranteed when the channel resource blocks are shared. The interference intensity of the mth D2D pair that shares the nth channel resource block is used as the preference value, and it can be expressed as

$$\rho_{(n,m)} = p^D_m g_{D_{n,m,B}}, \tag{14}$$

where $g_{D_{n,m,B}}$ is the communication link gain between the mth D2D pair sharing the nth channel resource block and the base station. If the preference value of the mth D2D pair is lower, the interference to the CU sharing the same channel resource is smaller. Therefore, the D2D pair is more likely to reuse this resource block.

The preference sequence of the mth D2D pair is a set of preference values for the mth D2D pair that shares different channel resources. In order to optimize the sum transmission rate of all D2D pairs, the preference sequence is adopted in coalition initialization. The coalition initialization process based on the preference sequence includes four steps:

(1) The first step: calculating the preference value of the 1st D2D pair according to Equation (14), arranging the preference values in ascending order to form the preference sequence (denoted as T_1)

(2) The second step: calculating the transmission rate of the 1st D2D pair and the corresponding CU in the order of the T_1, respectively. If the transmission rate is lower than the rate threshold, the calculation is stopped. Otherwise, the preference values that make the transmission rate satisfy the transmission rate threshold will form a new preference sequence (denoted as T_1')

(3) The third step: repeatedly obtaining the mth D2D pair preference sequence T_m' according to the first and second steps, until all $T_m' (m \in M)$ have been obtained

(4) According to $T_m' (m \in M)$, all D2D pairs which share the same resource block are determined and the corresponding D2D pairs form an initial coalition

4.2. Overlapping Coalition Game

Definition 2. It is assumed that the coalition structure CS_p is described as $CS_p = \{S_1 \cdots, S_a, \cdots, S_b, \cdots, S_N\}$ and the mth D2D pair belongs to the coalition of S_a. If the mth D2D pair switchs from S_a to S_b, the coalition structure $CS_q = \{S_1, \cdots, S^q_a, \cdots, S^q_b, \cdots, S_N\}$ is formed, where $S^q_a = S_a \setminus m$ and $S^q_b = S_b \cup \{m\}$.

The coalition game guideline is given as

$$CS_p \triangleright CS_q \Leftrightarrow \begin{cases} v\left(m, S^q_b\right) > v(m, S_a), \\ v\left(S^q_b, CS_q\right) \geq v\left(S_b, CS_p\right), \\ v\left(CS_q\right) > v\left(CS_p\right), \end{cases} \tag{15}$$

where the first inequation of (15) means that the utility value of the mth D2D pair in the coalition of S^q_b is larger than that in S_a. And the second inequation of (15) means that the utility value of S^q_b is no less than that of S_b. The third inequation of (15) represents that the utility value of coalition structure CS_q will be greater than that of CS_p. If the D2D pair who meets the above three conditions, it can switch from one coalition to another. According to (14), the preference values

for the mth D2D pair sharing all channel resource is obtained. The mth D2D pair chooses the coalition with a lower preference value to join.

If the coalition consists of only one CU, which means that there is no any D2D pair in the coalition. Therefore, the corresponding coalition switch guideline is given as follows:

$$CS_p \triangleright CS_q \Leftrightarrow \begin{cases} v\left(m, S_b^q\right) > v(m, S_a), \\ v\left(CS_q\right) > v\left(CS_p\right). \end{cases} \tag{16}$$

As the channel resource has not been used by any D2D pair, the D2D pair was randomly selected to join a new coalition if two conditions are satisfied: (i) the individual utility of the D2D pair is increased and (ii) the total utility of the new coalitional structure is increased. Eventually, the total transmission rate of D2D pairs and the utility value of coalition structure will be improved after multiple switching.

The channel resource allocation is determined through randomly selection [13] or cooperative game [14] to improve the D2D transmission sum rate. This work shows that the D2D transmission sum rate can be further enhanced by introducing the candidate sequence in the overlapping coalition game. The candidate sequence S_0 contains all D2D pairs in the network. This sequence always remains unchanged, and it is represented as $S_0 = \{1, \cdots m, \cdots, M\} (m \in D)$.

Definition 3. Considering two coalition structures $CS_p = \{S_1, \cdots, S_a, S_b \cdots, S_N\}$ and $CS_q = \{S_1, \cdots, S_a^q, S_b^q \cdots, S_N\}$. For the coalition S_a, the m'th D2D pair in the candidate sequence S_0 wants to join or replace the mth D2D pair in S_a, so $S_a^q = S_a \cup \{m'\}, m' \in S_0, m' \notin S_a$, or $S_a^q = (S_a \setminus m) \cup \{m'\}$. $\exists a \neq b, S_a^q \cap S_b^q \neq \phi$.

The guideline of D2D pairs in the candidate sequence to join the coalition or replace the D2D pair in the coalition is expressed as

$$CS_p \triangleright CS_q \Leftrightarrow v\left(S_a^q, CS_q\right) \geq v\left(S_a, CS_p\right). \tag{17}$$

The m'th D2D pair in the candidate sequence S_0 can join or replace the mth D2D pair in S_a if the utility of S_a^q is no less than that of S_a.

In order to reduce the times of game, the proposed algorithm sets a historical information table $H(m, S_l)$. If the mth D2D pair already exists in the coalition S_l or has been refused to join the coalition S_l, it is set that $H(m, S_l) = 1$; otherwise, $H(m, S_l) = 0$.

$$H(m, S_l) = \begin{cases} 1, m \in S_l \text{ or } m \text{ has been refused by } S_l, \\ 0, \text{otherwise}. \end{cases} \tag{18}$$

Algorithm 1 summarizes the resource allocation algorithm.

4.3. Power Allocation. In the many-to-many scenario, it is not easy to perform power control while allocating channel resources. Therefore, the power of each D2D pair is allocated after the coalition structure is formed.

Each D2D pair sends its channel status information to the base station, and the base station sets the transmit power of the corresponding D2D pair. It is assumed that the transmit power level is $\Psi = \{1, 2, \cdots, u_m \cdots, Q\}$, where Q is the maximum power level. The maximum transmit power $p_D^{\max}$ of each D2D pair on each subchannel is a fixed value. The power interval is $p_u = p_D^{\max}/Q$. According to the power level, the transmit power of the mth D2D pair can be expressed as

$$p_m^D = u_m p_u. \tag{19}$$

In the process of power allocation, the transmission rate of each CU and each D2D pair must meet the minimum rate requirement. The optimization goal of the power allocation is to improve the coalition utility. The transmit power of all D2D pairs is allocated according to the preference sequence. The power allocation strategy is given as follows:

(1) The first step: for the coalition $S_n (n \in N)$, allocating the highest levels of power to the corresponding D2D pair, which the interference to the CU in the coalition of S_n is the smallest

(2) The second step: if the conditions shown in Equations (6), (7), (8), and (9) are met, the corresponding transmit power of the D2D pair will be allocated

(3) The third step: if the conditions shown in Equations (6), (7), (8), and (9) are not met, reducing one of the power levels, calculating the transmission rate, and judging whether the conditions mentioned above are satisfied. If satisfied, the corresponding transmit power will be allocated. Otherwise, further reducing one of the power levels until the conditions mentioned above are satisfied

(4) The fourth step: selecting the next D2D pair (the transmit power has not been allocated) in S_n which the interference to the CU in the coalition of S_n is the smallest

(5) The fifth step: selecting the next coalition to allocate the transmit power until the transmit power of all D2D pairs in the cell are allocated

4.4. Complexity and Convergence. It can be seen from Algorithm 1 that the computational complexity is related to the number of channel resources N and the D2D pairs M. During the initial process of coalition game, the D2D pair selects the most suitable coalition to join according to the preference sequence of the D2D pair, which can reduce the switch times for the D2D pair to join the corresponding coalitions. Moreover, the history information table $H(m, S_l)$ is introduced to prevent the D2D pairs from rejoining the same coalition. In general, the computational complexity of this algorithm is less than $O(N \times M)$. The worst-case occurs

Step 1: Initialize
1: $S_n = \{n\}$ and $CS = \{S_1, \cdots, S_n, \cdots, S_N\}$;
Step 2: Overlapping coalition initialization
1: According to $\rho_{(n,m)} = p_m^D g_{D_{n,m,B}}$ and form T_m' (m from 1 to M);
2: According to $T_m'(m \in M)$, all D2D pairs sharing the same resource block are determined while satisfying Equations (6), (7), (8), and (9).
3: Corresponding D2D pairs form an initial coalition.
Step 3: Overlapping coalition game
1: $CS = \{S_1, \cdots, S_a, \cdots, S_n, \cdots, S_N\}$;
2: For S_a, a from 1 to N
3: In S_a, for the mth D2D pair ($m \in S_a$);
4: **if** $\rho_{(a,m)} > \rho_{(n,m)}$ and $H(m, S_n) = 0$ **then**
5: **if** Meet (15) or (16) and $H(m, S_a) = 1$ **then**
6: Join S_n, and set $H(m, S_n) = 1, H(m, S_a) = 0$;
7: **else**
8: Set $H(m, S_n) = 1$;
9: **end if**
10: **else**
11: The mth D2D pair stays in S_a.
12: **end if**
13: End for
14: **if** the number of D2D pairs in S_a does not changed **then**
15: **if** in S_0, the m'th D2D pair meets Equation (17) and $H(m', S_a) = 0$ **then**
16: the m'th D2D pair join the coalition S_a or replace the m-th D2D pair, $H(m', S_a) = 1$;
17: **else**
18: Set $H(m', S_a) = 1$;
19: **end if**
20: **end if**
21: End for
22: Repeat Step 3 until the coalition structure remains unchanged in this round of game.
Step 4: Output
1: End the iteration and output the coalition structure.

Algorithm 1: Resource allocation algorithm based on overlapping coalition game

when all D2D pairs find the channel resources to reuse at the last switching; therefore, the computational complexity of the proposed algorithm is $O(N \times M)$. The computational complexity of the proposed algorithm is similar to that presented in [14], in which the computational complexity is $O(N \times M)$. The computational complexity of the proposed algorithm is a little better than that of the algorithm proposed in [15], which the computational complexity is $O(M/2 + N \times M)$.

The criterion of the coalition game is that each D2D pair carries out handover if its utility and the system utility are increased. If the D2D pair meets the switching conditions of Equations (15), (16), or (17), it means the utility of the D2D pair is not reduced. And the corresponding D2D pair can join the other coalitions. Otherwise, the D2D pair stays in the original coalition. If the number of D2D pairs and CUs are given, it can be seen that the total number of coalitions formed in Algorithm 1 is finite. And the system utility will reach the maximum value through the limited times of switching. Eventually, Algorithm 1 is converged and the stable coalition structure is formed.

The relationships between the system utility and the iterations with N=5 and M =100 is shown in Figure 2. It can be seen that the system utility will reach the maximum value through the limited iterations, in which a stable coalition structure will be formed.

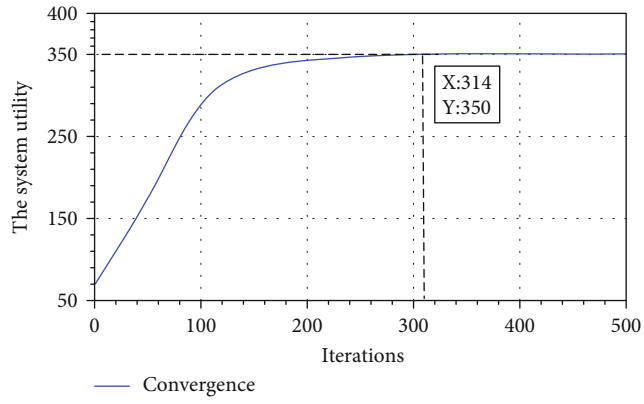


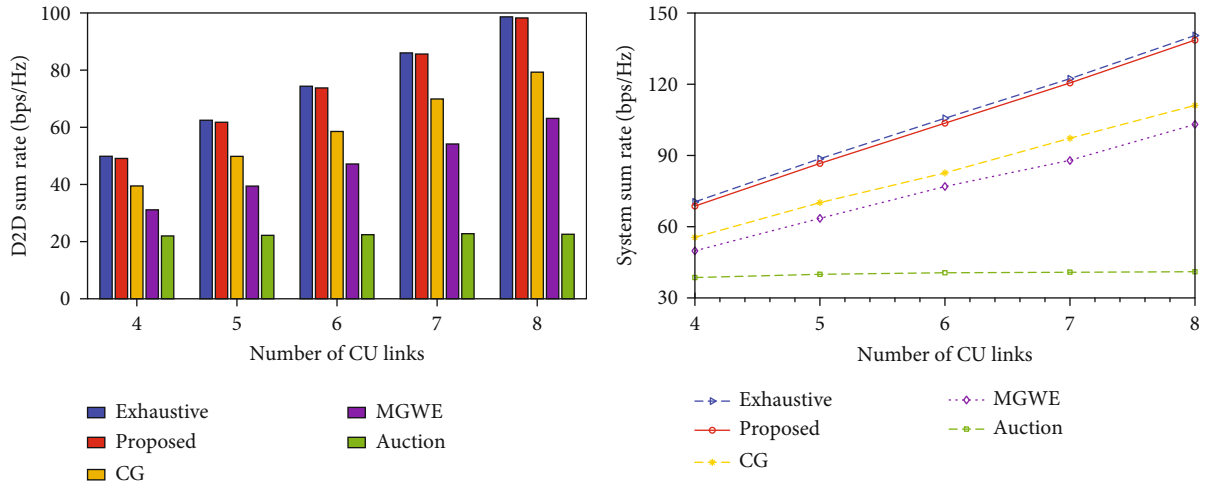
Figure 2: The relationships between the system utility and the iterations.

5. Simulation and Analysis

5.1. Simulation Design. This section verifies the performance of the proposed algorithm. It is assumed that the base station

Table 2: Simulation parameters.

Parameters	Value
Cell radius	500 m
Number of CUs N	4~8
Number of D2D pairs M	1~5
CUs' maximum transmission power $p_C^{\max}$	23 dBm
D2D maximum transmission power $p_D^{\max}$	13 dBm
CUs' rate threshold R_{th}^D	2 ~4 bps/Hz
D2D pairs rate threshold R_D	1 bps/Hz
D2D maximum transmission distance d	50 m
Noise power spectral density	-174 dBm/Hz
Resource block bandwidth	15 kHz
Path loss factor α	3
Multipath fading $\beta_{n,m}$ (exponential distribution mean)	1
Shadow fading $\lambda_{n,m}$ (logarithmic distribution standard deviation)	8 dB
The maximum power level Q	13



(a) D2D transmission rate

(b) System transmission rate

Figure 3: Effects of the CUs' number on transmission rate.

is located in the center of the cell, the CUs and D2D pairs are randomly scattered in the cell, and the cell shape is a regular hexagon. And assuming that the D2D pairs and CUs are stationary or at a low speed. Each coalition contains one CU. Each D2D pair can join multiple coalitions. The Rayleigh channel model has been adopted in the simulation. The path gain of the link from the nth CU to the receiver of the mth D2D pair can be expressed as

$$g_{n,m} = k\beta_{n,m}\omega_{n,m}\gamma_{n,m}^{-\alpha}, \tag{20}$$

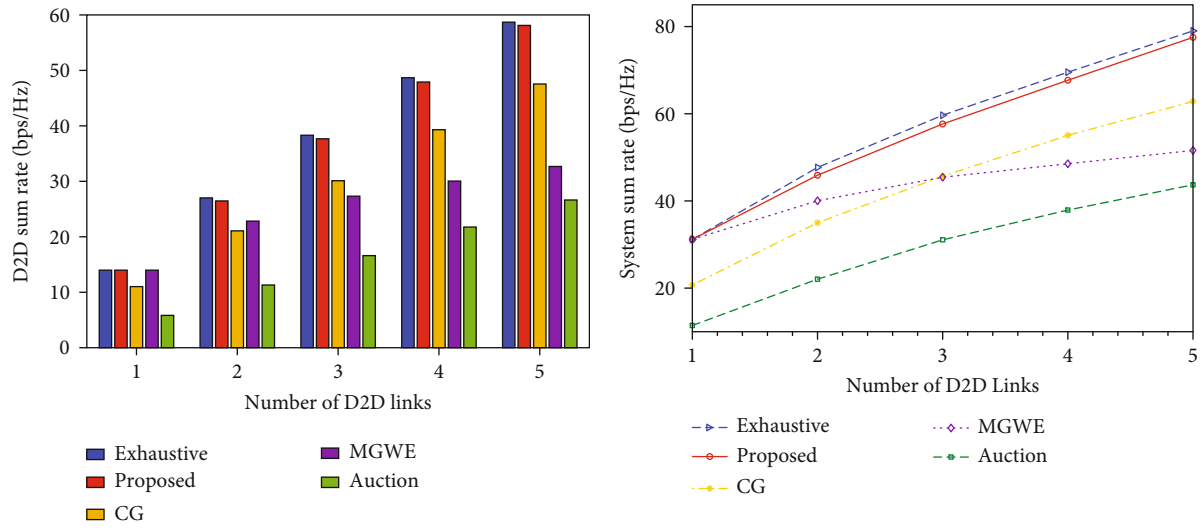
where k represents the path loss constant. $\beta_{n,m}$ with exponential distribution is the multipath fading parameter from the nth CU to the receiver of the mth D2D pair. And $\omega_{n,m}$ with log-normal distribution represents the shadow gain from the nth CU to the receiver of the mth D2D pair. $\gamma_{n,m}$ indicates the distance from the nth CU to the receiver of the mth D2D pair, and α indicates the path loss factor. Other simulation parameters are listed in Table 2, which is the same to that shown in [14].

The system transmission sum rate is the sum of the transmission rate of all D2D pairs and CUs. According to Equations (2) and (4), it can be expressed as

$$R_{\text{total}} = \sum_{n\in C}\sum_{m\in D} r_{m,n}^D + \sum_{n\in C} r_n^C. \tag{21}$$

In order to verify the performance of the proposed algorithm, this paper takes the transmission sum rate of all D2D pairs and the system transmission sum rate as indicators and carries out simulation verification on the numbers of the users and the transmission rate thresholds of the CUs.

The proposed algorithm is compared with the following four algorithms:



(a) D2D transmission rate

(b) System transmission rate

Figure 4: Effects of the D2D pairs' number on transmission rate.

(1) Exhaustive algorithm: the D2D pairs select coalitions to maximize the D2D system transmission rate by the exhaustive search, which means that search all possible coalitions to find the optimal solution. The algorithm is labeled as "Exhaustive"

(2) Cooperative game (CG) algorithm [14]: an overlapping coalitions game algorithm with cooperative optimization is proposed to maximize the system utility in terms of the sum rate of all D2D links. The algorithm is labeled as "CG"

(3) Matching game with externalities (MGWE) algorithm [15]: with signal-to-interference-plus-noise ratio constraints for both D2D devices and the cellular users, a resource allocation algorithm based on the many-to-many two-sided matching game with externalities to maximize the system sum rate. The matching game with externalities algorithm is labeled as "MGWE"

(4) Auction algorithm [32]: it is an iterative combinatorial auction algorithm with flexible power control, where the CUs are considered as bidders, D2D pairs as goods, and the cellular network plays a role as the auctioneer controlling the auction process. The algorithm is labeled as "Auction"

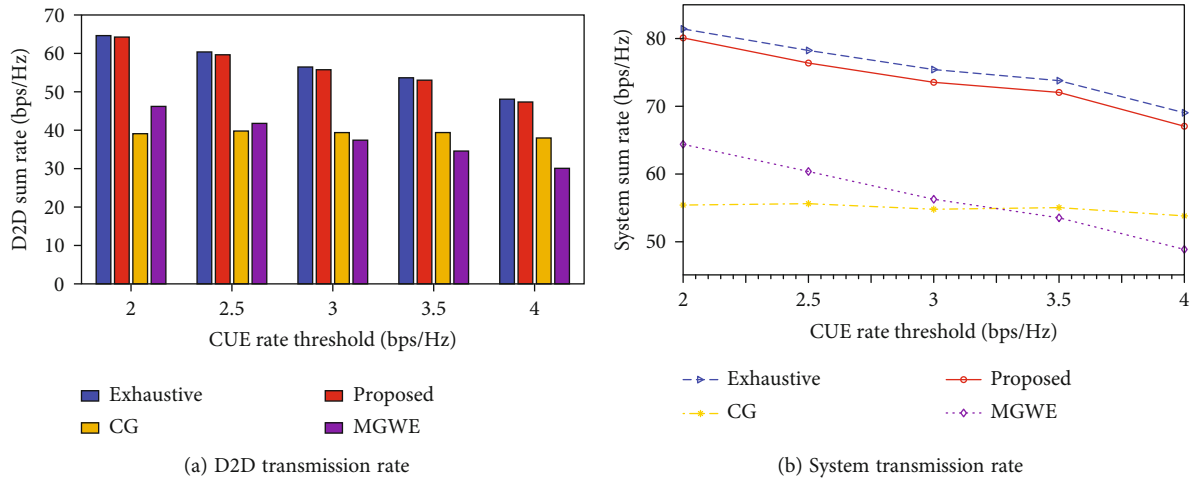
1000 times of simulation are carried out and each data point in the simulation results is the average value of 1000 times simulation. With $N = 4$ and $M = 5$ to obtain the D2D transmission sum rate, the running time of "Proposed," "CG," and "MGWN" algorithms is 10.465 ms, 11.857 ms, and 13.297 ms, respectively.

5.2. Results and Discussion. Figures 3(a) and 3(b) show the effect of CU link number on the transmission sum rate of all D2D pairs and the system transmission sum rate with $M = 4$, respectively. It can be seen that the transmission sum rate of all D2D pairs (the system) increases with the number of CUs becoming larger, which means the more coalitions that the D2D pair can choose to join. The D2D (the system) transmission sum rate in the many-to-many scenario by using the proposed algorithm is close to that by using the "Exhaustive" method, and the D2D (the system) transmission sum rate obtained by using the proposed algorithm is larger than that by using "CG," "MGWE," or "Auction" algorithms.

Figures 4(a) and 4(b) show the relationships of D2D link number to the D2D (the system) transmission sum rate with $N = 4$. It can be observed that the D2D and system transmission sum rate by using the proposed method increases with the number of the D2D pairs becomes larger. The performance of the proposed algorithm is close to that of the exhaustive method and is better than that of other three algorithms.

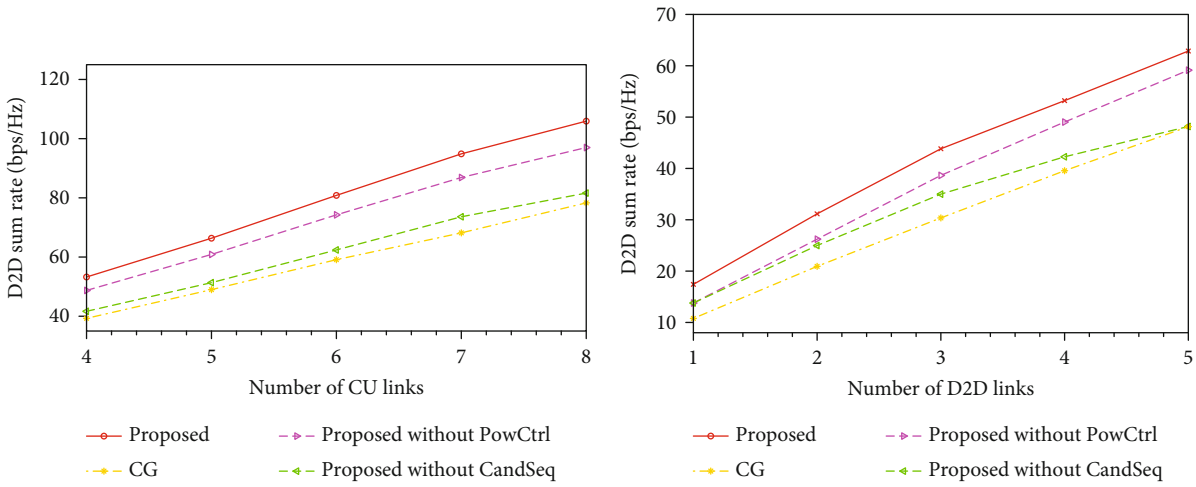
Figures 5(a) and 5(b) show the relationships of the D2D (the system) transmission sum rate varying with CU rate threshold, respectively. It can be seen that the D2D (the system) transmission sum rate becomes smaller as the rate threshold of CU is increased. It is because that the number of D2D pairs accessing the cellular channel becomes smaller with the increment of the CU rate threshold, which leads to the decrement of the D2D transmission sum rate. Compared with the "MGWE" algorithm, the proposed algorithm has a higher transmission sum rate and is close to the "Exhaustive" method. The D2D and system transmission sum rate by using the "CG" algorithm does not decrease rapidly as the rate threshold of the CUs becomes larger. Compared with the "CG" algorithm, the D2D (the system) transmission sum rate obtained by using the proposed algorithm varies more rapidly as the rate threshold of the CUs is increased.

Figures 6(a) and 6(b) show the impact of power allocation and candidate sequence on D2D performance. The "Proposed without PowCtrl" indicates the proposed algorithm includes the optimization procedure of candidate sequence and each



(a) D2D transmission rate (b) System transmission rate

Figure 5: Effects of CUs' rate threshold on transmission rate.



(a) Number of CU links (b) Number of D2D links

Figure 6: Effects of the users' number on transmission rate.

D2D pair has a fixed transmit power. The "Proposed without CandSeq" means that the proposed coalition game algorithm with power allocation does not include the optimization procedure of the candidate sequence.

It can be seen that the D2D transmission sum rate increases as the number of the D2D pairs or the CUs becomes larger. The D2D transmission sum rate obtained by using the proposed algorithm is better than that by using the overlapping coalition game algorithm with random initialization. It can be seen that the performance of the "proposed" or the "Proposed without PowCtrl" algorithm is better than that of the "Proposed without CandSeq" algorithm. It means that the optimization procedure of the candidate sequence in the algorithm can further improve the utility of the coalition structure and increase the D2D transmission sum rate. Moreover, the performance of the "proposed" algorithm is better than that of the "Proposed without PowCtrl" algorithm, which indicates that the appropriate power allocation can enhance the D2D transmission sum rate.

6. Conclusion

According to the analysis of the system model in many-to-many D2D communication, the resource allocation problem is formulated. An overlapping coalition game algorithm based on a candidate sequence is proposed to improve the D2D transmission sum rate. The preference sequence is adopted in the processing of coalition initialization. According to the preference sequence, a power allocation strategy is used to further improve the system utility. Simulation results show that the performance of the proposed algorithm including the optimization procedure of candidate sequence is better than that of the overlapping algorithm with random optimization. Compared to the "CG" and "MGWE" algorithms, when the number of cellular users is 8, and the number of D2D users is 4, the D2D transmission sum rate of the proposed algorithm is improved nearly 24% and 40%, respectively. Moreover, the system transmission rate has been improved nearly 25% and 35%, respectively.

Abbreviations

D2D: Device-to-device
CU: Cellular user
QoS: Quality of service
CSI: Channel state information
SINR: Signal to interference noise ratio.

Data Availability

The authors declare that all data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the National Key Research and Development Program of China under Grant No. 2018YFB2100100.

References

[1] S. Helal, F. C. Delicato, C. B. Margi, S. Misra, and M. Endler, "Challenges and opportunities for data science and machine learning in iot systems – a timely debate: part 1," *IEEE Internet of Things Magazine*, vol. 4, no. 1, pp. 46–52, 2021.

[2] Y. Shi, Y. Zhang, and J. Chen, "Cross-layer QoS enabled SDN-like publish/subscribe communication infrastructure for IoT," *China Communications*, vol. 17, no. 3, pp. 149–167, 2020.

[3] B. Yu, X. Zhang, F. Palmieri, E. Creignou, and I. You, "A deep learning approach for maximum activity links in D2D communications," *Sensors*, vol. 19, no. 13, p. 2941, 2019.

[4] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: a comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[5] Y. J. Hwang, J. Park, K. W. Sung, and S. L. Kim, "On the throughput gain of device-to-device communications," *ICT Express*, vol. 1, no. 2, pp. 67–70, 2015.

[6] S. Driouech, E. Sabir, and M. Bennis, "D2D mobile relaying for efficient throughput-reliability delivering in 5G," *2020 IEEE International Conference on Communications*, 2020, 7 pages, Dublin, Ireland, June 2020.

[7] H. Ji-Ai, J. Lu, L. Xu, and W. Chen, "Throughput maximization for multiple D2D group communications underlaying cellular networks," *Wireless Communications and Mobile Computing*, vol. 2020, 10 pages, 2020.

[8] M. Salehi, A. Mohammadi, and M. Haenggi, "Analysis of D2D underlaid cellular networks: SIR meta distribution and mean local delay," *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 2904–2916, 2017.

[9] G. Fodor, E. Dahlman, G. Mildh et al., "Design aspects of network assisted device-to-device communications," *IEEE Communications Magazine*, vol. 50, no. 3, pp. 170–177, 2012.

[10] J. Liu, Y. Kawamoto, H. Nishiyama, N. Kato, and N. Kadowaki, "Device-to-device communications achieve efficient load balancing in LTE-advanced networks," *IEEE Wireless Communications*, vol. 21, no. 2, pp. 57–65, 2014.

[11] R. Gour and A. Tyagi, "Cluster oriented resource allocation and power optimisation for D2D network in cellular communications," *IET Networks*, vol. 9, no. 4, pp. 170–179, 2020.

[12] J. Sun, Z. Zhang, H. Xiao, and C. Xing, "Uplink interference coordination management with power control for D2D underlaying cellular networks: modeling, algorithms, and analysis," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8582–8594, 2018.

[13] Y. Li, D. Jin, J. Yuan, and Z. Han, "Coalitional games for resource allocation in the device-to-device uplink underlaying cellular networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 7, pp. 3965–3977, 2014.

[14] J. Hu, W. Heng, Y. Zhu, G. Wang, X. Li, and J. Wu, "Overlapping coalition formation games for joint interference management and resource allocation in D2D communications," *IEEE Access*, vol. 6, pp. 6341–6349, 2018.

[15] J. Zhao, Y. Liu, K. K. Chai, Y. Chen, and M. Elkashlan, "Many-to-many matching with externalities for device-to-device communications," *IEEE Wireless Communications Letters*, vol. 6, no. 1, pp. 138–141, 2016.

[16] F. Jiang, B. Wang, C. Sun, Y. Liu, and R. Wang, "Mode selection and resource allocation for device-to-device communications in 5G cellular networks," *China Communications*, vol. 13, no. 6, pp. 32–47, 2016.

[17] Y. Cai, C. Ke, Y. Ni, J. Zhang, and H. Zhu, "Power allocation for NOMA in D2D relay communications," *China Communications*, vol. 18, no. 1, pp. 61–69, 2021.

[18] J. Gui and Z. Kai, "Cellular throughput optimization by game-based power adjustment and outband D2D communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, no. 1, pp. 1–225, 2018.

[19] L. Zhou, Y. Wu, and H. Yu, "A two-layer, energy-efficient approach for joint power control and uplink–downlink channel allocation in D2D communication," *Sensors*, vol. 20, no. 11, p. 3285, 2020.

[20] Y. Sun, F. Wang, and Z. Liu, "Coalition formation game for resource allocation in D2D uplink underlaying cellular networks," *IEEE Communications Letters*, vol. 23, no. 5, pp. 888–891, 2019.

[21] P. R. Teja and P. K. Mishra, "Sealed bid single price auction model (SBSPAM)-based resource allocation for 5G networks," *Wireless Personal Communications*, vol. 116, no. 3, pp. 2633–2650, 2021.

[22] H. Chen, D. Wu, and Y. Cai, "Coalition formation game for green resource management in D2D communications," *IEEE Communications Letters*, vol. 18, no. 8, pp. 1395–1398, 2014.

[23] P. Kong, "Multicell D2D communications for hierarchical control of microgrid system," *IEEE Systems Journal*, vol. 15, no. 2, pp. 1929–1938, 2020.

[24] Z. Qian, H. U. Liangshuai, C. Tian, and X. Wang, "Research on D2D multi-multiplex communication resource blocks allocation algorithm based on unbalanced solution," *Journal of Electronics Information Technology*, vol. 41, no. 12, pp. 2810–2816, 2019.

[25] B. Zhang, X. Mao, J. Yu, and Z. Han, "Resource allocation for 5G heterogeneous cloud radio access networks with D2D communication: a matching and coalition approach," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5883–5894, 2018.

[26] J. Lee and J. H. Lee, "Performance analysis and resource allocation for cooperative D2D communication in cellular networks

with multiple D2D pairs," *IEEE Communications Letters*, vol. 23, no. 5, pp. 909–912, 2019.

[27] X. Li, Y. Sun, L. Zhou, Y. Xu, and S. Zhou, "A resource allocation scheme based on predatory search algorithm for ultra-dense D2D communications," *Wireless Networks*, vol. 281, no. 7, pp. 1–9, 2019.

[28] L. Zhao, H. Wang, and X. Zhong, "Interference graph based channel assignment algorithm for D2D cellular networks," *IEEE Access*, vol. 6, pp. 3270–3279, 2018.

[29] S. Dominic and L. Jacob, "Distributed interference aware admission control and resource allocation for underlaying D2D communications in cellular networks," *Sadhana*, vol. 44, no. 6, pp. 1–5, 2019.

[30] D. Tsolkas, E. Liotou, N. Passas, and L. Merakos, "A graph-coloring secondary resource allocation for D2D communications in LTE networks," *2012 IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2012, pp. 56–60, Barcelona, Spain, Sept. 2012.

[31] H. Zhang, Y. Liao, and L. Song, "D2D-U: device-to-device communications in unlicensed bands for 5G system," *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3507–3519, 2017.

[32] W. Wei, Q. Wang, L. Yang, and X. Hu, "Auction based energy-efficient resource allocation and power control for device-to-device underlay communication," *2016 IEEE 84th Vehicular Technology Conference*, 2016, pp. 1–6, Montreal, QC, Canada, Sept. 2016.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8669941, 12 pages
https://doi.org/10.1155/2022/8669941

Research Article

SKIA-SH: A Symmetric Key-Based Improved Lightweight Authentication Scheme for Smart Homes

Bander A. Alzahrani,[1] **Ahmed Barnawi**,[1] **Abdullah Albarakati**,[1] **Azeem Irshad**,[2] **Muhammad Asghar Khan**,[3] **and Shehzad Ashraf Chaudhry**[4]

[1]*Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*
[2]*Department of Computer Science & Software Engineering, International Islamic University, Islamabad, Pakistan*
[3]*Hamdard Institute of Engineering & Technology, Islamabad 44 000, Pakistan*
[4]*Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey*

Correspondence should be addressed to Shehzad Ashraf Chaudhry; ashraf.shehzad.ch@gmail.com

Received 23 November 2021; Accepted 13 January 2022; Published 12 February 2022

Academic Editor: Hasan Ali Khattak

Being one of the finest applications of the IoT, smart homes (SHs) with an aim to improve quality of life are taking over the traditional lifestyles. The entities within a SH communicate with each other and with the environment including the users to transform daily life seamlessly enjoyable and easy. However, owing to the public communication infrastructure, the advantages of SH are subject to security and privacy issues. Recently, Yu et al. presented a privacy and security solution for SH environment. The scheme of Yu et al. is based on lightweight symmetric key functions. Although the scheme of Yu et al. exhibits the lightweight property, it is proven in this paper that their scheme cannot provide mutual authentication due to a crucial design fault. An improved scheme using symmetric key functions for SH (SKIA-SH) is proposed in this paper. The security of the proposed scheme is furnished through formal BAN logic followed by brief discussion on security attribute provision of the proposed SKIA-SH. The comparisons show that the proposed SKIA-SH provides the required security on the cost of slight increase in computation and communication costs. The simulation results show that the SKIA-SH completes an authentication round by exchanging 216 bytes in just 5.34 ms.

1. Introduction

The smart home (SH) is an emerging concept, and with the aid of 6G/IoT smart infrastructure, the SH concept is gradually overtaking traditional living styles. SH is a communication setup among the daily useable devices like lightbulbs, televisions, door lock, monitoring cameras, washing machines, and so on. The smart devices (SDs) within a SH interact with each other and with the users to provide seamless services and for transforming daily life more and more easy and enjoyable. The services include automatic door lock and unlock, switching on and off the lights and air conditioners, suspicious activity alarming, etc. In addition, the SH concept can be very useful for patients and elderly people through activity and health-related monitoring and support. The SDs in a SH communicate over the wireless insecure channel and the public Internet. Due to communication over insecure channels, the advantages of the SH are subject to several privacy and security issues [1, 2]. Such security and privacy issues can enable an entity with malicious intentions also called as an attacker to expose user-related sensitive data including the daily routines, habits, and so on, and this information can be used with wicked intentions. In addition, the SDs are lightweight devices, and deploying public key-based infrastructure (PKI) is not a viable solution for the SH environments as PKI can pose high computation and communication costs on the low powered SDs [3–5]. Therefore, symmetric key-based authentication schemes suit the SH environments [6–8].

Recently, many authentication schemes were proposed using symmetric and PKI-based cryptographic primitives. Some of the recently proposed schemes were proposed to

secure smart home (SH) environments [9, 10]. In 2021, Ali et al. explained the pitfalls of clogging attack and designed an elliptic curve-based authentication scheme to resist clogging attack. Physical capturing is also among the crucial class of attacks [11], and physical capturing of a smart device can lead to exposure of private information of the device and it can also lead to exposure of related and communicative devices present in the smart IoT environments. Irshad et al. [12] also proved that the authentication scheme of Tsai and Lo [13] lacks required security against server forgery and impersonation attack. Moreover, Maitra et al. [14] also proposed an improvement over Lee et al.'s ElGamal-based authentication method [15]. In 2020, Ali Khan et al. [16] and Wei et al. [17] proposed two separate methods to secure smart grid and USB mass storage communication, respectively. However, these schemes were proved insecure and impractical in [18, 19]. Using elliptic curve cryptography (ECC), Vaidya et al. [9] presented their designed authentication scheme for SH. Despite their claim of security and lightweight property, the scheme presented in [9] is prone to several attacks including user forgery, privileged insider (PI), and password guessing (PG) attacks. Santoso and Vun [10] also proposed an authentication scheme for smart devices in the SH environments. Yu et al. [20] in their recent study claimed that the scheme presented in [10] has weaknesses against PI and stolen verifier (SV) attacks. Wazid et al. [21] also proposed an authentication scheme, and in 2019, Lyu et al. [22] claimed that Wazid et al.'s scheme is prone to desynchronization and related attacks. Another authentication scheme was also proposed by Lyu et al. [22]. After that, in the same year, Shuai et al. [23] presented another authentication scheme. The scheme of Shuai et al. was also structured upon ECC, and despite the claims presented in [23], in 2021, Kaur and Kumar [24] simulated the insecurity of the scheme of Shuai et al. against PI, replay, session key exposure, and related attacks. Kaur and Kumar [24] also presented an improved authentication scheme using ECC and claimed that their ECC-based scheme not only extends security but is also lightweight. However, in 2021, Yu et al. [20] proved that the scheme presented by Kaur and Kumar is prone to several weaknesses including exposure of session key and insecurity against impersonation attack. Moreover, Yu et al. also claimed that the scheme of Kaur and Kumar cannot provide mutual authentication.

1.1. Motivations and Contributions. Very recently in 2020, Yu et al. [20] presented their designed authentication scheme for smart home. The scheme of Yu et al. was built on lightweight symmetric key operations (SKOs). They claimed that due to avoidance of PKI and usage of only SKO, their scheme not only is lightweight but also provides privacy and security to the SH devices. In this study, we analyze that in contrast to the claims of Yu et al., the scheme of Yu et al. cannot extend authentication among SH devices due to a crucial design flaw of their scheme. Hence, their scheme is not practical, and to fill the gap, we proposed a symmetric key-based improved lightweight authentication scheme for smart homes (SKIA-SH).

1.2. System Architecture. A standard smart home (SH) as adopted from Yu et al.'s scheme [20] is depicted in Figure 1. The authentication entities in a SH network consist of user/s with mobile device/s, the gateway, and the smart devices (SDs). The users can control the SDs remotely, and before deployment, the registration authority registers users and SDs and deploys secret and public parameters on the memory of users and SDs. The user monitors the working of SDs, and SDs communicate with user/s through the facilitation of gateways. The entities (smart devices) of a SH network are equipped with Wi-Fi and connect with each other and with gateway through public wireless channel. Moreover, the user connects with smart devices through gateway, and the channel used between a user and a gateway is the public Internet, which allows the communication administered remotely and globally. The communication of the entities of a SH through public wireless and Internet channels calls for a secure channel through authentication and key establishment between user/s and the gateway. The authentication and key exchange protect the information exchange through public wireless channel.

1.3. Adversarial Model. In a smart home (SH) communication architecture, one or more users communicate with smart devices (SDs) through facilitation of the gateway and on the public wireless channel. Therefore, SH is an attractive environment for malicious adversaries to launch several attacks including impersonation and forgery. As per the common adversary model DY [25], an adversary has the capabilities to listen to the channel and can read, modify, and jam a message exchanged between the entities of the SH [26, 27]. Moreover, the adversary can generate and send a fake message to any entity, whereas the current de facto adversary model CY [28] is adopted in this paper and in several other proposals [29, 30]. The CK adversary model considers a more strong attacker, where in addition to adversarial capabilities of DY model, the attacker can either compromise the long-term or short-term secrets both but not at the same time [31, 3232]. The CY model suggests to construct the session keys using both the long and short-term secrets and the session keys should be independent to each other.

2. Revisiting Yu et al.'s Scheme

In the following subsections, we revisit the scheme of Yu et al. [20], which provides the authentication among the IoT-based smart devices and the user with the help of gateway. The scheme is based on lightweight symmetric key operations. Before moving to the description of the Yu et al.' scheme, Table 1 is provided to explain the notations used throughout the whole paper.

2.1. Initialization. During manufacturing, the TP generates a private key K_{GR} and stores it in the memory of GK_r. Moreover, all the IoT-based smart devices SD_q: $\{q = 1, 2, \ldots, n\}$ are assigned unique identities ID_{sq}: $\{q = 1, 2 \ldots n\}$. The TP also generates and stores the secret keys

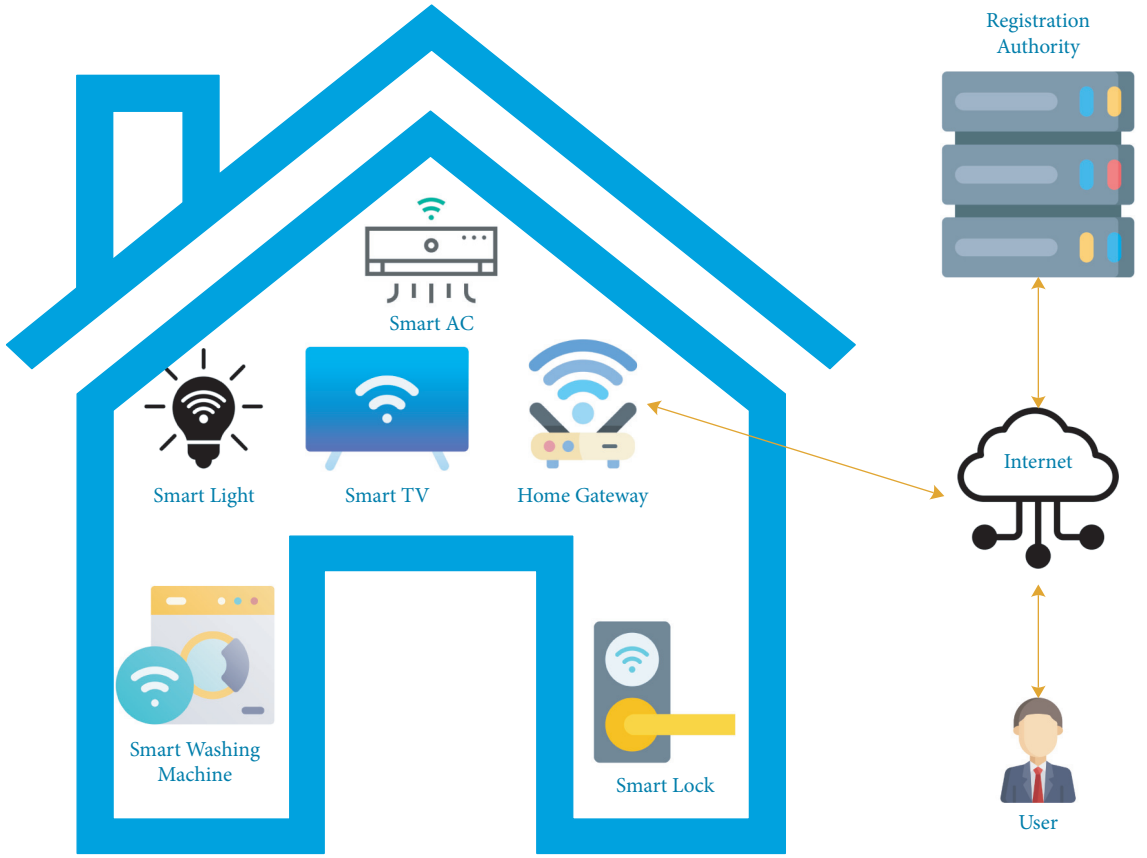


Figure 1: Smart home environment.

Table 1: Symbol guide.

Symbols	Explanations
GK_r	Gateway
SD_q	IoT device
U_p	p^{th} user
TP	Trusted third party
ID_{sq}	Identity of SD_q
ID_{up}	Identity of U_p
GID_{gr}	Identity of GK_r
β_{up}, γ_{up}	Fuzzy parameters
K_{GR}	Private key of GK_r
K_{UP}	Private key of U_p
K_{SQ}	Private key of SD_q
X_{pr}	Shared secret key among U_p and GK_r
X_{qr}	Shared secret key among SD_q and GK_r
$\oplus, H(.)$	XOR and hash operations

K_{SQ}: $\{q = 1, 2 \ldots n\}$ and stores it in the memory of each if SD_q: $\{q = 1, 2 \ldots n\}$.

2.2. User Registration. To initiate a registration request, the user U_p generates α_{up}, selects ID_{up} and PW_{up}, computes $Gen(Bio_{up}) = (\gamma_{up}, \beta_{up})$, $RID_{up} = h(ID_{up} \| \gamma_{up})$, and $RPW_{up} = h(PW_{up} \| \gamma_{up})$, and sends $\{RID_{up}, RPW_{up}, \alpha_{up}\}$ to TP through a private channel. The TP computes $X_{pr} = h(RID_{up} \| K_{GR} \| \alpha_{up})$, $A_1 = X_{PR} \oplus h(\alpha_{up} \| RPW_{up})$ and sends X_{pr} to GK_r. The GK_r now computes $L_{up} = h(GID_{gr} \| K_{GR}) \oplus X_{pr}$. The GK_r stores L_{up} into its own memory and the TP sends A_1 to U_p. U_p now computes $K_{UP} = h(ID_{up} \| PW_{up} \| \gamma_{up})$, $A_2 = E_{K_{UP}}(A_1)$, $A_3 = \alpha_{up} \oplus h(RID_{up} \| RPW_{up})$, and $A_4 = h(RID_{up} \| RPW_{up} \| \alpha_{up})$ and deletes A_1 and stores $\{A_2, A_3, A_4\}$ in the memory of SD_q.

2.3. Smart Device Registration. A SD_q generates α_{sq}, computes $PID_{sq} = h(SD_q \| \alpha_{sq})$, and sends the duo $\{PID_{sq}, \alpha_{sq}\}$ to TP. The TP now computes $X_{pr} = h(PID_{sq} \| K_{GR} \| \alpha_{sq})$ and stores $\{PID_{sq}, \alpha_{uq}\}$ in GK_r's database and sends X_{pr} to SD_q. The SD_q now computes $B_1 = h(SID_{sq} \| K_{SQ}) \oplus \alpha_{sq}$ and $B_2 = h(K_{SQ} \| \alpha_{sq}) \oplus X_{qr}$ and stores B_1, B_2 in its own memory.

2.4. Authentication. As summarized in Figure 2, the user U_p initiates authentication phase by entering the pair of his own identity and password $\{ID_{up}, PW_{up}\}$. The user terminal device computes $\gamma_{up} = Rep(Bio_{up}, \beta_{up})$, $RID_{up} = h(ID_{up} \| \gamma_{up})$, $RPW_{up} = h(PW_{up} \| \gamma_{up})$, and $K_{UP} = h(ID_{up} \| PW_{up} \| \gamma_{up})$. Now U_p extracts A_2, using K_{UP} decrypts A_2, and gets $A_1 = D_{K_{UP}}(A_2)$. U_p further computes $\alpha_{up} = A_3 \oplus h(RID_{up} \| RPW_{up})$ and $X_{pr} = A_1 \oplus h(\alpha_{up} \| RPW_{up})$. Now, U_p checks the equality $A_4 =_? h(RID_{up} \| RPW_{up} \| \alpha_{up})$, and if it holds, U_p selects/generates $\{T_1, r_{up}\}$ and proceeds with the authentication phase through execution of the following steps:

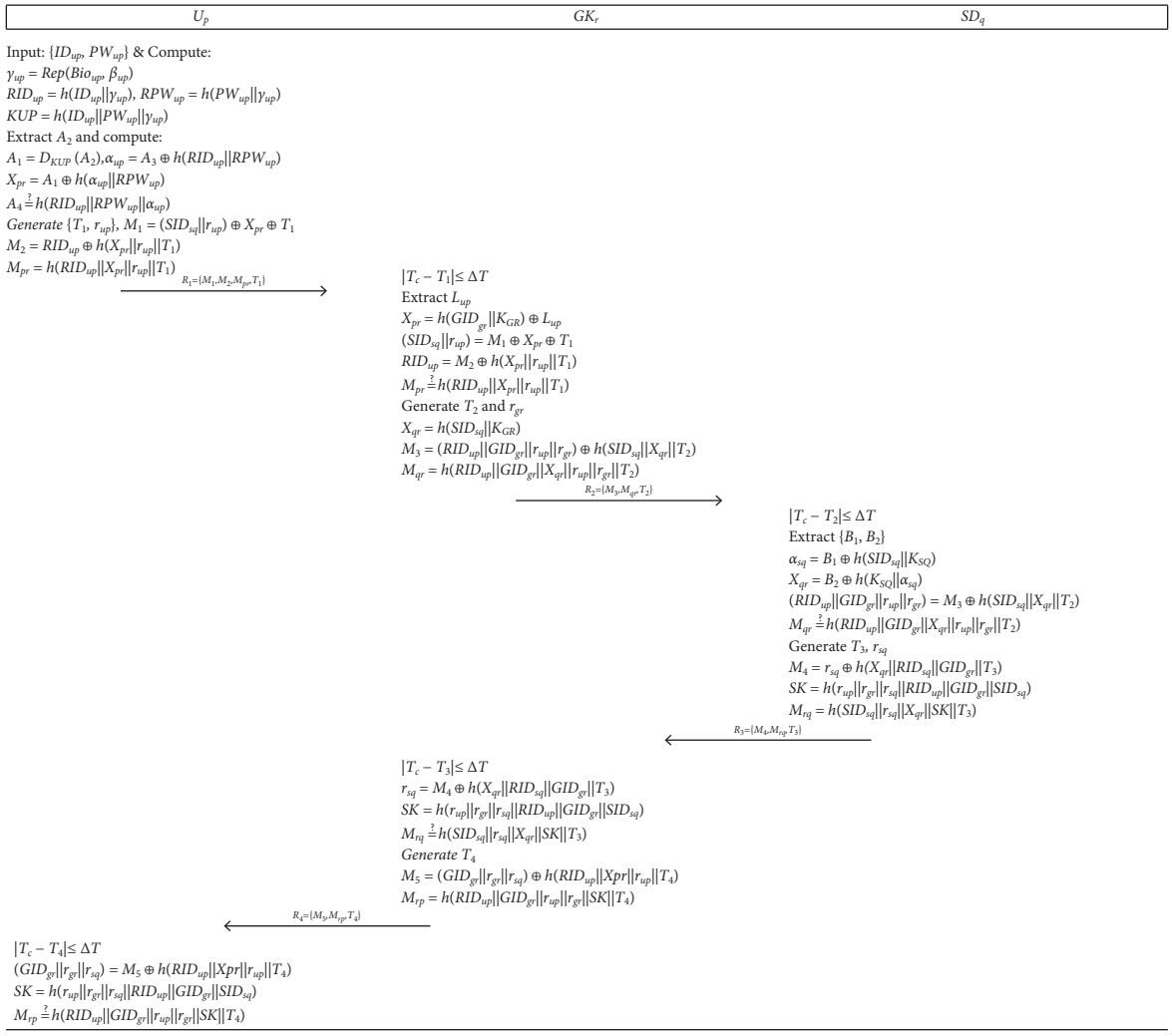


Figure 2: The scheme of Yu et al.

AY 1: $\mathbf{U_p} \longrightarrow \mathbf{GK_r}$: $\mathbf{R}_1 = \{\mathbf{M}_1, \mathbf{M}_2, \mathbf{M_{pr}}, \mathbf{T}_1\}$.

U_p computes $M_1 = (\mathrm{SID_{sq}} \| r_{\mathrm{up}}) \oplus X_{\mathrm{pr}} \oplus T_1$, $M_2 = \mathrm{RID_{up}} \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$, and $M_{\mathrm{pr}} = h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \mathrm{Vert} | r_{\mathrm{up}} \| T_1)$ and sends request message $R_1 = \{M_1, M_2, M_{pr}, T_1\}$ to GK_r.

AY 2: $\mathbf{GK_r} \longrightarrow \mathbf{SD_q}$: $\mathbf{R}_2 = \{\mathbf{M}_3, \mathbf{M_{qr}}, \mathbf{T}_2\}$.

GK_r on receiving $R_1 = \{M_1, M_2, M_{pr}, T_1\}$ checks $|T_c - T_1| \leq \Delta T$, where T_c is current timestamp recorded at GK_r and ΔT is the allowable time delay. On the successful validation of timestamp, GK_r extracts L_{up} and computes $X_{\mathrm{pr}} = h(\mathrm{GID_{gr}} \| K_{\mathrm{GR}}) \oplus L_{\mathrm{up}}$, $(\mathrm{SID_{sq}} \| r_{\mathrm{up}}) = M_1 \oplus X_{\mathrm{pr}} \oplus T_1$, and $\mathrm{RID_{up}} = M_2 \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$. Now, GK_r checks validity of $M_{pr} =_? h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$, and if it holds, GK_r selects/generates $\{T_2, r_{gr}\}$. Now, GK_r computes $X_{\mathrm{qr}} = h(\mathrm{SID_{sq}} \| K_{\mathrm{GR}})$, $M_3 = (\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}}) \oplus h(\mathrm{SID_{sq}} \| X_{\mathrm{qr}} \| T_2)$, and $M_{\mathrm{qr}} = h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| X_{\mathrm{qr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}} \| T_2)$. GK_r completes this step by sending $R_2 = \{M_3, M_{qr}, T_2\}$ to SD_q.

AY 3: $\mathbf{SD_q} \longrightarrow \mathbf{GK_r}$: $\mathbf{R}_3 = \{\mathbf{M}_4, \mathbf{M_{rq}}, \mathbf{T}_3\}$.

SD_q on receiving $R_2 = \{M_3, M_{qr}, T_2\}$ checks $|T_c - T_2| \leq \Delta T$, and on successful validation of timestamp, SD_q extracts $\{B_1, B_2\}$ from its memory and computes $\alpha_{\mathrm{sq}} = B_1 \oplus h(\mathrm{SID_{sq}} \| K_{\mathrm{SQ}})$, $X_{\mathrm{qr}} = B_2 \oplus h(K_{\mathrm{SQ}} \| \alpha_{\mathrm{sq}})$, and $(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}}) = M_3 \oplus h(\mathrm{SID_{sq}} \| X_{\mathrm{qr}} \| T_2)$. Now, SD_q checks validity of $M_{qr} =_? h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| X_{\mathrm{qr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}} \| T_2)$, and if it holds, SD_q selects/generates $\{T_3, r_{\mathrm{sq}}\} M_4 = r_{\mathrm{sq}} \oplus h(X_{\mathrm{qr}} \| \mathrm{RID_{sq}} \| \mathrm{GID_{gr}} \| T_3)$, $\mathrm{SK} = h(r_{\mathrm{up}} \| r_{\mathrm{gr}} \| r_{\mathrm{sq}} \| \mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| \mathrm{SID_{sq}})$, and $M_{\mathrm{rq}} = h(\mathrm{SID_{sq}} \| r_{\mathrm{sq}} \| X_{\mathrm{qr}} \| \mathrm{SK} \| T_3)$. SD_q now sends $R_3 = \{M_4, M_{rq}, T_3\}$ to GK_r.

AY 4: $\mathbf{GK_r} \longrightarrow \mathbf{U_p}$: $\mathbf{R}_4 = \{\mathbf{M}_5, \mathbf{M_{rp}}, \mathbf{T}_4\}$.

GK_r on receiving $R_3 = \{M_4, M_{rq}, T_3\}$ checks $|T_c - T_3| \leq \Delta T$, and on successful validation of timestamp, GK_r computes $r_{\mathrm{sq}} = M_4 \oplus h(X_{\mathrm{qr}} \| \mathrm{RID_{sq}} \| \mathrm{GID_{gr}} \| T_3)$ and $\mathrm{SK} = h(r_{\mathrm{up}} \| r_{\mathrm{gr}} \| r_{\mathrm{sq}} \| \mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| \mathrm{SID_{sq}})$. Now, GK_r checks validity of $M_{rq} =_? h(\mathrm{SID_{sq}} \| r_{\mathrm{sq}} \| X_{\mathrm{qr}} \| \mathrm{SK} \| T_3)$. On successful validation, GK_r generates $\{T_4\}$ and computes $M_5 = (\mathrm{GID_{gr}} \| r_{\mathrm{gr}} \| r_{\mathrm{sq}}) \oplus h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_4)$ and $M_{rp} = h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}} \| \mathrm{SK} \| T_4)$. Now, GK_r sends $R_4 = \{M_5, M_{rp}, T_4\}$ to U_p.

AY 5: U_p on receiving $R_4 = \{M_5, M_{rp}, T_4\}$ checks $|T_c - T_4| \leq \Delta T$, and on successful validation of timestamp, U_p computes $(\mathrm{GID_{gr}} \| r_{\mathrm{gr}} \| r_{\mathrm{sq}}) = M_5 \oplus h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_4)$ and session key $\mathrm{SK} = h(r_{\mathrm{up}} \| r_{\mathrm{gr}} \| r_{\mathrm{sq}} \| \mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| \mathrm{SID_{sq}})$. U_p checks the validity of $M_{rp} =_? h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}} \| \mathrm{SK} \| T_4)$. On successful validation, U_p considers SD_q and GK_r authenticates and keeps SK as the session key for future secure communication.

3. Weaknesses of Yu et al.'s Scheme

In this section, it is shown that the scheme of Yu et al. [20] cannot provide mutual authentication among the smart devices (SDs) of a smart home (SH). Specifically, in Yu et al.'s scheme, once GK_r receives the authentication request, it cannot recognize the user requesting the authentication. Therefore, the process may stop here and the scheme of Yu et al. cannot complete a round of authentication process. The following explanation of an authentication round of the scheme of Yu et al. can clarify the scheme's incorrectness:

(1) U_p first completes a login by entering his password, identity, and biometrics, and the user device computes and sends request message $R_1 = \{M_1, M_2, M_{pr}, T_1\}$ to GK_r.

$$\begin{aligned} M_1 &= (\mathrm{SID_{sq}} \| r_{\mathrm{up}}) \oplus X_{\mathrm{pr}} \oplus T_1, \\ M_2 &= \mathrm{RID_{up}} \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1), \\ M_{\mathrm{pr}} &= h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1). \end{aligned} \tag{1}$$

Now, U_p sends $R_1 = \{M_1, M_2, M_{pr}, T_1\}$ to GK_r.

(2) GK_r on receiving $R_1 = \{M_1, M_2, M_{pr}, T_1\}$, checks $|T_c - T_1| \leq \Delta T$. On successful validation of T_1, GK_r extracts L_{up} from its database and computes

$$X_{\mathrm{pr}} = h(\mathrm{GID_{gr}} \| K_{\mathrm{GR}}) \oplus L_{\mathrm{up}}, \tag{2}$$

$$(\mathrm{SID_{sq}} \| r_{\mathrm{up}}) = M_1 \oplus X_{\mathrm{pr}} \oplus T_1, \tag{3}$$

$$\mathrm{RID_{up}} = M_2 \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1). \tag{4}$$

(3) GK_r computes the shared key X_{pr} through equation (2), and for this, GK_r needs to extract L_{up}, from the database stored on the memory of GK_r. The database has the entries of the form $\{\mathrm{ID_{up}}, L_{\mathrm{up}}\}$: p: $1, 2 \ldots m$, if there are m users. To extract L_{up} from the database, GK_r first needs to recognize the specific user U_p with identity $\mathrm{ID_{up}}$. However, GK_r does not recognize U_p because it does not receive identity or any other user-related information in the request message R_1. Therefore, GK_r cannot extract L_{up} and equations (2), (3), and (4) cannot be resolved. Due to this incorrectness, the scheme of Yu et al. cannot complete even a round of authentication process.

4. SKIA-SH: Proposed Scheme

In this section, we present the improved scheme over Yu et al.'s scheme. For designing improved scheme, we take the initialization phase of Yu et al. as it was designed by Yu et al. Furthermore, the smart device registration phase is also taken as it is. The proposed scheme amends some steps in user registration and authentication phases to provide a scalable and correct mechanism for the provision of secure channel among a user and a smart device. The proposed symmetric key-based improved authentication scheme for smart homes (SKIA-SH) is described below.

4.1. SKIA-SH: User Registration. To initiate a registration request, the user U_p generates α_{up}, selects $\mathrm{ID_{up}}$ and $\mathrm{PW_{up}}$, computes $\mathrm{Gen}(\mathrm{Bio_{up}}) = (\gamma_{\mathrm{up}}, \beta_{\mathrm{up}})$, $\mathrm{RID_{up}} = h(\mathrm{ID_{up}} \| \gamma_{\mathrm{up}})$, and $\mathrm{RPW_{up}} = h(\mathrm{PW_{up}} \| \gamma_{\mathrm{up}})$ and sends $\{\mathrm{RID_{up}}, \mathrm{RPW_{up}}, \alpha_{\mathrm{up}}\}$ to TP through a private channel. TP computes $X_{\mathrm{pr}} = h(\mathrm{RID_{up}} \| K_{\mathrm{GR}} \| \alpha_{\mathrm{up}})$ and $A_1 = X_{\mathrm{PR}} \oplus h(\alpha_{\mathrm{up}} \| \mathrm{RPW_{up}})$ and sends X_{pr} to GK_r. GK_r now computes $L_{\mathrm{up}} = h(\mathrm{GID_{gr}} \| K_{\mathrm{GR}}) \oplus X_{\mathrm{pr}}$ and $\mathrm{PID_{up}} = h(\mathrm{ID_{up}} \| \alpha_{\mathrm{up}} \| X_{\mathrm{pr}})$. GK_r stores L_{up} and $\mathrm{PID_{up}} = h(\mathrm{ID_{up}} \| \alpha_{\mathrm{up}} \| X_{\mathrm{pr}})$ into its own memory, and TP sends $\{A_1, \mathrm{PID_{up}}\}$ to U_p. U_p now computes $K_{\mathrm{UP}} = h(\mathrm{ID_{up}} \| \mathrm{PW_{up}} \| \gamma_{\mathrm{up}})$, $A_2 = E_{K_{\mathrm{UP}}}(A_1)$, $A_3 = \alpha_{\mathrm{up}} \oplus h(\mathrm{RID_{up}} \| \mathrm{RPW_{up}})$, and $A_4 = h(\mathrm{RID_{up}} \| \mathrm{RPW_{up}} \| \alpha_{\mathrm{up}})$, deletes A_1, and stores $\{A_2, A_3, A_4, \mathrm{PID_{up}}\}$ in the memory of SD_q.

4.2. SKIA-SH: Authentication. The user U_p initiates authentication phase as shown in Figure 3, by entering the pair of his own identity and password $\{\mathrm{ID_{up}}, \mathrm{PW_{up}}\}$. The user terminal device computes $\gamma_{\mathrm{up}} = \mathrm{Rep}(\mathrm{Bio_{up}}, \beta_{\mathrm{up}})$, $\mathrm{RID_{up}} = h(\mathrm{ID_{up}} \| \gamma_{\mathrm{up}})$, $\mathrm{RPW_{up}} = h(\mathrm{PW_{up}} \| \gamma_{\mathrm{up}})$, and $K_{\mathrm{UP}} = h(\mathrm{ID_{up}} \| \mathrm{PW_{up}} \| \gamma_{\mathrm{up}})$. Now U_p extracts A_2, using K_{UP} decrypts A_2, and gets $A_1 = D_{K_{\mathrm{UP}}}(A_2)$. U_p further computes $\alpha_{\mathrm{up}} = A_3 \oplus h(\mathrm{RID_{up}} \| \mathrm{RPW_{up}})$ and $X_{\mathrm{pr}} = A_1 \oplus h(\alpha_{\mathrm{up}} \| \mathrm{RPW_{up}})$. Now, U_p checks the equality $A_4 =_? h(\mathrm{RID_{up}} \| \mathrm{RPW_{up}} \| \alpha_{\mathrm{up}})$, and if it holds, U_p selects/generates $\{T_1, r_{\mathrm{up}}\}$ and proceeds with the authentication phase through execution of the following steps:

AP 1: $\mathbf{U_p} \longrightarrow \mathbf{GK_r}$: $\mathbf{R_1} = \{\mathbf{M_1}, \mathbf{M_2}, \mathbf{M_{pr}}, \mathbf{T_1}\}$.

U_p computes $M_1 = (\mathrm{SID_{sq}} \| r_{\mathrm{up}}) \oplus X_{\mathrm{pr}} \oplus T_1$, $M_2 = \mathrm{RID_{up}} \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$, and $M_{\mathrm{pr}} = h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \mathrm{Vert} | r_{\mathrm{up}} \| T_1)$ and sends request message $R_1 = \{M_1, M_2, M_{\mathrm{pr}}, \mathrm{PID_{up}}, T_1\}$ to GK_r.

AP 2: $\mathbf{GK_r} \longrightarrow \mathbf{SD_q}$: $\mathbf{R_2} = \{\mathbf{M_3}, \mathbf{M_{qr}}, \mathbf{T_2}\}$.

GK_r on receiving $R_1 = \{M_1, M_2, M_{\mathrm{pr}}, \mathrm{PID_{up}}, T_1\}$ checks $|T_c - T_1| \leq \Delta T$, where T_c is current timestamp recorded at GK_r and ΔT is the allowable time delay. On successful validation of timestamp, GK_r, extracts L_{up} as per the $\mathrm{PID_{up}}$ from its database where the entries are of the form $\{\mathrm{PID_{up}}, \mathrm{ID_{up}}, L_{\mathrm{up}}\}$ and computes $X_{\mathrm{pr}} = h(\mathrm{GID_{gr}} \| K_{\mathrm{GR}}) \oplus L_{\mathrm{up}}$, $(\mathrm{SID_{sq}} \| r_{\mathrm{up}}) = M_1 \oplus X_{\mathrm{pr}} \oplus T_1$, and $\mathrm{RID_{up}} = M_2 \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$. Now, GK_r checks validity of $M_{pr} =_? h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$, and if it holds, GK_r selects/

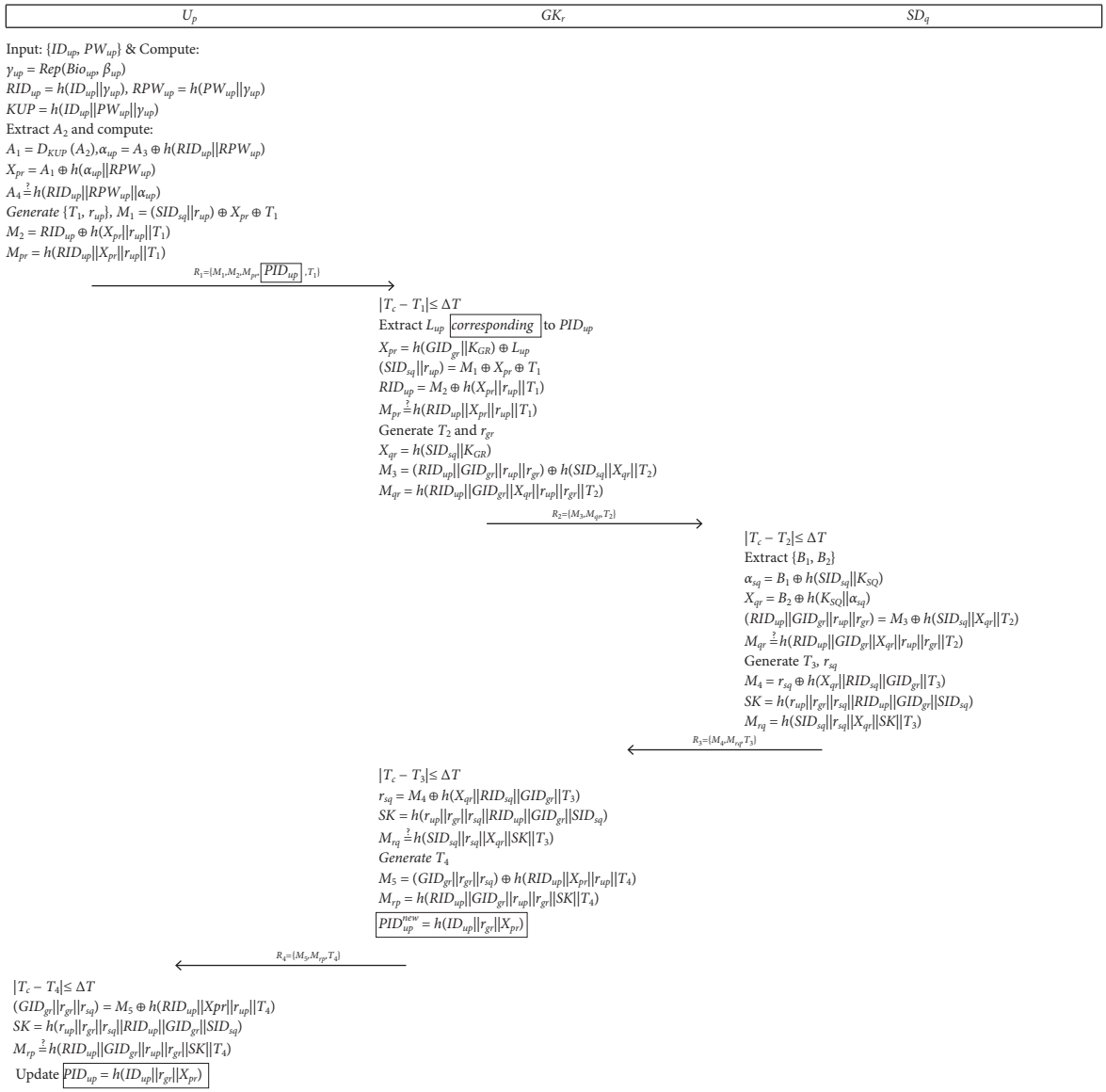


Figure 3: SKIA-SH: the proposed scheme.

generates $\{T_2, r_{gr}\}$. Now, GK_r computes $X_{qr} = h(\mathrm{SID_{sq}} \| K_{GR})$, $M_3 = (\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{up} \| r_{gr}) \oplus h(\mathrm{SID_{sq}} \| X_{qr} \| T_2)$, and $M_{qr} = h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| X_{qr} \| r_{up} \| r_{gr} \| T_2)$. GK_r completes this step by sending $R_2 = \{M_3, M_{qr}, T_2\}$ to SD_q.

AP 3: $\mathbf{SD_q} \longrightarrow \mathbf{GK_r}$: $\mathbf{R}_3 = \{\mathbf{M}_4, \mathbf{M_{rq}}, \mathbf{T}_3\}$.

SD_q on receiving $R_2 = \{M_3, M_{qr}, T_2\}$ checks $|T_c - T_2| \leq \Delta T$, and on successful validation of timestamp, SD_q extracts $\{B_1, B_2\}$ from its memory and computes $\alpha_{sq} = B_1 \oplus h(\mathrm{SID_{sq}} \| K_{SQ})$, $X_{qr} = B_2 \oplus h(K_{SQ} \| \alpha_{sq})$, and $(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{up} \| r_{gr}) = M_3 \oplus h(\mathrm{SID_{sq}} \| X_{qr} \| T_2)$. Now, SD_q checks validity of $M_{qr} \stackrel{?}{=} h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| X_{qr} \| r_{up} \| r_{gr} \| T_2)$, and if it holds, SD_q selects/generates $\{T_3, r_{sq}\}$ $M_4 = r_{sq} \oplus h(X_{qr} \| \mathrm{RID_{sq}} \| \mathrm{GID_{gr}} \| T_3)$, $SK = h(r_{up} \| r_{gr} \| r_{sq} \| \mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| \mathrm{SID_{sq}})$, and $M_{rq} = h(\mathrm{SID_{sq}} \| r_{sq} \| X_{qr} \| SK \| T_3)$. SD_q now sends $R_3 = \{M_4, M_{rq}, T_3\}$ to GK_r.

AP 4: $\mathbf{GK_r} \longrightarrow \mathbf{U_p}$: $\mathbf{R}_4 = \{\mathbf{M}_5, \mathbf{M_{rp}}, \mathbf{T}_4\}$.

GK_r on receiving $R_3 = \{M_4, M_{rq}, T_3\}$ checks $|T_c - T_3| \leq \Delta T$, and on successful validation of timestamp, GK_r computes $r_{sq} = M_4 \oplus h(X_{qr} \| \mathrm{RID_{sq}} \| \mathrm{GID_{gr}} \| T_3)$ and $SK = h(r_{up} \| r_{gr} \| r_{sq} \| \mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| \mathrm{SID_{sq}})$. Now, GK_r checks validity of $M_{rq} \stackrel{?}{=} h(\mathrm{SID_{sq}} \| r_{sq} \| X_{qr} \| \mathrm{SK} \| T_3)$. On successful validation, GK_r generates $\{T_4\}$ and computes $M_5 = (\mathrm{GID_{gr}} \| r_{gr} \| r_{sq}) \oplus h(\mathrm{RID_{up}} \| X_{pr} \| r_{up} \| T_4)$, $M_{rp} = h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{up} \| r_{gr} \| \mathrm{SK} \| T_4)$ and $\mathrm{PID_{up}^{new}} = h(\mathrm{ID_{up}} \| r_{gr} \| X_{pr})$. GK_r stores $\mathrm{PID_{up}^{new}}$ in its database in some temporary variable alongside $\{\mathrm{PID_{up}}, \mathrm{ID_{up}}, L_{up}\}$, where

PID_{up} is the old identity. GK_r keeps identity pair $\{PID_{up}, PID_{up}^{new}\}$ until it receives next authentication to avoid any identity de-synchronization, and on next successful login, both identities are updated. Finally, GK_r sends $R_4 = \{M_5, M_{rp}, T_4\}$ to U_p.

AP 5: U_p on receiving $R_4 = \{M_5, M_{rp}, T_4\}$ checks $|T_c - T_4| \leq \Delta T$, and on successful validation of timestamp, U_p computes $(GID_{gr} \| r_{gr} \| r_{sq}) = M_5 \oplus h(RID_{up} \| X_{pr} \| r_{up} \| T_4)$ and session key $SK = h(r_{up} \| r_{gr} \| r_{sq} \| RID_{up} \| GID_{gr} \| SID_{sq})$. U_p checks the validity of $M_{rp} =_? h(RID_{up} \| GID_{gr} \| r_{up} \| r_{gr} \| SK \| T_4)$. On successful validation, U_p computes $PID_{up}^{new} = h(ID_{up} \| r_{gr} \| X_{pr})$ and updates PID_{up} with PID_{up}^{new} and considers SD_q and GK_r authenticates and keeps SK as the session key for future secure communication.

5. Formal Security Analysis through BAN

We present the formal security analysis of the proposed scheme through employing the Burrows–Abadi–Needham logic (BAN) logic [33]. In this BAN logic analysis, we discuss the security evaluation with an emphasis on mutual authenticity among legal participants, protection of session key, and the key distribution among the participants.

(i) $S| \equiv : X$the principle S believes X.

(ii) $S \triangleleft X$: S sees X.

(iii) $S| \sim X$: S once said X and believes that X is true.

(iv) $S| \Rightarrow X$: S has jurisdiction over X.

(v) $(\#(X))$: X is not replayed and is fresh.

(vi) (X, X'): X and X' are parts of a hash digest message.

(vii) $\langle X, X' \rangle_k$: X and X' are exchanged using mutually agreed key k.

(viii) $S \leftrightarrow_K S'$: the communication among S and S' is secured using K as the key.

Some rules that are used in the analysis are given below:

R_1: message meaning rule:

$$\frac{S| \equiv S \xrightarrow{K} S', S \triangleleft \langle X \rangle_{X'}}{S| \equiv S'| \sim X}. \tag{5}$$

R_2: nonce verification rule:

$$\frac{S| \equiv \#(X), S| \equiv S'| \sim X}{S| \equiv S'| \equiv X}. \tag{6}$$

Rule 3: jurisdiction rule:

$$\frac{S| \equiv S' \Rightarrow X, S| \equiv S'| \equiv X}{S| \equiv X}. \tag{7}$$

Rule 4: freshness conjunction rule:

$$\frac{S| \equiv \#(X)}{S| \equiv \#(X, X')}. \tag{8}$$

Rule 5: belief rule:

$$\frac{S| \equiv (X), S| \equiv (X')}{S| \equiv (X, X')}. \tag{9}$$

Rule 6: session key rule:

$$\frac{S| \equiv \#(X, S|) \equiv S' \equiv X}{S| \equiv S \leftrightarrow_K S'}. \tag{10}$$

(i) G-1: $GK_r| \equiv (GK_r \leftrightarrow_{SK} U_p)$.

(ii) G-2: $GK_r| \equiv U_p| \equiv (GK_r \leftrightarrow_{SK} U_p)$.

(iii) G-3: $U_p| \equiv (GK_r \leftrightarrow_{SK} U_p)$.

(iv) G-4: $U_p| \equiv GK_r| \equiv (GK_r \leftrightarrow_{SK} U_p)$.

(v) G-5: $SD_q| \equiv (SD_q \leftrightarrow_{SK} U_p)$.

(vi) G-6: $U_p| \equiv (SD_q \leftrightarrow_{SK} U_p)$.

The idealized form of the communication messages is given below:

(vii) R_1: $U_p \longrightarrow GK_r$: M_1, M_2, M_{pr}, T_1: $\{\langle SID_{sq}, r_{up}, T \rangle_{1X_{pr}}, \langle RID_{up} \rangle_{h(X_{pr}, r_{up}, T_1)}, (RID_{up}, \backslash\backslash r_{up}, T_1)_{X_{pr}}, T_1\}$.

(viii) R_2: $GK_r \longrightarrow SD_q$: M_3, M_{qr}, T_2: $\{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr} \rangle_{h(SID_{sq}, X_{qr}, T_2)}\}$.

(ix) R_3: $SD_q \longrightarrow GK_r$: M_4, M_{rq}, T_3: $\{\langle r_{sq} \rangle_{h(X_{qr}, RID_{sq}, GID_{gr}, T_3)}, (SID_{sq}, r_{sq}, X_{qr}, T_3)_{SK}, T_3\}$.

(x) R_4: $GK_r \longrightarrow U_p$: M_5, M_{rp}, T_4: $\{\langle GID_{gr}, r_{gr}, r_{sq} \rangle_{h(RID_{up}, X_{pr}, r_{up}, T_4)}, (RID_{up}, GID_{gr}, \backslash\backslash r_{up}, r_{gr}, T_4)_{SK}, T_4\}$.

To prove the model, we construct the following premises.

(xi) κ_1: $U_p| \equiv \#(T_1)$.

(xii) κ_2: $GK_r| \equiv \#T_2$.

(xiii) κ_3: $SD_q| \equiv \#T_3$.

(xiv) κ_4: $U_p| \equiv (U_p \leftrightarrow_{X_{Pr}} GK_r)$.

(xv) κ_5: $U_p| \equiv (U_p \leftrightarrow_{SK} SD_q)$.

(xvi) κ_6: $GK_r| \equiv (GK_r \leftrightarrow_{L_{up}} U_p)$.

(xvii) κ_7: $GK_r| \equiv GK_r \leftrightarrow_{X_{qr}} SD_q$.

(xviii) κ_8: $SD_q| \equiv (SD_q \leftrightarrow_{SK} U_p)$.

(xix) κ_9: $SD_q| \equiv SD_q \leftrightarrow_{SK} GK_r$.

(xx) κ_{10}: $U_p| \equiv GK_r| \Rightarrow (U_p \leftrightarrow_{M_{rp}} GK_r)$.

(xxi) κ_{11}: $GK_r| \equiv U_p| \Rightarrow (U_p \leftrightarrow_{M_{pr}} GK_r)$.

(xxii) κ_{12}: $SD_q| \equiv U_p| \Rightarrow (U_p \leftrightarrow_{r_{up}} SD_q)$.

(xxiii) κ_{13}: $GK_r| \equiv SD_q| \Rightarrow (SD_q \leftrightarrow_{M_{rq}} GK_r)$.

(xxiv) κ_{14}: $SD_q| \equiv GK_r| \Rightarrow (U_p \leftrightarrow_{r_{gr}} GK_r)$.

(xxv) κ_{15}: $U_p| \equiv SD_q| \Rightarrow (U_p \leftrightarrow_{r_{sq}} GK_r)$.

Next we use the designed idealizations in the following formulations. Considering R_1 and R_2 of the idealized formalization:

(i) R_1: $U_p \longrightarrow GK_r$: M_1, M_2, M_{pr}, T_1: $\{\langle SID_{sq}, r_{up}, T_1 \rangle_{X_{pr}}, \langle RID_{up} \rangle_{h(X_{pr}, r_{up}, T_1)}, (RID_{up}, r_{up}, \backslash\backslash T_1)_{X_{pr}}, T_1\}$.

(ii) R_2: $GK_r \longrightarrow SD_q$: M_3, M_{qr}, T_2: $\{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr}\rangle_{h(SID_{sq}, X_{qr}, T_2)}\}$.

Employing seeing rule for R_1 and R_2, we get

(i) F_1: $GK_r \backslash lh\ dM_1, M_2, M_{pr}, T_1$: $\{\langle SID_{sq}, r_{up}, T_1\rangle X_{pr}, \backslash\backslash \langle RID_{up}\rangle_{h(X_{pr}, r_{up}, T_1)}, (RID_{up}, r_{up}, T)_{1X_{pr}}, T_1\}$.

(ii) F_2: $SD_q \backslash lh\ d\ M_3, M_{qr}, T_2$: $\{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr}\rangle \backslash\backslash \_h(SID_{sq}, X_{qr}, T_2)\}$.

According to $F_1, F_2, \kappa_8, \kappa_9$, and message meaning rule, we have

(iii) F_3: $GK_r| \equiv U_p \sim \{\langle SID_{sq}, r_{up}, T_1\rangle_{X_{pr}}, \langle RID_{up}\rangle \backslash\backslash \_h(X_{pr}, r_{up}, T_1), (RID_{up}, r_{up}, T_1)_{X_{pr}}, T_1\}$.

(iv) F_4: $SD_q| \equiv GK_r \sim \{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr}\rangle \backslash\backslash \_h(SID_{sq}, X_{qr}, T_2)\}$.

(v) Employing F_3, κ_1, freshness conjucatenation, and nonce verification rules, we have

(vi) F_5: $GK_r| \equiv U_p \equiv \{\langle SID_{sq}, r_{up}, T_1\rangle_{X_{pr}}, \langle RID_{up}\rangle \backslash\backslash \_h(X_{pr}, r_{up}, T_1), (RID_{up}, r_{up}, T_1)_{X_{pr}}, T_1\}$.

On applying F_4, κ_2, freshness conjucatenation, and nonce verification rules, we get

(i) F_6: $SD_q| \equiv GK_r \equiv \{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr}\rangle \backslash\backslash \_h(SID_{sq}, X_{qr}, T_2)\}$.

After applying F_5, κ_{12}, and jurisdiction rule,

(ii) F_7: $GK_r| \equiv \{\langle SID_{sq}, r_{up}, T\rangle_{1X_{pr}}, \langle RID_{up}\rangle_{h(X_{pr}, r_{up}, T_1)}, \backslash\backslash (RID_{up}, r_{up}, T_1)_{X_{pr}}, T_1\}$.

Using F_6, κ_{14}, and jurisdiction rule,

(i) F_8: $SD_q| \equiv \{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr}\rangle_{h(SID_{sq}, X_{qr}, T_2)}\}$.

After applying F_5, F_7, and session key rule, we get

(i) F_9: $GK_r| \equiv GK_r \leftrightarrow_{SK} U_p$ (G-1).

Using $F_5, F_7, \kappa_6, \kappa_8$, and nonce verification rule, we get

(i) F_{10}: $SD_q| \equiv SD_q \leftrightarrow_{SK} U_p$ (G-5).

Using R_3 of the idealized form:

(i) R_3: $SD_q \longrightarrow GK_r$: M_4, M_{rq}, T_3: $\{\langle r_{sq}\rangle_{h(X_{qr}, RID_{sq}, GID_{gr}, T_3)}, (SID_{sq}, r_{sq}, X_{qr}, T_3)_{SK}, T_3\}$.

By applying seeing rule for R_3, we get

(i) F_{11}: $GK_r \triangleleft M_4, M_{rq}, T_3$: $\{\langle r_{sq}\rangle_{h(X_{qr}, RID_{sq}, GID_{gr}, T_3)}, (SID_{sq}, r_{sq}, X_{qr}, T_3)_{SK}, T_3\}$.

Employing F_{11}, κ_7, and message meaning rule, we get

(i) F_{12}: $GK_r| \equiv SD_q \sim \{\langle r_{sq}\rangle_{h(X_{qr}, RID_{sq}, GID_{gr}, T_3)}, \backslash\backslash (SID_{sq}, r_{sq}, X_{qr}, T_3)_{SK}, T_3\}$.

On applying $F_{12}, \kappa_3, \kappa_{13}$, freshness conjucatenation, and nonce verification rules, we have

(i) F_{13}: $GK_r| \equiv SD_q| \equiv \{\langle r_{sq}\rangle_{h(X_{qr}, RID_{sq}, GID_{gr}, T_3)}, \backslash\backslash (SID_{sq}, r_{sq}, X_{qr}, T_3)_{SK}, T_3\}$.

(ii) $U_p| \equiv (GK_r \leftrightarrow_{SP} U_p)$ (G-3).

(iii) $U_p| \equiv GK_r| \equiv (GK_r \leftrightarrow_{SP} U_p)$ (G-4).

Next, using R_4 idealized form:

(i) R_4: $GK_r \longrightarrow U_p$: M_5, M_{rp}, T_4: $\{\langle GID_{gr}, r_{gr}, r_{sq}\rangle_{h(RID_{up}, X_{pr}, r_{up}, T_4)}, (RID_{up}, GID_{gr}, r_{up}, \backslash\backslash r_{gr}, T_4)_{SK}, T_4\}$.

By using seeing rule for R_4, we get

(i) F_{14}: $U_p \triangleleft M_5, M_{rp}, T_4$: $\{\langle GID_{gr}, r_{gr}, r_{sq}\rangle \backslash\backslash \_h\ RID_{up}, X_{pr}, r_{up}, T_4, (RID_{up}, GID_{gr}, r_{up}, r_{gr}, T_4)_{SK}, T_4\}$.

By using $F_{14}, \kappa_4, \kappa_5, \kappa_{11}$, and message meaning rule, we have

(i) F_{15}: $U_p| \equiv GK_r \sim \{\langle GID_{gr}, r_{gr}, r_{sq}\rangle_{h(RID_{up}, X_{pr}, r_{up}, T_4)}, \backslash\backslash (RID_{up}, GID_{gr}, r_{up}, r_{gr}, T_4)_{SK}, T_4\}$.

By applying $F_{15}, \kappa_2, \kappa_3$, freshness conjucatenation, and nonce verification rules, we have

(i) F_{16}: $U_p| \equiv GK_r| \equiv \{\langle GID_{gr}, r_{gr}, r_{sq}\rangle_{h(RID_{up}, X_{pr}, r_{up}, T_4)}, \backslash\backslash (RID_{up}, GID_{gr}, r_{up}, r_{gr}, T_4)_{SK}, T_4\}$.

By applying $F_{16}, \kappa_4, \kappa_{10}, \kappa_{15}$, and jurisdiction rule, we get

(i) F_{17}: $U_p| \equiv \{\langle GID_{gr}, r_{gr}, r_{sq}\rangle_{h(RID_{up}, X_{pr}, r_{up}, T_4)}, (RID_{up}, \backslash\backslash GID_{gr}, r_{up}, r_{gr}, T_4)_{SK}, T_4\}$.

Through F_{17}, we apply the session key rule as

(i) F_{18}: $GK_r \equiv U_p| \equiv GK_r \leftrightarrow_{SK} U_p$ (G-2).

By applying $F_{18}, \kappa_2, \kappa_{14}$, we use the session key rule as

(i) F_{19}: $U_p| \equiv SD_q \leftrightarrow_{SK} U_p$ (G-6).

This BAN logic analysis proves sufficiently that our contributed model achieves the targeted goals by attaining mutual authenticity among the legal entities of the system.

5.1. Informal Security Analysis. An informal security discussion on the security features of the proposed scheme is provided in the following.

5.1.1. Mutual Authentication. In the proposed scheme, all participating entities such as U_p, GK_r, and SD_q mutually authenticate one another. GK_r authenticates U_p after extracting L_{up}, computing X_{pr}, and verifying M_{pr} factor with a fresh timestamp T_1. Similarly, GK_r authenticates SD_q after computing and evaluating the correctness of M_{rq} parameter. No malicious entity may compute r_{sq} factor without applying the shared secret X_{qr}. Likewise, U_p authenticates GK_r and SD_q on account of verification of M_{rp} factor. U_p knows that no adversary may calculate the constituent factors including SK, GID_{gr}, r_{gr}, and r_{sq} in further computing M_{rp} without using the shared secret X_{pr}. Finally, SD_q endorses both U_p and GK_r entities after verification of M_{qr} parameter. SD_q verifies the validity of RID_{up}, GID_{gr}, r_{up}, and r_{gr} factors due to the shared secret X_{qr}.

5.1.2. Anonymity and Untraceability. The proposed scheme remains anonymous due to the fact that U_p does not send its real identity ID_{up} in plaintext on insecure channel. To achieve this property, it computes RID_{up} by taking hash of

real identity ID_{up} along with high entropy random integer γ_{up}. Moreover, this hidden identity is submitted to GK_r under the cover of shared secret X_{pr}. An adversary may eavesdrop M_2 message from open channel; however, it may not extract either RID_{up} or the hidden identity ID_{up} from M_2. Similarly, our scheme is untraceable since no adversary can distinguish or trace the similarity among messages of various sessions of the same user. Thus, our scheme supports anonymity and untraceability for the user U_p.

5.1.3. Impersonation Attacks. Our scheme is resistant to U_p as well as GK_r impersonation attacks. The adversary may attempt to impersonate as U_p and for this, it can replay $R_1 = \{M_1, M_2, M_{pr}, T_1\}$ or can modify R_1 and send the R_1 to GK_r, the later may come to know the possibility of the impersonation attack if the M_{pr} is not satisfied. Similarly, if an adversary attempts to initiate GK_r impersonation attack towards U_p by manipulating the R_4 message, U_p may come to know about any forgery on part of adversary by constructing session key SK and verifying the M_{rp} equation. Hence, the proposed scheme resists any possibility of impersonation attack.

5.1.4. Replay Attack. The attacker may eavesdrop the contents exchanged on the public channel, and it can replay the eavesdroped contents. The proposed scheme may resist replay attack successfully since it employs timestamps $T_1 - T_4$ to ensure the freshness of each constructed and submitted message $R_1 - R_4$, respectively. An adversary may not compute fresh messages $R_1 - R_4$ without accessing the shared secrets X_{pr} as well as X_{qr} which are possessed by the legitimate entities of the system.

5.1.5. Stolen Verifier Attack. The proposed scheme is immune to stolen verifier attack by a possible malicious attacker. In our scheme, even if the adversary comes to know about the users' verifiers such as L_{up}, the adversary must need private key K_{GR} to compute X_{pr} and recover further information. It is too hard to guess the private secret key K_{GR} of GK_r for polynomial time adversary. Thus, our scheme is resistant to stolen verifier attack.

5.1.6. Man in the Middle Attack. In our scheme, if an attacker attempts to act as a malicious intermediary among U_p, GK_r, and SD_k entities by manipulating the messages $R_1 - R_4$, it will be detected in the verification procedures such as M_{pr}, M_{qr}, M_{rp}, and M_{rq} of respective entities. It is obvious from the subsection related to resistance from impersonation attacks that if an attacker attempts to replay or modify the parameters of intermediate messages, it will not succeed in these malicious attempts. Hence, our scheme can resist man in the middle attack successfully.

5.1.7. Perfect Forward Secrecy. The proposed scheme supports perfect forward secrecy because even if the private secret key K_{GR} of GK_r is revealed to the adversary, the latter will not be able to compute X_{pr} without accessing the parameter L_{up} which is stored in the repository of GK_r. Thus, the adversary may not compute current, previous, or future session keys, in case the long-term private secret of GK_r is exposed to the adversary.

5.1.8. SD_q Physical Capture. In proposed scheme, if the device SD_q is physically captured by the adversary while the latter extracts B_1 and B_2 from the memory of device, it will not be able to recover the shared secret X_{qr} for lacking access to the private key of SD_q. Moreover, even if the adversary is able to access the SD_q's private key, it will only be able to compute the session key of a particular device while the rest of the smart devices SD_q in the system will remain protected and the attacker will not be able to compute their session keys.

6. Comparisons

In the following subsections, we provide the comparisons of the proposed SKIA-SH and relevant schemes of Wazid et al. [21], Shuai et al. [23], Kaur and Kumar [24], and Yu et al. [20].

6.1. Security Features. The security attribute provision of the proposed SKIA-SH and related schemes [20, 21, 23, 24] is shown in Table 2. Referring to Table 2, except the proposed SKIA-SH scheme, all the related schemes presented in [20, 21, 23, 24] entail one or more weaknesses: the scheme of Yu et al. [20] has a faulty design and it cannot provide mutual authentication between a user and smart devices (SDs), which is proved in Section 3 of this paper. The scheme of Kaur and Kumar [24] has weaknesses against session key disclosure attack and it cannot provide mutual authentication between a user and SDs. The scheme of Shuai et al. [23] cannot resist offline password guessing, insider, replay, and session disclosure attacks, whereas, the scheme of Wazid et al. cannot provide forward secrecy and it cannot resist replay and de-synchronization attacks. Only proposed SKIA-SH provides requisite security attributes and is well suited for smart home (SH) environments.

6.2. Computation Cost. In this section, using a real-time experiment, we provide a comparative computation cost of our SKIA-SH and some of the recent schemes [20, 21, 23, 24]. We conducted the experiment using three devices and corresponding underneath hardware and softwares: ① A Xiaomi Redmi-Note-8 equipped with 4 GB RAM and with an Octa-core 2.01-GHz mprocessor and v-9 andriod MUI-V.11.0.7 operating system, the smart phone simulates a user/mobile-device, ② for GK_r, we adopted an Elite-Book HP 8460P equipped with 4 GB RAM and intel ③ 2.7 GHz mprocessor and th OS used is Ubuntune V.LTS-16, ④ the smart device SD_q is simulated through a Cortex:A53-ARMv8, Pi-B+, 64 bit: SoC, 1 GB: LPDDR2 SDRAM and 1.4 GHz mprocessor. Among other operations, the biohashing/fuzzy extraction T_{fb} is approximated with an elliptic-curve point multiplication T_{em}. The notations and

Table 2: Security features.

Schemes	Our scheme	[20]	[24]	[23]	[21]
MAP	✓	×	×	✓	✓
UAP	✓	✓	✓	✓	✓
SVP	✓	✓	✓	✓	✓
DSN	✓	✓	✓	✓	×
UIA	✓	✓	✓	✓	✓
RAP	✓	✓	✓	×	×
SKD	✓	✓	×	×	✓
PCA	✓	✓	✓	✓	✓
FSP	✓	✓	✓	✓	×
IAP	✓	✓	✓	×	✓
MMP	✓	✓	✓	✓	✓
OPG	✓	✓	✓	×	✓

Note. MAP: mutual authentication provision; UAP: user anonymity and privacy; PSV: stolen verifier protection; DSN: resistance to de-synchronization attack; UIA: user impersonation attack; RAP: replay attack protection; SKD: session key disclosure attack; PCA: protection from physical capture of smart device; FSP: forward secrecy provision; IAP: insider attack protection; MMP: man in middle attack; OPG: offline password guessing attack; ✓: attribute provision; ×: attribute non-provision.

Table 3: Running time.

Entity ⟶	U_p	GK_r	SD_q
↓ Operation			
T_{em}/T_{fb}	5.116	0.926	4.107
T_e	0.017	0.008	0.013
T_h	0.009	0.004	0.006

Note. T_{em}: point multiplication over ECC; T_{fb}: fuzzy extraction/biohashing; T_e: AES-128 block encryption/decryption operation; T_h: secure one-way hash operation.

Table 4: Comparisons of computation and communication costs.

Protocol	U_p	GK_r	SD_q	RT	Bytes ex.
Wazid et al. [21]	$1T_{fb} + 8T_h + 6T_e$	$7T_h + 11T_e$	$5T_h + 11T_e$	≈5.493 ms	376
Shuai et al. [23]	$1T_{fb} + 6T_h + 2T_{em}$	$7T_h + 1T_{em}$	$3T_h$	≈16.374 ms	208
Kaur and Kumar [24]	$1T_{fb} + 6T_h + 2T_{em}$	$8T_h + 1T_{em}$	$3T_h$	≈16.378 ms	224
Yu et al. [20]	$1T_{fb} + 12T_h + 1T_e$	$11T_h$	$7T_h$	≈5.327 ms	196
Proposed	$1T_{fb} + 13T_h + 1T_e$	$12T_h$	$7T_h$	≈5.34 ms	216

Note. RT: running time (ms); ex: exchange.

their corresponding running times on each device according to the conducted experiment are shown in Table 3. To furnish a round of authentication, U_p executes $1T_{fb} + 13T_h + 1T_e$ operations, in addition to $12T_h$ and $7T_h$ executed by GK_r and SD_q. The total running time (RT) on U_p side is ≈5.25 ms, the RT on GK_r is ≈0.048 ms, and the RT on SD_q through the experiment is ≈0.042 ms. Therefore, total RT of the proposed SKIA-SH is ≈5.34 ms. The RT to execute an authentication round of Yu et al.'s scheme is ≈5.327. Similarly, the RT of the schemes of Shuai et al., Kaur and Kumar, and Wazid et al. is ≈16.374, ≈16.378, and ≈5.493, respectively.

6.3. Communication Cost. This section shows the comparisons of our SKIA-SH and the schemes of [20, 21, 23, 24], and for computation cost (CC) comparisons, we adopted SHA-1 with 20-byte output size. The identities and time stamps are kept 8 bytes and 4 bytes, respectively. The random numbers are taken 20 bytes long, and the adopted encryption/decryption algorithm AES-128 also takes 16-byte input and 16-byte output. The size of a coordinate of elliptic curve point (ECP) is 20 bytes and the total length of an ECP is 20 + 20 = 40 bytes. The SKIA-SH (proposed scheme) completes an authentication round by exchanging four (4) messages: ① message sent by U_p to GK_r is $R_1 = \{M_1, M_2, M_{pr}, PID_{up}, T_1\}$. R_1 costs {20 + 20 + 20 + 20 + 4} = 84 bytes. ② Message sent by GK_r to SQ_q is $R_2 = \{M_3, M_{qr}, T_2\}$. R_2 costs {20 + 20 + 4} = 44 bytes. ③ Message sent by SQ_q to GK_r is $R_3 = \{M_4, M_{rq}, T_3\}$, and R_3 costs {20 + 20 + 4} = 44 bytes. ④ Likewise, the message sent by GK_r to U_p is $R_4 = \{M_5, M_{rp}, T_4\}$, and R_4 costs {20 + 20 + 4} = 44 bytes. Therefore, total bytes exchanged during a round of authentication cycle are {84 + 44 + 44 + 44} = 216 bytes. The communication cost of the Yu et al.'s scheme is {64 + 44 + 44 + 44} = 196 bytes. Similarly, the communication cost of the scheme of Shuai et al., Kaur and Kumar, and Wazid et al. is 208 bytes, 224 bytes, and 376 bytes, respectively. The computation and communication cost comparisons are also depicted in Table 4.

7. Conclusion

In this article, we highlighted the need of secure and communication between the smart devices and users through the facilitation of the gateway in the smart home (SH) settings of the IoT. We then reviewed a very recent authentication scheme of Yu et al. We proved that the symmetric key-based efficient and secure authentication scheme entails a critical design flaw, and owing to the explored design flaw, the scheme of Yu et al. cannot complete a cycle of authentication process. An improved scheme free of design flaws and based on only symmetric key function for SH (SKIA-SH) is proposed to mitigate the security and efficiency issues of the SH environments. The security of the SKIA-SH is substantiated through BAN logic. Moreover, we provided a brief discussion of the security attribute provision of the proposed SKIA-SH. To measure the performance, we set up a real-time experiment, and the results show that the SKIA-SH is more secure while it has slight over computation and communication costs when compared with original scheme of Yu et al. The SKIA-SH accomplishes the authentication among a user and a smart device involving gateway in 5.34 ms and by exchanging 216 bytes. As a future work, we intend to extend the proposed method to work in a building area network to provide central and apartment-based services.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, Saudi Arabia, under grant no. RG-3-611-41. The authors, therefore, acknowledge with thanks the DSR for technical and financial support.

References

[1] V. Sivaraman, H. H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IoT devices in the home: security and privacy implications," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 71–79, 2018.

[2] T.-Y. Wu, Z. Lee, L. Yang, and C.-M. Chen, "A provably secure authentication and key exchange protocol in vehicular ad hoc networks," *Security and Communication Networks*, vol. 2021, Article ID 9944460, 17 pages, 2021.

[3] P. Gope, H. Islam, M. S. Obaidat, R. Amin, and P. Vijayakumar, "Anonymous and expeditious mobile user authentication scheme for glomonet environments," *International Journal of Communication Systems*, vol. 31, no. 2, pp. 1–18, 2017.

[4] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, pp. 483–495, 2018.

[5] M. Tanveer, G. Abbas, Z. H. Abbas, M. Bilal, A. Mukherjee, and K. S. Kwak, "Lake-6sh: lightweight user authenticated key exchange for 6lowpan-based smart homes," *IEEE Internet of Things Journal*, vol. 1, 2021.

[6] S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. B. Zikria, "Rotating behind privacy: an improved lightweight authentication scheme for cloud-based IOT environment," *ACM Transactions on Internet Technology*, vol. 21, no. 3, 2021.

[7] M. Tanveer, A. U. Khan, N. Kumar, and M. M. Hassan, "Ramp-iod: a robust authenticated key management protocol for the internet of drones," *IEEE Internet of Things Journal*, vol. 1, 2021.

[8] F. Wu, L. Xiong, L. Xu, P. Vijayakumar, and N. Kumar, "A novel three-factor authentication protocol for wireless sensor networks with IOT notion," *IEEE Systems Journal*, vol. 15, no. 1, pp. 1120–1129, 2021.

[9] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for smart energy home area networks," in *Proceedings of the IEEE International Conference Consumer Electronics (ICCE)*, pp. 787-788, Las Vegas, NV, USA, January 2011.

[10] F. K. Santoso and N. C. H. Vun, "Securing IOT for smart home system," in *Proceedings of the International Symposium on Consumer Electronics*, Madrid, Spain, June 2015.

[11] S. A. Chaudhry, A. Irshad, J. Nebhen, and A. K. Bashir, "An anonymous device to device access control based on secure certificate for internet of medical things systems," *Sustainable Cities and Society*, vol. 75, Article ID 103322, 2021.

[12] A. Irshad, M. Sher, H. F. Ahmad, and B. A. Alzharani, "An improved multi-server authentication scheme for distributed mobile cloud computing services," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 10, no. 12, pp. 5529–5552, 2016.

[13] J.-L. Tsai and N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE systems journal*, vol. 9, no. 3, pp. 805–815, 2015.

[14] T. Maitra, M. S. Obaidat, R. Amin, S. H. Islam, S. A. Chaudhry, and D. Giri, "A robust elgamal-based password-authentication protocol using smart card for client-server communication," *International Journal of Communication Systems*, vol. 30, no. 11, Article ID e3242, 2017.

[15] Y.-C. Lee, Y.-C. Hsieh, P.-J. Lee, and P.-S. You, "Improvement of the ElGamal based remote authentication scheme using smart cards," *Journal of Applied Research and Technology*, vol. 12, no. 6, pp. 1063–1072, 2014.

[16] A. Ali Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, "Palk: password-based anonymous lightweight key agreement framework for smart grid," *International Journal of Electrical Power & Energy Systems*, vol. 121, 2020 [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061519340621, Article ID 106121.

[17] J. Wei, W. Liu, and X. Hu, "Secure control protocol for universal serial bus mass storage devices," *IET Computers & Digital Techniques*, vol. 9, no. 6, pp. 321–327, 2015.

[18] S. A. Chaudhry, "Correcting "palk: password-based anonymous lightweight key agreement framework for smart grid"," *International Journal of Electrical Power & Energy Systems*, vol. 125, Article ID 106529, 2021.

[19] M. F. Ayub, S. Shamshad, K. Mahmood, S. H. Islam, R. M. Parizi, and K.-K. R. Choo, "A provably secure two-factor authentication scheme for usb storage devices," *IEEE*

Transactions on Consumer Electronics, vol. 66, no. 4, pp. 396–405, 2020.

[20] S. Yu, N. Jho, and Y. Park, "Lightweight three-factor-based privacy- preserving authentication scheme for iot-enabled smart homes," *IEEE Access*, vol. 9, pp. 126186–126197, 2021.

[21] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 391–406, 2020.

[22] Q. Lyu, N. Zheng, H. Liu, C. Gao, S. Chen, and J. Liu, "Remotely access "my" smart home in private: an anti-tracking authentication and key agreement scheme," *IEEE Access*, vol. 7, pp. 41835–41851, 2019.

[23] M. Shuai, N. Yu, H. Wang, and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security," *Computers & Security*, vol. 86, no. 132–146, 2019.

[24] D. Kaur and D. Kumar, "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home," *Journal of Informatics*, vol. 58, pp. 2787–10279, 2021.

[25] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[26] C.-M. Chen and S. Liu, "Improved secure and lightweight authentication scheme for next-generation IOT infrastructure," *Security and Communication Networks*, vol. 2021, Article ID 6537678, 13 pages, 2021.

[27] L. Xiong, L. Tian, M. S. Obaidat, and F. Wu, "A lightweight privacy-preserving authentication protocol for vanets," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020.

[28] C. Ran and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 453–474, Springer, Innsbruck, Austria, June 2001.

[29] T.-Y. Wu, L. Yang, M. Qian, X. Guo, and C.-M. Chen, "Fog-driven secure authentication and key exchange scheme for wearable health monitoring system," *Security and Communication Networks*, vol. 2021, Article ID 8368646, 14 pages, 2021.

[30] Z. Ali, S. A. Chaudhry, and K. Mahmood, "A clogging resistant secure authentication scheme for fog computing services," *Computer Networks*, vol. 185, Article ID 107731, 2021.

[31] M. A. Saleem, S. H. Islam, S. Mahmood, and M. Hussain, "Provably secure biometric-based client-server secure communication over unreliable networks," *Journal of Information Security and Applications*, vol. 58, Article ID 102769, 2021.

[32] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2014.

[33] M. Burrows, M. Abadi, and R. Michael Needham, "A logic of authentication," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7665931, 15 pages
https://doi.org/10.1155/2022/7665931

Research Article

Energy-Aware Routing Protocol with Fuzzy Logic in Industrial Internet of Things with Blockchain Technology

Abolfazl Mehbodniya,[1] **Julian L. Webber**,[2] **Rashmi Rani**,[3] **Sayed Sayeed Ahmad**,[3] **Ihab Wattar**,[4] **Liaqat Ali**,[5] **and Stephen Jeswinde Nuagah**[6]

[1]*Department of Electronics and Communication Engineering, Kuwait College of Science and Technology (KCST), Kuwait*
[2]*Graduate School of Engineering Science, Osaka University, Osaka, Japan*
[3]*College of Engineering and Computing, Al Ghurair University, Dubai, UAE*
[4]*Department of Electrical Engineering and Computer Science, Cleveland State University, USA*
[5]*Department of Electrical Engineering, University of Science and Technology Bannu, Pakistan*
[6]*Department of Electrical Engineering, Tamale Technical University, Ghana*

Correspondence should be addressed to Stephen Jeswinde Nuagah; jeswinde@tatu.edu.gh

Received 9 November 2021; Accepted 1 December 2021; Published 31 January 2022

Academic Editor: Muhammad Asghar Khan

It is the expansion and use of the Industrial Internet of Things (IIoT) in various industrial sectors and applications that are referred to as the Industrial Internet of Things (IIoT). The Industrial Internet of Things includes industrial applications such as robots, medical devices, and software-defined manufacturing processes. In terms of energy conservation, routing is extremely essential. The creation of an energy effectual steering procedure leads to a substantial rise in energy consumption. To minimize network traffic and increase network life, the article presented an Industrial IoT Fuzzy Logic Energy-Aware Routing Protocol (FLEA-RPL), which decreases network traffic as well as improves network life. The most suitable parent for data transfer is selected based on, among other things, the routing parameters charge, residual energy, and expected transmission count. Since the load routing metric is taken into consideration during the construction of the route, the data traffic is spread across the network. This increases network's lifetime while maintaining a high packet delivery ratio. The proposed work proposes a Multilayer Energy-Aware Aware RPL (MCEA-RPL) cluster for the Internet of Things to decrease network data traffic while increasing the lifetime of the network. It is split into three phases, each including the creation of network rings, intraring divisions, and intercluster routing. First and foremost, the virtual ring is created in the network. Secondly, each ring forms an identical cluster and chooses the CH node. Finally, it is responsible for the maintenance and performance of the DODAG. Data transfer from the lesser sheet to the DODAG root is known as data transfer. By using Blockchain technology, the lifetime of a network may be extended by reducing the number of identical data package transfers. This article offers Enhanced Mobility Support RPL (EM-RPL) in Industrial IoT which enhances mobility support with blockchain and spreads system generation. It comprises two processes: a collection of the parental static node and selection of the parent moving node. The static parent selection method uses routing metrics load and residual energy to identify the parent that is most suited for data transfer. Two phases of mobile parent selection must be distinguished: data transmission and route rediscovery. The mobile node utilizes furious logic to compute the hand-off value of the metric packet errors ratio and the signal strength indication received from the base station. If the hand-off value exceeds the threshold limit, the DODAG route has to be changed to work correctly. The EM-RPL thus increases the package delivery rate by reducing the amount of route interruption caused by mobility, while offering an efficient handling mechanism.

1. Introduction

The Internet of Things (IoT) has garnered a portion of courtesy from academics in recent years. It is one of the most promising skills because it provides a host of solutions to problems in a wide range of fields. With its capacity to transfer information from one platform to another worldwide, the Internet is the backbone of a network's communication. Kevin Ashton invented the phrase "Internet of Things" at the MIT Auto-ID Laboratory in 1999. One billion gadgets are connected to the Internet, and any device may sense, collect, and send information from one device to another without someone interacting [1]. By 2020, the Cisco Internet of Things (IoT) team anticipates the Internet to connect billions of IoT devices. The Internet of Things is improving human lives, which include monitoring of public health, building automation, logistics, connected cars, intelligent city development (including the smart grid), intelligent homes, smart retail, intelligent farming, and other applications (e.g., [2]).

1.1. Structural Design of Industrial Internet of Things. The Industrial Internet of Things (IoT) can connect many physical items to the Internet. A consistent architecture is needed to store all the information in this instance as efficiently as feasible. Many academics have proposed many architecture models for the Internet of Things; however, none of them have yet fulfilled all architectural criteria. The architecture of the Internet of Things consists of three sheets: the perception layer, the application layer, and the network layer. Initially, sensors are placed at the perception layer to produce and transmit data via wireless devices into the network layer. Finally, the sensor information is read by the user via the network interface [3] in the application layer which is connected to the network layer. The Internet of Things (IoT) was generally developed in various applications utilizing a five-layered architecture. The Internet of Things is composed of conception, networks, middleware, applications, and business layers.

The Industrial Internet of Things strategies is frequently constrained to resources due to their low influence, incomplete computing power, and partial memory size. The lifespan of the network was one of the most significant objectives of the Internet of Things. As a result, energy-efficient methods are being developed in data transmission in IoT networks in demand to reduce the liveliness ingesting of the system and consequently network expenses (B. Ghaleb et al.) [4]. Many challenging factors in the creation of an effective routing protocol have been examined, all of which may affect network's overall performance. The routing protocol considers these challenges to create effective network communication. The IoT routing challenges are illustrated in Figure 1.

Efficient energy design: since the battery independently distributes and drives the nodes in the network, the network is highly dependable. As a consequence, energy conservation is needed to extend the usable lifespan of the system. The routing protocol is extremely useful when it comes to energy conservation. Energy may be saved during data packet transfer and the network lifetime can also be increased by using an efficient technique of road selection. When it originates to the Internet of Things, node deployment is contingent on the necessities of a specific application, whether it is deterministic or self-arranging. Data reporting model: it may be classified into four kinds: query-driven model, time-driven prototypical, event-driven prototypical, and hybrid prototypical. This model is based on Internet of Things applications. Regular data surveillance applications utilize the time-driven paradigm to regularly send sensor data to the sink node. The query-driven and event-driven models will assist time-critical applications [5]. A quick change in sensor data causes data to be sent from the source node to the sink node. The hybrid approach uses a combination of reporting methods and other variables for data transfer.

Physical environment communication range: each sensor node has a range of communication in the physical world on the Internet of Things. One of the most essential concerns when designing an Internet of Things routing system is the coverage area. Fault tolerance is important in data transmission because it enables continuous data flow. If a node emerges from nowhere, a battery depletion or other physical harm may lead to a failure. It affects network's overall operation. In such circumstances, the route must be reconstructed as quickly as feasible, to avoid network packet losses. Scalability is an essential need for big networks and a necessity for all networks. The routing protocol must thus be able to enable network scalability.

A method used to gather and aggregate data packets from different sensor nodes through an aggregate function is called the aggregate acquisition and aggregation of functions. This lowers the number of data transfers in the network. In time-constrained applications, the sensor node's requirement quickly sends information to the sink so that the quality of the service must always be good. In any other scenario, the application Internet of Things will not meet the required requirements and standards. As a consequence, one of the most essential things to consider while developing a routing protocol is the service quality (QoS) offered to consumers. The network data traffic is a measurement of the number of network data packets flowing across the network at any time. The routing protocol supports two-way data transmission. The pattern of traffic on the Internet of Things is different from the application. Mobility: mobility support is one of the hardest tasks on the Internet of Things. It is mainly due to system's wireless nature and the fact that the route may frequently be interrupted due to mobility. Therefore, it is necessary to redevelop the route in such a scenario.

Heterogeneity: depending on the application they are utilized, the responsibilities and capabilities of the sensor nodes vary. The variety of the nodes may provide technical challenges during the routing procedure. Some applications, for instance, employ a combination of different sensors to keep an eye on the surroundings.

To transmit sensor data wirelessly from one source node to extra, the sensor node uses infrared or radio frequency transmission as a communication medium to connect with other nodes. Multiple route propagation, high error rates,

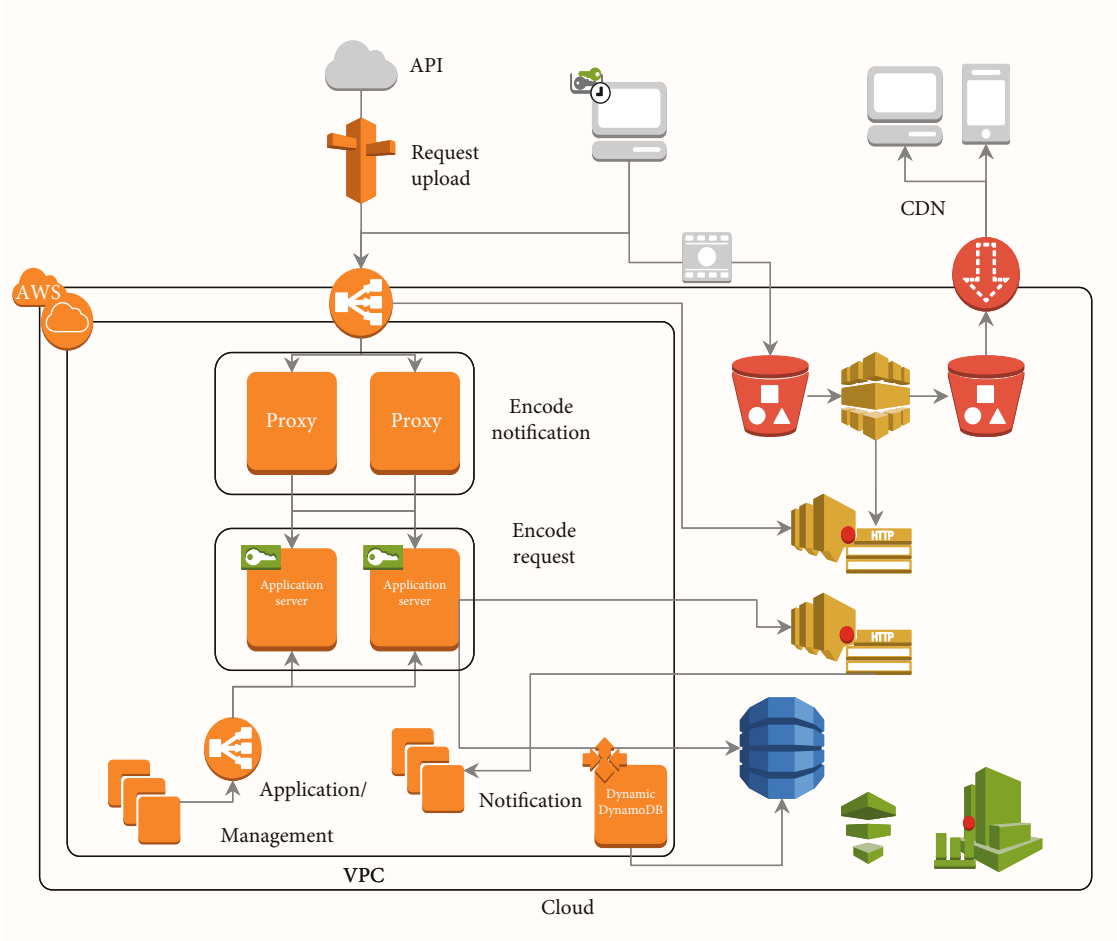


Figure 1: Workflow of in IIoT.

reflection, and fading are all problems linked with these two transmission techniques. The Internet of Things devices is extremely resource-restricted since they are battery-driven. Energy is one of the most critical concerns for applications on the Internet of Things. Because of the multihop network topology and a large amount of data traffic near the sink node, the energy is drained faster by nodes closer to the sinking node. This affects network's overall performance and operation. The routing metric hop count is used by traditional routing protocols for the creation of the DODAG. As it constantly uses the same path for data transmission, it causes an early energy loss at the nodes along that path, leading to path breaks. Routing factors such as residual energy (RER), loading, anticipated transmission count (ETX), and connection quality have thus to be taken into consideration throughout the whole construction phase. As a consequence, a routing protocol is needed, which uses calculation techniques of different routing metrics, based on the request needs. On the Internet of Things, data are sent via nodes to the sink node in a multihop way. All neighboring nodes may redundantly transmit the same data to the sink node, which results in an increased traffic load and wasteful use of energy. Energy conservation on the nodes is necessary, and this may be done by minimizing redundant data transfer. The clustering technique is the most effective means of decreasing energy usage at network nodes in the above-stated situation. The data packet is transmitted to the CH node by the cluster nodes. Once information is acknowledged from the CM nodes, the aggregate node transmits it to the processing sink node. As a consequence, clustering may assist conserve energy by dropping the number of statistics packets transferred from the source node to the sink node. Path breaks will arise because of node mobility. To continue with data transmission, the routing protocol must thus relearn the path. The interruption of the route has a greater impact on the performance of the routing protocol than on network performance. The mobility issue of the node has to be addressed. The routing protocol must contain a better hand-off mechanism to minimize the frequency of route interruptions caused by mobility, to identify an alternate method of continuing the transmission of information. Extending network's life span and enhancing mobility assistance is a tough task on the Internet of Things. Protocols that address the above-mentioned problems, in particular, are in great demand. Therefore, the following are the objectives of the project: this research is aimed at creating an energy-efficient protocol to route the Internet of Things by diversifying network traffic and minimizing overhead control messages. The purpose of this article is to propose a cluster-based Internet of the Things routing protocol

to reduce network data traffic and to enhance the mobility support of nodes throughout the Internet of Things. Section 2 includes literature survey. Section 3 represents the methodology, whereas Section 4 represents the experimental results, and conclusion ends with Section 5.

2. Review of the Literature

It is intended for use in Small Control and Reduction System (LLN) and selects, among other factors, the most suitable parent to transport information packages from source to sink nodes. The Internet of Things devices usually has less power, less memory, and less capacity for processing. The IETF has standardized the RPL to satisfy the Long-Term Network (LLN) ([2]) requirements. RPL generates a DODAG to be used to convey participant data containers to the origin of the DODAG, controlled by the participant. Each sink node has a distinct DODAG that is kept. DODAG form refers to the first node as the DODAG root, the second node level to the leaf node, and the other nodes to the middle nodes. In the DODAG representation, the edge which corresponds to the DODAG root upwards is called an upward road, and vice versa, the edge which correlates with the DODAG root downwards. It contains the DODAG rank, RPLInstanceID, DODAG version number, and DODAGID, all needed for the RPL network topology [6].

The RPLInstanceID identifies all DODAGs in the network with the same objective function and organizes them under a single-instance number. The DODAGID provides the DODAG with the unique identification to find it on the network. If the DODAG detects a new route, the version number changes to reflect the change. The distance between the member and the DODAG origin is abundant. The participant node chooses the optimal parent for data transmission from the available choices using the neutral purpose. The neutral purpose is calculated based on the routing data and intended to minimize road costs in the network. Every node in RPL may have either a storage mode or a nonstorage mode, depending on its purpose. During storage, the node receives and transmits information to its parent node. If the node does not store data, it transmits the data to its parent node. The RPL supports traffic patterns such as multipoint, point-to-point, and multipoint traffic patterns. The RPL uses the trickling timer to minimize the overhead control during the route construction process. You may specify predefined time intervals from 1 to 1,000,000 seconds with the trickling timer. It includes three parameters, connexion redundancy inspection, minimal intervals, and maximum intervals, indicated by K, $I_{\min}$, and $I_{\max}$. To begin with, the counter C value is set to zero. Whenever the sweeping timer gets a continuous transmission for the length of the sweeping interval specified in DODAG, the counter C value is increased until the supplied K value is reached. In addition, for several reasons, the DODAG root fails, including energy depletion, network congestion, node failure, and other problems.

A. Hassan et al. [7] presented an energy-conscious routing method to prolong the lifetime of LLNs. The inadequate selection of paths leads to early battery depletion and a bottleneck problem near the origin of DODAG. It selects the optimal DODAG parent based on routing [8] factors such as the Battery Depletion Index (BDI) and the Energy Relationships (RER). The simulation is conducted using the COOJA simulator. It is worth noting that the proposed energy-conscious routing increases the lifetime of the LLN while at the same time reducing the delay about RPL, ETX-RPL, and MRHOF-RPL. However, since the connection measurements during the route building process are not taken into consideration, the energy-conscious RPL proposed increases the packet loss ratio.

The dynamic and efficient parent selection technique for LLN RPL has been introduced, according to W. B. Heinzelman et al. [9]. It uses the metrics load and RER to decide which parent is most suited to data transfer. In addition, the construction of topology in the MAC layer is changed as a consequence of this protocol. As a consequence, the traffic load spreads throughout the network. The results indicate that network stability is increased while network traffic is distributed equally among nodes inside the LLN network. The reproduction is showed using COOJA. The efficiency of the dynamic parent collection RPL is significantly greater compared to traditional RPL. It extends the lifetime of the LLN and decreases the latency at a similar period. Bhandari et al. have proposed an RPL procedure for IoT monitoring applications [9] and is called the Congestion Aware RPL (CA-RPL). It focuses mostly on congestion across the nodes of the network, as the name suggests. It proposed a new parent selection mechanism in RPL which takes into consideration congestion. It uses the multicriteria decision-making technique to decrease congestion throughout the network (MCDM). For data transmission, ETX, RER, neighborhood index, and queue use routing characteristics are used to identify which parent is the one that is most suitable for data transmission. The simulation is conducted using the COOJA simulator.

M. S. Tomar et al. [10] have developed a novel target function for multiway ad hoc low-power networks that improve network longevity. The first objective function searches for the shortest route for data transmission by utilizing latency, buffer occupancy, bandwidth, and ETX routing parameters to find the shortest route. The second objective function uses the greedy approach to choose the parent most suitable for information transmission. The simulation is conducted using the COOJA simulator. It has been noted that the overall performance of the network also increases when the number of gateways rises. It also shows that the greedy approach is better than the end-to-end strategy since it does not take into consideration the obligation cycle when choosing a parent. The metrics buffer occupancy and delay values, however, operate on the level of the node and their values change often.

The context-aware and load-balanced routing protocol (CL-RPL) for the Internet of Things have already been developed by Iova et al. [11]. The rapid data flow of LLN adds to the problem of early battery depletion, which our approach addresses. With the use of queue metrics and RER, a context-aware objective function was proposed for the parent selection which was dependent on the context

of the choice. The reproduction is led using the COOJA simulator. The efficacy of CL-RPL is evaluated and opposed to standard RPL. It increases the overall network performance about lifetime and end-to-end latency. However, it may lead to higher packet loss under certain network conditions.

S. Izquierdo et al. [12] created an energy-conscious Internet of Things RPL. Two proposed objective functions have been identified, particularly the parent energy objective function (PEOF1) and the parent energy target function (PEOF2) (PEOF2). Both goal functions take into consideration the ETX and RER routing metrics for parent selection. The PEOF1 objective function uses RER to choose the parent best suitable for the transmission of data packets. The objective function PEOF2 uses the RER to identify the path between participating nodes and the DODAG root. The simulation is conducted using the Contiki COOJA 2.7 simulator. To evaluate its performance, it benefits from the symmetrical and asymmetrical features of the proposed procedure. It is worth noting that the PEOF2 is much better than the V. Karagiannis et al. [13] proposed a multipath selection approach for cache-based use in the RPL. However, the comparison of performance is done just with PEOF and PEOF2. Energy consumption is a key problem in low-power and loss networks. Many research initiatives are aimed at reducing the quantity of energy used by the grid. The energy equalization routing method and cache usage algorithm should be used to choose the most efficient data transmission path. The simulation is conducted using the COOJA simulator. Compared to RPL, the proposed multirouting protocol minimizes energy use while increasing reliability at the same time. On the other side, the node extremely rapidly depletes the energy supply when it is close to the sink.

R. Khan et al. [14], LLN proposed an expanded Kalman-based RPL filtering (EKFRPL). RPL does not offer mobility function support. Because of these network performance restrictions, existing routing methods are affected by problems such as slow response and poor overall network performance. EKF-RPL is proposed as a solution since it enables more mobility while prolonging the generation of the system. The simulation is done using the COOJA simulation program. The EKF-RPL presentation is assessed using together with the exact model and the reproduction. The findings are promising if the efficiency of EKF is compared with the efficiency of existing mobility aid techniques [15]. It has been shown that EKF-RPL provides better performance based on energy usage, responsiveness, control overhead, and packet loss. On the other hand, EKF-RPL does not take into consideration network latency and scalability.

The cheap data and accountancy blockchain concepts in the industrial sector may stimulate the creation of new technologies that will allow companies and individuals to create cryptocurrencies and accounting programs that revolutionize their respective areas of expertise. In general, the blockchain will offer companies and individuals a safer and more reliable alternative to conventional shipping and delivery techniques. The blockchain will allow companies to retain shipping data across many devices in the logistics sector while preventing them from being held by criminals. As it allows supply shift to function more efficiently and with more trust, blockchain technology has the potential to increase logistics interoperability. Individuals profit from the blockchain because it monitors what and where they have spent their money, ensures that their credentials are safe, and gives them a feeling of security that is not accessible via analog methods [16]. The safety of industrial control systems (ICS) in the IIoT is a major problem [17]. The inherent security of blockchain may make industrial control systems (ICS) more resistant to manipulation on the Internet of Things (IoT), but blockchain can open the door to a variety of cyber security options that might affect entire eighth ecosystems. For example, the blockchain can ensure that the whole ecosystem is secure from the start and irreversible. Because IIoT is a large network that connects a large number of strategies, the IIoT is susceptible to a large number of vulnerabilities. The number of vulnerabilities will increase quickly as more devices are connected to IIoT. In the meanwhile, cryptographic algorithms are limited in life before they become inoperable, which means, if hackers learn and adapt to more advanced hacking methods, even the safest algorithms may be jeopardized. Many devices have limited resources in the IIoT, which is another reason (e.g., smart sensors, microcontrollers, etc.)

Blockchain nodes may often be split into two types: complete (FN) and lightweight (LN):

(i) Full node, capable of downloading and verifying all of blocks and transactions, and • Light node, with just a few blocks and transactions to be verified. FN may serve as a mining node, which implies the blockchain can be generated

Lightweight node (LN): due to the restricted available resources, LN can only store and analyze part of the data on a blockchain. In the Internet of Things, lightweight intelligent devices (sensors) may operate as an LN, offering fresh transactions spread among nodes and eventually incorporated as a block in the blockchain.

3. Industrial Internet of Things with Routing Protocol That Is Based on Fuzzy Logic

RER routing measurement has a FLEA-RPL maximization property while ETX and Load have the same minimizing property. The average weighted method for parent selection does not apply to these routing characteristics since they are too complex. This results in the usage of the fuzzy logic of the proposed protocol to calculate routing metrics [18]. In particular, it provides a new objective function (OF) for parent selection which measures the quality of the DODAG hierarchical parental node designated. FLEA-RPL implements the OF to select the best suitable DODAG parent node from which data from participants to DODAG root may be sent. FLEA-RPL is a routing protocol in which utilizes fuzzy logic for routing metrics to assess the parent node quality. There are three fluid input variables, RER, ETX, and Load, and one fluid output variable, the quality of life of the parent. Generally, it is responsible for fluctuating and defuzzing data for the selection of routes.

The quantity of network data that passes through the network during a particular period is called traffic load, and the goal load balancing function is responsible for spreading the load amongst the nodes within the network. It modifies the traffic load to reflect children's numbers [19]. The traffic load on this track is calculated on the P path between the source node q and DODAG root in

$$\underline{\text{Load}}\ \text{Pqg DoDAG root}) = \sum_{x=1}^{Z} \text{Load}(x), \tag{1}$$

where x and n are a single node in a path P and a total number of nodes in a path P respectively. The traffic load of particular node x is calculated in

$$\text{Load}(x) = \underset{m=1}{\textbf{child}\_\text{count}(m)}, \tag{2}$$

where m and n are the number of nodes in x that are children of x and the total number of nodes in x, respectively.

3.1. Estimated Number of Transmissions. The quality of the path between the participant and the DODAG root is determined. It estimates the number of transmissions and transmissions required to reach the DODAG root node successfully. ETX connection: this statistic evaluates the quality of the connection between the two DODAG nodes. The quantity of data packets received successfully by the recipient is indicated by the transmission of forwarding information. The reverse data delivery indication shows the number of accreditations received by the sender.

The data supply shall be specified by letter FD, whereas the data supply shall be indicated by letter RD. Route ETX: this measure assesses the route quality among a member node and the root node of DODAG. According to Equation (3), the path ETX P may be calculated from the source q to the DODAG root.

$$\text{ETX}(x) = \frac{1}{\text{FD}\times}|\text{RD}, \tag{3}$$

where x and n are individual nodes and a total number of nodes in a path P, respectively.

3.2. Fuzzification. It shows the sharp input as a fuzzy input. The required inputs are the DODAG link and node information. The main words language variable and membership function are presented below in futile logic.

3.3. Linguistic Variable. The language variable plays a crucial role in futile logic. It is a variable that stores the value separate from the numbers in terms of words or phrases. Table 1 provides the language variables for input and output routing metrics.

3.4. Membership Function. The language variable plays a crucial role in futile logic. It is a variable that stores the value separate from the numbers in terms of words or phrases. Table 1 provides the language variables for input and output

Table 1: Linguistic variables.

Routing metrics	Linguistic variables
Load	Light, normal, and heavy
RER	Low, average, and full
ETX	Short, average, and long
Neighbor quality	Awful, very bad, bad, very good, good, excellent

routing metrics, h_1, i_1, and j_1. The parameters h_1 and j_1 are the base of the

$$\mu_{c1}(z) = \begin{cases} 0, & z \le h_1, \\ \dfrac{Z - h_1}{i_1 - h_1}, & h_1 < z \le i_1, \\ \dfrac{j_1 - z}{j_1 - i_1}, & i_1 < z < j_1, \\ 0, & j_1 \ge z. \end{cases} \tag{4}$$

The trapezoidal curve is a true value vector y, including four scalars, h_2, i_2, j_2, and k_2 parameters. The parameters h_2 and k_2 are both little and upper curve limits. Similarly, the i_2 and j_2 parameters represent both lower and higher support limits. The trapezoidal function is often represented

$$\mu_{c2}(y) = \begin{cases} 0, & y \le h_2, \\ \dfrac{y - h_2}{i_2 - h_2}, & h_2 < z < i2, \\ 1, & i_2 < z \le j_2, \\ \dfrac{j_2 - y}{j_2 - k_2}, & j_2 < z < k_2, \\ 0, & k_2 \ge z, \end{cases} \tag{5}$$

$$\text{Light}\ (\ \text{Load}\ ) = \begin{cases} 1, & \text{if Load} \le 2, \\ \dfrac{\text{Load} - 3}{6 - 3}, & 3 < \text{Load} < 5, \\ 0, & \text{if Load} \ge 5. \end{cases} \tag{6}$$

The load membership function is the load in the network nodes. The traffic load may be expressed by the linguistic variable as heavy, normal, and light Z. Latib et al. [20]. The language variable membership function light load may be seen in Equation (6). Likewise, the membership function for additional linguistic variables of traffic load may be expressed. The membership function may also be expressed for the other ETX, RER, and neighboring node quality measures. The load membership feature is illustrated in Figure 2. The RER membership shows the current energy in the RPL router.

The membership of RER value ranges between 0 and 1. The FLEA-RPL selects the parent node with maximum residual energy. The RER membership is depicted in Figure 3.

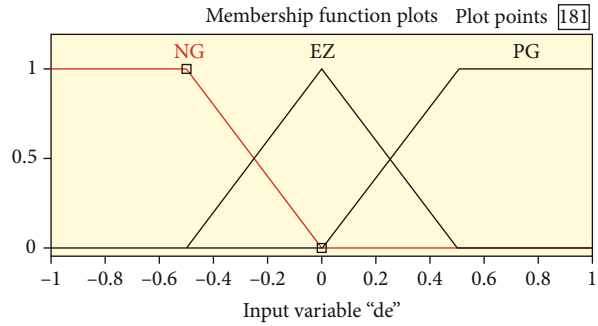


Figure 2: Membership function of load.

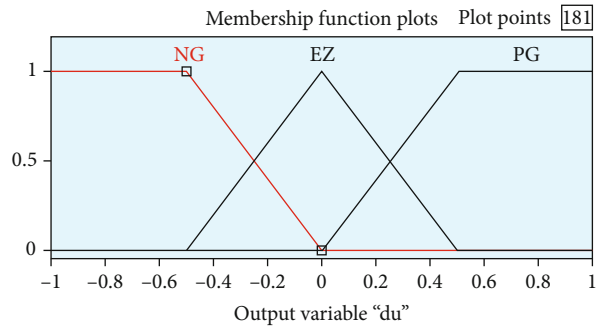


Figure 3: Membership function of RER.

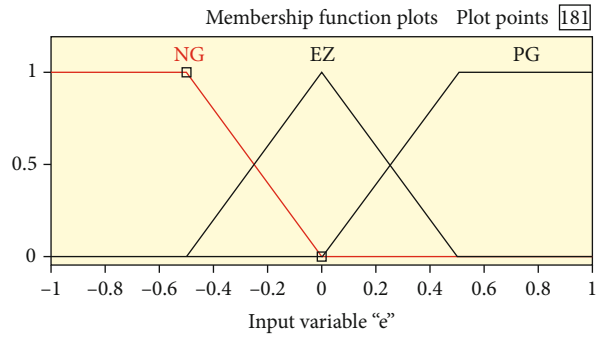


Figure 4: Membership function of ETX.

ETX's membership function represents the link quality between the participant and the DODAG root. The linguistic variables of the fuzzy output variable are excellent, very good, good, low good, bad, low bad, and awful S. Izquierdo et al. [12]. The membership of neighbor quality is shown in Figure 4.

Figure 5 represents the neighborhood quality of the membership function.

3.5. Fuzzy Rule. It is a combination of input and output fuzzy variables [21]. In FLEA-RPL, the fuzzy inputs are RER, ETX, and Load, and the fuzzy output is the quality of the neighbor node. The fuzzy rule base contains twenty-seven rules, as there are three input fuzzy variables [22] and membership functions for each input variable. The output of the three-membership function determines the quality of the neighbor node. The fuzzy input variables and fuzzy rules are adjusted according to the application requirements [23]. Mamdani model is a popular and commonly used fuzzy inference system [12]. It evaluates the fuzzy rules of FLEA-RPL using the If-Then rule. It provides the results according to the network conditions. Table 2 demonstrates the fuzzy rules.

3.6. Defuzzification. Defuzzification is one of the significant processes in a fuzzy inference system [24], which converts the fuzzy output into a single crisp value. Its value ranges from 0 to 100. In FLEA-RPL, the weighted average method is used for defuzzification, and its representation is given in

$$S = \frac{\sum_{j=1}^{N} W_j \times \mu_c(W_j)}{\sum_{j=1}^{N} \mu_c(W_j)}, \tag{7}$$

where S represents the crisp set value and c is a fuzzy region. N indicates the total number of fuzzy rules, μ_c is a predicate truth value of domain W, and W_j is a domain value of particular rule j.For example, the parent preferred contains Load, RER, and ETX metrics, and their values are 2, 175, and 10. Language variables for FLEA-RPL are Light and Standard for Load, Full for RER, and Short for ETX. For Light, Normal, Full, and Short, the membership values are 0.5, 0.5, 1, and 1 for the language variables. FLEA-RPL produces two rules in the fuzzification process [25]. For the example above, rules 1 and 4 match the fuzzy rule base [25]. The output of the rules is excellent. Both rules have an output value of 0.5. The qualitative value of neighboring values is 70 and 86 correspondingly for the membership of the Very Good and Excellent. The value of fuzzification is determined in

$$S = \frac{(0.5 \times 70 + 0.5 \times 86)}{(0.5 + 0.5)} = 78. \tag{8}$$

Likewise, FLEA-RPL calculates the quality of the preferred parent. Finally, the participant node chooses the parent node with the maximum crisp value [25]. In DODAG, the participant node x calculates the rank value from the rank of the parent node and its *rank increase*. The *rank increase* value is computed from the *step* and *minHopRankIncrease*. The *step* value is calculated using the objective function. The *minHopRankIncrease* is an inbuilt value, which is 256 by default. The rank calculation is given in

$$\text{rank}\ (x) = \text{rank}\ (\text{parentNode}) + \text{rankIncrease}, \tag{9}$$

$$\text{rankIncrease} = \text{step} + \text{minHopRankIncrease}. \tag{10}$$

The route may be created in FLEA-RPL in two distinct methods. First, the participant deliberately transmits the DIS message to the DODAG root. Secondly, the DODAG sends the DIO message periodically to its neighbors. To transmit data, the suggested protocol conducts parent selection using fuzzy logic [26]. The method for selecting the parent is illustrated in Figure 6. To maintain the topology across network nodes [26], the DODAG begins the trickle timer (I). The starting counter value C is 0. The time interval of the

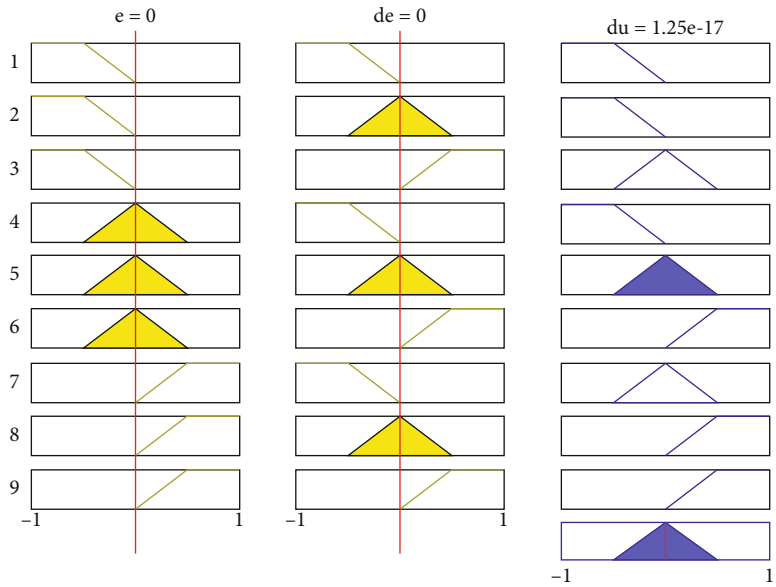


Figure 5: Membership function of neighbor quality.

Table 2: Fuzzy rules.

S. no.	Residual energy	ETX	Load	Quality of neighbor
1	Full	Short	Light	Excellent
2	Full	Average	Light	Very good
3	Full	Long	Light	Good
4	Low	Short	Light	Good
5	Low	Average	Light	Bad
6	Low	Long	Light	Low bad
7	Average	Short	Light	Very good
8	Average	Average	Light	Good
9	Average	Short	Light	Good
10	Full	Short	Normal	Very good
11	Full	Average	Normal	Good
12	Full	Long	Normal	Bad
13	Low	Short	Normal	Bad
14	Low	Average	Normal	Low bad
15	Low	Long	Normal	Bad
16	Average	Short	Normal	Good
17	Average	Average	Normal	Low good
18	Average	Long	Normal	Low bad
19	Full	Short	Heavy	Good
20	Full	Average	Heavy	Bad
21	Full	Long	Heavy	Good
22	Low	Short	Heavy	Low bad
23	Low	Average	Heavy	Bad
24	Low	Long	Heavy	Awful
25	Average	Short	Heavy	Bad
26	Average	Average	Heavy	Low bad
27	Average	Long	Heavy	Bad

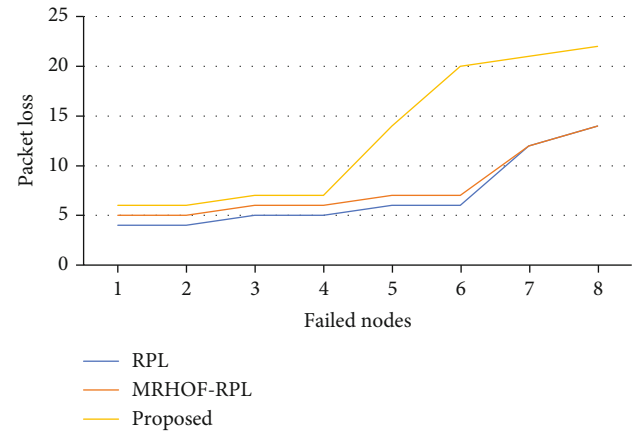


Figure 6: Average packet loss ratio in the node failure scenario.

trickle timer is from I_{min} to I_{max}. In RPL, the standard values of I_{min} and I_{max} are 12 ms and 10 ms. The participant delivers the response message to its parent node at the DODAG within the trickle interval. Finally, the parent node delivers its appropriate participant the DAO-ACK message [27]. The parent selection pseudocode is provided in the algorithm. Figure 7 represents the Optimization Algorithm Flowchart. The Optimization algorithm decides the best features in the system.

The DODAG is first created in the intercluster routing [28]. The CH node chooses the optimum data transmission cluster parent node. The DIOC message is sent to all CM nodes in the cluster. The CH node waits till the answers from the CM nodes come to an end. Once the answer has been received, the CH node transmits the CH-ACK message to the appropriate CM nodes in the cluster. MCEA-RPL retains the CH node during upward routing in two states: the original parent and the suboptimal parent. The suboptimal parent gathers data from all CM nodes and aggregates it.

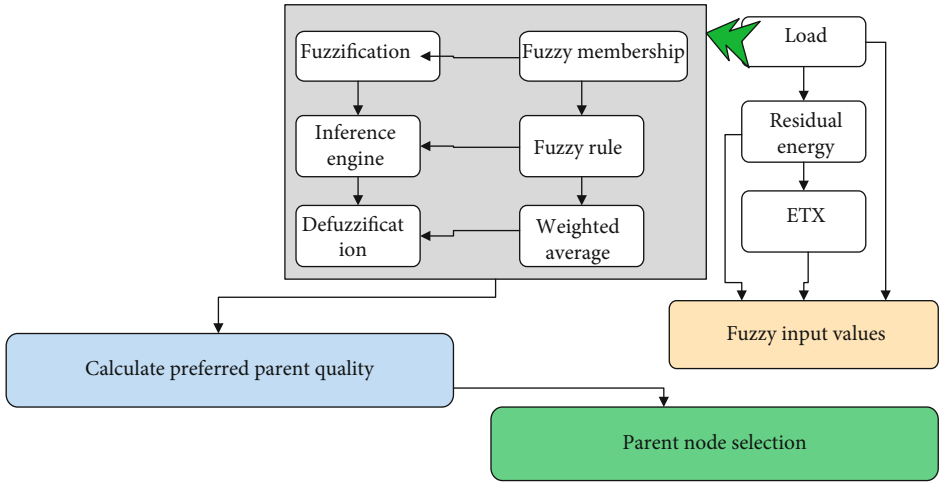


Figure 7: Parent selection mechanism.

Input: parentNodeList
Output: bestPreferredParentNode
1: **procedure** PARENT SELECTION
2: *begin*:
3: bestParentNodeRank = ∞
4: **for** preferredParentNodeId ∈parentNodeList **do**
5: rank(particpant)=rank(parentNode)+rankIncrease;
6: rankIncrease=step + minHopRankIncrease
7: Create linguistic variable and membership of Load, ETX, and RER
8: Make fuzzy rule base
9: Evaluate the generated rules with fuzzy rule base
10: Perform the defuzzification process
12: **if** bestParentNodeRank > preferredParentNodeRank **then**
13: bestParentNodeRank=preferredParentRank
14: **end if**
15: **end for**
16: **while** preferredParentNodeRank == bestParentNodeRank **do**
17: participantNodeId=preferredParentNodeId
18: **end while**
19: Return bestPreferredParentNode
20: **end procedure**

Algorithm 1: Parent selection algorithm.

The initial optimal parent transmits the data to the ideal CH parent node in the upper ring. Parent's suboptimal parent is provided with the DIOC control message. In the chosen field, the DIOC message contains the parent information. During parent selection, a suboptimal parent selects the best CH parent for data transmission via the ETX and RER parameters. Fuzzy Inference System (FIS) is an important part of the fuzzy logic system which is used to map input and output values using fuzzy logic [29]. In FIS, the key operations are fusing, inference engine, fusing rules, and defusing.

4. Experimental Results and Analysis

4.1. Simulation Setup. The Leistung Using a COOJA network simulator, FLEA-RPL protocols have been tested and compared with common RPL, FL-RPL, and MRHOF-RPL protocols. The Tmote Sky is installed randomly in the network region (600 m/600 m). A DODAG root node with hundred RPL routers is included in the replication. The simulation is carried out in three situations with a transmission rate of data of one, six, and ten packets per minute [30]. The findings indicate the average values received from the simulation. Table 3 illustrates the setup and parameters of the simulation.

4.2. Performance Metrics. The following measurements [31] assess FLEA-RPL performance.

Rest of energy: it indicates how much energy the node has.

Packet loss ratio: defined as the proportion among the entire and the source number of failed packets and the total number of data packets.

Table 3: Simulation setting and parameters.

Parameters used for simulation	Values
OS	Contiki 2.7
Number of nodes	100 RPL routers and 1 DODAG root
Data packet timer	60 sec
Simulation duration	1 hour
MAC/adaptation layer	ContikiMAC/6LowPAN
Full battery	1500 mA
Network area	$600 \times 600\ m^2$
Radio environment	Unit disk graph medium
Simulator	COOJA
Minimum DIO interval	12
Node type	Tmote sky
DIO interval doubling	10
Routing protocol	RPL

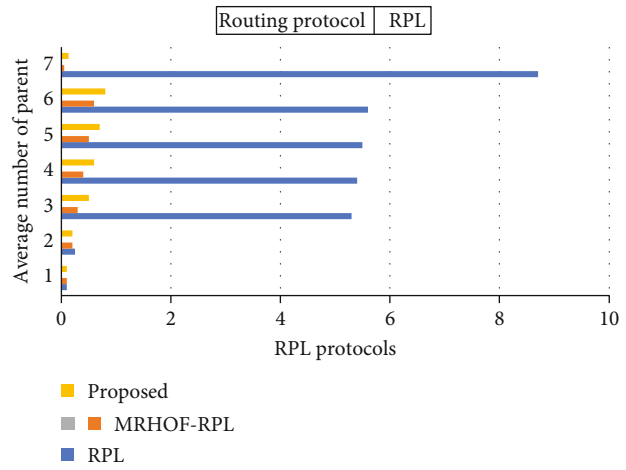


Figure 8: Various RPL protocols with parental changes in data.

End-to-end delay: this is an average period to correctly transmit the information from source to destination.

Parent change number: indicates how many times parent changes occur throughout the simulation.

4.3. Performance Evaluation Results. The performance of FLEA-RPL is evaluated via simulation. Control overhead, latency from end to end, residual power, power consumption, and packet loss ratio are the assessment parameters. The FLEA-RPL is compared with the current known RPL and MRHOF-RPL routing protocols [32].

Scenario 1: data transfer rate within a minute

Figure 8 shows parental change values for different RPL protocols with one packet a minute transmission rate. The parental modification value of FLEA-RPL is recorded to evaluate the network stability and is compared to the conventional RPL, FL-RPL, and MRHOF-RPL. Standard RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL changes parent values are 0.2, 0.28, 0.25, and 0.17 correspondingly. The parent change value in FLEA-RPL is low compared with RPL,

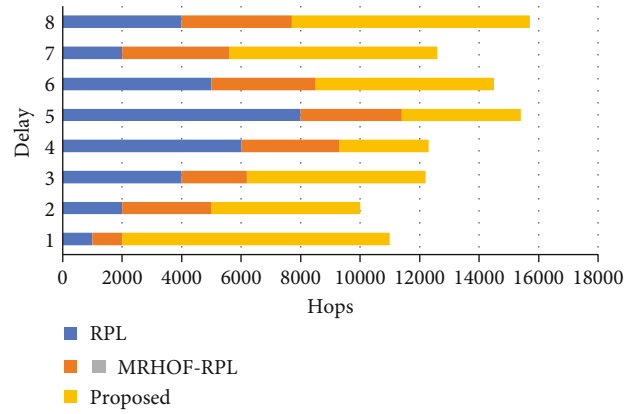


Figure 9: End-to-end delay versus number of hops.

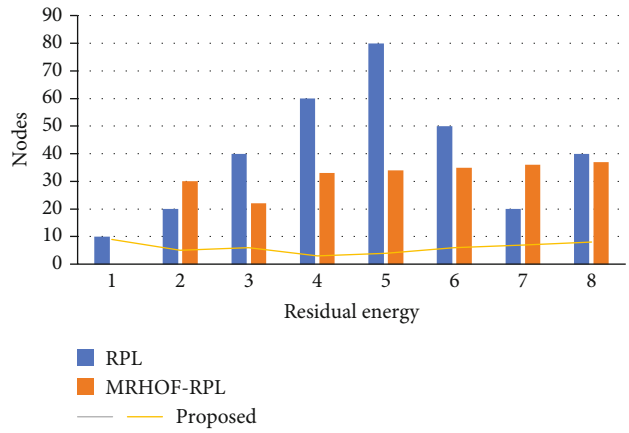


Figure 10: Residual energy of network nodes.

MRHOF-RPL, and FL-RPL. It is primarily related to the load metric for the selection of the parent node. FLEA-RPL thus chooses the finest parent in the DODAG and extends network's lifespan.

Figure 8 shows the average hops end-to-end latency. The RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL standards are 3.8, 3.2, 3.7, and 2.9 seconds. The result indicates that the FLEA-RPL requires less time than other RPL, FL-RPL, and MRHOF-RPL protocol standards. The diversification of network traffic across the network during parent selection.

Figure 9 shows the network node residual energy with a data transmission rate of one packet a minute. FLEA-RPL shows that 90% of network nodes have residual energy ranging from about 84% to 87%. The remaining 10% of the network nodes contain residual energy between 90% and 92%. In comparison to conventional RPL, FL-RPL, and MRHOF-RPL, FLEA-RPL exhibits improved network life and residual energy. Due to RER consideration, the optimum parent selection to transmit data to the root of DODAG is selected.

Figure 10 illustrates the RPL, FL-RPL, FLEA-RPL, and MRHOF-RPL packet loss ratio by changing one packet per minute by network size with data transmission rate. The percentage of the packet loss in RPL is large, given the number of hops for parent selection alone [32]. For parent

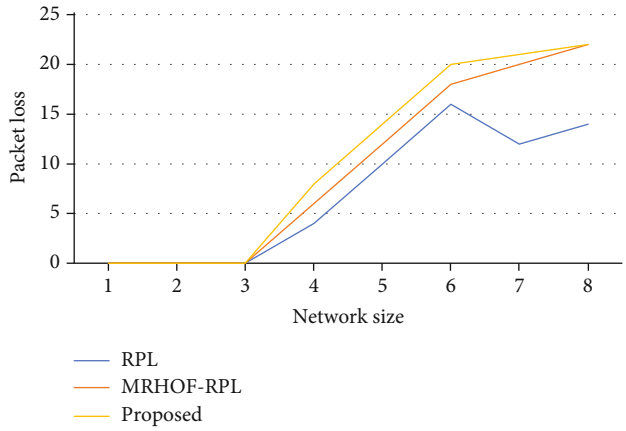


Figure 11: Ratio of network size and packet delivery.

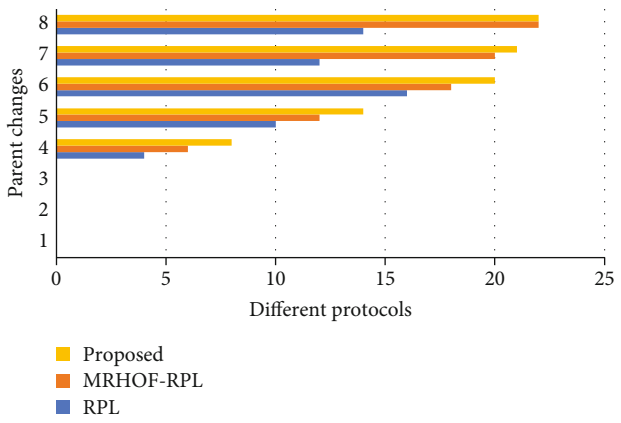


Figure 12: Average number of data concerning various RPL protocol.

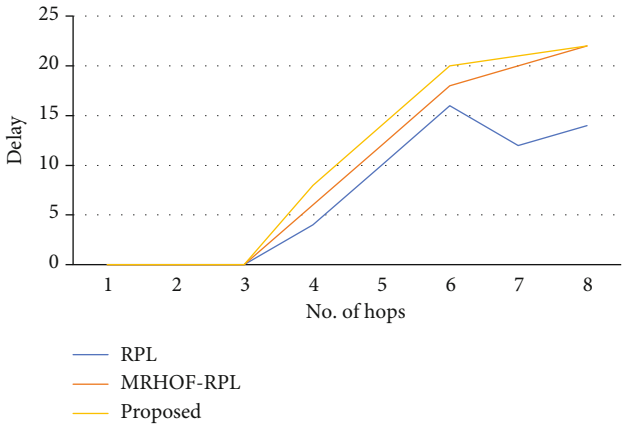


Figure 13: End-to-end delay versus number of hops.

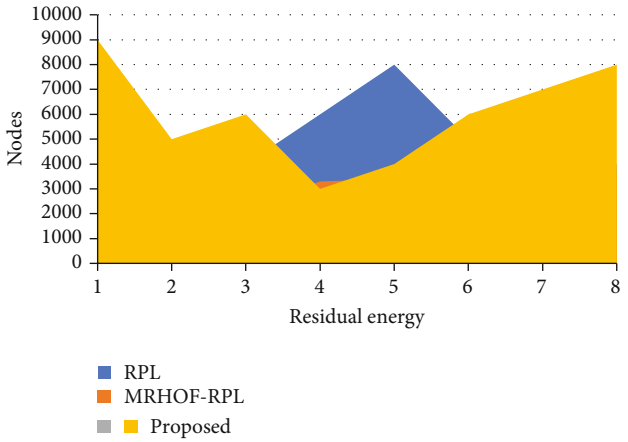


Figure 14: Residual energy of network nodes.

selection, MRHOF-RPL solely considers the ETX measure. The battery is thus prematurely depleted and causes a significant loss of packets. For a network size of 100 nodes, the conventional RPL, FL-RPL, MRHOF RPL, and FLEA-RPL packet loss ratios are 6%, 4%, 5.8%, and 3.8%, respectively. It is experimental that the loss of packets rises with the increased amount of nodes.

Figure 11 demonstrates the loss of packets when nodes fail. The number of nodes that have failed ranges from 0 to 30. It is found that the data loss rises when the failing nodes are increased [33]. FLEA-RPL decreased a packet loss ratio of 11% to 2 and 4%, respectively, for a failed node size of 30 compared with RPL, FL-RPL, and MRHOF-RPL. It is due to the traffic burden in conjunction with ETX and RER for choosing parents. As a result of the number of node failures, the DODAG root may fail because of the exchange of control packets for the route setup.

Scenario 2: data transfer rate with a limited number of data

Figure 6 depicts the parent alteration values of various RPL protocols. To assess the network stability, the parental change value of FLEA-RPL is noted, and its value is likened with standard RPL, FL-RPL, and MRHOF-RPL. The parent change values of standard RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL are 0.3, 0.4, 0.35, and 0.28, respectively. It is observed that the parent change value in FLEA-RPL is low compared to RPL, FL-RPL, and MRHOF-RPL. Figure 12 represents the average number of data concern. It is mainly due to the consideration of the load metric for the parent node selection.

The above Figure 13 depicts the regular end-to-end delay in the number of hops. The end-to-end interruption of standard RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL is 5.5, 5, 4.8, and 4.2 seconds, respectively. The results show that FLEA-RPL takes less delay compared to other protocols standard RPL, FL-RPL, and MRHOF-RPL. It is due to the diversification of network traffic during the parent selection across the network. Figure 14 illustrates network node residual energy with a data transfer rate of six packets per minute. In FLEA-RPL, it is noted that 90% of the network node's residual energy ranges between 62% and 66% approximately. The rest 10% of the network nodes have residual energy around 70% to 72%. FLEA-RPL shows increased network lifetime and residual energy compared to the standard RPL, FL-RPL, and MRHOF-RPL.

The above Figure 14 depicts the packet loss of RPL, FL-RPL, FLEA-RPL, and MRHOF- RPL by varying the network size with the data transfer rate of six packets per minute. The

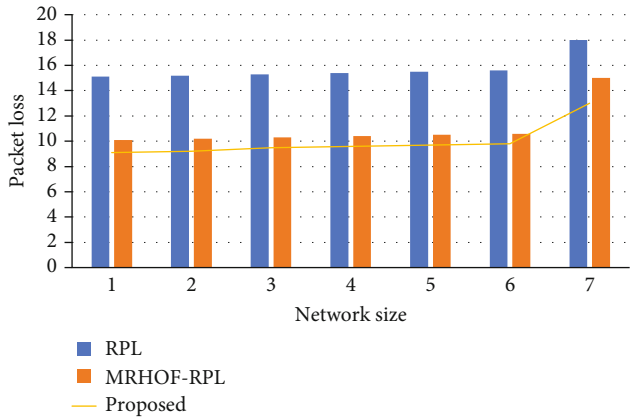


Figure 15: Packet loss in the network.

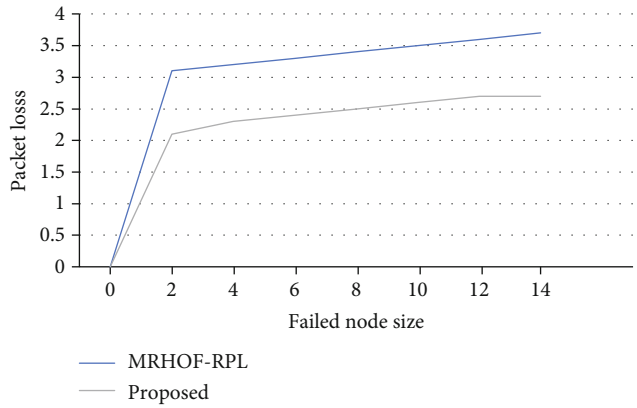


Figure 16: Node failure scenario with lesser packet loss.

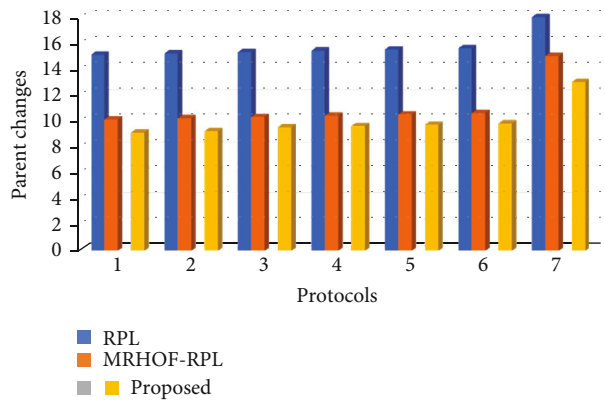


Figure 17: Comparison with different scenarios in the system.

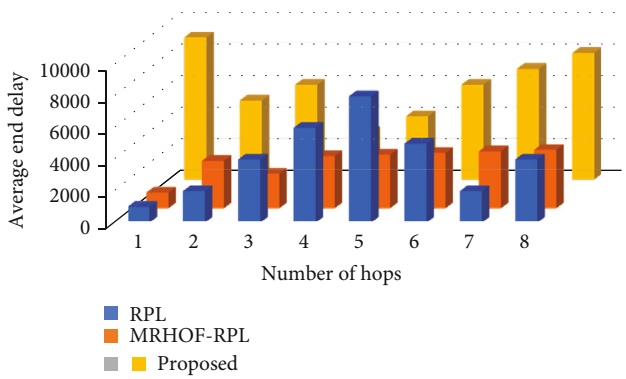


Figure 18: Delay time between the nodes.

number of failed nodes varies from 0 to 30. It is observed that there is an increase in packet loss, as the number of faulty nodes increases. As RPL does not consider the link quality metric for the parent selection, it results in high packet loss. MRHOF-RPL considers only the link quality for the parent selection. Hence, the battery depletes early, resulting in high packet loss. For a network size of 100 nodes, the packet loss ratio of standard RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL is 13%, 8%, 12%, and 7%, respectively.

Figure 15 depicts the packet damage in the occurrence of failed nodes, by the transfer rate of six packets per minute. The number of failed nodes varies from 0 to 30. It is observed that there is an increase in data damage, as the number of faulty nodes increases. As RPL does not reflect the link value metric for the parent collection, it results in high packet loss. For a failed node size of 30, FLEA-RPL has reduced the packet loss ratio by 7%, 2%, and 4%, respectively, compared to RPL, FL-RPL, and MRHOF-RPL. It is due to the consideration of traffic load along with ETX for the parent selection [34].

Scenario 3: transmission of data within a certain period

Figure 16 depicts the parent alteration values of various RPL protocols with the transfer rate of ten packets per minute. To assess the network stability [35], the parent change value of FLEA-RPL is noted, and it is compared with standard RPL, FL-RPL, and MRHOF-RPL. The parent change values of standard RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL are 0.4, 0.5, 0.45, and 0.35, respectively. It is observed that the parent change value in FLEA-RPL is low compared to RPL, FL-RPL, and MRHOF-RPL. It is due to the consideration of the load metric for the parent node selection. Thus, FLEA-RPL chooses the optimal parent in the DODAG, and it prolongs the network lifetime.

Figure 17 depicts the end-to-end delay corresponding to the number of hop counts. The latency of standard RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL are 6.5, 6, 5.5, and 5 seconds, respectively. The result shows that the FLEA-RPL takes a smaller amount of interruption compared to other protocols standard RPL, FL-RPL, and MRHOF-RPL. It is due to the diversification of network traffic during the parent selection across the network.

Figure 18 shows the residual energy of network nodes when data is transferred at a rate of ten packets per minute, as shown in the example above. There are several interesting findings in FLEA-RPL, such as the fact that the total residual energy of network nodes varies between 51 percent and 56 percent. When compared to the conventional RPL, FL-RPL, and MRHOF-RPL, the FLEA-RPL exhibits increased network lifespan and residual energy, respectively. It is because of the evaluation of RER that the optimum parent selection for data transfer to the DODAG root has been determined for data transmission.

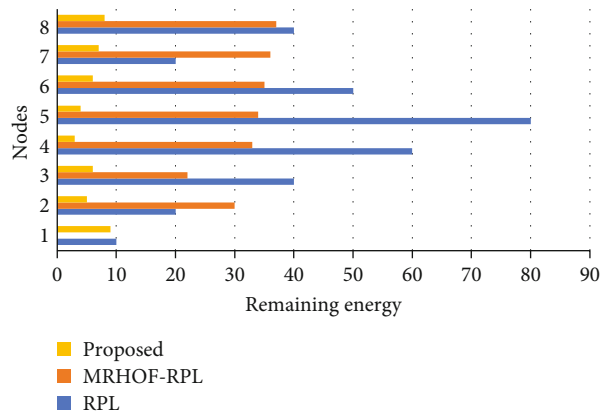


Figure 19: Network nodes residual energy.

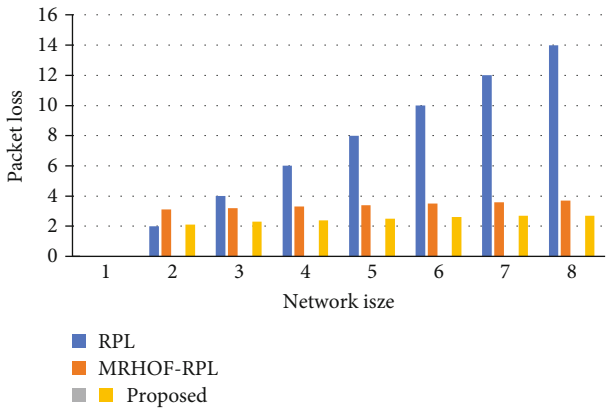


Figure 20: Ratio between packets and the network within the system.

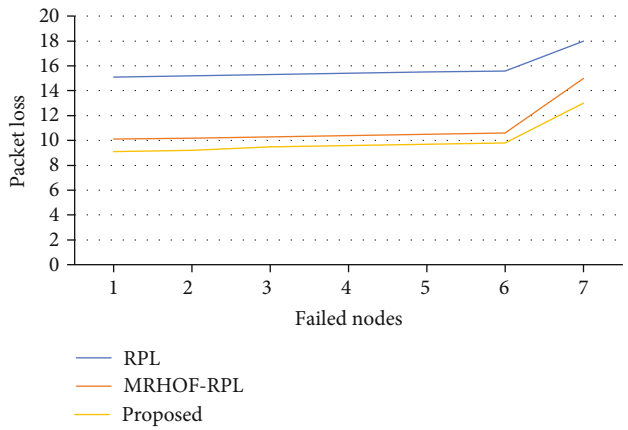


Figure 21: Ratio between packet loss and attempted nodes in the protocol.

Figure 19 depicts the packet loss ratio of RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL as a function of network size for the four types of RPL. Packet loss ratios of conventional RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL are 17 percent, 16 percent, 13 percent, and 10 percent for networks with 100 nodes, respectively, according to the packet loss ratio table. As the number of network nodes grows, it has been found that the amount of packet loss increases as a result. It is due to the evaluation of traffic load, as well as ETX, while making the decision on which parent to use.

Figure 20 depicts the device packet loss in the attendance of failed nodes. The number of failed nodes varies from 0 to 30. It is observed that there is an increase in packet loss, as the number of faulty nodes increases. As RPL does not consider the link quality metric for the parent selection, it results in high packet loss. For a failed node size of 30, FLEA-RPL has reduced the packet loss ratio by 15%, 8%, and 10%, respectively, compared to RPL, FL-RPL, and MRHOF-RPL. Figure 21 represents the packet loss and the attempted nodes in the routing protocol.

5. Conclusion

Because the Industrial Internet of Things devices are energizing, it is essential to route the liveliness on the nodes. The research effort aims to address the Internet of Things routing protocol issues. This is why an enhancement is being made to the standard RPL routing protocol. A Fuzzy Logic-based Energy-Aware RPL (FLEA-RPL) protocol is first and primarily proposed for the Internet of Things. To choose the most suitable route for data transfer, it utilizes a flushing logic for ETX, Load, and RER indicators. The results of the simulation show that it increases the lifetime of the network to a certain extent. Second, the Internet of Things (IoT) Multilayer Energy-Aware RPL (MCEA-RPL) protocol is recommended. The network is organized into clusters of the same size. It then combines fluid logic with the RER and ETX routing parameters to find the greatest way for data transfer. The information is gathered via the cluster head node, then the aggregated data is sent to the sink node. The results of the simulation suggest that as indicated in the table, MCEA-RPL extends network life compared to existing routing protocols. Thirdly, the Internet of Things Enhanced Mobility Support RPL (EM-RPL) protocol is proposed. For the calculation of the hand-off value, the fuzzy logic is applied to the RSSI and PER metrics. If the hand-off value goes above the threshold limit, the system immediately starts to look for an alternate path to avoid the issue. As a consequence, it reduces the number of route breaks caused by movement and the quantity of data transfer. As a result of the simulation results, it is evident that EM-RPL improves network node mobility. Many routing techniques are proposed in this research to prolong the Internet of Things network life. However, as explained shortly below, the proposed work may be extended in the future. A limited number of sink nodes are used in the present research to collect information from the network, which simplifies the architecture.

Data Availability

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] O. Gaddour, A. Koubaa, and M. Abid, "Quality-of-service aware routing for static and mobile IPv6-based low-power and lossy sensor networks using RPL," *Ad Hoc Networks*, vol. 33, no. 1, pp. 233–256, 2015.

[2] O. Gaddour, A. Koubaa, R. Rangarajan, O. Cheikhrouhou, E. Tovar, and M. Abid, "Co-rpl: Rpl routing for mobile low power wireless sensor networks using corona mechanism," in *Proceedings of the 9th IEEE international symposium on industrial embedded systems (SIES 2014)*, pp. 200–209, Pisa, Italy, 2014.

[3] F. Gara, L. B. Saad, E. B. Hamida, B. Tourancheau, and R. B. Ayed, "An adaptive timer for rpl to handle mobility in wireless sensor networks," in *2016 International wireless communications and mobile computing conference (IWCMC)*, pp. 678–683, Paphos, Cyprus, 2016.

[4] B. Ghaleb, A. Y. Al-Dubai, E. Ekonomou, I. Romdhani, Y. Nasser, and A. Boukerche, "A novel adaptive and efficient routing update scheme for low-power lossy networks in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5177–5189, 2018.

[5] Z. Latib, A. Jamil, N. Alduais, J. Abdullah, L. Audah, and R. Alias, "Strategies for a better performance of rpl under mobility in wireless sensor networks," in , Article ID 020002*AIP Conference Proceedings*, vol. 1883, 2017.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): a vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[7] A. Hassan, S. Alshomrani, A. Altalhi, and S. Ahsan, "Improved routing metrics for energy constrained interconnected devices in low-power and lossy networks," *Journal of Communications and Networks*, vol. 18, no. 3, pp. 327–332, 2016.

[8] S. Goyal and T. Chand, "Improved trickle algorithm for routing protocol for low power and lossy networks," *IEEE Sensors Journal*, vol. 18, no. 5, pp. 2178–2183, 2018.

[9] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.

[10] M. S. Tomar and P. K. Shukla, "Energy Efficient Gravitational Search Algorithm and Fuzzy Based Clustering With Hop Count Based Routing For Wireless Sensor Network," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27849–27870, 2019.

[11] O. Iova, F. Theoleyre, and T. Noel, "Using multiparent routing in rpl to increase the stability and the lifetime of the network," *Ad Hoc Networks*, vol. 29, no. 1, pp. 45–62, 2015.

[12] S. Izquierdo and L. R. Izquierdo, *Mamdani Fuzzy Systems for Modelling and Simulation: A Critical Assessment*, vol. 21, no. 3, pp. 1–15, 2017.

[13] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," *Transaction on IoT and Cloud computing*, vol. 3, no. 1, pp. 11–17, 2015.

[14] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *2012 10th international conference on frontiers of information technology*, pp. 257–260, Pakistan, Islamabad, 2012.

[15] T. Harshavardhana, B. Vineeth, S. Anand, and M. Hegde, "Power control and cross-layer design of rpl objective function for low power and lossy networks," in *2018 10th International Conference on Communication Systems and Networks (COMSNETS)*, pp. 214–219, Bengaluru, India, 2018.

[16] H. Kharrufa, H. Al-Kashoash, and A. H. Kemp, "A game theoretic optimization of rpl for mobile internet of things applications," *IEEE Sensors Journal*, vol. 18, no. 6, pp. 2520–2530, 2018.

[17] H.-S. Kim, H. Cho, H. Kim, and S. Bahk, "Dt-rpl: diverse bidirectional traffic delivery through rpl routing protocol in low power and lossy networks," *Computer Networks*, vol. 126, no. 1, pp. 150–161, 2017.

[18] H.-S. Kim, J. Paek, and S. Bahk, "Qu-rpl: queue utilization based rpl for load balancing in large scale industrial applications," in *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 265–273, Seattle, WA, USA, 2015.

[19] J. Ko and M. Chang, "Momoro: providing mobility support for low-power wireless applications," *IEEE Systems Journal*, vol. 9, no. 2, pp. 585–594, 2015.

[20] H. Lamaazi, N. Benamar, and A. J. Jara, "Rpl-based networks in static and mobile environment: a performance assessment analysis," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 320–333, 2018.

[21] U. P. Rao, P. K. Shukla, C. Trivedi, and S. Gupta, *Blockchain for Information Security and Privacy*, Z. S. Shibeshi, Ed., Auerbach Publications, 1st edition, 2021.

[22] H. Lamaazi and N. Benamar, "OF-EC: a novel energy consumption aware objective function for RPL based on fuzzy logic.," *Journal of Network and Computer Applications*, vol. 117, no. 1, pp. 42–58, 2018.

[23] P. Kautoo, P. K. Shukla, and S. Silakari, "Trust formulization in dynamic source routing protocol using SVM," *International Journal of Information Technology and Computer Science (IJITCS)*, vol. 6, pp. 43–50, 2014.

[24] B. Butani, P. K. Shukla, and S. Silakari, "An exhaustive survey on physical node capture attack in WSN," *International Journal of Computer Applications*, vol. 95, no. 3, pp. 32–39, 2014.

[25] R. Bhatt, P. Maheshwary, P. Shukla, P. Shukla, M. Shrivastava, and S. Changlani, "Implementation of Fruit Fly Optimization Algorithm (FFOA) to escalate the attacking efficiency of node capture attack in Wireless Sensor Networks (WSN)," *Computer Communications*, vol. 149, pp. 134–145, 2020.

[26] R. Gupta and P. K. Shukla, "Performance analysis of anti-phishing tools and study of classification data mining algorithms for a novel anti-phishing system," *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 7, no. 12, pp. 70–77, 2015.

[27] A. S. Rajawat, P. Bedi, S. B. Goyal et al., "Securing 5G-IoT device connectivity and coverage using Boltzmann machine keys generation," *Mathematical Problems in Engineering*, vol. 2021, Article ID 2330049, 10 pages, 2021.

[28] M. K. Ahirwar, P. K. Shukla, and R. Singhai, "CBO-IE: a data mining approach for healthcare IoT dataset using chaotic biogeography-based optimization and information entropy,"

Scientific Programming, vol. 2021, Article ID 8715668, 14 pages, 2021.

[29] M. Gupta, K. K. Gupta, M. R. Khosravi, P. K. Shukla, S. Kautish, and A. Shankar, "An intelligent session key-based hybrid lightweight image encryption algorithm using logistic-tent map and crossover operator for internet of multimedia things," *Wireless Personal Communications*, vol. 121, 2021.

[30] A. Khare, R. Gupta, and P. K. Shukla, "Improving the protection of wireless sensor network using a black hole optimization algorithm (BHOA) on best feasible node capture attack," in *IoT and Analytics for Sensor Networks. Lecture Notes in Networks and Systems*, P. Nayak, S. Pal, and S. L. Peng, Eds., vol. 244, Springer, Singapore, 2022.

[31] M. Gupta, K. K. Gupta, and P. K. Shukla, "Session key based novel lightweight image encryption algorithm using a hybrid of Chebyshev chaotic map and crossover," *Multimedia Tools and Applications*, vol. 80, no. 25, pp. 33843–33863, 2021.

[32] A. K. Saxena, S. Sinha, and P. Shukla, "Design and development of image security technique by using cryptography and steganography: a combine approach," *International Journal of image, Graphics and Signal Processing (IJIGSP)*, vol. 10, no. 4, pp. 13–21, 2018.

[33] N. Tarwani, U. Chourasia, and P. K. Shukla, "Survey of cyberbullying detection on social media big-data," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 831–835, 2017.

[34] D. Parwani, A. Dutta, P. K. Shukla, and M. Tahiliyani, "Various techniques of DDoS attacks detection and prevention at cloud: a survey," *Oriental Journal of Computer Science & Technology*, vol. 8, pp. 110–120, 2015.

[35] J. Mahatpure, M. Motwani, and P. K. Shukla, "An electronic prescription system powered by speech recognition, natural language processing and blockchain technology," *International Journal of Scientific & Technology Research*, vol. 8, no. 8, pp. 1454–1462, 2019.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3426811, 8 pages
https://doi.org/10.1155/2022/3426811

Research Article

Secure Data Transmission Using Quantum Cryptography in Fog Computing

Cherry Mangla,[1] **Shalli Rani**,[1] **and Henry Kwame Atiglah**[2]

[1]*Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab 140401, India*
[2]*Department of Electrical and Electronics Engineering, Tamale Technical University, Ghana*

Correspondence should be addressed to Henry Kwame Atiglah; hkatiglah@tatu.edu.gh

Received 26 November 2021; Accepted 3 January 2022; Published 22 January 2022

Academic Editor: Muhammad Asghar Khan

Fog computing's idea is to bring virtual existence into objects used on a daily basis. The "objects" layer of fog architecture is also known as the smart object layer (SOL). SOL has provided the fog network with a strong platform to outperform. Although the fog architecture decentralizes data, uses more data centers, and collects and transmits it to adjacent servers for faster processing in fog networks, it faces several security challenges. The security problems of fog computing need to be alleviated for the exploitation of all benefits of fog computing in classical networks. This article has addressed the security challenges in fog computing, potential solutions via quantum cryptography, a use case portraying the importance of quantum cryptography in fog computing along future scope, and research directions.

1. Introduction

In the continuous evolution of the computer age, increased demand for Internet of Things (IoT) devices and the cloud has requested a middleware. To cater to the request, fog computing has emerged to provide fast and secure services. Fog computing's idea is to bring virtual existence into objects used on a daily basis. The "objects" layer of fog architecture is also known as the smart object layer (SOL). SOL has provided the fog network with a strong platform to outperform. Although the fog architecture decentralizes data, uses more data centers, and collects and transmits it to adjacent servers for faster processing, it faces several security challenges. The security problems of fog computing need to be alleviated for the exploitation of all benefits of fog computing and IoT in classical networks.

It has extended the cloud-based framework to the edge of the structure by increasing data transformation and decision making on IoT fog devices and allowing more effective communication with mediator nodes. Fog computing has extended the cloud architecture by using fog nodes (FN) on the edge of the network. It has integrated IoT and cloud concepts to provide various characteristics like low latency and location awareness, support for geographic distribution, end device mobility, the capacity of processing a high number of nodes, wireless access, real-time applications, improved quality of service, and heterogeneity [1, 2]. Fog servers act as mini data centers for various applications such as smart cities, big data analysis, and distributed data collections.

Although all these characteristics are prominent in fog computing, security is rising as one of the most gigantic challenges for it. Some current solutions in the context of cloud architecture may address some of the security problems. However, security is still one of the main concerns while collecting and processing data from various sources, and the most popular way to tackle it is data encryption. With the advent of differently distributed frameworks like cloud computing, IoT, and fog computing, securing ubiquitary computation that involves many collaborations is considered an open research area that has attracted the attention of researchers to develop novel protocols. Existing security protocols include Transport Layer Security (TLS), Secure Socket Layer (SSL), and Internet Protocol security (IPsec). Recent works primarily focus on the challenges and solutions of fog computing to safeguard data

from various threats. Consequently, quantum cryptography has begun to replace the traditional methods of encryption for enhanced data security [3, 4].

Quantum computing (QC) is a way that provides a new approach to computation over classical computing. The laws of quantum mechanics provide power to QC over classical systems. Quantum cryptography is one of the branches of QC, responsible for the secure transmission of data from one point to another. Although researchers are working on all the fields of quantum cryptography to make it work, right now only Quantum Key Distribution (QKD) is the part that is providing quantum security over classical networks in securing key exchange. The quantum channel being provided by QKD is safe from all types of attacks (classical adversary and quantum adversary). In QC, the processing is more fast and secure. QC is working on the laws of real parallel computing. Quantum cryptography is difficult to breach because it operates on both states (1 and 0) at the same time. In quantum cryptography, photons keep on spinning, which means they keep on changing the position, making the qubits dynamic in nature. Consequently, the problem of intrusion is avoided on a large scale with quantum cryptography. It can be used to secure the fog architecture where data of heterogeneous devices is gathered and processed, while increasing the transmission speed of data by having data centers in various parts of the city. In this paper, we are proposing the use of QKD for secure key exchange in fog computing architecture.

The rest of the paper is organized as follows: in the second section, we discuss fog computing architecture; next, in the third section, security attacks on the fog architecture's different communication layers (as discussed in Figure 1) are discussed. In the next section, solutions for fog computing security issues in quantum cryptography are discussed along with the importance of using quantum cryptography over classical cryptography, followed by a use case in Section V, illustrating the importance of secure and fast data transmission in the case of healthcare along with open research challenges in Section VI. Lastly, the article is concluded with the future scope.

2. A Brief Introduction to Fog Computing Architecture

Fog computing is a highly virtualized platform, and it is not a substitute for cloud computing. It provides storage, computation, and networking services between conventional cloud data centers and end devices. Fog computing architecture is a distributed computational framework that expands the cloud computing model by shifting data processing closer to end devices. It results in low system response, by reducing the time taken by the huge data transmission traveling from devices to cloud and vice versa in IoT. Fog architecture as shown in Figure 1 is a three-layer architecture. The first layer is composed of end devices of IoT (known as end-users), the second layer of fog architecture consists of FN and fog services known as the fog layer, and the third layer is comprised of cloud data centers. The core layer of fog architecture works as a gateway between FN and the cloud. It has dedicated interfaces to communicate with the fog layer. Fog layers can have multiple numbers of FNs to interact with end-users and to process the related information. The FN can be small cell base stations with proper storage, cellular base stations with processing capability, and Wi-Fi access points which can be placed on fixed locations (such as high buildings and roadside units) or mobile things (such as buses and trains).

In the given architecture, the core layer of the network has software-defined networking (SDN) nodes that accurately supervise the network and has extensive governance. Before transmitting the data of end devices of the bottom layer to the cloud, fog computing eliminates all potentially bad and ambiguous contents to reduce the load of the cloud. This is where security challenges arise and can make the transmission vulnerable. The main reason for the vulnerable security attacks is the direct interaction of the fog computing layer with heterogeneous devices. A strong and novel mechanism is required to mitigate this challenge. In subsequent sections, we have summarised all the popular attacks on various layers of fog architecture. In Section IV, solutions to all these attacks in QKD are mentioned after discussing, in brief, the importance of quantum cryptography over classical cryptography in the future.

3. Attacks on Network Communication Layers of Fog Computing

Various attacks on three layers (mentioned in Figure 1) are as follows.

3.1. Cloud Layer. It is the uppermost layer of fog architecture. It is comprised of the workings of both the physical layer and the data link layer. It consists of many sensing technologies, for instance, radio-frequency identification (RFID) tags, wireless sensor networks (WSNs), and near-field communications (NFCs), which all contribute towards building IoT infrastructure [5, 6]. The cloud layer has the following security challenges:

(a) *Node capturing*: node capturing changes or destroys the identification of physical objects which are part of IoT.

(b) *Spoofing*: hackers change the sensed data which ultimately changes the digital signals.

(c) *Denial of service (DoS)*: transmission of data to the upper layer for network transmission and processing is denied.

3.2. Edge Layer. It consists of the workings of network and transport layers. It receives the data from the cloud layer and transfers it to the fog server to process it further. A massive amount of data is generated by day-to-day objects, in which data is processed using various network technologies, such as LANs, WANs, and transmission mediums like Wi-Fi, Bluetooth, and Zigbee. The security challenges faced by the edge layer are as follows:

(a) *Selective forwarding*: in selective forwarding, data packets are selectively dropped or blocked by malicious nodes.

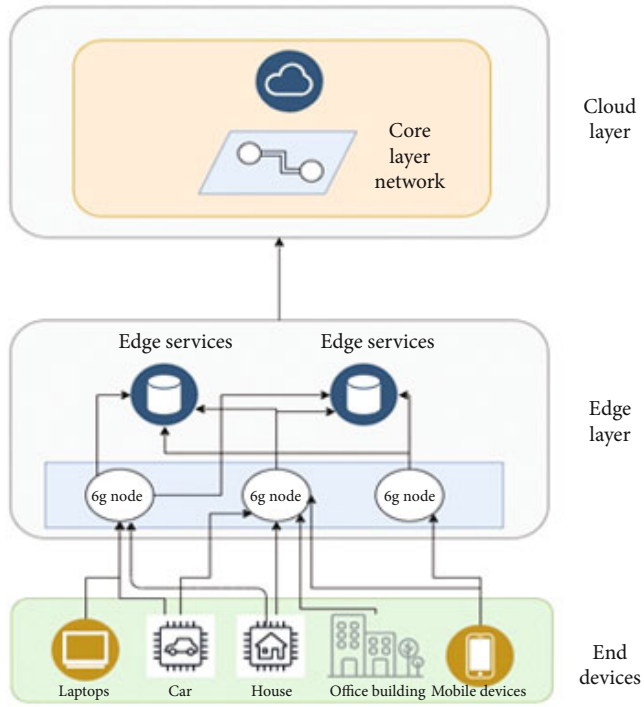


Figure 1: Fog computing architecture.

(b) *Blackhole*: false routing information is created, and all the data packets are forwarded to that address.

(c) *Wormhole*: false storage information is given to bits of data during relocation.

3.3. End Layer. The end layer consists of two parts: (a) user and (b) business layer aspects. Various applications are being differentiated using various IoT application deployment platforms [7, 8]. Security attacks faced by the end layer are as follows:

(a) *Sniffers/loggers*: personal information (like passwords and credit/debit card details) is extracted by attackers using sniffing.

(b) *Phishing attack*: credentials are accessed using the email address of the main authority, through which data can be damaged.

(c) *Node identification*: every phase of the application has a different set of users; attackers gain illegal access by harming the application.

(d) *Distributed DoS*: single system is attacked using multiple infected systems.

4. Mitigation of Fog Computing Security Issues in Quantum Cryptography

Fog computing is used as an extra layer to provide an advantage between the IoT devices and the cloud layer. It helps to reduce the load on the cloud because processed data is transmitted to the FN. There are many challenges at the fog layer in terms of security and reliability of transmitted data due to direct transmission with end devices. Here, we are proposing the use of quantum cryptography's QKD as a solution to secure it from classical as well as quantum adversaries. In subsection A, we are illustrating the importance of QKD over classical security schemes, and the B subsection is showing various QKD protocols that can be used to mitigate various above-mentioned attacks.

4.1. Importance of QKD Over Classical Cryptography. A few major differences between the classical and the quantum cryptography are illustrated in this subsection. Fog computing is an emerging technology that plays a major role in future applications. So it is necessary to secure it from classical as well as quantum adversaries. Public key cryptography schemes are easily breakable using quantum computers as shown by Shor in 1994 [9]. Also, all the classical algorithms are venerable to quantum cryptography [10]. In [11], the authors have proposed the use of blind quantum computing in fog architecture, making it feasible to merge quantum with fog computing. In this article, we have proposed the use of the QKD scheme in fog architectures to secure it against attacks in the near future. Table 1 illustrates the major differences between classical cryptography and quantum cryptography.

(a) *Fundamental dimension*: in classical cryptography, there is no such principle by which it can be defined whether the network is eavesdropped or not, whereas in quantum cryptography, two devices share correlated states; if an intruder tries to eavesdrop at any point, the state of the photon instantly changes providing more security.

Table 1: Comparison of classical cryptography and quantum cryptography.

	Classical cryptography	Quantum cryptography
Fundamental dimension	In classical cryptography, an eavesdropping attack cannot be detected as the number of keys keeps increasing every 18 months on average.	In quantum cryptography, it is easy to detect eavesdropping due to principles of quantum mechanics; minimum changes are required, i.e., it incurs less cost.
Commercial dimension	Classical cryptography can be implemented on small hardware.	Quantum cryptography is in the infant stage and requires a lot of work to shrink on small hardware.
Application dimension	Security is provided through factors of large numbers in classical cryptography.	Shor's algorithm has proven that factors of any large numbers can be easily found, leaving classical cryptography insecure.
Technological dimension	Can transmit data to any length	Quantum cryptography has only achieved a maximum of 4600 km.

(b) *Commercial dimension*: although classical cryptography is more scalable than quantum in recent times as not all the channels are made of optic wires when quantum computers will be on the market, it will be necessary to secure classical networks instead of changing the whole.

(c) *Application dimension*: most of the classical cryptography schemes are based on the factorization of the two highest prime numbers, which can be easily calculated with parallel computing of quantum principles. Shor has proven it in 1994. So all the classical cryptography schemes are vulnerable to the future of computing.

(d) *Technological dimension*: in this field, recently, quantum cryptography is lacking as classical cryptography can provide security to any length, whereas quantum cryptography has achieved the maximum of 4600 km distance [12].

In article [13], the authors have compared the performance of various block ciphers (DES (Classical and Quantum), TDES (Classical and Quantum), Blowfish (Classical and Quantum), AES (Classical and Quantum)) and the Avalanche Effect based on encryption time, decryption time, and throughput for various file sizes from 100 kb to 600 kb. Their experiments are clearly showing the better performance of quantum cryptography. They have used the BB84 protocol of QKD for comparison. Figure 2 shows the results of the throughput with various file sizes of all four schemes in both classical and quantum key exchanges.

4.2. Quantum Key Distribution: A Solution to the Fog Computing Security Threats. Machines that are based on quantum mechanical principles (superposition and entanglement) are known as quantum computers. The quantum computer can process numerous combinations of ones and zeros at the same time at a very high speed, which is termed parallel processing, making its working more complex than traditional systems and helping to easily compute the security algorithms based on mathematical computations. Therefore, it is hard to breach the key distribution performed using quantum mechanics principles. QKD is the only cryptographic scheme of quantum cryptography that can be performed on classical systems to provide a more secure key exchange. Other cryptographic schemes are mentioned by many researchers [14], but only QKD feasibly works over classical networks.

Security threats of authentication in the fog layer can be mitigated with the help of QKD. In the various critical applications of IoT such as smart health, smart grid and smart industries, etc. authentication and privacy are the major challenging issues. End Layer works as a front face in the fog hierarchy. Where the main security issue is authentication. Due to the user interface its security issues and solutions are a bit different from other layers. For data transmission, it is very crucial to secure the Edge layer, as the whole data is stored and processed on the edge layer. It is necessary to secure the data, keeping in mind the CIA model (confidentiality, availability, and integrity). Major attacks on this layer are DoS and eavesdropping.

The cloud layer of the fog hierarchy is also known as end devices. Various technologies are used to collect data from various devices like WSN, RFID tags, and NFC. Because of the heterogeneous data of IoT devices gathered in the fog layer, security becomes a crucial aspect even in fog computing.

In Figure 3, at the different layers of fog hierarchy, we have shown the potential threats and their solutions in the form of quantum cryptography protocols. The properties on which the protocols are working are also discussed adjacent to the solutions.

The following is the description of various attacks on different layers of fog architecture (Figure 1).

4.2.1. Security Solutions in Cloud Layer. The security issues in the cloud layer of fog architecture can be resolved via quantum computing's property "Superposition." Using the superposition property of quantum computing, data can be kept safe. It changes the position of qubits when intruders try to read the data. This property is used in following QKD protocols to mitigate security threats in the cloud layer of fog computing.

(a) *BB84*: a secure channel is established between sender and receiver, using polarized photons to mitigate authentication issues in fog computing [15].

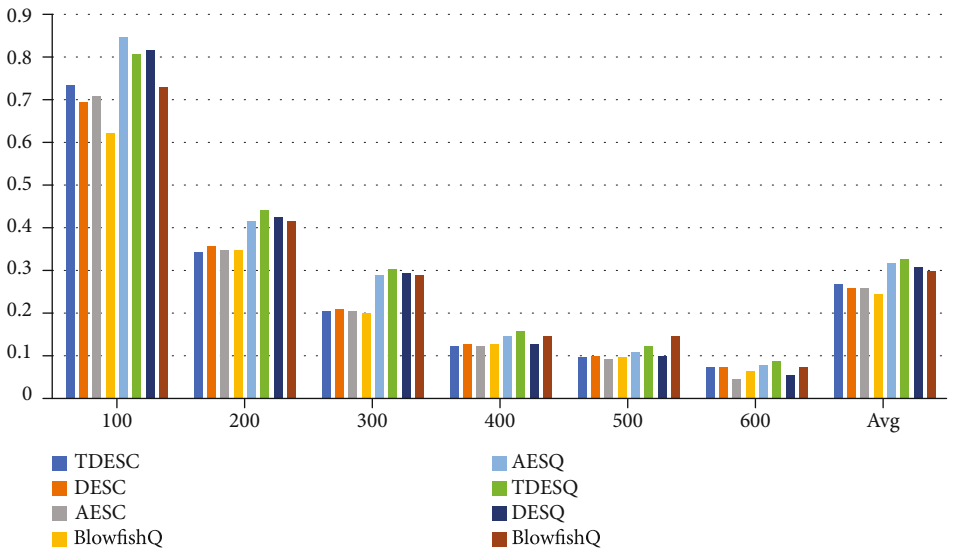


Figure 2: Throughput with different file sizes [13].

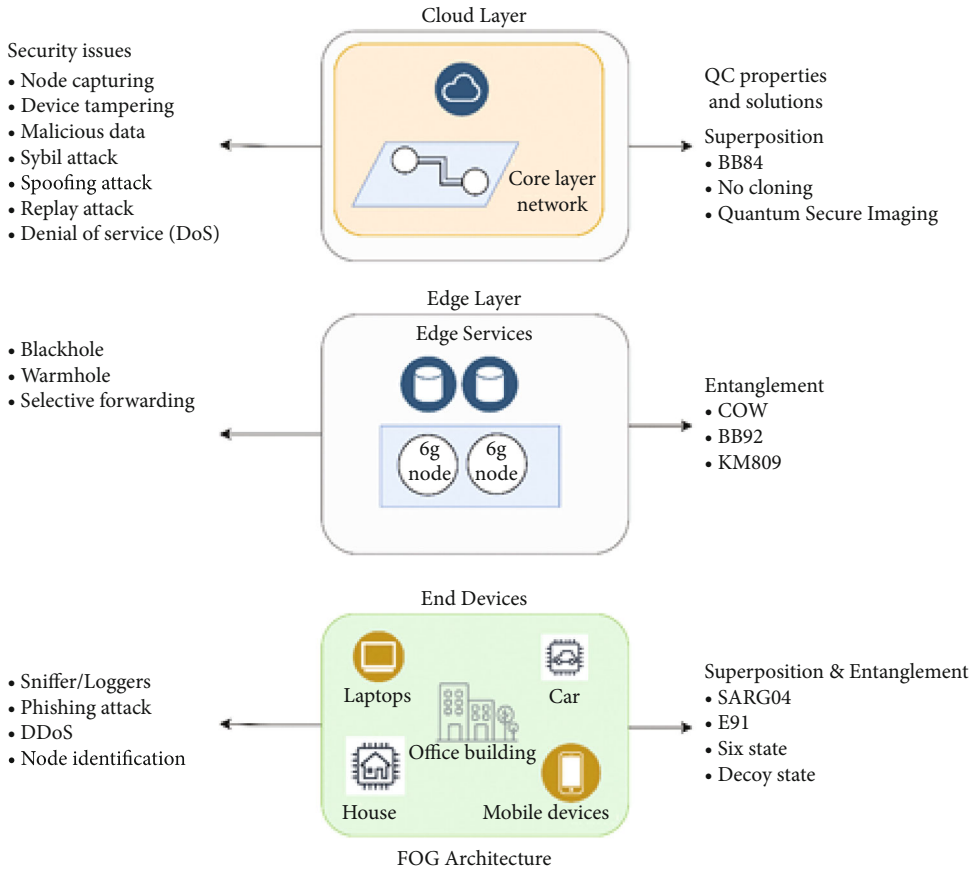


Figure 3: The security threats and solutions using quantum cryptography classification in fog computing.

(b) *No-cloning theorem*: in QC, no-cloning theorem never let copy data, copying data is one of the main issues of fog networks, i.e., adding fake nodes by copying data. As photons travel from one place to another, they keep on changing their positions.

(c) *Quantum secure imaging*: this is used to secure the layer from signal jamming.

4.2.2. Security Solutions in Edge Layer. To secure the edge layer, protocols based on quantum entanglement can be helpful. Secoqc QKD network, KMB09, photon spinning, COW protocol, and BB84 are these properties. No one can access the data when entanglement-based protocols are used on the edge layer of fog computing. Quantum annealing is a way to find the best solution for problems having multiple variables. Current quantum computers can only implement quantum annealing [16, 17], a subset of a quantum computer. Although only quantum annealing can be implemented, it embeds the properties of both quantum superposition and quantum entanglement. The following protocols are based on these properties:

(a) In Secoqc, QKD's maximum number of keys is generated and stored. These are used according to the traffic on the network. In this, it will help in the selective forwarding issue [6]

(b) COW (coherent one-way) protocol works on the principle of quantum entanglement. It transmits the data at the speed of light

(c) The KMB09 protocol works on the Heisenberg uncertainty principle. It is impossible to know simultaneously the exact position and momentum of a particle

4.2.3. Solutions in End Layer. QKD's protocols used to alleviate security issues in the end layer are using both properties of QC: superposition and entanglement. The following are the protocols against the security threats of the end layer in the fog hierarchy.

(a) The E91 protocol works on the property of entanglement, where both the sender and the receiver could have one photon each. Therefore, sniffers will not be able to log in to the system

(b) The six-state uses a six-state polarization scheme on three orthogonal bases

5. A Potential Use Case: Integrated Fog-Assisted and Quantum Secure Health Care System

We used an integrated fog-assisted and quantum secure health care system as an example use case to elaborate the importance of quantum cryptography protocol encryption in fog computing architecture and networks. An integrated fog-assisted and quantum secure health care system is illustrated to give benefits like anytime availability of patient's information for subscribing proper medication and treatment depending upon history and patient's data to save patients. In this use case, the whole scenario is divided into two subsystems.

5.1. Healthcare Subsystem for Limited Area. The healthcare subsystem for the limited area is subdivided into handling and monitoring patient data in a limited area, for instance, in region 1 of Figure 4. For sending and receiving signals for a region's fog node, a patient should be in the vicinity of it to communicate with that specific node. A patient wearing smart equipment can send numerous pieces of information about its location and everything when it comes to the coverage area of a specific fog node. The communication between the fog node and the patient's smart device makes sure the nearest specialist is based on the saved information of the patient. Patient health data is the most sensitive data, which needs strong encryption. Therefore, that data is encrypted using QKD's BB84 encryption to safeguard it from intruders. The healthcare system working in a limited area can receive the patent's file through that smart device and follow the following steps:

(a) *Step 1*: the fog node monitors and controls the health data of the patient. If the patient needs any help, then this system can provide the patient's data and it will be mapped with the medical history of the patient. Hospitals just need to authenticate the data by putting the patient's medical id on the server. On the fog node, an intelligent secure heath care control algorithm (limited area) is implemented. By using real-time patient data, it calculates the health condition of the patient. For instance, if any patient's pacemaker is not working (medical equipment), then doctors receive real-time data of the patient. This step should be implemented in real-time. Due to traveling, the response time can get impacted as the fog nodes change when the region changes and the smart device has to cope with frequently changing nodes, so the traveling time shows some impact.

(b) *Step 2*: the fog node performs some crucial steps such as it encrypts the data, preprocesses it, and changes it to statistical information useful to medical personnel before storing it to cloud servers.

5.2. Healthcare Subsystem for Large Area. The healthcare subsystem for a large area is responsible for handling the medical data from a large area perspective, for instance, combined regions 1 to 4 in Figure 4. Figure 4 depicts the distant cloud server which collects information from all the four fog nodes present in all four regions. Data mining is performed to mine the medical information. There are two algorithms used to process the data in a large area: one is an intelligent health care algorithm (for a large area) and the other one is a dynamic transmission algorithm. In the large area healthcare subsystem (on the cloud), a more difficult intelligent healthcare algorithm is used as compared to the one used in the fog nodes of the different regions. The reason for the different levels of complication is that the one present on the cloud is responsible for predicting the medical issues based on historical data as well as the real-time data fog nodes are sending. It takes more time

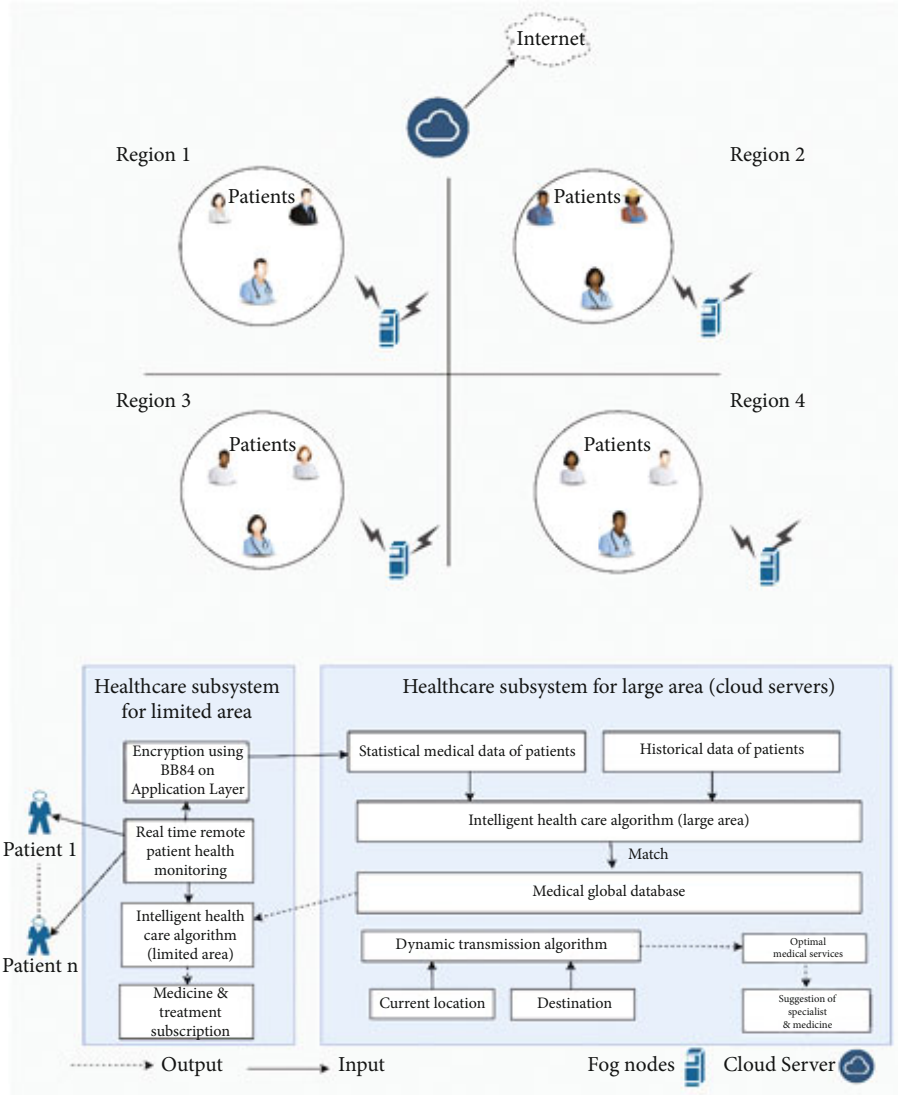


Figure 4: A fog-assisted health care system: an overview.

in processing on cloud servers than on fog nodes. Here, fog computing provides an advantage as the processing and capturing of data is done in two steps now. The mining results of this algorithm subscribe best medical treatment and medicines based on large area data comparison. After taking decisions, the results are sent to all the fog nodes in the city. The main aim is to save personal medical information by QKD protocol and process of authentication to avoid the manipulations of data of patients.

6. Open Research Challenges of Fog Computing

The network of the fog layer is dynamic in nature due to the mobility of end devices. It poses the following research challenges of quantum cryptography in fog computing:

(i) *Infrastructure*: most infrastructure problems occur when fog nodes are not communicating, then quantum cryptography requires an extra layer of security against the malicious data being uploaded on FN. This requires the development of new techniques of security.

(ii) *Virtualization*: it is the act of creating virtual network nodes when end users are being assigned different nodes continuously, as per the dynamic nature of fog nodes, it surges the problems of the virtual machine (VM) lifecycle, container, and context awareness. Quantum key distribution protocols are implemented by researchers as per the requirements of hardware for random key generation. However, if the nodes will also keep on changing, it will accelerate the problem which is again a major security threat.

(iii) *Resources and tasks*: tasks and resources are scheduled as per the time and availability correspondingly between end-users and fog nodes. The management can be better handled by QKD which will also safeguard the data. Due to the dynamic requirements of

resources as well as tasks, random key generation of quantum is an open research issue.

(iv) *Programmability*: the task of session management is difficult, and quantum cryptography algorithms for different sessions need different random key generations. Research is required to develop the common interface gateway of quantum cryptography for heterogeneous sessions of a single user.

7. Conclusion

In this article, a general description of fog computing's architecture is given along with security issues on its various layers. Quantum cryptography's QKD is provided as a solution for the security issues present on various layers of fog's architecture. A use case based on fog computing and quantum cryptography is illustrated along with a few open research challenges. Fog computing can make better decisions, and the service can be improved in the future. No system in today's world can be completely attack-free; researchers are working on providing a secured fog framework to keep the communications secure enough. The fog system's primary focus is on the need of decentralizing the safety model, and one of the best solutions currently is quantum cryptography. QKD can help in the data-sensitive applications of fog such as healthcare, critical industrial processes, and border security surveillance.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

References

[1] M. Pourkiani, M. Abedi, and M. A. Tahavori, "Improving the quality of service in wbsn based healthcare applications by using fog computing," in *2019 International Conference on Information and Communications Technology (ICOIACT)*, pp. 266–270, Yogyakarta, Indonesia, 2019.

[2] J. T. Chiang, J. J. Haas, J. Choi, and H. Yih-Chun, "Secure location verification using simultaneous multilateration," *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 584–591, 2012.

[3] R. A. Malaney, "Location-dependent communications using quantum entanglement," *Physical Review A*, vol. 81, no. 4, article 042319, 2010.

[4] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Generation Computer Systems*, vol. 108, p. 909, 2018.

[5] S. Wang, Y. Hou, F. Gao, and X. Ji, "A novel IoT access architecture for vehicle monitoring system," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 639–642, Reston, VA, USA, 2016.

[6] M. Dianati and R. Alléaume, "Transport layer protocols for the secoqc quantum key distribution (QKD) network," in *32nd IEEE Conference on Local Computer Networks (LCN 2007)*, pp. 1025–1034, Dublin, Ireland, 2007.

[7] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog computing security challenges and future directions [energy and security]," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 92–96, 2019.

[8] X. Li Da, W. He, and S. Li, "Internet of things in industries: a survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[9] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Santa Fe, NM, USA, 1994.

[10] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[11] Q. Zhiguo, K. Wang, and M. Zheng, "Secure quantum fog computing model based on blind quantum computation," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–11, 2021.

[12] Y.-A. Chen, Q. Zhang, T.-Y. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[13] P. Siva Lakshmi and G. Murali, "Comparison of classical and quantum cryptography using QKD simulator," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pp. 3543–3547, Chennai, India, 2017.

[14] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, no. 1, pp. 351–382, 2016.

[15] T. R. Raddo, S. Rommel, V. Land, C. Okonkwo, and I. T. Monroy, "Quantum data encryption as a service on demand: Eindhoven QKD network testbed," in *2019 21st International Conference on Transparent Optical Networks (ICTON),*, pp. 1–5, Angers, France, 2019.

[16] A. Nanda, D. Puthal, S. P. Mohanty, and U. Choppali, "A computing perspective of quantum cryptography [energy and security]," *Consumer Electronics Magazine*, vol. 7, no. 6, pp. 57–59, 2018.

[17] M. Jünger, E. Lobe, P. Mutzel et al., "Quantum annealing versus digital computing," *Journal of Experimental Algorithmics (JEA)*, vol. 26, pp. 1–30, 2021.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6953125, 27 pages
https://doi.org/10.1155/2022/6953125

Research Article

A Secure and Efficient Energy Trading Model Using Blockchain for a 5G-Deployed Smart Community

Adamu Sani Yahaya,[1] Nadeem Javaid,[1,2] Sameeh Ullah,[3] Rabiya Khalid,[1] Muhammad Umar Javed,[1] Rehan Ullah Khan,[4] Zahid Wadud,[5] and Muhammad Asghar Khan[6]

[1]*Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan*
[2]*School of Computer Science, University of Technology Sydney, Ultimo, NSW 2007, Australia*
[3]*School of Information Technology, Illinois State University USA, Normal, IL 61761, USA*
[4]*Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia*
[5]*Department of CSE, University of Engineering and Technology Peshawar, Peshawar 25000, Pakistan*
[6]*Hamdard Institute of Engineering and Technology, Hamdard University, Islamabad 44000, Pakistan*

Correspondence should be addressed to Nadeem Javaid; nadeemjavaidqau@gmail.com

Received 16 August 2021; Revised 17 December 2021; Accepted 23 December 2021; Published 17 January 2022

Academic Editor: Giuseppe Piro

A Smart Community (SC) is an essential part of the Internet of Energy (IoE), which helps to integrate Electric Vehicles (EVs) and distributed renewable energy sources in a smart grid. As a result of the potential privacy and security challenges in the distributed energy system, it is becoming a great problem to optimally schedule EVs' charging with different energy consumption patterns and perform reliable energy trading in the SC. In this paper, a blockchain-based privacy-preserving energy trading system for 5G-deployed SC is proposed. The proposed system is divided into two components: EVs and residential prosumers. In this system, a reputation-based distributed matching algorithm for EVs and a Reward-based Starvation Free Energy Allocation Policy (RSFEAP) for residential homes are presented. A short-term load forecasting model for EVs' charging using multiple linear regression is proposed to plan and manage the intermittent charging behavior of EVs. In the proposed system, identity-based encryption and homomorphic encryption techniques are integrated to protect the privacy of transactions and users, respectively. The performance of the proposed system for EVs' component is evaluated using convergence duration, forecasting accuracy, and executional and transactional costs as performance metrics. For the residential prosumers' component, the performance is evaluated using reward index, type of transactions, energy contributed, average convergence time, and the number of iterations as performance metrics. The simulation results for EVs' charging forecasting gives an accuracy of 99.25%. For the EVs matching algorithm, the proposed privacy-preserving algorithm converges faster than the bichromatic mutual nearest neighbor algorithm. For RSFEAP, the number of iterations for 50 prosumers is 8, which is smaller than the benchmark. Its convergence duration is also 10 times less than the benchmark scheme. Moreover, security and privacy analyses are presented. Finally, we carry out security vulnerability analysis of smart contracts to ensure that the proposed smart contracts are secure and bug-free against the common vulnerabilities' attacks. The results show that the smart contracts are secure against both internal and external attacks.

1. Introduction

Globally, the residential smart homes' market size is expected to be more than $50 billion before the year 2023. It is also observed that the number of households, which migrates to smart homes, has increased at an annual average growth rate of 14% from 2017. The increase in the number of smart homes has two impacts: benefits and issues. The benefits of the increase in the smart homes include saving of money, time, and energy as well as increase in the user

comfort. However, privacy and security challenges increase. In smart grids, a nanogrid is a smart home that has energy storage and generation sources, e.g., small scale wind turbines and photovoltaics [1]. The generated energy is stored using batteries and plug-in Electric Vehicles (EVs). A group of connected nanogrids within nearby neighborhoods establishes a microgrid, which allows local energy trading between the smart homes. There are two approaches to perform energy trading in the power system: centralized and distributed. The centralized approach is also known as the traditional energy trading system. It is a conventional approach that the smart grid uses for energy management. In the approach, a central control unit is used that manages, processes, and regulates energy transactions. However, this approach has some challenges, such as a single point of failure and security-privacy-related problems. Among the solutions provided to solve the centralized approach problems is the introduction of a distributed model. In [2], the authors propose a Peer-to-Peer (P2P) method for smart grid operations. The work provides an overview of the proposed strategies for wireless communication, distributed P2P energy trading, and P2P power grid control unit that enables the smart grid operations. The authors in [3] propose an energy trading model between islanded microgrids using distributed convex optimization techniques. In the model, a subgradient-based cost minimization algorithm is implemented, which converges to an optimal solution with minimum communication overhead. In [4], the authors propose a virtual framework incorporated with communication constraints, which also considers its impact on energy trading cost. The authors modify the distributed energy trading framework considered in the literature with more communication constraints, where the impact of the resulting virtualized microgrid framework is investigated on the overall trading costs. The authors in [5] propose a hierarchical framework to identify and categorize the key technologies and elements involved in P2P energy trading. The framework is developed and simulated using game theory. In distributed energy systems, adversary users heavily threaten the security and privacy of the system through many malicious exploitations [6], e.g., node impersonation, falsification, privacy leakages, and advertising fraudulent energy services.

Environmental pollution and climate change are major issues that disturb the Smart Communities (SCs). These issues are caused due to a tremendous increase in greenhouse gas emissions generated from fossil fuel-based vehicles. The introduction of EVs is among the solutions that are generally being accepted to resolve the environmental pollution problems [7]. As a long-term automotive technology, EVs are becoming popular in minimizing the total dependency on fossil fuel-based vehicles and reducing the emissions of greenhouse gas. However, as the number of EVs increases, the unorganized charging of EVs creates a new peak load. The reason is that it causes a serious energy instability problem in the distributed energy system. In order to overcome this issue, the capacity of power delivery is increased to solve the needs of new peak demand that is generated by the unorganized EVs. However, this results in a huge infrastructure cost. Moreover, a smart grid-based method is developed to enable EVs to communicate with the power grid and manage their charging needs. However, this process can cause a single point of failure as it is implemented in a centralized model. In addition, demand-supply mismatch and lack of trust challenges are still not resolved in the energy system. Another solution to manage energy for both residential homes and EVs is by exploring load forecasting models. In [8], the authors propose a Recurrent Inception Convolution Neural Network (RICNN) that combines 1-Dimensional CNN (1-D CNN) and Recurrent Neural Network (RNN) to forecast consumers' energy usage. The 1-D convolution inception module is used to calibrate the time forecasting, and the hidden state vector values are computed from the nearest time steps. The model is verified in terms of energy usage data of three large energy distribution complexes in South Korea. The authors in [9] present a probabilistic forecasting model for consumers to predict uncertainty and variability of the future load. In the model, Long Short-Term Memory (LSTM) is adopted to learn both the short-term and long-term dependencies among the load dataset. Pinball loss is used for training the parameters. The experiments are conducted using an open source dataset of Ireland. However, the energy management models, i.e., load forecasting models, use a centralized approach, which inherited its challenges.

Currently, as a result of the high benefit of Fifth-Generation (5G) technology against the previous-generation technologies (first generation–fourth generation) in terms of the number of network connections, power consumption, security, reliability, and transfer speed, various countries across the world have adopted it [10, 11]. Based on [12], the 5G network is found to be very flexible and multifunctional. Therefore, different problems are solved in terms of power application and cost analysis. The 5G technology provides intelligence, sensing, and convergence of pervasive broadband that makes a great change in the SC and smart industrial markets. Using 5G technology in a smart grid, novel business frameworks are created at both the consumer and utility sides with fog and edge computing together with intelligent and automated controls [13]. The technology depends on very small cell functions for its slicing network that gives various advantages at the transmission side and the distribution side to perform on in a ubiquitous fashion. Therefore, the need for 5G in smart grids and other places where new power grids can benefit the access of information is highly required. A lot of research works have been conducted to explore the potential benefit of using 5G technology for the demand response management and Internet of Things in smart grids [14, 15]. However, the full potentials of 5G technology in smart grids are not utilized.

To address the above mentioned challenges, an efficient solution is required to ensure irrevocable, transparent, and distributed digital transactions. Blockchain technology is a distributed network that is able to solve the problems associated with the centralized approach [16, 17]. It addresses the problems in a decentralized and distributed manner. Using the blockchain, transactions are stored in a decentralized system [18]. The network's nodes in the blockchain maintain all of the executed transactions. Thus, compromising

the security of the network is merely not possible as it needs to control the miners that maintain the entire network security [19]. The blockchain users that are responsible for securing, verifying, and adding transactions into blocks of the network are called miners or validators. The mining process is performed according to the rules given by a consensus mechanism [20–22]. A consensus mechanism in the blockchain is used to permit untrusted peers to agree on the global state of the network [23]. In the blockchain, each block is cryptographically linked with its prior block forming a secured chain [24]. However, the lack of trust and privacy of users and demand-supply mismatch are still not fully solved using blockchain.

This research work proposes a distributed, verifiable, anonymous, and privacy-preserving energy trading system. The system enables users to trade and communicate securely using blockchain in 5G network. In the system, a reputation-based privacy-preserving EVs' matching scheme is proposed. Also, the proposed system incorporates identity-based encryption (ID-based encryption) and homomorphic encryption (HE) techniques to protect the privacy of the transactions and users, respectively. An energy allocation model is also proposed in order to motivate residential prosumers to participate in the energy trading. The model is developed based on the consumers' historical contributions and the type of their transactions.

The remainder of this paper is structured as follows. Sections 2 and 3 present the related work and problem statement, respectively. Sections 4, 5, 6, 7, and 8 discuss the proposed system model, proposed solutions, proposed methodology, and its security and privacy analyses. Section 9 presents the simulation results and their discussion while the conclusion and future work are given in Section 10.

2. Related Work

In this section, a detailed literature review is presented, which is divided into energy trading and EVs' charging load forecasting.

2.1. Energy Trading. In [19], the authors propose a localized P2P energy trading model for EVs using consortium blockchain. The model uses an iterative double auction mechanism to optimize price and quantity of energy during trading. Furthermore, the goal of the model is to maximize social welfare and to protect EVs' privacy. The authors in [25] analyze the effects of the EV's charging position. The results show that charging at foreign stations can cause penetration of privacy far more than charging at home. The authors in [26] propose an effective privacy reservation system for EVs and charging stations. The system also provides penalty and authentication mechanisms. However, the system is centrally controlled and managed, which makes the management more challenging when the number of users increases. In [27], the authors implement an integrated system that combines charging prioritization, encryption mechanism, and payment framework for the dynamic charging model. Computational and communication overheads are reduced in the system. However, the system does not eliminate the issue of a single point of failure.

In [28], the authors develop an accurate, confidential, and automated model for charging stations' selection based on EVs' distance and energy cost. They also implement a blockchain-based payment mechanism where EVs send their charging requests and charging stations send proposals, which is similar to an auction mechanism. However, increasing the overall system's efficiency is not considered in the model. In [29], the authors propose a secure communication model that has a privacy-preserving payment process for EVs' monitoring system. In addition, communication and computational overheads are reduced in the model. However, a mechanism to authenticate and verify users in the model is not included. In [30], a new communication model for on-the-move charging of EVs based on a subscribe/publish method for dissemination of appropriate data to EVs is proposed. The model allows the EVs' users to make optimal decisions about where to charge their EVs. In [31], a three-party model that is integrated with EVs in a smart grid context is proposed. In the model, two schemes are also proposed that focus on EV-centered and SC-centered. Furthermore, a demand-on-schedule energy management system is proposed. The system combines SCs and EVs to achieve an efficient resource management system in the power generation network. The model allows complex and flexible interactions between energy grids, SCs, and EVs.

2.2. Electric Vehicles' Charging Load Forecasting. The authors in [32] propose a one-step short-term load forecasting for the EV model using CNN with a niche immunity lion technique. The model is improved by incorporating niche immunity to obtain better forecasting results. As shown in the experimental results, traditional forecasting models have less accuracy than the deep learning models when the dataset is small. Similarly, authors in [33] propose a model for short-term load forecasting by incorporating LSTM in the conventional RNN scheme. LSTM solves the gradient vanishing problem in the RNN network. The authors in [34] propose an LSTM model for electricity load forecasting of individual residential homes.

In [35], the authors propose a system that predicts the daily load of EV charging stations using the Back Propagation Neural Network (BPNN). A fuzzy clustering approach based on the method of transfer closure is implemented to pick the actual load data, which is similar to the predicted data to enhance the predictive precision. However, BPNN causes overfitting and gets trapped into the local minimum easily. Similarly, in [36], the authors propose a short-term load forecasting scheme for EVs' charging stations using Radial Basis Function Neural Networks (RBFNNs). The proposed scheme is modified using the fuzzy control theory [37] to address the issues of trapping into local minimum and overfitting. The experimental results show that the forecasting accuracy increases exponentially. However, the forecasting systems are implemented using a centralized approach, which are prone to privacy- and security-related issues, and a single point of failure.

3. Motivation, Problem Statement, and Contributions

This section presents the motivation, problem statement, and research contributions.

3.1. Motivation and Problem Statement. The attention of many automobile companies has been attracted to develop EVs as a result of the excessive greenhouse gas emissions from petroleum machines. Concerning this, the automobile companies manufacture a large number of EVs to provide an eco-friendly and sustainable conveyance system. However, this results in an insufficient charging infrastructure to cater to the needs of energy users due to massive penetration of EVs in the SC. Many research works provide solutions to the lingering problems. For example, inefficient allocation of resources, leakage of sensitive information of EVs, and a single point of failure are the problems in the existing works, which are not fully solved. Therefore, improvements in the literature are strongly needed. The authors in [38] propose a model for distributed privacy preserving and efficient matching of charging demander with charging suppliers. This model uses the bichromatic mutual nearest neighbor (BMNN) to address the issue of exposing driving patterns, schedules, and whereabouts of EVs. However, the pieces of information transmitted or received are not verified and not guaranteed to be from legitimate users.

On the other hand, blockchain permits users to have a distributed and decentralized P2P network where nontrusted users communicate verifiably with each other. Several methods to secure P2P energy trading are proposed in the blockchain-based models. In [44], the authors propose an optimal scheduling algorithm for charging Hybrid EVs (HEVs). The model adopts consortium blockchain to ensure the users' privacy and secure the energy trading. In the model, the scheduling algorithm is aimed at reducing energy cost and optimizing the satisfaction function of users while targeting different performance metrics. The targeted metrics include waiting time, EV driving speed, discharging location, and charging entities. The optimization technique used in solving the problem is an improved Nondominated Sorting Genetic Algorithm (NSGA). However, the privacy of transmitted information is not guaranteed using blockchain technology alone [45, 46]. The reason is that the contents of all monetary balance and transactions are visible to the public, which allows the information to be easily accessed. Also, consortium blockchain is partially secure and less efficient as compared to other categories of blockchain technology. Similarly, in [39], the authors examine the adaptability of consortium blockchain to set up a stable electricity trading network. The blockchain-based network provides distributed storage and maintenance of the authorized nodes. However, relying on the merits of consortium blockchain cannot guarantee the reliability of the network's security. Also, it does not prevent the information from internal attackers. The authors in [40] propose an effective solution to reduce the excessive operational overhead in the trading model. The overhead increases when nodes are motivated to use local energy out of their self-interest as elaborated in [47]. As a result, it may be tantamount to a high cost of transportation for the trading partners. However, this mechanism decreases the financial benefits of the system. Also, privacy and security of the trading data are overlooked.

In terms of optimal energy allocation, many research works are studied in the literature based on prosumers' reputation. These works use different performance parameters to determine the reputation. The performance metrics used are historical energy supply contribution, rate of past participation of a prosumer, and load demand in the current time interval. The authors in [41, 48] propose a contribution-based allocation of energy policy to establish models that simplify energy trading in the electricity markets. In these models, the energy allocator collects excess energy from providers and allocates it to the energy deficit prosumers. However, these models do not consider the starvation level (SL) of consumers and the design of a proper mechanism to detect malicious energy transactions. The authors in [42] propose a novel Starvation-Free Optimal Energy Allocation Policy (SF-OEAP). The model is based on three parameters for prosumers in the smart distributed network of an energy market. The parameters are revenue index, prediction accuracy, and energy starvation. The Distribution System Operator (DSO) collects excess energy from energy generators and performs a fair energy allocation between consumers. However, the authors in [41, 42, 48] do not consider any mechanism to detect malicious transactions, which plays an important role to determine the reward for the prosumers and make the system free from malicious activities. In spite of the observable advantages of using blockchain [19, 39, 43] to establish a trustworthy platform, the privacy concern and other related issues still restrict its implementation in energy trading systems. In this study, a mechanism to solve the privacy and security issue and the lack of optimal fairness in energy allocation is proposed. The challenges to be solved also include operational inefficiency of the system, a single point of failure, and absence of an optimal scheduling algorithm for users. The proposed research work is an extension of [49, 50]. Table 1 shows the comparison between the proposed model and the existing models.

3.2. Research Contributions. The primary contributions of the proposed work are presented as follows.

(i) A secure energy trading model and an optimal energy scheduling algorithm for users are proposed using blockchain and smart contract. The proposed model ensures that the transaction is verified and it came from a legitimate user

(ii) An improved privacy-preserving and EVs' matching mechanism is proposed by integrating the reputations of users. The mechanism helps to prevent exposing the EVs' privacy

(iii) A novel method for calculating the reward index (RI) between prosumers is proposed. Furthermore, a Reward-based Starvation-Free Energy Allocation Policy (RSFEAP) algorithm is presented to

Table 1: The comparison of the proposed model with existing models.

References	A	B	C	D	E	F
Base paper 1 [19]	Yes	No	No	Yes	No	No
Base paper 2 [38]	No	Yes	Yes	No	No	No
Base paper 3 [39]	Yes	No	No	Yes	No	No
Base paper 4 [40]	Yes	No	No	Yes	No	No
Base paper 5 [41]	No	No	Yes	No	No	No
Base paper 6 [42]	No	No	Yes	No	No	No
Base paper 7 [43]	Yes	No	No	Yes	No	No
Proposed model	Yes	Yes	Yes	Yes	Yes	Yes

A: blockchain; B: encryption; C: fair allocation algorithm; D: malicious detection; E: privacy and security analysis; F: reputation.

distribute energy between prosumers. The proposed algorithm motivates prosumers to subjectively share their resources. It also ensures efficient and stable operations of the network as well as establishes a fair trading environment

(iv) ID-based encryption and HE techniques are incorporated into the proposed system to protect the privacy of the transactions and users, respectively

(v) A short-term load forecasting model for EVs' charging using multiple linear regression (MLR) is proposed to accurately plan and manage the uncertainty of EVs' intermittent charging behavior

(vi) Simulation study and theoretical analysis are employed to show the effectiveness of the proposed system. Furthermore, the security vulnerabilities of the smart contracts are analyzed to make the system bug-free against attacks

4. The Proposed System Model

The proposed system model deployed in the 5G network is divided into two components: residential energy prosumers and EVs. The model is discussed in the following sections.

4.1. Electric Vehicles' Component. In Figure 1, the overall system model is presented. The proposed system model is divided into two components: EVs and residential energy prosumers. In the EVs' component, the component is categorized into three parts: (i) privacy-preserving search and match scheduling, (ii) validation of transactions and blockchain-based EVs' energy trading, and (iii) load forecasting for EVs. The proposed component has two users groups, which are energy-buying EVs (EBEVs) and energy-selling EVs (ESEVs). Examples of ESEVs are V2V chargers, public/private charging stations, and residential stations. The system is assumed to have no central scheduler. In the EVs' component, the EBEV user initiates a local query using communication devices that help to search for available ESEV in the 5G-deployed SC. The communication between EBEVs and ESEVs is done by either Long-Term Evolution (LTE) or Dedicated Short-Range Communications (DSRC). More elaboration about the communication devices can be found in [38]. ESEVs receive a charging request from EBEVs and respond them in a distributed fashion.

In this component, the selection of ESEVs is based on their reputation points. The reputation points are submitted to and retrieved from the blockchain. This ensures the integrity of the reputation points and also verifies its source. By considering the reputation points, the EVs' locations are outright hidden. In the model, it is assumed that all EVs are situated within a short proximity. Thus, the EVs' reputation points are considered instead of the distance between EBEVs and ESEVs. When the EVs' selection is complete, the ESEV's location to EBEV is identified using Partially HE (PHE). After the completion of the search and match process, the energy trading takes place using a smart contract along with the monetary process. Additionally, the information of EBEVs and ESEVs is verified and is stored in the blockchain.

Moreover, EVs have more benefits over the conventional vehicles based on oil supply safety, containment of global warming, emissions reduction, and energy savings. However, as the number of EVs increases in SC, the load profile distributed energy network greatly changes [51]. As a result, the power grids' reliability and stability can occur because of the charging demand randomness and the intermittent behavior of renewable energy source [52]. To tackle the aforementioned problem, load forecasting is required. The integration of forecasting models for EVs' charging is a possible method to reduce energy transmission line loss and enhance the usage of local energy consumption as well as improve the advantage of renewable energy development where the generated energy is directly sold to EVs. Therefore, EVs' load forecasting is introduced to properly plan and manage the intermittent charging and discharging behavior of the vehicles.

4.1.1. Homomorphic Encryption. HE is a cryptographic system, which was first proposed in 1970s [53]. It is an encryption process that allows a specific type of mathematical computation to be executed on a ciphertext, which further generates another ciphertext. Thus, the output of the generated encrypted text matches the plaintext operations as if the operations are performed directly on the plaintext without any sign of distortion or alteration. This method allows users to perform operations on an encrypted data without knowing the real data supplied from the sender or having the public key to decrypt the encrypted message. It also provides the prospect for privacy preservation in many applications, e.g., storing data in cloud, and improving election security and transparency. Furthermore, HE solves the challenges of maintaining the confidentiality of processed and stored data in a database faced by other non-HE techniques. It is subdivided into Fully HE (FHE) and PHE [54]. FHE allows all computations (multiplication and addition) on ciphertext while PHE supports either multiplication or addition. In this paper, Paillier's cryptosystem is used, which is classified under PHE. It is more efficient and simpler than the FHE scheme [55]. The Paillier system has three steps: decryption,

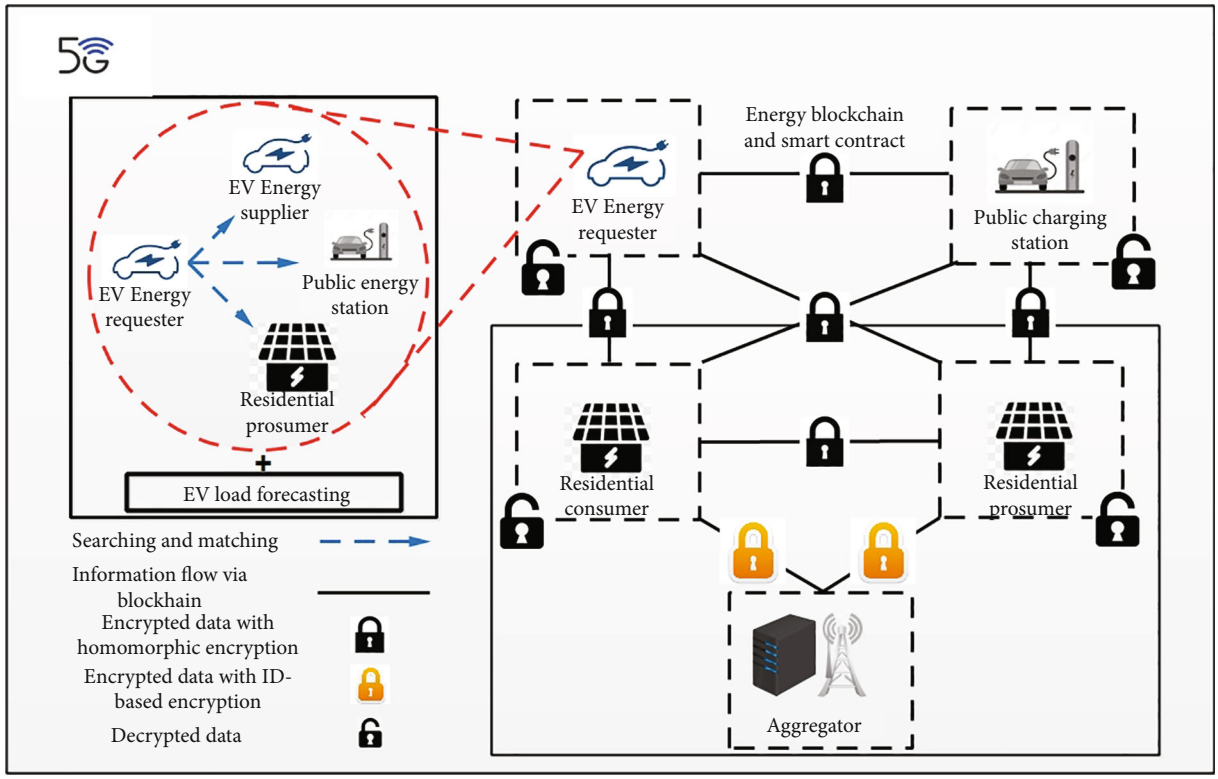


Figure 1: The proposed system model.

encryption, and key generation. The equations of the cryptosystem are adopted from [38].

p and q are two large prime numbers that are selected with the same bit length in the key generation step, setting $n = pq$ and $\lambda = (p-1)(q-1)$. μ and g are computed from λ and n, which are $\mu = (\lambda \bmod n^2)^{-1} \bmod n$, and $g = (n+1)$. The encryption and decryption keys are defined as (n, g) and (λ, μ), respectively. A random integer $r \varepsilon \mathbb{Z}_n$ is selected when encryption is performed on a plaintext (i.e., $E(a, r)$).

At the encryption step, the data is encrypted using the following equation.

$$E(a, r) = g^a . r^n \bmod n^2. \tag{1}$$

While at the decryption step, the data is decrypted using the following equation.

$$D(b) = \left(L(E(a, r))^{\lambda} \bmod n^2\right)\mu \bmod n, \tag{2}$$

where $L(u) = (u-1)/n$. Both encryption and decryption functions must satisfy the following equations.

$$\begin{aligned} E(a) \cdot E(c) &= E(a + c), \\ E(a)^c &= E(ac), \end{aligned} \tag{3}$$

where a and c are plaintexts.

4.1.2. Adversary Model. In the proposed model, an Honest-but-Curious (HBC) adversary model is adopted specifically at the privacy-preserving search and match part. The commonly used adversary model in studying privacy-preserving matching profile is HBC [56]. The users in this model carefully report and respond to other users' queries. In this model, we assume that some nodes in the blockchain are malicious nodes, which can attack the system in two ways.

(Q_1) The attacker will try to understand other users' location even though they are not matched

(Q_2) The attacker may try to understand and change reputations of other users to gain advantage of being selected

It is further assumed that the attacker has adequate power to breach any node's privacy in the system. Also, the attackers are unable to take over more than 51% of the computational power in the blockchain. It is further assumed that the minority nodes in the network have malicious behavior and are not more than 50%.

4.2. Residential Energy Component. The residential energy component is also an important component in the proposed system model. This component consists of an aggregator (AG) and a set of participating prosumers (Prosumer_1, $\text{Prosumer}_2, \cdots, \text{Prosumer}_n$) in the distributed network. The prosumers in the network are interlinked and share energy using dedicated power-sharing lines. Both AG and prosumers interact and trade energy through the blockchain. It is assumed that in a given time slot, every prosumer is able to produce energy G, and it has a load L. When $G_j \geq L_j$,

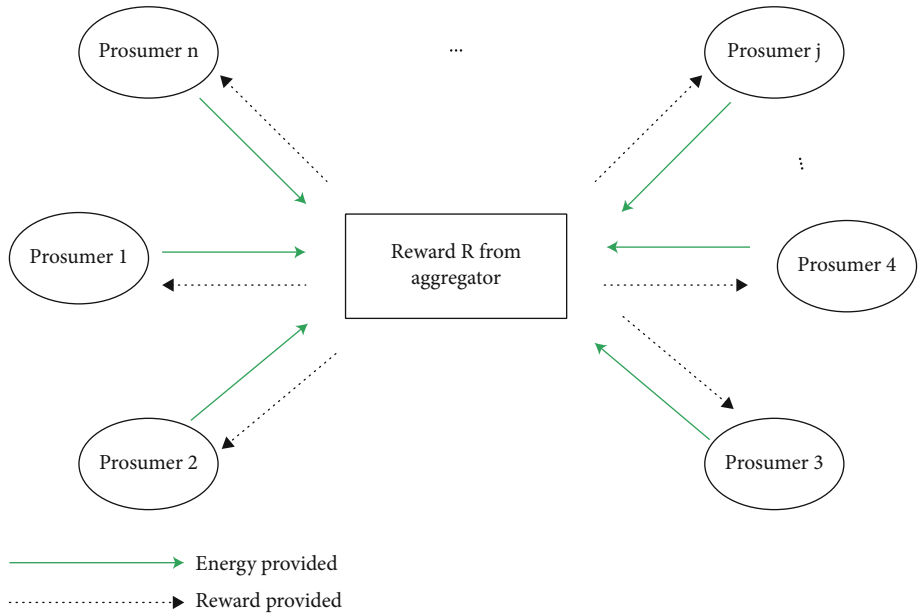


Figure 2: Reward allocation.

the jth prosumer becomes the energy seller (provider), whereas, when $G_j < L_j$, the prosumer becomes the energy buyer (consumer) and purchases energy either from the main grid or another prosumer with surplus energy. AG is an autonomous entity between the seller and buyer that gathers the surplus energy from the energy providers. AG is encouraged to have its own energy storage devices to store energy and maintain the system's stability and reliability, e.g., ultracapacitor and batteries. The sum of surplus energy from providers is given as $E_{j,as} = G_j - L_j$, $E = \sum_{j \in \text{Prosumer}} (E_{j,as})$.

A typical scenario where consumers request energy from AG is depicted in Figure 1. AG plays a good role in this component as an independent system. It is an equitable entity, which has full control over prosumers. Additionally, AG uses the RSFEAP algorithm to allocate the available energy to consumers, which is collected from the providers and distributed to the consumers. Besides that, AG distributes rewards to prosumers after the collection of all necessary transactions' data, as shown in Figure 2. Moreover, the data used to communicate between AG and prosumers is invariably passed through an encryption mechanism before the communication takes place. The encryption technique used in this component is ID-based encryption. The details of the encryption process are presented in Section 7.1.

5. The Proposed Solution for Electric Vehicles' Component

In this section, privacy-preserving reputation-based distributed matching, smart contracts, and EVs' charging load forecasting are discussed.

5.1. Privacy-Preserving Reputation-Based Distributed Matching. In this study, a blockchain-based decentralized and distributed reputation system is proposed. The complete layout of the proposed system is given in Algorithm 1. In the system, once EBEV makes a request for charging, the algorithm checks for ESEV that has the highest reputation points without considering the distance. If ESEV with the highest reputation points accepts the charging request from EBEV, then the algorithm matches ESEV with EBEV. Otherwise, ESEV with the second-highest reputation points will be considered by the algorithm. The sequence continues until EBES and ESEV are matched. To preserve the privacy of EVs, ESEVs are chosen based on their reputation points without considering the information on EBEV's whereabouts. After selecting ESEV, communication between the two parties takes place using the Paillier cryptosystem based on homomorphic computation.

5.1.1. Calculating Reputation. EBEVs submit ratings of ESEV after the energy trading task is completed. Afterwards, the process of calculating reputation points is initiated in the blockchain. At the initial stage, EVs first register themselves and obtain initial reputation and credibility points. These points are publically available for all the involved EVs. The actual reputation is the total accumulated rating provided by the EBEV users for the services received along with the raters' credibility, which are discussed and presented in Section 5.2.2. The usage of the credibility method gives more weight to the reputation points of a rater with higher credibility as compared to the one with less credibility. The mechanism to obtain the EVs' credibility is not extensively discussed in this research. When EBEVs are confirmed to be trustworthy, their credibility increases; otherwise, their credibility decreases.

5.1.2. Privacy-Preserving Reputation-Based Distance and Location Calculations. To compute the distance between EBEV and ESEV, the EBEV user needs to know the ESEV's

```
Input: D and S;
Output: matched result;
1: function Generic-matching(D, S)
2:     i = 1 ;
3:     whileD not matched with Sdo
4:         Find distance of D based on reputation in a privacy
5:         preserved manner;
6:         ifS_i accepts the request then
7:             Match D with S_i;
8:             Break;
9:         i + +;
```

Algorithm 1: Generic-matching function.

```
Output: send distance;
1: function EBEV()
2:     notmatched = True;
3:     whilenotmatcheddo
4:         System broadcast the need for matching;
5:         if only one supplier S_1 responds then
6:             S = S_1 ;
7:         else
8:             S = select the ESEV user with the highest-reputation points;
9:         Sendmessage(propose, D, S);
10:        msg = getMessage();
11:        if msg = accepted then
12:            add EBEV's loc(x, y) and calculate encrypted squared distance;
13:            Sendmessage(encrypted(distance));
14:            notmatched = False;
```

Algorithm 2: EBEV function.

reputation points, which are retrieved from the blockchain. EBEV ensures that the reputation points are verified because they are stored in the blockchain. This method gives a logical approach to hide the ESEV location. Let the ciphertext of a be $E(a)$ using the Paillier cryptosystem. Also, an encrypted squared distance computation between an ESEV S_j at location $\text{loc}_{S_j} = (x_j, y_j)$ and an EBEV D_i at location $\text{loc}_{D_i} = (x_i, y_i)$ is achieved using the following equations [38].

$$\begin{aligned} Dist(i,j) &= |loc_{D_i} - loc_{S_j}| = (x_i - x_j)^2 + \left(y_i - y_j\right)^2, \\ E(Dist(i,j)) &= E\left(x_i^2 - 2x_i x_j + x_j^2 + y_i^2 - 2y_i y_j + y_j^2\right). \end{aligned} \tag{4}$$

In the proposed model, each EV has PHE keys to encrypt the transactions between ESEV and EBEV. Furthermore, Algorithms 2 and 3 are inspired from [38], which show the communication between EBEV and ESEV in a privacy-preserved manner.

5.2. Smart Contracts of Energy Blockchain. In a blockchain network, smart contracts are a collection of rules that digitally facilitates, enforces, and verifies the contract made by the participants in the network [57]. The smart contract provides a credible transaction that is made automatically without involving a third-party. In addition, the transaction that is performed using a smart contract is traceable, auditable, and irrevocable. The proposed smart contracts in this model, i.e., reputation and energy trading, are discussed in the following sections.

```
Output: request result;
1: function ESEV()
2:     notmatched = True;
3:     whilenotmatcheddo
4:         msg = getMessage ;
5:         ifmsg.type = propose & S_i accept proposal then
6:             respond with encrypted loc(x,y);
7:             Sendmessage(accept, S, D);
8:             notmatched = False;
9:         else
10:            Sendmessage(reject, S, D);
```

Algorithm 3: ESEV function.

5.2.1. Smart Contract for Energy Trading. The energy trading smart contract comprises of three essential functions: selling, buying, and creating storage. The selling and buying functions work hand-in-hand, which enable EVs to sell or buy energy. When the energy trading begins, the smart contract

```
Input: energy requested from EBEV;
Output: (1) ESEV gives energy to EBEV; (2) EBEV sends money to ESEV;
1: function EnergyTrading()
2:     if(EBEV available balance < EV's charging cost)then
3:         returnfalse;
4:     if(ESEV available energy < EV's requested energy)then
5:         returnfalse;
6:     if(EBEV storage < amount of energy purchased)then
7:         returnfalse;
8:     else
9:         Subtract amount from EBEV's account balance;
10:        Add amount to ESEV account balance;
11:        Store transaction;
12:        Subtract energy from storage of ESEV;
13:        Add energy to storage of EBEV;
14:        Store transaction;
15     returnupdated information;
```

Algorithm 4: Smart contract for energy trading.

first checks the available credit of EBEV. It is necessary to confirm whether the EBEV user has enough money to purchase energy or not. Afterwards, it also checks whether ESEV has enough energy to sell or not. The smart contract also checks whether EBEV has enough energy storage capacity to accommodate the purchased energy or not. After all conditions are checked and returned true, then the ESEV's account is credited with the digital coin while it is deducted from EBEV's account. On the other hand, the energy from the storage of ESEV is subtracted and is added to the EBEV's storage. The *createstorage* function allows ESEVs to display the amount of available energy to sell out with their respective prices. The pseudocode of the energy trading's smart contract is given in Algorithm 4.

5.2.2. Reputation-Based Smart Contract. EBEV contacts ESEVs through the smart contract to utilize their charging services. In the public setting, various ESEVs are available with different capabilities, intentions, and services. After interacting with an ESEV, the EBEV user evaluates ESEV based on its energy services that affects the energy demander. The reputation points of each ESEV depend on EBEVs' ratings. Due to the fact that some EBEVs may misbehave, therefore, their integrity must be taken into consideration. EBEV with higher credibility point acts honestly as compared to one with less points. Therefore, EBEV rates ESEVs fairly to increase their credibility significantly. The reputation points are the cumulated ratings of EBEVs with their credibility points. The smart contract for reputation comprises two main functions: the *viewing aggregated feedback* and *feedback submit*. The *viewing aggregated feedback* allows both EBEVs and ESEVs to check their available ratings. The *feedback submit* function allows EBEVs to assess ESEV after a transaction of energy takes place. The ESEVs' reputation is calculated using the following equation [58].

$$R_I = \frac{\sum_{m=0}^{M} Cred_m \times R_m}{\sum_{m=0}^{M} Cred_m}, \tag{5}$$

where I is a unique identification for each ESEV that is evaluated while the total number of EBEV-rated ESEVs is M. The credibility of EBEV m is $Cred_m$. R_m is the rating of node I given by EBEV m, and the total reputation points of node I is R_I. To reduce the execution and transaction gas consumption of the blockchain, the mathematical computations for reputation and EBEVs' credibility are done off-chain. Off-chain computation is defined as the computational model where the functions of state transition are calculated by a trusted entity that is not on the blockchain. The resulting transition state then continues on-chain after verifying the computation of the state transition [59]. The computation results are transferred to the reputation's smart contract for further processing. The pseudocode of the smart contract for reputation is given in Algorithm 5.

5.3. Energy Load Forecasting for Charging Consumption Based on Multiple Linear Regression. In this work, a forecasting approach is employed to predict the EVs' charging consumption load based on regression analysis. Regression analysis [60] is a type of predictive technique for modeling and investigating relationship between independent and dependent variables. These predictive techniques are commonly used for forecasting, time series modeling, and finding a collective relationship between variables. Regression analysis is divided into linear, multiple logistics, polynomial, stepwise, ridge, lasso, and elasticNet regression. In this model, MLR is used.

5.3.1. Multiple Linear Regression. MLR determines the relationship between the variables that are independent and dependent. The equations presented for MLR are adopted from [61], which are expressed in the following equation.

$$y = \alpha_0 + \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_r x_r + \varepsilon, \tag{6}$$

where y is the EVs' charging load consumption, $x_1, x_2, \cdots, x_r$ are the independent variables, $\alpha_1, \alpha_2, \cdots, \alpha_r$ are regression coefficients with respect to the independent variables,

Output: *(1) EBEV rated ESEV; (2) EV view reputation points;*
1: **function** SubmitFeedback()
2: *Positive or negative rating point is added;*
3: **return***True;*
4: **function** ViewFeedback()
5: **Return***aggregated feedback;*

Algorithm 5: Smart contract for reputation.

and ε denotes the error rate. For multiple observations, Equation (6) is split as presented in the following equation.

$$\begin{aligned} y_1 &= \alpha_0 + \alpha_1 x_{11} + \alpha_2 x_{12} + \cdots + \alpha_r x_{1r} + \varepsilon_1, \\ y_2 &= \alpha_0 + \alpha_1 x_{21} + \alpha_2 x_{22} + \cdots + \alpha_r x_{2r} + \varepsilon_2, \\ &\cdots \\ y_i &= \alpha_0 + \alpha_1 x_{i1} + \alpha_2 x_{i2} + \cdots + \alpha_r x_{ir} + \varepsilon_i, \\ &\cdots \\ y_n &= \alpha_0 + \alpha_1 x_{n1} + \alpha_2 x_{n2} + \cdots + \alpha_r x_{nr} + \varepsilon_n. \end{aligned} \tag{7}$$

These equations are represented in the form of matrices as follows.

$$y = \alpha X + \varepsilon, \tag{8}$$

where,

$$\begin{aligned} y &= \begin{bmatrix} y_1 \\ y_2 \\ . \\ . \\ . \\ y_n \end{bmatrix}, X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1r} \\ x_{21} & x_{22} & \cdots & x_{2r} \\ & & . & \\ & & . & \\ & & . & \\ x_{n1} & x_{n2} & \cdots & x_{nr} \end{bmatrix}, \\ \alpha &= \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ . \\ . \\ . \\ \alpha_r \end{bmatrix}, \varepsilon = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ . \\ . \\ . \\ \varepsilon_n \end{bmatrix}. \end{aligned} \tag{9}$$

The matrices y and X contain information of both dependent and independent variables of the actual data. The α from Equation (8) is derived by Equation (10) using the least square method.

$$\alpha = \left(X'X\right)^{-1} X'y. \tag{10}$$

According to Equation (10), used to calculate the α regression coefficient, the expected load could be predicted as represented in Equation (11) using the MLR method.

$$\hat{y} = X\alpha. \tag{11}$$

$\hat{y}$ is the forecasted value of y. In this model, error is the absolute difference between the actual and forecasted values.

6. The Proposed Solution for Residential Prosumers' Component

The role of blockchain in fair energy trading and the method to compute rewards for prosumers are discussed in this section. According to the energy requirement, every energy consumer decides its starvation parameter and sends it to AG. AG uses the RSFEAP algorithm to distribute energy across all prosumers based on their energy contribution, type of transactions, and starvation parameters.

6.1. Fair Energy Trading Using Blockchain Technology. In this study, a blockchain-based model is developed to decentralize the energy systems. The model comprises of energy consumers, energy providers, and AG as users. These users coordinate and communicate via blockchain to facilitate the decentralization of energy demand and generation. However, maintaining and storing energy transactions using a centralized system is still an open research problem. Therefore, transactions in energy trading are coordinated, recorded, and maintained with the support of blockchain technology in a decentralized manner. The blockchain technology has many features: consensus mechanism, self-enforced smart contract, immutability, etc. A consensus mechanism is a collection of protocols that enables untrusted prosumers to agree on a global state of the network. In this work, Proof of Work (PoW) [62] is used. A self-enforced smart contract is an agreement embedded as a computer code that is managed by the blockchain. The information immutability feature helps to ensure that the transactions recorded on the blockchain remain unaltered after miners' verification.

6.2. Parameters for Fair Energy Allocation. This section discusses the parameters used for the energy allocation algorithm across residential prosumers.

6.2.1. Starvation Level Parameter. The consumers in the reward based energy allocation model are served with excessive energy available in the system. It is found that some prosumers in the network show a negligible contribution, have a high rate of malicious transactions, or are incapable of contributing energy. In this case, the

consumers might not receive energy, and they need to purchase the required energy at a very high price from the main grid. In RSFEAP, the minimum energy requirement of each prosumer is represented in the form of percentage. The starvation factor S is used to define the threshold for the energy requirement. Based on the threshold, each consumer meets its minimum energy requirement $S \times E_{arq}$ to avoid energy starvation. The SL parameter is calculated using the following equation [42].

$$\mathrm{SL} = \left(1 - \frac{E_{allocR}}{E_{arq}}\right) \times E_{allocR}. \tag{12}$$

At every time slot, AG receives details of providers' excess energy E_{as} and consumers' energy request E_{arq}. RSFEAP guarantees optimal prosumer-generated energy allocation E_{allocR} to each consumer.

6.2.2. Reward Index. In this model, RI plays a vital role for a fair energy allocation. It is mandatory to compute the RI carefully to have fair energy allocation and trading mechanisms. In the process of deciding the reward of a prosumer i, two factors are considered, which are given below.

(1) The amount of energy contributions provided by the prosumer in the past

(2) The number of valid or malicious transactions performed in the present or past by the prosumers

Hence, RI is computed as follows.

$$Y_i = 1 - e^{(-\theta/100)}, \tag{13}$$

$$\theta = \begin{cases} 0, & \text{if valid transaction,} \\ 1, & \text{if malicious transaction,} \end{cases} \tag{14}$$

$$C_i = C_i - (C_i \times Y_i), \tag{15}$$

$$\mathrm{RI}_i = \frac{C_i}{C_{\mathrm{Total}}}. \tag{16}$$

In Equations (13)–(16), C_i is the amount of energy contributions provided by a prosumer till the present interval and C_{Total} is the sum of the energy contributions recorded by AG till the present interval. Y_i is the quantifier for valid and malicious transactions recorded by the miners in the blockchain while θ is the index of each transaction (valid or malicious) recorded. In the computation of RI, both energy contributions and transaction types are treated with equal preference. However, there may be a situation where AG gives a higher preference to the type of transactions executed rather than the energy contributed. In such a situation, the preference values of a user will be multiplied by the weight factor $\rho(\rho > 0)$. We assume to take the value of ρ as 1 in this paper since preferences to both transaction types and energy contributions provided in the past are the same. Therefore, a prosumer that shares surplus energy in the past will get rewards in the future when energy is needed. The reward depends on the type of transactions conducted by the prosumer, which decreases with an increase in malicious activity during energy transactions. Conclusively, when a prosumer purchases energy, AG and miners store the information about the exact net energy shared by the prosumer in the blockchain ledger. AG uses the information to compute the RI and update it regularly. RI is considered in RSFEAP to show the consistency and credibility of prosumers in the system.

6.2.3. Valid and Malicious Transactions. The valid and malicious transaction (VMT) algorithm consists of punishment and reward mechanisms. There are two types of actions to be punished: first, when consumer i attempts to alter his record to favor himself; second, when consumer i broadcasts a forged request. On the other hand, it is rewarded when a prosumer i acts honestly and performs a valid transaction. As shown in Algorithm 6, if a malicious transaction is not detected by the miners, the transaction is said to be valid and its index θ_i will be set to zero (0). Therefore, the prosumers' RI will increase. On the other hand, if a malicious act is detected based on the mentioned actions, then AG will collect evidence to make a judgment and send it to the miners for validation. If any prosumer is caught with malicious activity, its transaction index θ_i will increase by 1, which will decrease the RI.

6.3. Optimization Formulation. AG optimally distributes energy to every consumer based on the aforementioned parameters. Hence, to efficiently allocate energy $A_i(E_{i,allocR})$ to meet the consumers' demand, an optimization problem is formulated. The optimization formulation given in this research is similar to [42].

$$\max \sum_{i \in Cs} A_i(E_{i,allocR}), \tag{17}$$

such that, $S \times E_{i,arq} \leq E_{i,allocR} \leq E_{i,arq}$,

$$\sum_{i \in Cs} E_{i,allocR} \leq E. \tag{18}$$

According to the optimization problem given in Equation (17), some assumptions are made. AG will not distribute energy $E_{i,allocR}$ to the consumer that will exceed its energy requirement $(E_{i,arq})$ and will fall below its starvation level $(SL \times E_{i,arq})$. Therefore, the consumer will be able to satisfy its minimum demand. Also, RSFEAP places a restriction on the total energy distributed to the consumers so that it cannot exceed the total energy aggregated from prosumers with surplus energy E. The consumers' objective functions are given from the AG perspective, as shown in the following equation.

$$A_i(E_{i,allocR}) = \alpha RI_i E_{i,allocR} + \beta SL_i. \tag{19}$$

Solving the following constrained optimization problem, RSFEAP of AG is developed.

Input θ_i, C_i, C_{Total};
Output C_{Total} *and* C_i;
1: **function** FindMaliciousTransaction(θ_i, C_i, C_{Total})
2: **if***(malicious transaction)***then**
3: $\theta_i = \theta_i + 1$;
4: $Y_i = 1 - e^{(-\theta/100)}$;
5: $Ci = C_i - (C_i \times Y_i)$;
6: *Update* C_{Total} *with new* C_i;
7: **else**
8: *Update* C_i;
9: *Update* C_{Total} *with new* C_i;
10: **return** C_{Total} *and* C_i;

Algorithm 6: VMT algorithm.

(a) *Problem 1*: let the set of all consumers be $Cs = \{1, 2, \cdots, n\}$, $\bar{E_{arq}} = \{E_{1,arq}, E_{2,arq}, \cdots, E_{n,arq}\}$ be the set of exact energy request by the consumers, and $\bar{C} = \{C_1, C_2, \cdots, C_n\}$ be the set of energy contributions made by the prosumers. The optimal value of the optimization is computed using the following equation.

$$\max \sum_{i \in Cs} \alpha RI_i E_{i,allocR} + \beta SL_i, \tag{20}$$

such that $S \times E_{i,arq} \leq E_{i,allocR} \leq E_{i,arq}$,

$$\sum_{i \in Cs} E_{i,allocR} \leq E, \tag{21}$$

where β and α are that weight factors, which are used to control the preference of every parameter of RSFEAP. $\beta + \alpha = 1$ and $0 \leq \beta, \alpha \leq 1$.

(b) *Solution*: if $\sum_{i \in Cs} E_{i,allocR} \leq E$, then all consumers are allocated with their requested energy, i.e., $E_{i,allocR} = E_{i,arq}$. On the other hand, an optimal energy allocation mechanism is used for the nontrivial case, i.e., when considering $\sum_{i \in Cs} E_{i,allocR} > E$. In such a situation, one can obtain closed-form solution given by Theorem 1.

(c) *Theorem 1*: an optimized allocation of energy $E^*_{i,allocR} = \{E^*_{i,allocR} \mid i \in Cs\}$ from the defined problem is given below

$$E^*_{i,allocR} = \begin{cases} \dfrac{(\alpha RI_i + \beta - \upsilon)}{2\beta} E_{i,arq}, & \text{if } E_{i,allocR} > S \times E_{i,arq} \\ & \text{and} < E_{i,arq}, \\ S \times E_{i,arq}, & \text{if } E_{i,allocR} \leq S \times E_{i,arq}, \\ E_{i,arq}, & \text{otherwise}, \end{cases} \tag{22}$$

where υ is a real number that satisfies $\sum_{i \in Cs} E^*_{i,allocR} = E$.

(d) *The proof that shows that the objective function is concave*:

$$\begin{aligned} A_i(E_{i,allocR}) &= \alpha RI_i E_{i,allocR} + \beta SL_i, \\ A_i(E_{i,allocR}) &= \alpha RI_i E_{i,allocR} + \beta \left(\left(1 - \frac{E_{allocR}}{E_{arq}} \right) \times E_{allocR} \right), \\ A_i'(E_{i,allocR}) &= \alpha RI_i + \beta - \frac{2\beta E_{allocR}}{E_{arq}}, \\ A_i''(E_{i,allocR}) &= -\frac{2\beta}{E_{arq}} \end{aligned} \tag{23}$$

Since the second derivative of the objective function is negative where $0 < \beta \leq 1$, then it is purely concave function.

(e) *Proof*: since all the constraints are linear and the objective function is purely concave, the conditions of Karush-Kuhn-Tucker (KKT) [42] guarantee *Problem* 1 given as follows.

(1) *Complementary slackness*:

$$\lambda_i h_i(x^*) = 0. \tag{24}$$

(2) *Primal feasibility*:

$$h_i(x^*) \leq 0, g_j(x^*) = 0. \tag{25}$$

(3) *Dual feasibility*:

$$\lambda_i = 0. \tag{26}$$

(4) *Stationary*:

$$0 \in \partial f(x^*) + \sum_{i=1}^{m} \lambda_i \partial h_i(x^*) + \sum_{j=1}^{r} \upsilon_j \partial g_j(x^*). \tag{27}$$

Generally, the constraint vectors are represented as

single column vectors.

$$h(x) = \begin{bmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_m(x) \end{bmatrix}, g(x) = \begin{bmatrix} g_1(x) \\ g_2(x) \\ \vdots \\ g_r(x) \end{bmatrix}. \quad (28)$$

We define m lagrange multipliers for λ_i inequality constraints and r multipliers υ_j for r equality constraints. Hence,

$$\lambda = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{bmatrix}, \upsilon = \begin{bmatrix} \upsilon_1 \\ \upsilon_2 \\ \vdots \\ \upsilon_r \end{bmatrix}. \quad (29)$$

From Equation (27), $\partial f(x^*)$ is derived as given in the following equation.

$$\partial f(x^*) = \partial A_i(E_{i,allocR}), \quad (30)$$

which is further simplified to the following equation:

$$\partial f(x^*) = \alpha RI_i + \beta - \frac{2\beta E^*_{i,allocR}}{E_{i,arq}}. \quad (31)$$

In Equation (27), the second term can be represented as given in Equation (32) below. φ in the expression is used for the second inequality constraint.

$$\sum_{i=1}^{m} \partial h_i(x^*) = -\lambda_i + \varphi_i. \quad (32)$$

And the last term in Equation (27), can be shown as

$$\sum_{j=1}^{r} \partial g_j(x^*) = \upsilon. \quad (33)$$

By solving Equations (31), (32), and (33), the stationary condition in Equation (27) is satisfied, which is expressed in the following equation.

$$\alpha RI_i + \beta - \frac{2\beta E^*_{i,allocR}}{E_{i,arq}} + \lambda_i - \varphi - \upsilon = 0. \quad (34)$$

In the primal feasibility condition, $h_i(x^*) \le 0$, and $g_j(x^*) \le 0$ is solved as

$$S \times E_{i,arq} - E^*_{i,allocR} \le 0, \quad (35)$$

$$E^*_{i,allocR} - E_{i,arq} \le 0, \quad (36)$$

where Equations (35) and (36) give the following equation.

$$\sum_{i=1}^{n} E^*_{i,allocR} \le 0, \quad (37)$$

while the complementary slackness condition is shown as

$$\lambda_i \left(S \times E_{i,arq} - E^*_{i,allocR}\right) = 0, \quad (38)$$

$$\varphi_i \left(E^*_{i,allocR} - E_{i,arq}\right) = 0. \quad (39)$$

Finally, the dual feasibility condition in Equation (26) is expressed in the following equation.

$$\lambda_i = 0, \varphi_i = 0. \quad (40)$$

The inequality constraint and objective function are convex and differentiable while the equality constraint functions are affine. Therefore, the KKT conditions have an optimal solution [48, 63]. To satisfy Equation (40), three possible cases are generated for $E^*_{i,allocR}$: $S \times E_{i,arq} \le E^*_{i,allocR} \le E_{i,arq}$, $E^*_{i,allocR} = E_{i,arq}$, and $S \times E_{i,arq} = E^*_{i,allocR}$. We first consider a case $S \times E_{i,arq} \le E^*_{i,allocR} \le E_{i,arq}$. It is clear that $\lambda_i = 0$ and $\varphi_i = 0$. The λ_i and φ_i values are then substituted in the stationary condition in Equation ((27)), and the result of $E^*_{i,allocR}$ is generated as follows.

$$\alpha RI_i + \beta - \frac{2\beta E^*_{i,allocR}}{E_{i,arq}} - \upsilon = 0, \quad (41)$$

$$\alpha RI_i + \beta - \upsilon = \frac{2\beta E^*_{i,allocR}}{E_{i,arq}}, \quad (42)$$

where Equation (42) is further simplified to give the following equation.

$$\frac{\alpha RI_i + \beta - \upsilon}{2\beta} E_{i,arq} = E_{i,allocR^*}. \quad (43)$$

Considering a case $E^*_{i,allocR} = E_{i,arq}$, there exists a value of λ_i taken from Equation (39). The value of φ_i can be substituted in the stationary condition in Equation (27), and the $E^*_{i,allocR}$ results are given as follows.

$$\alpha RI_i + \beta - \frac{2\beta E^*_{i,allocR}}{E_{i,arq}} - \varphi_i - \upsilon = 0, \quad (44)$$

$$\frac{(\alpha RI_i + \beta - \upsilon)E_{i,arq}}{2\beta} - E^*_{i,allocR} = \frac{\varphi_i E_{i,arq}}{2\beta}, \quad (45)$$

where Equations (44) and (45) are further simplified to give the following equation:

$$\frac{(\alpha RI_i + \beta - \upsilon)E_{i,arq}}{2\beta} = E^*_{i,allocR} + \frac{\varphi_i E_{i,arq}}{2\beta} \ge 0, \quad (46)$$

which produces

$$\frac{(\alpha RI_i + \beta - \upsilon)E_{i,arq}}{2\beta} \geq E_{i,arq}. \tag{47}$$

Furthermore, we consider a case $S \times E_{i,arq} = E^*_{i,allocR}$ where $\varphi = 0$ from complementary slackness condition in Equation (39). The value of φ_i can be substituted in the stationary condition in Equation (27), and the $E^*_{i,allocR}$ results are given in Equations (48)–(51).

$$\alpha RI_i + \beta - \frac{2\beta E^*_{i,allocR}}{E_{i,arq}} + \lambda_i - \upsilon = 0, \tag{48}$$

$$\frac{(\alpha RI_i + \beta - \upsilon)E_{i,arq}}{2\beta} - E^*_{i,allocR} = -\frac{\lambda_i E_{i,arq}}{2\beta}, \tag{49}$$

$$\frac{(\alpha RI_i + \beta - \upsilon)E_{i,arq}}{2\beta} = E^*_{i,allocR} - \frac{\lambda_i E_{i,arq}}{2\beta} \geq 0, \tag{50}$$

which produce

$$\frac{(\alpha RI_i + \beta - \upsilon)E_{i,arq}}{2\beta} \geq S \times E_{i,arq}. \tag{51}$$

Therefore, there exists an optimal allocation of energy $E^*_{i,allocR} = \{E^*_{i,allocR} \mid i \in Cs\}$ of Problem 1 in Equation (22). From the three cases given above and the primal feasibility condition in Equation (37), the optimal solution is given by Equation (22). Furthermore, the solution to the problem defined in this paper uses quadratic programming. It is because the objective function is a quadratic problem with linear constraints.

6.4. Energy Allocation Algorithm. Before the energy transactions start, the prosumers' information is collected by AG to allocate the energy to them. For each time interval, the total available energy provided by the energy providers is E and the total energy needed by the energy consumers is E_c. In this work, the proposed energy allocation algorithm, i.e., Algorithm 7, is derived from [42], and it has two conditions, which are as follows:

(1) When the total energy request from consumers E_c is less than or equal to the total energy available E

(2) When the total energy request from consumers E_c is greater than the total energy available E

In the first condition, consumers receive the same amount of energy that they requested. In the second condition, consumers receive an optimal amount of energy as shown in Algorithm 7 (lines 12–22). In these lines, the interior point method of quadratic programming is used to solve the optimization problem where the optimal allocation of energy is produced. A MATLAB function called *quadprog*( )*function* (line 21) is often used to solve a quadratic objective function. This function requires various input parameters, both in the form of vectors and matrices. These input parameters are the Hessian matrix H, vector f^T, upper bound *ub*, lower bound *lb*, and inequality constraints A and b. Hessian matrix H as shown in lines 13 and 14 of Algorithm 7 is a symmetric matrix. f^T (line 14) is a vector represented as the linear term of the objective function (line 13). The linear coefficient in inequality constraint is represented as A, and the constant vector of overall surplus energy in the current time interval is represented as b. The boundaries for energy allocations $S \times E_{i,arq} \leq E_{i,allocR} \leq E_{i,arq}$ are represented as the upper and lower bound vectors (line 18). *ub* is the maximum limit set by AG for over allocating energy to consumers. On the other hand, *lb* is the lower threshold value set by each consumer to stop himself from falling into starvation. Therefore, these input parameters help the *quadprog*()*function* to be executed and return the optimal energy allocation vector E_{allocR}.

7. Proposed Methodology

7.1. Privacy and Security Construction for Residential Prosumers. In this research work, an encryption mechanism is used to protect users' information for the residential prosumer component. Sensitive data that does not affect the trading mechanism is encrypted and is stored in the blockchain. The focus of the research is to partially encrypt the users' data by allowing the energy and price values to be sent unencrypted to the blockchain. This process allows the energy traders to participate in trading without adding burden to the system by concealing irrelevant information. It is important to use encryption techniques to turn the plaintext into ciphertext to maintain the system's security and improve the users' privacy in the blockchain. Therefore, an asymmetric encryption technique is used to encrypt the data before recording it on the blockchain. Moreover, a privacy protection technique, i.e., ID-based encryption, is implemented. The technique that is used is based on the bilinear map theory. It is known that the Ethereum blockchain does not support complex mathematical computations [59]. Moreover, the Ethereum blockchain is adopted due to its stronger security capability and less time consumption as compared to IOTA during validation process [64]. Therefore, all the complex computations are done off-chain, and the computed results are forwarded to the blockchain for further computation and storage. Similarly, the blockchain execution and transaction costs are reduced, and also, the efficiency of the allocation process is not affected. In order to protect the users' information, additional encryption techniques are required. Therefore, in the proposed system, ID-based encryption and HE techniques are adopted.

7.2. Bilinear Map Theory. This section presents bilinear map theory as follows.

(i) The three cyclic groups of prime order P are denoted as G_1, G_2, and G_3

(ii) g_1 and g_2 are generated from G_1 and G_2, respectively, as $g_1 \in G_1$ and $g_2 \in G_2$

(iii) Bilinear map is presented as $e(,)$: $G_1 \times G_2 \longrightarrow G_3$

The bilinear map properties are given as follows:

Input: E_{arq}, E_{as}, C;
Output: E_{allocR};
1: $t = 1$;
2: **while** $t \le N$ *time-slots* **do**
3: $E = \sum_{i=1}^{k} E_{i,as}$;
4: $E_c = \sum_{i=1}^{k} E_{i,arq}$;
5: $C_{\text{Total}} = \sum_{i=1}^{k} C_i$;
6: *Compute RI for each consumer using Equation ((16));*
7: **if** $E_c \le E$ **then**
8: **for** $i = 1$ *to n number of consumers* **do**
9: $E_{i,allocR} = E_{i,arq}$;
10: **else**
11: $f(E_{i,allocR}) = \sum_{i \in Cs} \alpha RI_i E_{i,allocR} + \beta(1 - E_{i,allocR}/E_{i,arq}) \cdot E_{i,allocR}$;
12: $f(E_{i,allocR}) = 1/2 E_{i,allocR}^{T} H E_{i,allocR} + f^{T} E_{i,allocR}$;
13:
14: $H = \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix}, f^{T} = \begin{bmatrix} a_{11} \\ a_{22} \\ \vdots \\ a_{nn} \end{bmatrix}$;
15:
16: $A = [a_{11}\ a_{22}\ \cdots\ a_{nn}]$, $b = [E]1$;
17:
18: $ub = \begin{bmatrix} E_{1,arq} \\ E_{2,arq} \\ \vdots \\ E_{n,arq} \end{bmatrix}, lb = \begin{bmatrix} S \times E_{1,arq} \\ S \times E_{2,arq} \\ \vdots \\ S \times E_{n,arq} \end{bmatrix}$;
19:
20: $E_{i,allocR} = quadprogr(H, f, A, b, lb, ub)$;
21: $t{+}{+}$;

Algorithm 7: RSFEAP algorithm.

(i) *Nondegenerate*: $e(g_1, g_2) \neq 1$

(ii) *Bilinear*: $\forall v \in G_1, \forall u \in G_2$, and $b, a \in \mathbb{Z}$, we have $e(v^b, u^a) = e(v, u)^{ba}$

The proposed scheme is defined by Boneh and Franklin's ID-based system, implemented in 2001 [65], which can be used for privacy protection in the blockchain. The following are the steps of the encryption process.

7.2.1. Initialization. Construct two groups of elliptic curves G_1, G_2 such that $|G_1| = |G_2| = q$, $e(,)$: $G_1 \times G_1 \longrightarrow G_2$ is a bilinear map and $P \in G_1$ is a generator. $s \in \mathbb{Z}_q^*$ is randomly selected, and s is defined as the master key where $P_{pub} = s \cdot P$ can be calculated. Let $h : \{0,1\}^n \longrightarrow G_1$, $h_1 : \{0,1\}^n \longrightarrow G_2$, and $h_2 : \{0,1\}^n \longrightarrow \mathbb{Z}_q^*$ be the three cryptographic hash functions. The system's parameters are published as $\{G_1, G_2, e, , n, q, P, P_{pub}, h(\,), h_1(\,), h_2(\,)\}$.

7.2.2. Generating Private and Public Keys

(i) User A registers with AG using its ID number and personal information

(ii) The client generates a public key based on the ID of A, which produces $\Pi_{id} = h(id)$

(iii) Private Key Generator (PKG) calculates the A's private key locally as $S_{id} = s.\Pi_{id}$, then passes it to A via a secure channel

7.2.3. Sending Message to the Blockchain

(i) Initially, user A encrypts a private message M as follows

(a) Picks $r \in \mathbb{Z}_q^*$

(b) Calculates $g_{id} = e(\Pi_{id}, P_{pub})$, $V = r \cdot P$

(c) $U = M \otimes h_1(g_{id}^r)$

(ii) After encryption, the user sends the encrypted message (V, U) to the blockchain

7.2.4. Getting Message from the Blockchain

(i) System sends encrypted message (V, U) to A and A decrypts data as follows

(a) $M = U \otimes h_1(e(S_{id}, V))$, where M is just the plaintext

8. Security and Privacy Analyses

This section analyzes the privacy and security of the energy trading model. The model is analyzed on the bases of the secret key security, passive attack, and disguised attack. Moreover, the smart contracts are analyzed using the Oyente security analysis tool.

8.1. Security of Secret Key. The most essential and sensitive part of the ID-based encryption technique is the master or secret key. Once the secret key is revealed, the whole system is under threat. Therefore, the secret key must be cautiously and carefully stored. In traditional encryption systems, central authority controls and manages the secret key, which raises issues of security and centralization. However, in this model, each node generates its master key instead of a single PKG. Similarly, for the EV's component, the communication is done using Paillier encryption, which allows the receiver of the encrypted message to perform an action on the ciphertext without having the keys. Therefore, in encryption, sharing of keys is not required. These encryption processes resolve the centralization and security problems of the secret keys.

8.2. Passive Attack. The passive attack comprises traffic analysis and information monitoring. In a transaction, the passive attacker can have access to two different types of users' information: data and addresses. The address is not reversible because it is a user's hash signature. Thus, the only target point of the attacker is the plaintext information given by the users and is the focus of this research work. The ID-based encryption technique is used to protect and encrypt information where only a string of unrecognized characters can be seen. Similarly, for the EV's component, Paillier encryption is used to protect the privacy of the users' location. These strings are readable when the user is in possession of the private key, which makes the system passive attack resistant.

8.3. Disguise Attack. In this attack, a disguised attacker may have the ID of the legitimate user, so he can pretend to be another user. Even if the attacker receives the encoded data, it is difficult to regenerate the original information without the private key. Thus, this makes the system resistant to the disguised attacker. Further, different cases of EVs' security and privacy issues exist. Therefore, three (3) propositions are defined and analyzed.

Proposition 1. *The attacker cannot learn other users' location information in the system before matching with the users* (Q_1).

We assume that users interact with each other via secure channels, i.e., through the blockchain or the Paillier encryption technique. The Paillier encryption technique allows ESEV to work on encrypted data without knowing the actual information from the EBEV user. Additionally, the selection of ESEVs is based on the reputation values they have before the match is made. This makes the proposed system conceal the location information of both ESEVs and EBEVs.

Proposition 2. *The internal and external attacks from the computing nodes cannot compromise the proposed system* (Q_2).

It is clear that the reliability of the proposed system depends on the security provided by the blockchain. Generally, it is assumed that the attacker cannot control more than 51% of the computing nodes in the blockchain. The internal and external attacks on the computing nodes are unable to breach the whole system because the attackers need to control more than 50% of the nodes. PoW consensus mechanism prevents the system from both internal and external attacks.

Proposition 3. *All energy trading tasks are open and trustworthy in the proposed system* (Q_2).

All operations in the smart contracts are constantly executed on blockchain and the computed results are stored in it. This process guarantees the trustworthiness of the system. Also, the operations and the results obtained are verified by the miners in the proposed system. Conclusively, the data stored in the blockchain is made tamper-proof and traceable.

8.4. Vulnerability Analysis of Smart Contract. This section discusses the security vulnerability analyses of the smart contracts. It also highlights the best way to develop and write smart contracts, so that they can withstand all possible attacks. In addition to the encryption mechanism, blockchain technology is used to strengthen the overall security of the system. The blockchain comes with its advantages as well as some security problems. Among the security challenges, blockchain provides a solution to the Distributed Denial of Service (DDoS) attack. The reason is that all energy transactions are recorded on the private Ethereum storage in a decentralized and distributed fashion and therefore are not prone to a single point of failure. This technology has the ability to store data that cannot be altered or changed (immutability feature) as long as it is confirmed by the validators. The blockchain's immutability feature helps to ensure the integrity of all shared data between the involved parties. The data can only be attacked if and only if an attacker or group of attackers control more than 50% of the network. Moreover, this type of attack is almost impossible in the proposed system because the network uses the PoW consensus mechanism.

Smart contracts' developers must ensure that the contract code is free of bugs and security vulnerabilities. The proposed smart contracts are analyzed using Oyente security

analysis tool to check for the known bugs and security vulnerabilities. The security vulnerabilities include reentrancy vulnerability, timestamp dependence, callstack depth vulnerability, transaction ordering attack, parity multisig bug 2, and assertion failure. The results of the proposed smart contracts analysis are presented in Table 2. The EVM byte codes are evaluated by Oyente and the corresponding call graphs are produced for each contract. Oyente conducts the block-level smart contract code analysis by following the rules given in Ethereum's yellow papers [58, 66]. The results show that the proposed smart contract is secure and resistant to all the aforementioned attacks and vulnerabilities. It also shows that there is no unhandled exception, which may result in overflow or underflow of integer operations in the proposed smart contract's callee and caller functions. Moreover, external calls are reduced and all evaluations are performed to ensure gas availability. The external call reduction prevents the proposed smart contract from reentracy attack. Similarly, external calls are also reduced to protect the system from callstack attacks. Table 2 also shows that there is no possible vulnerability associated with the proposed smart contracts, which may lead to timestamp dependency, transaction ordering dependency, and parity multisig bug 2 issues.

Table 2: Report of the security vulnerability using Oyente tool for energy trading and reputation smart contracts.

Parameters	1	2
EVM code coverage	47.9%	42.5%
Integer underflow	False	False
Integer overflow	False	False
Parity multisig bug 2	False	False
Callstack depth attack vulnerability	False	False
Transaction-ordering dependence (TOD)	False	False
Timestamp dependence	False	False
Reentrancy vulnerability	False	False

1: energy trading contract; 2: reputation contract.

9. Simulation Results

This section presents the experimental setup and the simulation results of the proposed energy trading model.

9.1. Experimental Setup. The network topology of 100 ESEVs and 100 EBEVs is generated within an area of 1 km by 1 km. The locations of ESEVs and EBEVs are allocated with uniform distribution. Generally, 512-bit primes for q and p, as given in Paillier's cryptosystem, are used for the PHE calculations. The smart contracts are implemented on the Ethereum blockchain. The Ethereum blockchain is adopted due to its stronger security capability and less time consumption as compared to IOTA during validation process [64]. For fair energy allocation, four energy prosumers and one AG are considered. A day of 24 hours is divided into 24 slots (interval of 1 hour each). The data used for the prosumers' first 4 time intervals is obtained from study [42]. The computational experiments are conducted on a desktop computer with the following specifications: AMD E1-6015 APU with Radeon (TM) R2 graphics, 1.4 GHz processor, operating system is Microsoft Windows 10 with 4.00 GB of RAM, and codes are executed using MATLAB2018a. The values of S, α, and β are set as 0.8, 0.6, and 0.4 in the simulations, respectively. The dataset used for the EVs' charging load forecasting is taken from [67]. Figure 3 shows the normalized EVs' charging load of Boulder city, Colorado, from 1st January 2018 to 30 May 2019 (17 months). The dataset contains transactions of EV charging for different locations. It consists of numerous metadata for the charging transactions like plug type, charging time, and gasoline savings. In the proposed work, the energy consumption and charging time are considered. For regression models, the most popular performance measures are forecasting accuracy, Mean Square Error (MSE), Mean Absolute Error (MAE), Mean Absolute Percentage Error (MAPE), and Root Mean Square Error (RMSE) [68]. Therefore, in the proposed model, we use the same parameters.

9.2. Results for the Electric Vehicle Component. In this section, performance metrics and experimental results for the EVs' component are discussed.

9.2.1. Performance Metrics for the Electric Vehicle Component. The effectiveness of the performance of the EVs' component is evaluated using the following performance metrics. For the searching and matching algorithm, convergence duration is used. For evaluating the EVs' load forecasting accuracy, MSE, MAE, MAPE, and RMSE are used. For the blockchain, execution and transaction gas consumption are used for the performance evaluation. The performance parameters are discussed as follows.

(i) *Convergence duration*: it is the aggregated time interval that the algorithm requires to converge. It includes both computational and communication overheads that are caused by the transmitted messages and encryption process, respectively

(ii) RMSE, MAPE, MAE, and MSE are defined in the following equations [69]

$$\text{RMSE} = \sqrt{\sum_{i=1}^{w} \frac{(y_i - \hat{y}_i)^2}{y_i}}, \tag{52}$$

$$\text{MAPE} = \frac{1}{w} \sum_{i=1}^{w} \left| \frac{y_i - \hat{y}_i}{y_i} \right|, \tag{53}$$

$$\text{MAE} = \frac{1}{w} \sum_{i=1}^{w} |y_i - \hat{y}_i|, \tag{54}$$

$$\text{MSE} = \sum_{i=1}^{w} \frac{(y_i - \hat{y}_i)^2}{w}, \tag{55}$$

where y_i and $\hat{y}_i$ are the actual and forecasted EVs'

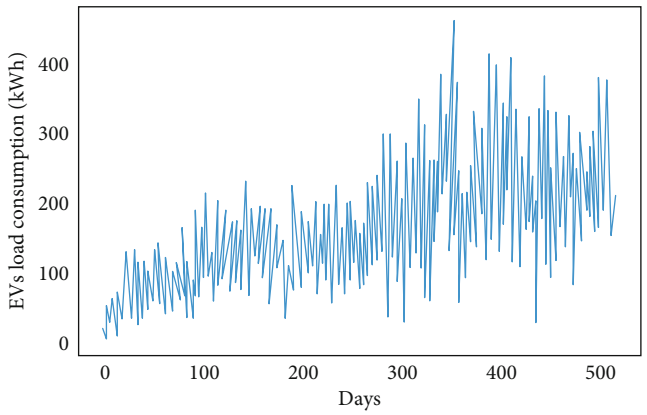


Figure 3: Normalized EVs' load consumption.

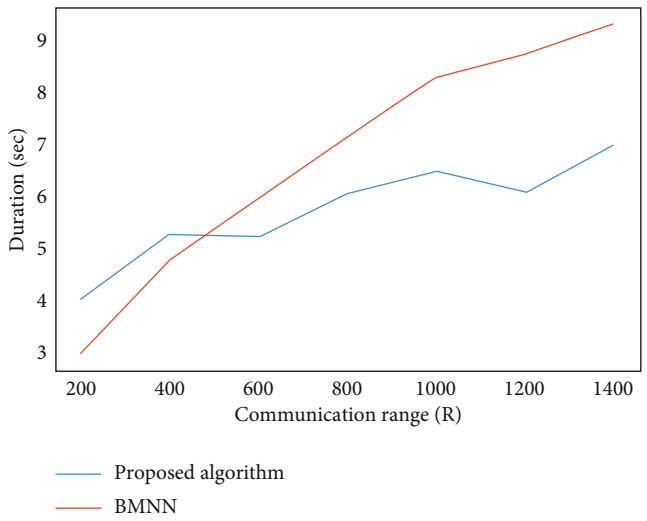


Figure 4: Total convergence duration of the proposed matching of EBEV with ESEV.

Table 3: Energy trading smart contract cost.

Function	1	2	3
GiveKwh	43257	20577	6.3834E-14
CreateStorage	126906	104866	2.31772E-13
SellEnergy	23796	796	2.4592E-14
BuyEnergy	23574	574	2.4148E-14
Contract creation	1826521	1335125	3.16165E-12

1: transactional cost (Gwei); 2: executional cost (Gwei); 3: actual cost (Ether).

Table 4: Reputation smart contract cost.

Function	1	2	3
Submit feedback	440697	417057	8.57754E-13
Contract creation	2017617	1478941	3.49656E-12

1: transactional cost (Gwei); 2: executional cost (Gwei); 3: actual cost (Ether).

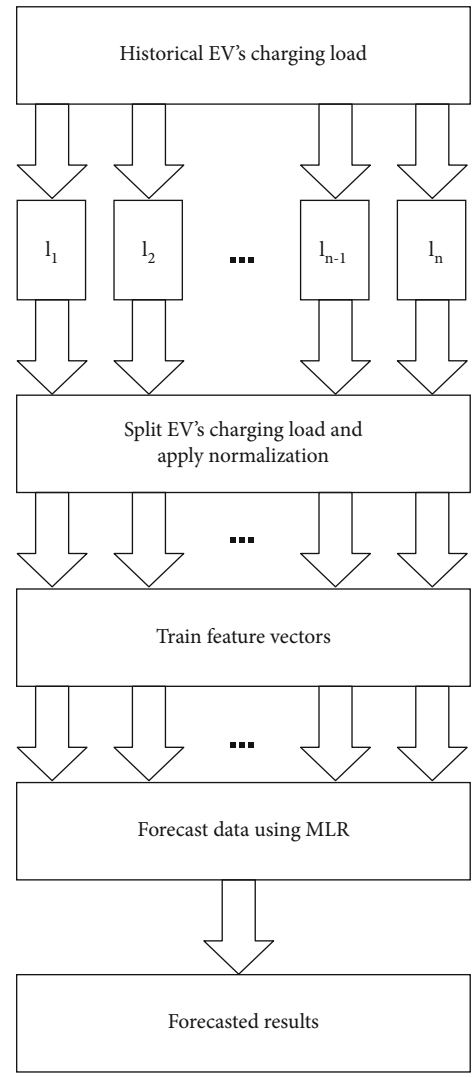


Figure 5: EV load forecasting model.

charging loads at point i, respectively, while the total number of EVs' charging points is w.

(iii) *Executional and transactional costs*: executional cost is the operational cost consumed for each line of code in the smart contract's function. The total amount of gas consumed by smart contracts' functions for sending data to the blockchain is called the transactional cost

9.2.2. Results of Reputation-Based Privacy-Preservation for the Matching EVs. In Figure 4, a comparison between the existing BMNN-based matching algorithm [38] and the proposed reputation-based matching algorithm in terms of convergence duration is presented. In the proposed reputation process, AG arranges EVs in a list according to their reputation points. So, an EBEV selects ESEV with the highest reputation that is presented at the top of the list. On the other hand, to find the perfect match, EBEV communicates with all the closest EVs when using the BMNN-matching process.

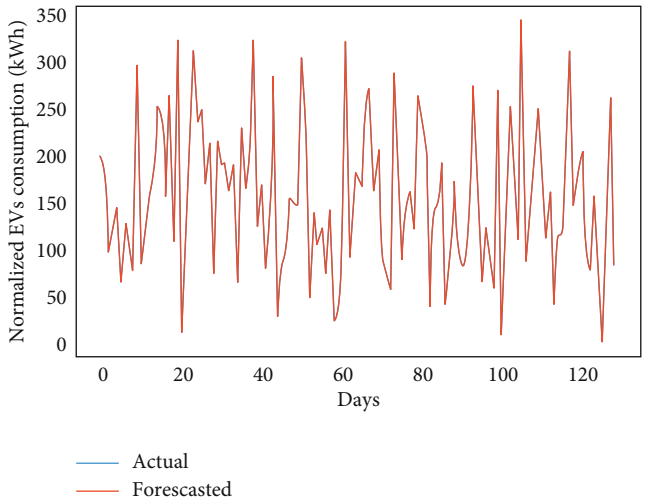


Figure 6: Comparison of actual and forecasted EVs' energy load consumption.

Table 5: Forecasting error comparison.

MSE	MAE	RMSE	MAPE	Accuracy
0.0188	0.6161	0.7501	0.7480	99.2519

Because of this, the matching algorithm based on BMNN increases additional communication and computational overheads. The overall convergence duration of the BMNN-based matching algorithm is compared with the proposed algorithm as shown in Figure 4. In all situations, as the communication range increases, and the number of rounds grows, such that no EV accepting the charging request is left. Thus, the communication duration also grows. The proposed algorithm's overall convergence duration reduces by approximately 2000 ms as compared to that of the BMNN algorithm's convergence duration.

9.2.3. Results of Reputation and Energy Trading Using Blockchain. Smart contracts are deployed to perform energy trading between EBEVs and ESEVs. Tables 3 and 4 depict the numerical findings of the transactional and executional costs for the proposed smart contracts: reputation and energy trading. The important functions of the proposed smart contracts include the *GiveKwh*, *CreateStorage*, *SellEnergy*, *BuyEnergy*, and *ContractCreation* functions. From the tables, it is shown that the maximum gas is consumed by the *CreateStorage* function. The reason is that the information uploaded on the proposed system requires more time and cost as compared to other functions. The gas consumption depends on the data size, which will be added to the proposed energy trading system. The other functions are *GiveKwh*, *SellEnergy*, *BuyEnergy*, and *ContractCreation* which consume the least cost as the functions do not require additional uploading data.

9.2.4. Results of EVs' Charging Load Forecasting Using MLR. A short-term charging load forecasting model using MLR is proposed to manage and plan for EVs' charging behavior as shown in Figure 5. Incorporating the forecasting model in the proposed system can help both the charging stations and EVs to properly plan ahead of the EVs' charging in order to maintain the usage of EVs and balance the energy consumption in SC as well as to perform a profitable energy trading. The forecasting model is divided into five stages, which are the input stage, splitting EVs' dataset and normalization stage, training stage, forecasting stage, and the final stage where the forecasting results are obtained. Figure 3 shows the normalized EVs' charging load of Boulder city, Colorado, from 1st January 2018 to 30 May 2019 (17 months). The normalization graph shows different variations of energy consumption across the days. The dataset is divided into training and testing samples at a ratio of 75 : 25. Afterwards, the normalized data is forwarded to the forecasting engine for prediction. The actual and the forecasted EVs' charging load are presented in Figure 6. In the figure, the red curve is the forecasted load and the blue curve is the actual load. As shown in the figure, the proposed model gives excellent prediction results. The forecasted result almost fits in the actual data, which shows a high accuracy of the proposed forecasting model. Error rates of the performance metrics are given in Table 5. From both the table and figure, it is observed that the result of the proposed forecasting model is good as the error rates from all the performance metrics are significantly low. To be precise, the forecasted accuracy of the proposed model is 99.25%.

From Figure 6, it is seen that the MLR model accurately maps the actual consumption of the electricity load. This implies that the model intelligently avoids the chance of overfitting during the forecasting of unseen periods of electricity consumption. Moreover, the forecasting curve of the MLR model shows that it perfectly learns the complex patterns of the data during the testing phase. Furthermore, overfitting a regression scheme is caused as a result of trying to estimate many parameters from very scanty data. However, to estimate the coefficients for the entire terms in the proposed scheme, a single sample is used for each polynomial, interaction, and predictor. In addition, we avoid overfitting using the cross-validation method.

9.3. Results for Residential Prosumers' Component. In this section, performance metrics and experimental results for the residential prosumers' component are presented.

9.3.1. Performance Metrics for the Residential Prosumers' Component. The performance of the residential prosumers' component is evaluated using the following performance metrics: RI, type of transactions performed, the energy contributed, average convergence time, and the number of iterations.

9.3.2. Experimental Results for Residential Prosumers' Component. The energy providers and consumers with surplus and deficit energy register their energy requests with AG via blockchain-based smart contracts. The data used

Table 6: Overall energy allocation.

Slot	E_{areq} (MWh)	E_c (MWh)	E (MWh)	E_{as} (MWh)	E_{allocR} (MWh) RSFEAP	E_{alloc} (MWh) SF-OEAP	RI
T1	[−18,−9, 0, 0]	27	22	[0, 0, 15, 7]	[14.8,7.2,0, 0]	[14.8,7.2,0, 0]	[20,20,30,15]
T2	[−6,−11,−11, 0]	28	23	[0, 0, 0, 23]	[4.8,8.8,9.4,0]	[4.8,8.8,9.4,0]	[5,30,45,30]
T3	[−8, 0,−17, 0]	25	21	[0, 4, 0, 4]	[6.4,0, 14.6,0]	[6.4,0, 14.6,0]	[5,30,30,20]
T4	[−15,−17, 0, 0]	32	26	[0, 0, 13, 13]	[12,14,0, 0]	[12,14,0, 0]	[5,30,30,20]

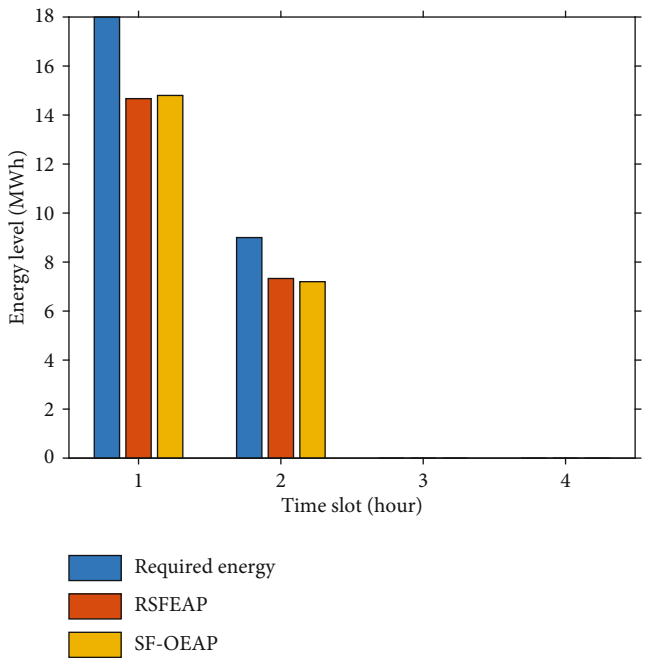


Figure 7: Comparison of allocated energy ($E_{i,allocR}$) to prosumers at T1 time slot.

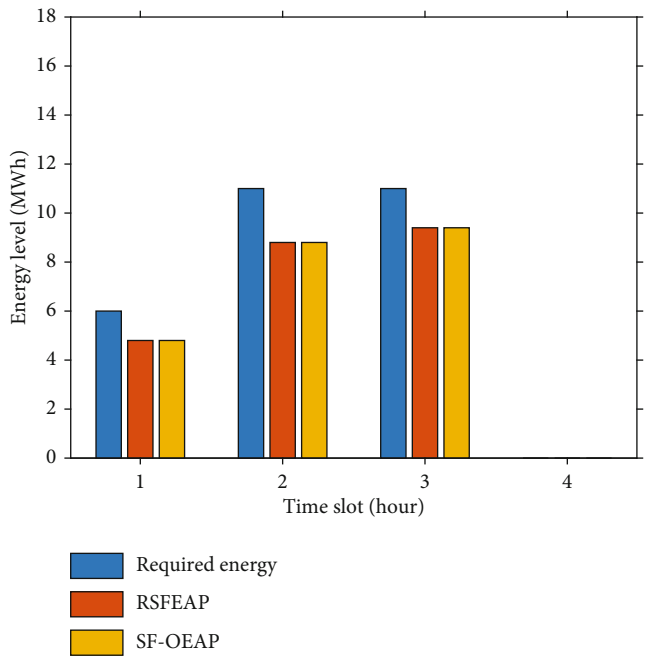


Figure 8: Comparison of allocated energy ($E_{i,allocR}$) to prosumers at T2 time slot.

for the simulations is taken from [42] and is presented in Table 6. In this scenario, some users are registered as energy consumers while others are registered as energy providers. The prosumers' registration takes place via blockchain. According to previous research works [70–72], transactions using blockchain are proved to be secured, distributed, traceable, and verifiable. In this research work, a cryptosystem technique using the ID-based encryption technique is incorporated into the system that helps to conceal energy transactional data.

In T1, two prosumers, i.e., Prosumer 1 and Prosumer 2, which are energy consumers, register their energy requests as 18 MWh and 9 MWh, respectively. On the other hand, Prosumer 3 and Prosumer 4, which are energy providers, register their surplus energy as 15 MWh and 7 MWh, respectively. The total surplus energy at time interval T1 is 22 MWh. After receiving the registered information, AG checks the available energy E and the total energy that is requested by the energy consumers E_c using the proposed RFEAP algorithm, i.e., Algorithm 7. If $E_c \leq E$, then the situation is simple; therefore, AG distributes the total surplus energy based on the exact amount of consumers' energy requests. If the aforementioned condition is false, AG uses the second condition, i.e., $E_c > E$, for optimal allocation of energy between consumers that use the novel RI-based algorithm. Considering the situation in T1, $E_c > E$; therefore, the surplus energy is allocated using the second condition of the fair energy allocation algorithm. Also, AG uses Algorithm 6 and Equation (16) to compute the RI's parameter that helps to optimally allocate energy to consumers. The values of RI and energy allocated for consumers in different time slots are given in Table 6. From the table, it is depicted that RI for the consumers at T1 is the same, which makes the algorithm serve the consumers with equal importance. In this case, the optimal energy allocation for Prosumer 1 and Prosumer 2 is to get energy according to the ratio of their request, i.e., 14.8 MWh and 7.2 MWh, respectively. In the second time interval T2, Prosumer 1, Prosumer 2, and Prosumer 3 are all energy consumers while Prosumer 4 is the energy provider. The total surplus energy at the time interval is 23 MWh, and the total energy requested by the consumers is 28 MWh. It is observed in Table 6 that the Consumer 3 gets higher consideration for the allocation of energy because it has higher RI value than both Prosumers 1 and 2. Moreover, Prosumer 2 gets higher preference than Prosumer 1 because of the similar reason for Prosumer 3.

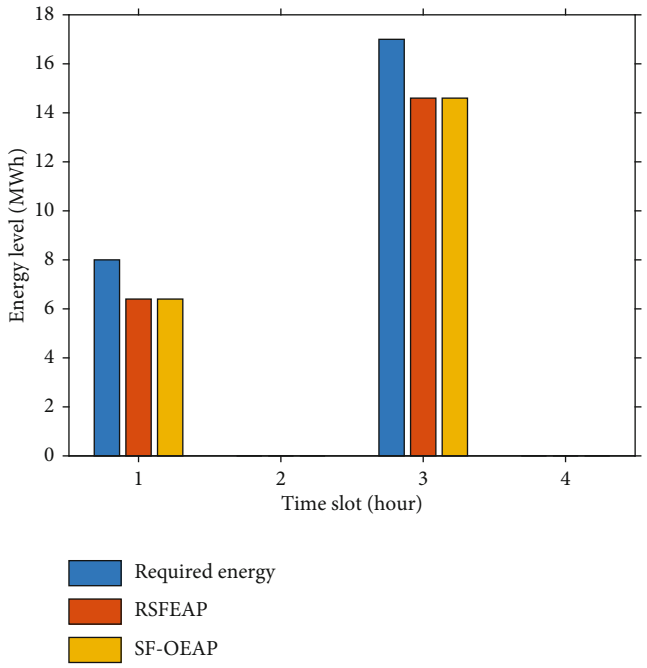


Figure 9: Comparison of allocated energy ($E_{i,allocR}$) to prosumers at T3 time slot.

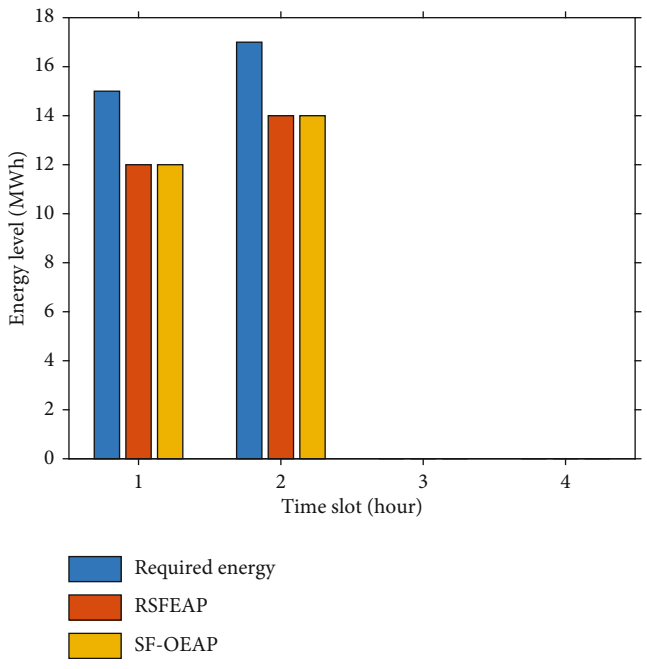


Figure 10: Comparison of allocated energy ($E_{i,allocR}$) to prosumers at T4 time slot.

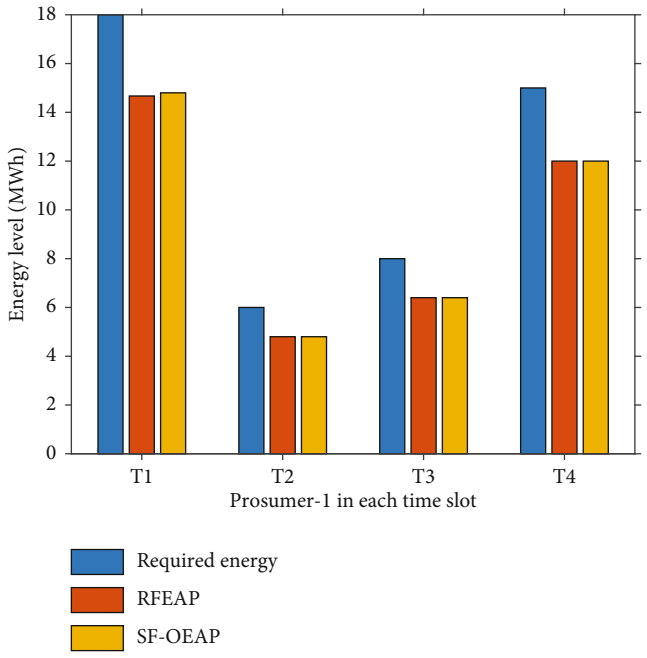


Figure 11: Comparison of energy allocated ($E_{1,allocR}$) to consumer-1 in each time slot.

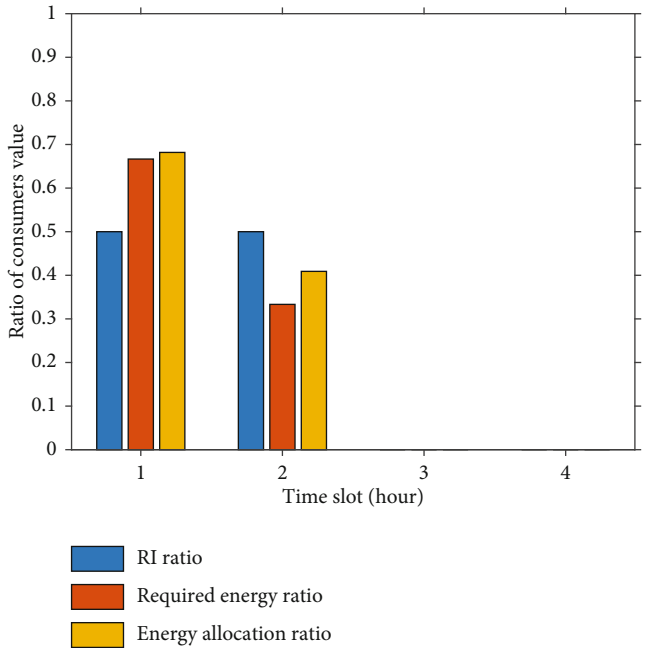


Figure 12: Impact of reward index on energy allocation to prosumers at T1 time slot.

The same process of the proposed reward energy allocation is applied for T3 and T4, in which the energy is fairly distributed between the consumers.

Note that the empty bars in Figures 7–11 depict that the prosumers are energy providers at those time intervals during fair energy allocation. The energy allocation for Prosumer 1 across all the four time intervals is given in Figure 11. It is observed that the RI of Prosumer 1 has the highest value at T1 as shown in Table 6; therefore, RSFEAP gives higher preference to it when allocating energy, whereas the other consumers share the remaining surplus energy based on their SL and RI. In other time intervals, the same rule applies to other consumers. As discussed previously, the starvation value and RI of each prosumer depends on the energy requested, past contributions, and type of transactions. The impact of RI on the fair energy allocation for

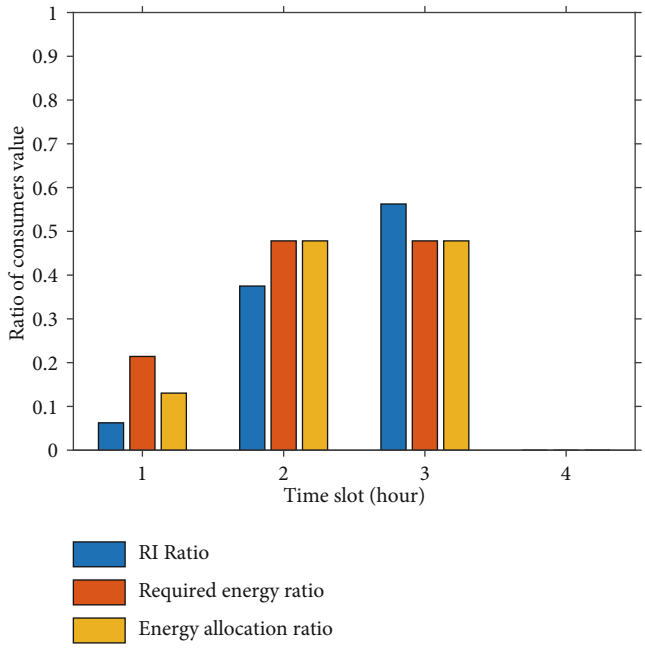


Figure 13: Impact of reward index on energy allocation to prosumers at T2 time slot.

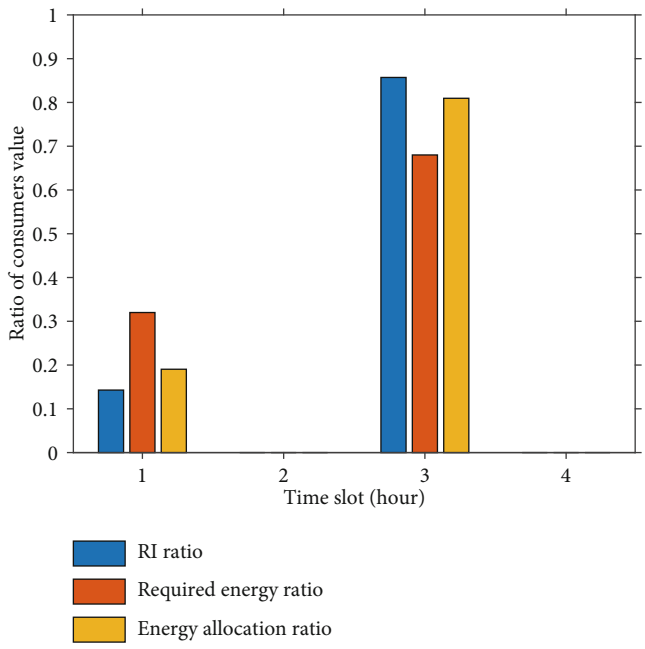


Figure 14: Impact of reward index on energy allocation to prosumers at T3 time slot.

all of the time slots is presented in Figures 12–15. Important ratios, i.e., $RI_i/Sum(\bar{RI})$, $E_{i,allocR}/E$, and $E_{i,arq}/E_c$ for the energy prosumers are investigated during the fair energy distribution. Here, $RI_i/Sum(\bar{RI})$ is the ratio of each energy consumer's RI to the total RI of all the energy consumers, $E_{i,allocR}/E$ is the ratio of each allocated energy for a consumer to the sum of all the surplus energy during the allocation, and $E_{i,arq}/E_c$ is the ratio of each actual energy request by a

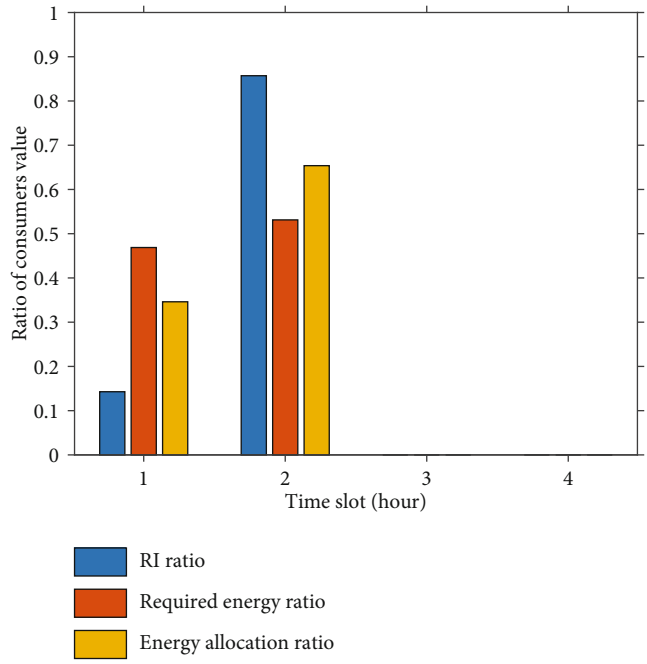


Figure 15: Impact of reward index on energy allocation to prosumers at T4 time slot.

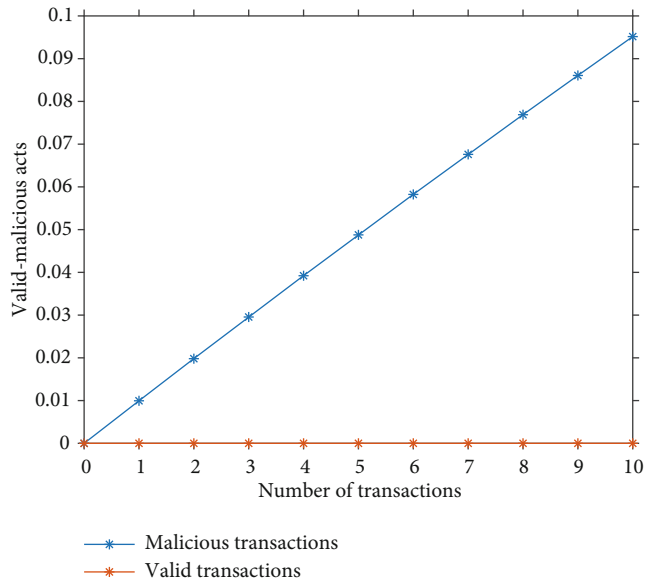


Figure 16: The valid and malicious transactions in the system.

consumer to the sum of all consumers' energy requests. In Figures 12–15, it is shown that the amount of allocated energy is large when the RI ratio is large; otherwise, it is less. The effects of malicious and valid transactions are also investigated as depicted in Figures 16–18. It is clearly shown in Figures 16 and 17 that an increase in malicious transactions decreases the amount of energy contributions made by the prosumers. On the other hand, an increase in the number of honest and valid transactions increases the energy contributions. The valid and malicious transactions directly affect RI of each prosumer as shown in Figure 18. As observed

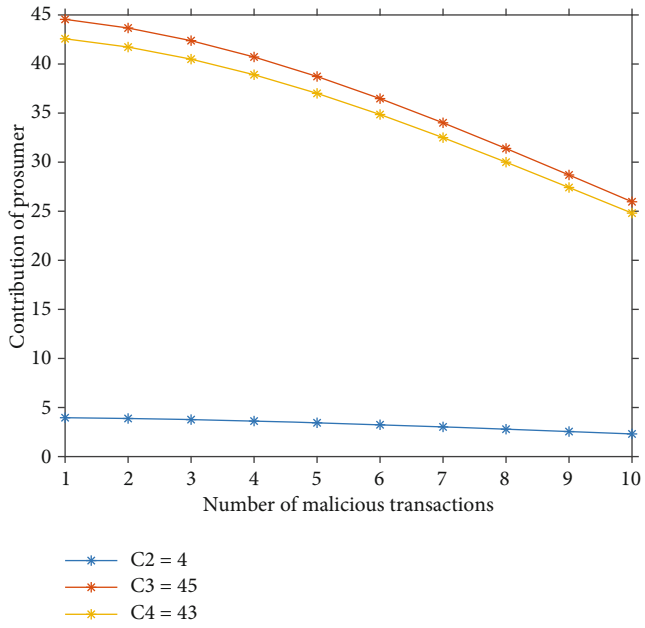


Figure 17: Impact of malicious transactions in the energy contribution for C_2, C_3, and C_4.

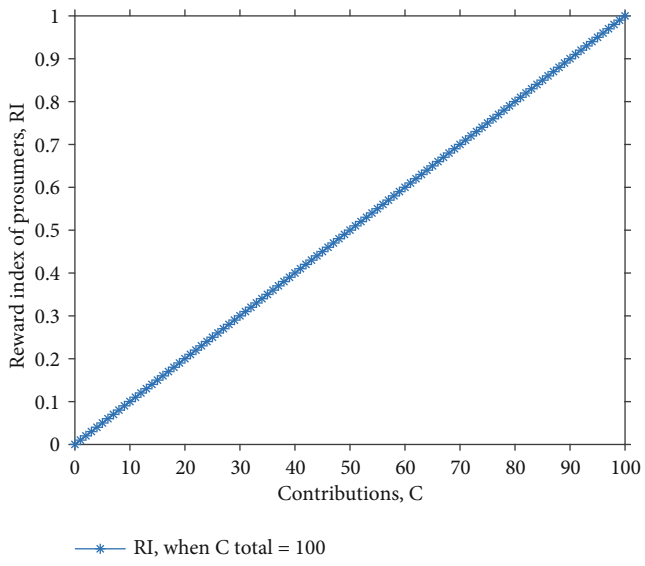


Figure 18: The effects of contributions on energy allocation.

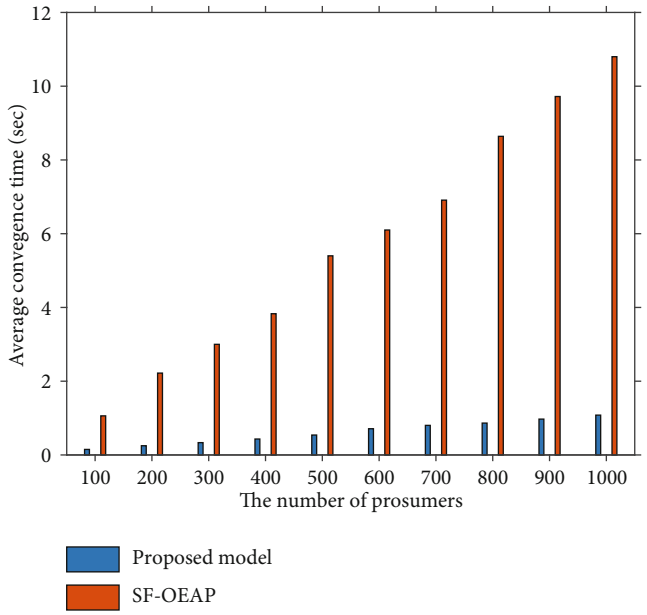


Figure 19: Average convergence time against the number of prosumers.

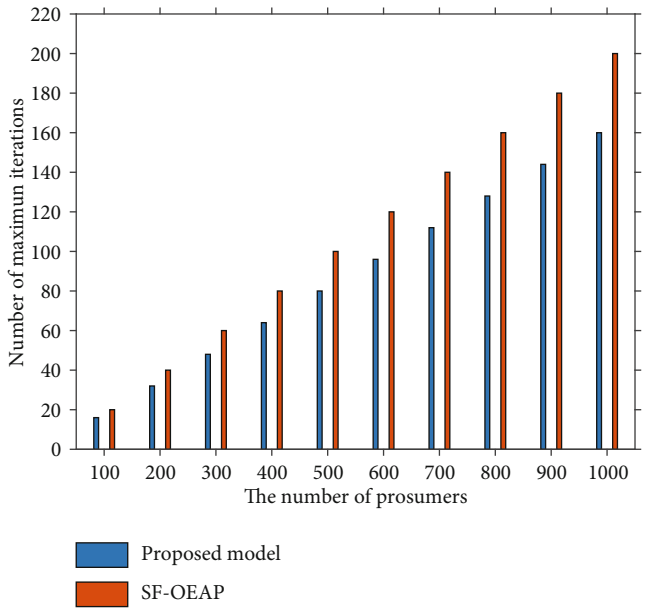


Figure 20: Number of maximum iterations against number of prosumers.

from the figure, when prosumers' contributions increase, RI also increases. The model prevents the proposed system against continuous malicious transactions. The comparison of energy level generated for each consumer by RSFEAP and SF-OEAP [42] is shown in Figures 7–10. In terms of average convergence time and maximum iterations, the proposed model is better than the SF-OEAP algorithm [42]. The convergence time and maximum iterations of the proposed model are shown in Figures 19 and 20, respectively. The results in Figure 19 show that the number of iterations increases with the increase in the number of prosumers where the number of iterations for 50 prosumers is 8, which is less than than the number of benchmark scheme's iterations. Similarly, the convergence time for the proposed model is approximately 10 times less than the benchmark algorithm. The reason is that the proposed algorithm performs the energy allocation based on reputation value, which is obtained directly from the blockchain. While in the benchmark algorithm, all the computations are done in the algorithm. As a result, the computational time and the number of iterations are reduced. This shows that the proposed model is faster than the benchmark schemes for implementation in real-time electricity market.

10. Conclusion and Future Work

This study proposes a blockchain-based privacy-preserving energy trading system for 5G-deployed SCs. The proposed system has two components: EVs and residential prosumers. In the proposed system, an RSFEAP algorithm for residential homes and a reputation-based distributed matching algorithm of EBEV with ESEV are presented. The RSFEAP algorithm is proposed to efficiently allocate energy to the residential consumers. The matching algorithm is proposed to match ESEV with EBEV in a secured and distributed manner. A short-term load forecasting model for EVs' charging using MLR is proposed to plan and manage the uncertainty of the charging behavior of EVs. The proposed system integrates ID-based encryption and HE techniques to protect the privacy of transaction data and users, respectively. Simulations are conducted and findings depict that the proposed system achieves promising performance. In the simulations, the EVs' charging load forecasting shows a better performance with an accuracy of 99.25%. In the RSFEAP, the number of iterations for 50 prosumers is 8, which is smaller than the benchmark scheme while the convergence duration is also 10 times less than the benchmark scheme. RSFEAP ensures a fair distribution of energy to each consumer in the energy-distributed system. Similarly, the proposed matching algorithm of EBEV with ESEV converges faster as compared to the existing BMNN algorithm with convergence duration of approximately 2000 ms. In the blockchain, the proposed smart contracts consume reasonable executional and transactional costs. Furthermore, in the proposed system, privacy and security and smart contract analyses are performed. The obtained results depict that the proposed smart contracts and overall system are bug-free and secure against security attacks and vulnerabilities.

In future, we intend to improve the EVs' charging load forecasting efficiency as well as the prediction accuracy. The increase in the number of charging EVs increases the amount of data, which will be used for improving EVs' charging load forecasting. Furthermore, the performance of the proposed system will be optimized and explored using hardware implementation. The integration of encryption mechanism, allocation algorithm, and blockchain in energy trading domain is still an open research topic and will be considered.

Nomenclature

1-D CNN: 1-Dimensional convolutional neural network
AG: Aggregator
BPNN: Back propagation neural network
BMNN: Bichromatic mutual nearest neighbor
CNN: Convolutional neural network
DSRC: Dedicated short-range communication
EBEVs: Energy-buying EVs
ESEVs: Energy-selling EVs
EVs: Electric Vehicles
FHE: Fully HE
HBC: Honest-but-Curious
HE: Homomorphic encryption
HEVs: Hybrid EVs
ID-Based: Identity-based
IoE: Internet of energy
KKT: Karush-Kuhn-Tucker
LSTM: Long short-term memory
LTE: Long-term evolution
MAE: Mean absolute error
MAPE: Mean absolute percentage error
MLR: Multiple linear regression
MSE: Mean square error
NSGA: Nondominated sorting genetic algorithm
P2P: Peer-to-peer
PHE: Partially HE
PKG: Private key generator
PoW: Proof of work
RBFNN: Radial basis function neural network
RI: Reward index
RICNN: Recurrent inception convolution neural network
RMSE: Root mean square error
RNN: Recurrent neural network
RSFEAP: Reward-based starvation-free energy allocation policy
SCs: Smart communities
SF-OEAP: Starvation-free optimal energy allocation policy
SG: Smart grid
SL: Starvation level
V2G: Vehicle-to-grid
V2V: Vehicle-to-vehicle
E_{arq}: Actual energy request of consumers
y: Actual EVs' load
E_{as}: Available surplus energy of provider
L: Energy demand
$E(a)$: Encryption of the plaintext a
$\hat{y}$: Forecasted EVs' charging load consumption
G: Generation of energy
E_{allocR}: Optimal energy allocation
S: Starvation factor
E_c: Sum of available energy from providers
E: Sum of energy requested from consumers
M: Sum of valid and malicious transactions
C: The amount of energy contributed by prosumer
$Cred_m$: The credibility value of m
G_1, G_3, and G_3: Three cylic groups of prime order
Y_i: The quantifier for valid and malicious transactions recorded by the miners
C_{Total}: The total energy contributed
$\text{Loc}(x, y)$: The location of the user
R_m: The rating given by node m
R_I: The reputation value of node I
θ: Transaction index
p and q: Two prime numbers that are selected for the HE
δ: Regression coefficient.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] D. Burmester, R. Rayudu, W. Seah, and D. Akinyele, "A review of nanogrid topologies and technologies," *Renewable and Sustainable Energy Reviews*, vol. 67, pp. 760–775, 2017.

[2] A. Pouttu, J. Haapola, P. Ahokangas et al., "P2P model for distributed energy trading, grid control and ICT for local smart grids," in *2017 European Conference on Networks and Communications (EuCNC)*, pp. 1–6, Oulu, Finland, 2017.

[3] D. Gregoratti and J. Matamoros, "Distributed energy trading: the multiple-microgrid case," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 4, pp. 2551–2559, 2015.

[4] K. Anoh, D. Bajovic, D. Vukobratovic, B. Adcbisi, D. Jakovetic, and M. Cosovic, "Distributed energy trading with communication constraints," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–6, Sarajevo, Bosnia and Herzegovina, 2018.

[5] C. Zhang, J. Wu, Y. Zhou, M. Cheng, and C. Long, "Peer-to-peer energy trading in a microgrid," *Applied Energy*, vol. 220, pp. 1–12, 2018.

[6] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 88–98, 2017.

[7] J. A. Lopes, F. J. Soares, and P. M. Almeida, "Integration of electric vehicles in the electric power system," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 168–183, 2011.

[8] J. Kim, J. Moon, E. Hwang, and P. Kang, "Recurrent inception convolution neural network for multi short-term load forecasting," *Energy and Buildings*, vol. 194, pp. 328–341, 2019.

[9] Y. Wang, D. Gan, M. Sun, N. Zhang, Z. Lu, and C. Kang, "Probabilistic individual load forecasting using pinball loss guided LSTM," *Applied Energy*, vol. 235, pp. 10–20, 2019.

[10] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, and J. Yan, "5G network-based Internet of Things for demand response in smart grid: a survey on application potential," *Applied Energy*, vol. 257, article 113972, 2020.

[11] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[12] "5G and the internet of energy," December 2021. https://www.navigantresearch.com/reports/5g-and-theinternet-of-energy.

[13] S. Sofana Reka, T. Dragičević, P. Siano, and S. R. S. Prabaharan, "Future generation 5G wireless networks for smart grid: a comprehensive review," *Energies*, vol. 12, no. 11, p. 2140, 2019.

[14] H. C. Leligou, T. Zahariadis, L. Sarakis, E. Tsampasis, A. Voulkidis, and T. E. Velivassaki, "Smart grid: a demanding use case for 5G technologies," in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 215–220, Athens, Greece, 2018.

[15] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *Journal of Network and Computer Applications*, vol. 122, pp. 50–60, 2018.

[16] M. U. Javed, N. Javaid, A. Aldegheishem, N. Alrajeh, M. Tahir, and M. Ramzan, "Scheduling charging of electric vehicles in a secured manner by emphasizing cost minimization using blockchain technology and IPFS," *Sustainability*, vol. 12, no. 12, p. 5151, 2020.

[17] O. Samuel and N. Javaid, "A secure blockchain–based demurrage mechanism for energy trading in smart communities," *International Journal of Energy Research*, vol. 45, no. 1, pp. 297–315, 2021.

[18] A. S. Yahaya, N. Javaid, F. A. Alzahrani et al., "Blockchain based sustainable local energy trading considering home energy management and demurrage mechanism," *Sustainability*, vol. 12, no. 8, p. 3385, 2020.

[19] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[20] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed vehicular networks," *Applied Sciences*, vol. 10, no. 6, p. 2011, 2020.

[21] R. Khalid, N. Javaid, A. Almogren, M. U. Javed, S. Javaid, and M. Zuair, "A blockchain-based load balancing in decentralized hybrid P2P energy trading market in smart grid," *IEEE Access*, vol. 8, pp. 47047–47062, 2020.

[22] A. S. Yahaya, N. Javaid, M. U. Javed, M. Shafiq, W. Z. Khan, and M. Y. Aalsalem, "Blockchain-based energy trading and load balancing using contract theory and reputation in a smart community," *IEEE Access*, vol. 8, pp. 222168–222186, 2020.

[23] W. Wang, D. T. Hoang, P. Hu et al., "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[24] O. Samuel, A. Almogren, A. Javaid, M. Zuair, I. Ullah, and N. Javaid, "Leveraging blockchain technology for secure energy trading and least-cost evaluation of decentralized contributions to electrification in sub-Saharan Africa," *Entropy*, vol. 22, no. 2, p. 226, 2020.

[25] L. Langer, F. Skopik, G. Kienesberger, and Q. Li, "Privacy issues of smart e-mobility," in *IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society*, pp. 6682–6687, Vienna, 2013.

[26] J. K. Liu, W. Susilo, T. H. Yuen et al., "Efficient privacy-preserving charging station reservation system for electric vehicles," *The Computer Journal*, vol. 59, no. 7, pp. 1040–1053, 2016.

[27] M. Nabil, M. Bima, A. Alsharif et al., "Priority-based and privacy-preserving electric vehicle dynamic charging system with divisible e-payment," in *Smart Cities Cybersecurity and Privacy*, pp. 165–186, Elsevier, 2019.

[28] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science-Research and Development*, vol. 33, no. 1-2, pp. 71–79, 2018.

[29] Z. Yang, S. Yu, W. Lou, and C. Liu, "P^2: privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[30] Y. Cao, N. Wang, G. Kamel, and Y.-J. Kim, "An electric vehicle charging management scheme based on publish/subscribe communication framework," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1822–1835, 2015.

[31] R. Zhang, X. Cheng, and L. Yang, "Energy management framework for electric vehicles in the smart grid: a three-party game," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 93–101, 2016.

[32] J. Zhu, Z. Yang, Y. Guo, J. Zhang, and H. Yang, "Short-term load forecasting for electric vehicle charging stations based on deep learning approaches," *Applied Sciences*, vol. 9, no. 9, pp. 1723–1735, 2019.

[33] Y. Li, Y. Huang, and M. Zhang, "Short-term load forecasting for electric vehicle charging station based on niche immunity lion algorithm and convolutional neural network," *Energies*, vol. 11, no. 5, pp. 1–25, 2018.

[34] J. Vermaak and E. C. Botha, "Recurrent neural networks for short-term load forecasting," *IEEE Transactions on Power Systems*, vol. 13, no. 1, pp. 126–132, 1998.

[35] D. L. Marino, K. Amarasinghe, and M. Manic, "Building energy load forecasting using deep neural networks," in *IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society*, pp. 7046–7051, Florence, Italy, 2016.

[36] W. G. Zhang, F. X. Xie, M. Huang, J. Li, and Y. F. Li, "Research on short-term load forecasting methods of electric buses charging station," *Power System Protection and Control*, vol. 41, no. 4, pp. 61–66, 2013.

[37] D. Chang, R. Jie, Z. Jianwei, D. Xiaoyan, G. Wenjie, and Z. Zhisheng, "Study on short term load forecasting of electric vehicle charging station based on RBF-NN," *Journal of Qingdao University*, vol. 4, pp. 44–48, 2014.

[38] F. Yucel, K. Akkaya, and E. Bulut, "Efficient and privacy preserving supplier matching for electric vehicle charging," *Ad Hoc Networks*, vol. 90, pp. 101730–101740, 2019.

[39] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2017.

[40] W. Hou, L. Guo, and Z. Ning, "Local electricity storage for blockchain-based energy trading in industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3610–3619, 2019.

[41] A. M. Jadhav and N. R. Patne, "Priority-based energy scheduling in a smart distributed network with multiple microgrids," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3134–3143, 2017.

[42] N. A. Funde, M. M. Dhabu, P. S. Deshpande, and N. R. Patne, "SF-OEAP: starvation-free optimal energy allocation policy in a smart distributed multimicrogrid system," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4873–4883, 2018.

[43] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[44] X. Huang, Y. Zhang, D. Li, and L. Han, "An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains," *Future Generation Computer Systems*, vol. 91, pp. 555–562, 2019.

[45] S. Meiklejohn, M. Pomarole, G. Jordan et al., "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 conference on Internet measurement conference*, pp. 127–140, Barcelona Spain, 2013.

[46] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*, pp. 839–858, San Jose, CA, USA, 2016.

[47] W. Hou, Z. Ning, X. Hu et al., "On-chip hardware accelerator for automated diagnosis through human–machine interactions in healthcare delivery," *IEEE Transactions on Automation Science and Engineering*, vol. 16, no. 1, pp. 206–217, 2019.

[48] S. Park, J. Lee, S. Bae, G. Hwang, and J. K. Choi, "Contribution-based energy-trading mechanism in microgrids for future smart grid: a game theoretic approach," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 7, pp. 4255–4265, 2016.

[49] A. S. Yahaya, N. Javaid, R. Khalid, M. Imran, and N. Naseer, "A blockchain based privacy-preserving system for electric vehicles through local communication," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, 2020.

[50] A. S. Yahaya, N. Javaid, R. Khalid, M. Imran, and M. Guizani, "A blockchain-based privacy-preserving mechanism with aggregator as common communication point," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, 2020.

[51] T. Rui, C. Hu, G. Li, J. Tao, and W. Shen, "A distributed charging strategy based on day ahead price model for PV-powered electric vehicle charging station," *Applied Soft Computing*, vol. 76, pp. 638–648, 2019.

[52] J. Zhao, C. Wan, Z. Xu, and J. Wang, "Risk-based day-ahead scheduling of electric vehicle aggregator using information gap decision theory," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1609–1618, 2017.

[53] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 24–43, Springer, Berlin, Heidelberg, 2010.

[54] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop, ACM*, pp. 113–124, Chicago Illinois USA, 2011.

[55] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 223–238, Springer, Berlin, Heidelberg, 1999.

[56] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: privacy-preserving personal profile matching in mobile social networks," in *2011 Proceedings IEEE INFOCOM*, pp. 2435–2443, Shanghai, China, 2011.

[57] Z. Su, Y. Wang, X. Qichao, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet of Things Journal*, vol. 6, pp. 286–297, 2018.

[58] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, "IoT public fog nodes reputation system: a decentralized solution using Ethereum blockchain," *IEEE Access*, vol. 7, pp. 178082–178093, 2019.

[59] J. Eberhardt and J. Heiss, "Off-chaining models and approaches to off-chain computations," in *Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, pp. 7–12, Rennes France, 2018.

[60] D. C. Montgomery, E. A. Peck, and G. Geoffrey Vining, *Introduction to Linear Regression Analysis*, vol. 821, John Wiley & Sons, 2012.

[61] A. Y. Saber and A. K. M. Rezaul, "Short term load forecasting using multiple linear regression for big data," in *2017 IEEE symposium series on computational intelligence (SSCI)*, pp. 1–6, Honolulu, HI, 2017.

[62] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, 2017.

[63] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[64] "IOTA vs Ethereum: what are the differences? Do both fullfill a need?," 2019, November 2021, https://cryptalker.com/iota-Ethereum/.Access.

[65] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in *Annual international cryptology conference*, pp. 213–229, Springer, Berlin, Heidelberg, 2001.

[66] G. Wood, "Ethereum: a secure decentralised and generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[67] City of Boulder Colorado, "Electric vehicle charging station dataset," 2019, July 2021, https://bouldercolorado.gov/services/electric-vehicle-charging-stations.

[68] S. Jahandideh, S. Jahandideh, E. B. Asadabadi et al., "The use of artificial neural networks and multiple linear regression to predict rate of medical waste generation," *Waste Management*, vol. 29, no. 11, pp. 2874–2879, 2009.

[69] A. Yang, W. Li, and X. Yang, "Short-term electricity load forecasting based on feature selection and least squares support vector machines," *Knowledge-Based Systems*, vol. 163, pp. 159–173, 2019.

[70] M. T. Devine and C. Paul, "Blockchain electricity trading under demurrage," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2323–2325, 2019.

[71] J. H. Huh and S. K. Kim, "The blockchain consensus algorithm for viable management of new and renewable energies," *Sustainability*, vol. 11, no. 11, pp. 1–30, 2019.

[72] G. Bansal, A. Dua, G. S. Aujla, M. Singh, and N. Kumar, "SmartChain: a smart and scalable blockchain consortium for smart grid systems," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, Shanghai, China, 2019.

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 7817249, 12 pages
https://doi.org/10.1155/2021/7817249

Research Article

A Novel Routing Protocol for Realistic Traffic Network Scenarios in VANET

Gagan Deep Singh,[1] **Sunil Kumar**,[1] **Hammam Alshazly**,[2] **Sahar Ahmed Idris**,[3] **Madhushi Verma**,[4] **and Samih M. Mostafa**[2]

[1]*University of Petroleum and Energy Studies, Dehradun-, 248007 Uttarakhand, India*
[2]*Faculty of Computers and Information, South Valley University, Qena 83523, Egypt*
[3]*College of Industrial Engineering, King Khalid University, Abha, Saudi Arabia*
[4]*School of Engineering and Applied Sciences, Bennett University, Greater Noida, India*

Correspondence should be addressed to Hammam Alshazly; hammam.alshazly@sci.svu.edu.eg

Received 10 October 2021; Accepted 11 November 2021; Published 9 December 2021

Academic Editor: Mohammed H. Alsharif

The vehicular ad hoc network (VANET) has traditional routing protocols that evolved from mobile ad hoc networks (MANET). The standard routing protocols of VANET are geocast, topology, broadcast, geographic, and cluster-based routing protocols. They have their limitations and are not suitable for all types of VANET traffic scenarios. Hence, metaheuristics algorithms like evolutionary, trajectory, nature-inspired, and ancient-inspired algorithms can be integrated with standard routing algorithms of VANET to achieve optimized routing performance results in desired VANET traffic scenarios. This paper proposes integrating genetic algorithm (GA) in ant colony optimization (ACO) technique (GAACO) for an optimized routing algorithm in three different realistic VANET network traffic scenarios. The paper compares the traditional VANET routing algorithm along with the metaheuristics approaches and also discusses the VANET simulation scenario for experimental purposes. The implementation of the proposed approach is tested on the open-source network and traffic simulation tools to verify the results. The three different traffic scenarios were deployed on Simulation of Urban Mobility (SUMO) and tested using NS3.2. After comparing them, the results were satisfactory and it is found that the GAACO algorithm has performed better in all three different traffic scenarios. The realistic traffic network scenarios are taken from Dehradun City with four performance metric parameters including the average throughput, packet delivery ratio, end-to-end delay, and packet loss in a network. The experimental results conclude that the proposed GAACO algorithm outperforms particle swarm intelligence (PSO), ACO, and Ad-hoc on Demand Distance Vector Routing (AODV) routing protocols with an average significant value of 1.55%, 1.45%, and 1.23% in three different VANET network scenarios.

1. Introduction

VANETs have evolved as a key solution of intelligent transport systems (ITS). The existing technologies and swarm intelligence are also integrating with VANET to realize its actual purpose. VANET routing protocols are evolved from the standard preexisting protocols like Dynamic Source Routing (DSR) and AODV. DSR and AODV were found efficient and best suitable for multihop wireless ad hoc networks and Internet of Things (IoT) devices [1]. While designing any of the VANET, scenarios for Vehicle-to-Vehicle (V2V) communication must focus on all the aspects of VANET routing. These days, the technological upgrades are very frequent and fast. Hence, soon, it will be noticed that the deployment of the 5G GSM network invades in Vehicle-to-Infrastructure (V2I) setup. That results in the inception of V2V and V2I in the Urban Intelligent Transportation Systems (UITS). The emergence of IoT in near future will boost VANET communication through machine learning and data analysis. VANET is made through vehicles independently communicating among themselves. These vehicles can be assumed as nodes capable enough to

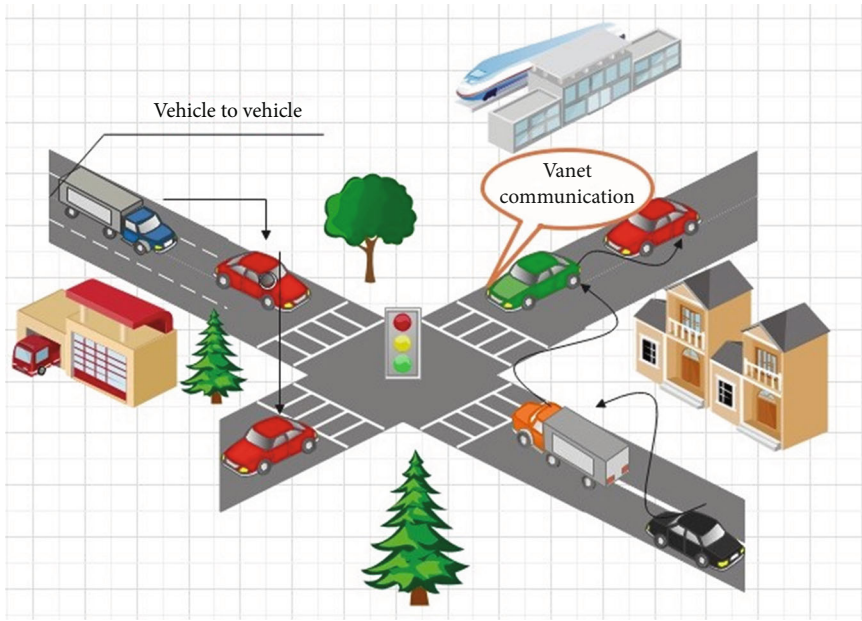


Figure 1: VANET structure.

establish wireless communication with other nodes, giving birth to entirely a new shared mesh network with the self-organizing property. It generates huge possibilities to develop numerous applications for VANET. These applications can make the road travel experience easy, safe, more entertaining, and efficient. It will also help decrease the traveling time; road traffic congestion helps avoid congested areas, increase road capacity, and be usable during emergencies, thus, resulting in lesser fuel wastage [2]. Ultimately, the environment will be cleaner. At present, various VANET routing protocols and wireless standards are already available, but none of them is yet able to provide the universal routing solution for VANET realistic scenarios [3].

Figure 1 presents the VANET structure showing how the vehicle is passing a broadcast message to other vehicle nodes and creates a VANET environment. In this dynamic structure, vehicles communicate with each other to broadcast the information. The routing plays an integral role in this structure, and different routing challenges are faced in this type of vehicular networks such as dynamic topology, availability and reliability of network throughput, realistic traffic scenarios, unpredictable driver's driving psychology, and inadequate routing algorithm for all types of vehicular traffic scenarios. The research paper addresses the identified challenges and provides an effective routing mechanism focusing on performance metrics like average throughput, packet delivery ratio, and end-to-end delay in VANET routing.

The major contributions of this research paper are as follows:

(i) A novel genetic algorithm-based ant colony optimization technique (GAACO) was proposed to optimize the routing algorithm for three realistic traffic scenarios

(ii) The proposed algorithm validated the VANET routing performance with average throughput, packet delivery ratio, end-to-end delay, and packet loss

(iii) The performance of the proposed GAACO is discussed and compared with the traditional protocols using the NS3.26 simulator with standard and realistic traffic scenarios

The rest of the paper is structured as follows. The various research issues of VANETs with the significance of routing in VANETs are reviewed in Section 2. The methodology adopted along with the designed framework is discussed in Section 3. The experimental setup and results are discussed in Section 4. Section 5 draws the conclusion of this research work.

2. Overview of Previous Work

The routing protocols are responsible for providing the best suitable route among the nodes within its network. There are some standard routing protocols designed for VANET routing environments. These protocols are classified in various aspects, like quality of service (QoS), characteristics of the protocol, network structure, routing algorithm, and information dissemination [1]. The literature review of this paper discussed five major VANET routing protocols, which are presented in Figure 2.

Further, in the literature review, the routing protocols in VANET are classified into transmission strategies-based routing protocols and information-based routing protocols [4]. It is concluded during rigorous literature finding that routing information-based protocol is suitable for this research development, as this needs to devise efficient routing based on swarm intelligence. It is also confirmed

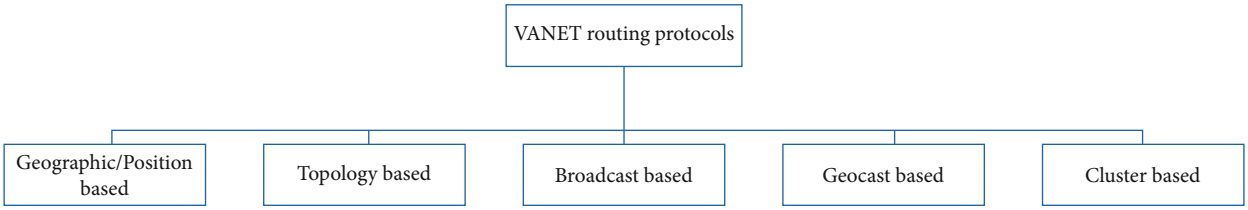


Figure 2: Classification of VANET routing protocols.

that the literatures are not concerned with transmission strategy-based protocol, as the research is not focusing on information dissemination issues and challenges in VANET [5].

Hence, this extensive literature survey can conclude that existing standard routing protocols are not suitable for VANET routing in all traffic scenarios. The information-based routing protocol can be classified into two classes, i.e., topology-based and geographic/position-based VANET routing protocols. Every node is aware of the network layout in topology-based routing, whereas each node knows the location of other nodes while forwarding the packet in position-based routing [6]. It was seen that VANETs are not scale-free networks as Gaussian probability circulations approximate their node degree distributions. However, the conduct of low-density VANETs is the same as to small-world networks, and connectivity is too low even to consider benefitting from the small-world property [7].

In [8], a navigation methodology that can gather online information of the roads through VANET can be used by the drivers to reach their destination in a distributed manner and real-time situation. The simulation test result shows that the new protocol increases the vehicle's rate of local awareness through simulated barriers. Exchanged messages updated the neighbouring vehicle's records and increased attention to different nodes that cooperatively forwarded demands and solutions. Intervehicular interaction that assessed another independent WiMAX framework is proposed in [9]. The broad simulation was acknowledged in the OPNET framework for the design of the WiMAX-mesh framework. In [3], the authors presented their platooning algorithm based on swarm-based intelligence. This algorithm applied two different factors to decrease the travel time. It insisted on green traffic signal time that makes the traffic-free path for the vehicle movement. Then, the proposed preemptive traffic signal approach is combined with an existing modified ACO technique to design platooning of the vehicles. These characteristics concluded the platooning algorithm is an efficient way to minimize the waiting time of the commuters. In [10], the authors introduced an investigation of different simulation instruments accessible for VANET. VANET simulators' taxonomy assists future VANET analysts to pick an ideal simulator, which is most appropriate for VANET scheme objectives. Two AODV protocols, P-AODV and improved AODV, are examined and dependent on some parameters [11].

The available routing protocols are unable to facilitate VANET with efficient routing in major traffic scenarios [1]. The Optimized Link State Routing Protocol (OLSR) is

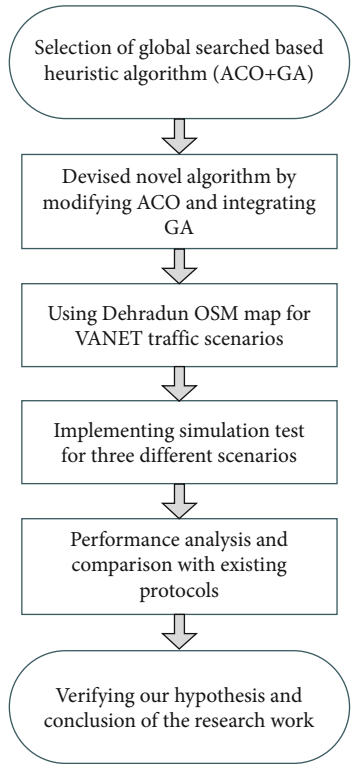


Figure 3: The adopted methodology.

not preferred as it requires high bandwidth to process and to identify the best network route [12]. In [13], GA is applied to manage the multicast routing through computational intelligence. A stable routing protocol resolves the node disconnection in VANET that was tested and alerted the disconnection before occurrence [14]. The multiconstrained QoS aware routing algorithm is also developed using ACO-based swarm intelligence techniques. As a result, the traffic type data-based QoS network can be achieved. So, security in VANET is also attained through a reliable QoS algorithm [15]. In VANET, the ACO and DSR protocols have also been proposed as routing options that use stable routing in a variety of VANET scenarios [16]. To monitor real-time performance, an eco-friendly ACO-based routing method was presented that shares roadway linkages. The novel feedback and cost updating technique are used to resolve the weakness of VANET routing [17]. In [18], the authors proposed Prediction-based Greedy Perimeter Stateless Routing (PGPSR), which is a modified version of Greedy Parameter Stateless Routing (GPSR). PGPSR is more efficient than the standard GPSR because packet delivery ratio

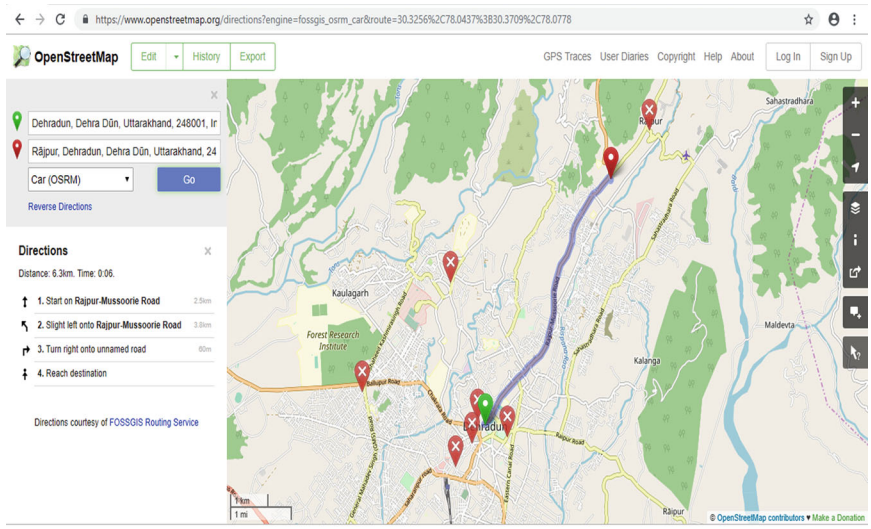


Figure 4: OSM map of Dehradun Clock Tower to Mussoorie Rajpur Road.

(PDR) and maximum throughput are found to be increased in VANET routing. However, it does not fit dense and sparse network scenarios due to the significant delay in calculations and its complex computations. In [19], the authors proposed the GA technique for VANET to locate the best population of vehicles that generated and managed data flow and reduce the bandwidth utilization in wireless network. Using random values of the initial population size is reduced based on corresponding effect coefficients.

In [20], both PSO and ACO are considered in the vehicular network for enhancing the performance of VANET. Multiple routes from the source to the destination are established with uniform density of the vehicles using ACO. In [21], a new approach has been proposed and compared with the existing algorithms. The proposed algorithm showed improved performance in terms of delay time reduction, throughput, stability up gradation, and lifetime.

The improved genetic algorithm-based routing optimization technique (IGAROT) is presented in [22]. This GA variant replaces the selection technique with the k-means clustering method adopting from the same concept of a novel clustering-based genetic algorithm for the route optimization technique proposed in another approach [23]. IGAROT utilizes the vehicle density required in communication for VANET scenarios that randomly initialize individual populations. That provides the initial solution for the defined search space. Likewise, in a low-density VANET communication scenario with 20 vehicles, this makes a randomly generated initial population size of 1 by 20. In this way, IGAROT creates unique generations by selecting the best solutions from the initial population. That comes after many generations to give the best solution. A new metaheuristic Giza pyramid construction (GPC) algorithm is presented in [24]. It helped to review the technologies, best optimum methods, and strategies of that time.

VANETs are unable to meet the exact needs and applications of all users. For example, in real-time situations, the emergency signals have to be forwarded with minimum latency and high priority; however, messages like infotainment and hello/hi can be put up in queue and latency. Hence, in sparse and dense networks, the minimum calculated desired time (MCDT) technique is suggested, and data dissemination is performed using a context-aware congestion resolution protocol. MCDT determines the node connectivity through a peak-stable link [25, 26]. Modified lion algorithm (LA) is also used to compare with GA, and performance analysis was done for cost, complexity, and convergence. The simulation analysis of modified LA with respect to standard GA and LA proved the superiority of the modified LA [27]. In this literature study, the analysis of the related works in the last ten years was presented and then reviewed. Through that, the research approach is formed for efficient routing in VANET. The experimental test is performed on a realistic simulation environment using only open-source software tools like network simulator (NS) and SUMO.

3. The Developed Methodology

Simulations are used to test the performance of traditional and newly developed VANET routing algorithms. Many of them are suitable for the desired traffic scenario. But none of them can provide suitable results for three distinctive traffic scenarios. ACO technique with GA approach is selected and deployed for testing the performance in the selected scenarios along with two other traditional routing protocols of VANET. Then, simple traffic scenarios and complex traffic scenarios are used to generate the simulation environment. For a realistic traffic network scenario, the Dehradun City map of Clock Tower to Mussoorie-Rajpur road is imported from http://www.openstreemap.org [28]. The stepwise approach is adapted to complete this proposed research work as shown in Figure 3.

Then, a new algorithm is devised as per requirement analysis, by changing the position and updating the preexisting ACO by mutation features of GA. Hence, a new GAACO

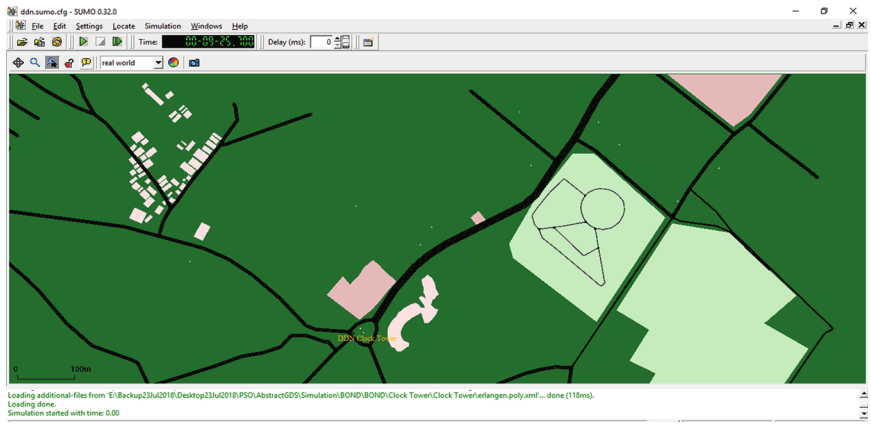


Figure 5: SUMO map generated through netconvert command for Dehradun Clock Tower to Mussoorie Rajpur Road.

Input: $S_I = \{S_1, S_2, S_3, \cdots .S_i\}$ //scenarios in VANET
$CP_K = \{CP_1, CP_2, CP_3, \cdots .CP_k\}$ $\forall\, CP_K \in \overset{i}{_{I=1}}(S_I)$
$itr \coloneqq 0$ and $G \coloneqq 0$ //itr & G are iteration and generation resp
Max_{itr}= maximum number of iteration
£ = threshold value
Ω = node density
T_{cong}= total traffic congestion
Output: $\lambda_R = optimized\ traffic\ route$

1. **Repeat while** $\boldsymbol{itr} \neq \text{Max}_{itr}$
2. $\lambda_{R_A} = \left\{ \begin{array}{l} \text{Call Algorithm 2}\ (S_I, CP_K, £) \\ \text{Call Algorithm 3}\ (S_I, CP_K, £) \\ \text{Call Algorithm 4}\ (S_I, CP_K, £) \end{array} \right\}$
   $\forall\, CP_K \in \overset{i}{_{I=1}}(S_I)$, $\lambda_{R_A} = \{\lambda_{R_1}, \lambda_{R_2}, \lambda_{R_3}, \cdots \cdots \cdots .\lambda_{R_a}\}$ and $R_A = \{R_1, R_2, R_3, \cdots .R_z\}$
3. **If** $(T_{cong} \leq \Omega)$ do
4. **If** $(\lambda_{R_A}\ better\ that\ \lambda_{R_{A+1}})$ where $\overset{a}{_{A=1}}\lambda_{R_A}$ and $\overset{z}{_{\alpha=1}}R_\alpha$
5. **Save** R_α
6. Find λ_{R_A} and call corresponding algorithm
7. **End if**
8. **End if**
9. **End while**

Algorithm 1: Optimized result based on the output of GA and ACO evaluation.

algorithm is proposed by rearranging the ACO population and integrating it with the GA algorithm. The experimental result shows the positive results of the algorithm on "Dehradun Clock Tower" to "Mussoorie-Rajpur Road" city route imported from http://openstreetmap.org [28]. The screenshots of the OpenStreamMap (OSM) map and generated route map are shown in Figures 4 and 5, respectively.

The selection of the population, crossover, and mutation is used for the VANET routing with ACO. In each iteration, a new population of the same size can be generated from the current population using three basic operations on the individuals of the population. GA is best suited for ACO techniques with road traffic scenarios in VANET as it is capable to adapt the routing alterations as per the need of the traffic scenarios.

The proposed algorithm is verified by validating the simulation results for three different traffic scenarios [3]. The algorithm devised for the research work is presented in Algorithm 1.

Further, the devised Algorithm 1 was deployed and tested using simulation experiments for all the mentioned algorithms as in Algorithm 2 to Algorithm 5. The methodology applied for simulation tests is elaborated as per Algorithm 1. The three different scenarios were designed in a simulation environment. The simple traffic network, complex traffic network, and Dehradun realistic city traffic network scenarios are implemented and tested to capture the routing performance data.

Algorithm 2 presents the deployment of PSO at three proposed traffic scenarios. This algorithm is used to run the simulation for gathering the data of the defined

```
    Compute initial speed limits, computational parameters (CP_K) and velocity (£), POS = position of each node
1.      P ⟵ 0 //for iteration
2.      While P ≠ END
3.          Do //for each particle
4.              Compute £ and CP_K
5.              If (CP_K ∈ i_{I=1}(S_I)
6.                  Evaluate CP_K
7.                  Compute new velocity £
8.                  Update POS
9.                  P = P +1
10.             End if
11.         End do
12.     End
```

Algorithm 2: PSO $(S_I, CP_K, £)$.

```
    Initialization for X⟶ 1 to x
    Generate initial position of each swarm
1.    P⟵ 0 //for iteration
2.    While P ≠ END
3.    Calculate best position from node density
4.        Do //for each particle
5.            Compute £ and CP_K
6.            If (CP_K ∈ i_{I=1}(S_I)
7.                Evaluate CP_K
8.                Compute new velocity £
9.                P = P +1
10.           End if
12.       End do
13.   End while
```

Algorithm 3: ACO $(S_I, CP_K, £)$.

```
    Input: AS swarm size (total number of ants)
           A_L initial location of ant ∀ L ∈ {1, 2, 3,……,l}
           I_tr used for iteration number {20-40}
  Output: Optimized route
1.      Set I_tr =0, gen =0;
2.      Initialize GA, ACO
3.          Call Algorithm 5 (GA for swarm position)
4.              Max(generation)
5.              Gen++
6.              Continue;
7.          End for
8.        Initialize pheromone
9.      For I_tr ⟵ 1 to T
10.             ANT_i++;
11.             Update(pheromone);
12.     End for
13.     Return optimized_solution;
```

Algorithm 4: Proposed GAACO for optimizing parameter.

performance metrics. It is tested for average throughput, packet delivery ratio, end-to-end delay, and packet loss. All the values are tabulated for three proposed traffic scenarios for further analysis in comparison to ACO and devised GAACO algorithms.

Similarly, Algorithm 3 presented here is ACO technique that best suits the three proposed traffic scenarios. ACO is also deployed to run the simulation on these three traffic scenarios and to record the data of the opted performance metrics. The same method is applied to test for average throughput, packet delivery ratio, end-to-end delay, and packet loss. All the values are tabulated in comparison with PSO and devised GAACO algorithms.

Algorithm 4 presents our devised algorithm in a combination of ACO along with GA features. ACO is applied and has been tweaked by integrating the GA approach through Algorithm 5.

Algorithm 4 works on the basic features of ACO optimizing techniques taken vehicle nodes as ants in the swarm. Then, the population is updated as and when required through the mutation feature of the GA approach as illustrated in Algorithm 5. Algorithm 4 calls Algorithm 5 to regenerate the vehicle nodes for the simulation. Through this, the updated population of the vehicle swarm can be generated in the proposed traffic scenarios which is very beneficial in a realistic city traffic network environment.

Similarly, Algorithm 5 is also used to deploy the simulation test for the proposed traffic scenarios and evaluate the results. Hence, the optimized result is captured for further analysis and conclusion. The four selected performance metrics are used for all of the three scenarios during the implementation of PSO, ACO, and GAACO. The next part of the paper presents the framework designed to perform the simulation experiments and discussions of the results with the final analysis.

4. Experiments and Results

The methodology developed and applied for this research test provides a much simpler and faster way for performing experiments and getting results. For all the experimental setups, the test deployed on the computing machine with Corei7-8700 3.2 GHz of processor and a minimum of 16 GB RAM is required. That was the HP workstation used from the University of Petroleum and Energy Studies,

```
1.      T⟵ 0 //for iteration
2.      Initialize S(T) //initial population
3.      Evaluate S(T) with computational parameters
5.      While T ≠ END
6.          Do
7.                  Recombine S(T) to yield crossover C(T)
8.                  Evaluate C(T)
9.                  Select S(T +1) from S(T) and C(T)
10.                  T = T +1
11.         End
12.     End
```

Algorithm 5: GA for initial and updated swarm position.

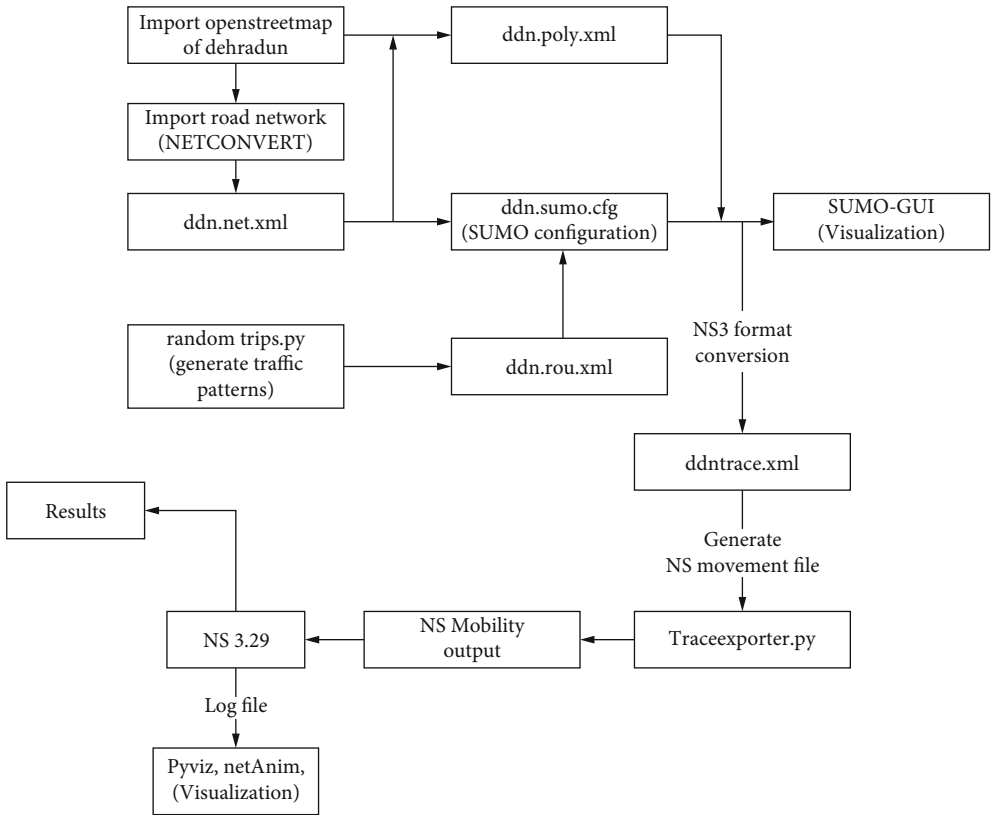


Figure 6: Framework used for simulation experiments.

Computer Laboratory, IT Tower, ITLab102_PC35. There was a need to repeat the simulation tests multiple times to verify the results, as reading may vary due to the machine's poor performance. Figure 6 illustrates the framework of the process used for all the research simulation tests. The below-designed framework was implemented for repetitive simulation tests on an HP workstation machine through the open-source operating system Ubuntu 16.04 release [29]. The traffic simulator used is SUMO 0.32 [30] and Network Simulator NS-3.26 [31, 32] for all the research tests.

The simulations were carried by importing the real city scenario map of Dehradun City from OpenStreetMap [33] for a realistic approach. Then, this was converted for the SUMO network. The region from Clock Tower to Mussoorie Rajpur Road is selected as it is the most congested route because of the heavy traffic going to Mussoorie from various regions during peak season times. The mentioned details in Table 1 illustrate the characteristics of the simulation parameters.

This paper presents the results from the point of view of four significant performance metrics, i.e., average throughput, packet delivery ratio, end-to-end delay, and packet loss. The simulation was performed for three VANET scenarios. The first is for simple, the second is for complex traffic networks, and the third is for real city Dehradun traffic

Table 1: Simulation parameters with specifications.

Parameters	Specification details
Open source OS	Ubuntu 16.04
Open source network simulator	NS3.26
Open source traffic simulator	Simulation of urban mobility (SUMO-0.32)
Open street map for Dehradun City vehicle traces	http://www.openstreetmap.org
Model	Manhattan mobility model
Transmission network range	150 to 200 m
Size of data packets	200 bytes
Interval	0.02 seconds
Data rate	2 Mbps
Protocol	MAC layer 802.11p
Velocity	20 to 80 km/h (above 80 is not permitted in Dehradun)

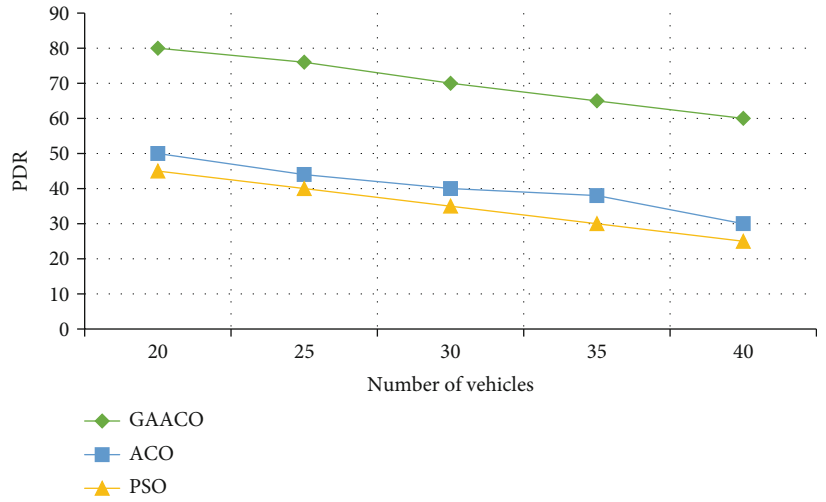


Figure 7: Performance analysis of packet delivery ratio computed for simple traffic network at a random speed.

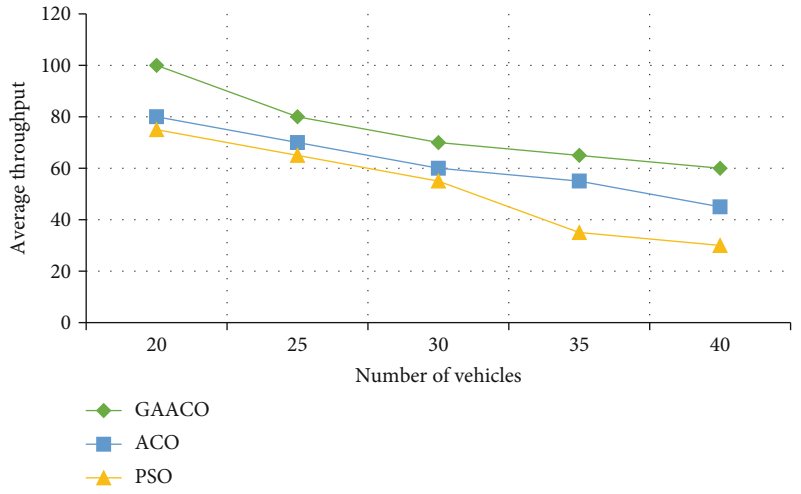


Figure 8: Performance analysis of average throughput computed for simple traffic network at a random speed.

scenarios. The above-discussed methodology is followed and tested for PSO, ACO, AODV, and GAACO routing protocols. The performance analysis is shown in graphs as per Figures 7–12.

In addition to the above-depicted comparison, the performance of the proposed GAACO is also compared with ACO, PSO, and AODV routing protocols from the point of view of end-to-end delay and packet loss. Figures 13

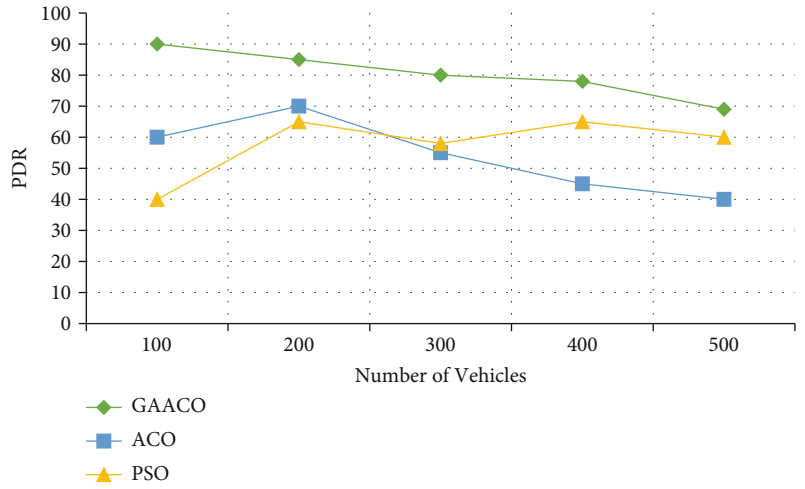


Figure 9: Performance analysis of packet delivery ratio computed for complex traffic network at a random speed.

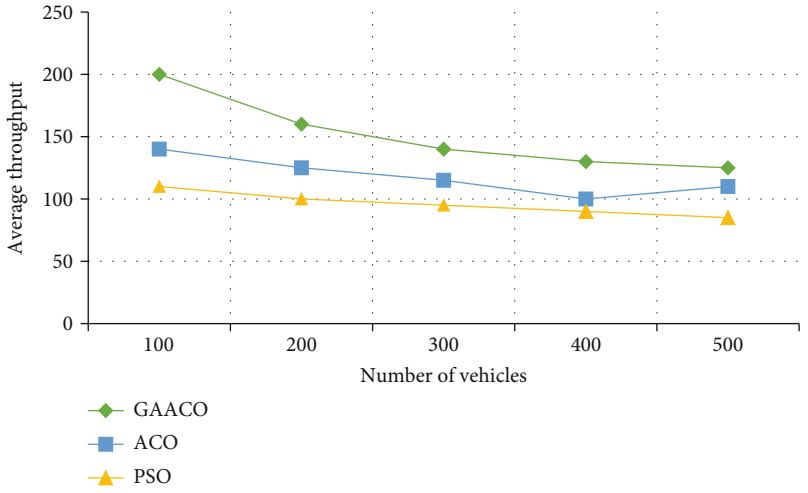


Figure 10: Performance analysis of average throughput w.r.t. no. of vehicles for dense network.

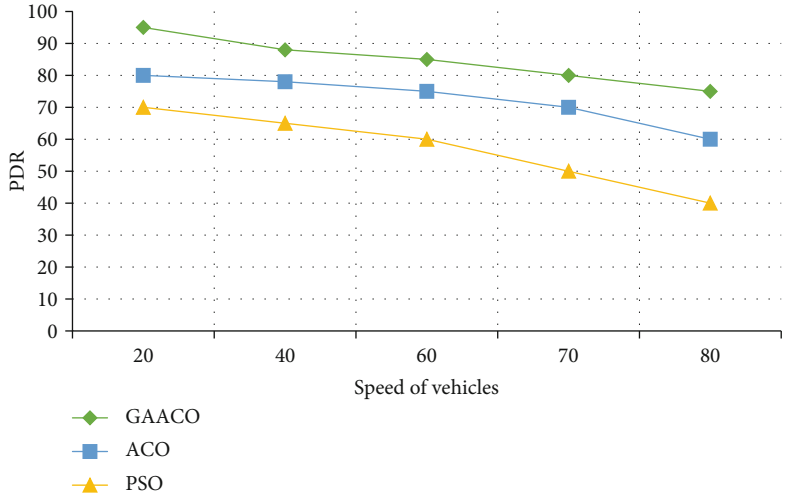


Figure 11: Performance analysis of packet delivery ratio computed for Dehradun realistic traffic scenario.

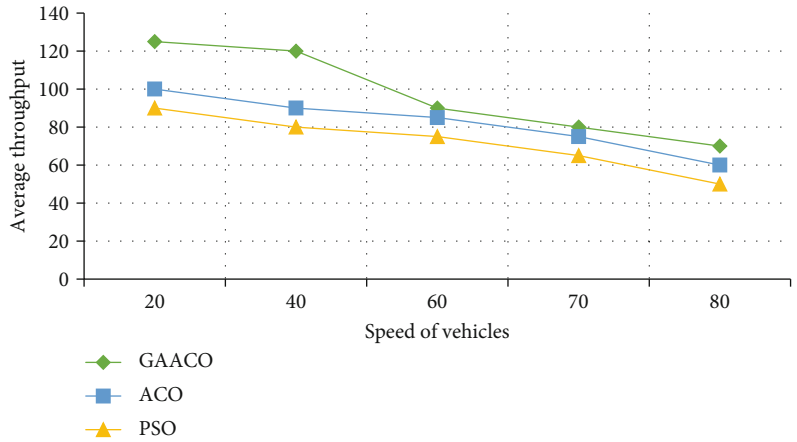


Figure 12: Performance analysis average throughput computed for Dehradun realistic traffic scenario.

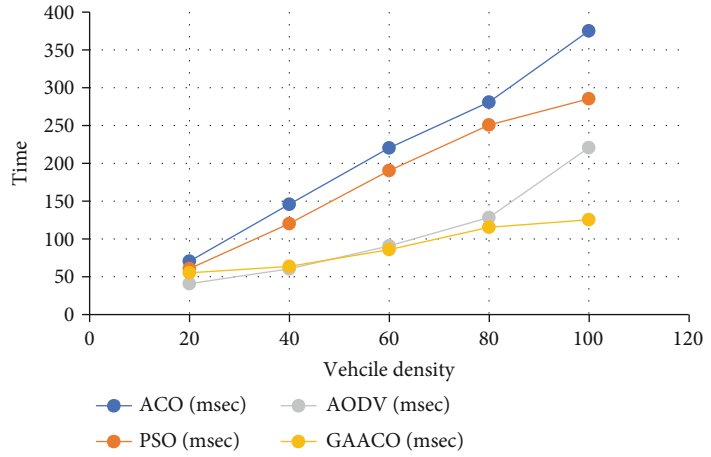


Figure 13: Performance analysis for end-to-end delay.

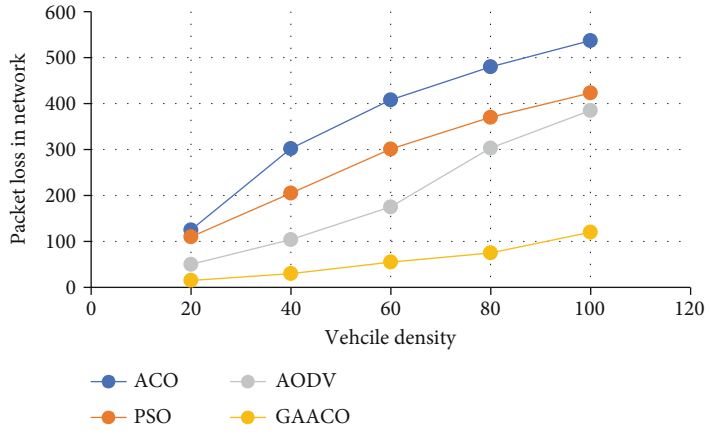


Figure 14: Performance analysis for packet loss in the network.

and 14 show that the proposed algorithm surpassed the compared algorithms in the selected VANET traffic scenarios.

Table 2 shows that the GAACO has better performance for two standard performance metrics in three distinctive VANET traffic network scenarios, i.e., simple traffic, complex traffic, and Dehradun Mussoorie-Rajpur road realistic traffic network scenarios. The performance significance statistics are shown in comparison with PSO and ACO with respect to GAACO in Table 2.

Table 2: Performance comparison with existing approaches.

Routing algorithm	Performance significance comparison		
	Simple traffic network	Complex traffic network	Dehradun realistic traffic scenario
PDR performance significance of GAACO with PSO	1.9%	1.4%	1.5%
PDR performance significance of GAACO with ACO	1.7%	1.5%	1.1%
Average throughput performance significance of GAACO with PSO	1.4%	1.6%	1.3%
Average throughput performance significance of GAACO with ACO	1.2%	1.3%	1.2%

5. Conclusion

In this paper, the discussion on various research areas of VANET was presented, and a detailed review has been done on various traditional and metaheuristics VANET algorithms. Considerable amount of work has been done in the field of VANET routing, but such works are limited to specific scenarios and routing. They are also not able to fulfill the present challenges in various traffic routing scenarios. There is a huge scope to develop and test much better efficient routing that can work in multiple traffic scenarios. The present work has been done to fulfill the gap that has been presented through research challenges in VANET. Some techniques proved better in sparse networks while others in dense networks. Similarly, no such technique exists in the literature that can provide a solution to VANET routing for realistic traffic scenarios with a hybrid algorithm that incorporates swarm intelligence and genetic algorithm. The newly devised GAACO algorithm is compared on three different VANET traffic scenarios, and it is found that GAACO has performed better for three distinctive VANET network traffic scenarios. The significance of GAACO is found to be superior with an average significant value of 1.55%, 1.45%, and 1.23% for PSO, ACO, and AODV routing protocols with respect to simple traffic, complex traffic, and Dehradun realistic VANET traffic scenarios, respectively. Hence, this can be confidently concluded that the newly devised GAACO has the features that are best suited for considered VANET traffic routing environments. The routing performance is noticeably improved when it is tested for packet delivery ratio and average throughput. Moreover, there were improvements in end-to-end delay and packet loss in a network. The future scope of this research can be considered to test and implement the proposed algorithm in other VANET scenarios with different performance metrics. The same can also be tested in flying ad hoc network (FANET) and intra-satellite communications for space research programs.

Data Availability

No external data was used to support the conducted experiments.

Conflicts of Interest

The authors declare that they have no conflict of interest.

Acknowledgments

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University through the Research Groups Program under Grant RGP.2/53/42.

References

[1] G. D. Singh, R. Tomar, H. G. Sastry, and M. Prateek, "A review on VANET routing protocols and wireless standards," in *Smart Innovation*, vol. 78 of Systems and Technologies, pp. 329–340, Springer, Singapore, 2018.

[2] G. D. Singh, M. Prateek, and G. Hanumat Sastry, "Swarm intelligence based algorithm for efficient routing in VANET," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 5, pp. 1124–1136, 2020.

[3] G. D. Singh, M. Prateek, and G. Hanumat Sastry, "Swarm intelligence based efficient routing algorithm for platooning in VANET through ant colony optimization," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9, pp. 1238–1244, 2019.

[4] S. Singh and G. S. Aujla, "A closer look through routing protocols in vehicular ad hoc networks (VANETs)," *IOSR Journal of Engineering*, vol. 4, no. 6, pp. 58–64, 2014.

[5] M. Chaqfeh, A. Lakas, and I. Jawhar, "A survey on data dissemination in vehicular ad hoc networks," *Vehicular Communications*, vol. 1, no. 4, pp. 214–225, 2014.

[6] C. Ksouri, I. Jemili, M. Mosbah, and A. Belghith, "VANETs routing protocols survey: classifications, optimization methods and new trends," in *International Workshop on Distributed Computing for Emerging Smart Networks*, pp. 3–22, Springer, Cham, 2019.

[7] J. Bhatia, R. Dave, H. Bhayani, S. Tanwar, and A. Nayyar, "SDN-based real-time urban traffic analysis in VANET environment," *Computer Communications*, vol. 149, pp. 162–175, 2020.

[8] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. Li, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Transactions on Computers*, vol. 63, no. 2, pp. 510–524, 2012.

[9] P. D. Dorge, G. H. Raisoni, and M. B. Chakole, "Implementation of MIMO and AMC techniques in WiMAX network based VANET system implementation of MIMO and AMC techniques in WiMAX network based VANET system," *International Journal of Information Technology and Computer Science (IJITCS)*, vol. 8, no. 2, pp. 60–68, 2016.

[10] V. Patel, M. Chaturvedi, and S. Srivastava, "Comparison of SUMO and SiMTraM for Indian traffic scenario

representation," *Transportation Research Procedia*, vol. 17, pp. 400–407, 2016.

[11] R. Cumbal, X. Calderon, R. Hincapie, L. Urquiza, and G. Arevalo, "Performance analysis of a VANET with optimal infrastructure location in setting urban," in *2018 IEEE Colombian Conference on Communications and Computing (COLCOM)*, Medellin, Colombia, May 2018.

[12] F. Goudarzi, H. Asgari, and H. S. Al-Raweshidy, "Traffic-aware VANET routing for city environments-a protocol based on ant colony optimization," *IEEE Systems Journal*, vol. 13, no. 1, pp. 571–581, 2018.

[13] C. H. Lee, K. G. Lim, M. K. Tan, R. K. Y. Chin, and K. T. K. Teo, "A genetic algorithm for management of coding resources in VANET," in *2017 IEEE 2nd International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, pp. 80–85, Kota Kinabalu, Malaysia, October 2017.

[14] Y. He, W. Xu, and X. Lin, "A stable routing protocol for highway mobility over vehicular ad-hoc networks," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pp. 1–5, Glasgow, UK, May 2015.

[15] M. H. Eiza, T. Owens, and Q. Ni, "Secure and robust multi-constrained QoS aware routing algorithm for VANETs," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 32–45, 2016.

[16] R. Kumar and S. K. Routray, "Ant colony based dynamic source routing for VANET," in *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, pp. 279–282, Bangalore, India, 2016.

[17] A. Elbery, H. Rakha, M. Y. Elnainay, F. Filali, and W. Drira, "Eco-routing: an ant colony based approach," in *International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2016)*, pp. 31–38, Rome, Italy, 2016.

[18] C. Wang, Q. Fan, X. Chen, and W. Xu, "Prediction based greedy perimeter stateless routing protocol for vehicular self-organizing network," in *IOP Conference Series: Materials Science and Engineering*, vol. 322, 2018no. 5, Article ID 052019.

[19] M. Jafer, M. A. Khan, S. Ur Rehman, and T. A. Zia, "Optimizing broadcasting scheme for VANETs using genetic algorithm," in *2016 IEEE 41st Conference on Local Computer Networks Workshops (LCN Workshops)*, pp. 222–229, Dubai, United Arab Emirates, 2016.

[20] B. Ranjan Senapati and P. Mohan Khilar, "Optimization of performance parameter for vehicular ad-hoc network (VANET) using swarm intelligence," in *Nature Inspired Computing for Data Science*, pp. 83–107, Springer, Cham, 2020.

[21] B. Dappuri, M. Amru, and A. M. Venkatanaga, "A stable routing algorithm based on link prediction method for clustered VANET," in *Recent Trends and Advances in Artificial Intelligence and Internet of Things*, pp. 85–95, Springer, 2020.

[22] H. Bello-Salau, A. M. Aibinu, Z. Wang, A. J. Onumanyi, E. N. Onwuka, and J. J. Dukiya, "An optimized routing algorithm for vehicle ad-hoc networks," *Engineering Science and Technology*, vol. 22, no. 3, pp. 754–766, 2019.

[23] A. M. Aibinu, H. B. Salau, N. A. Rahman, M. N. Nwohu, and C. M. Akachukwu, "A novel clustering based genetic algorithm for route optimization," *Engineering Science and Technology*, vol. 19, no. 4, pp. 2022–2034, 2016.

[24] S. Harifi, J. Mohammadzadeh, M. Khalilian, and S. Ebrahimnejad, "Giza pyramids construction: an ancient-inspired metaheuristic algorithm for optimization," *Evolutionary Intelligence*, pp. 1–19, 2020.

[25] M. L. Chiang, "Eventually byzantine agreement on CDS-based mobile ad hoc networks," *Ad Hoc Networks*, vol. 10, no. 3, pp. 388–400, 2012.

[26] G. D. Singh, M. Prateek, and G. H. Sastry, "A novel algorithm for efficient routing in vehicular ad hoc network using swarm intelligence optimization techniques," *International Journal of Advanced Science and Technology*, vol. 29, no. 7, pp. 1132–1143, 2020.

[27] M. B. Wagh and N. Gomathi, "Route discovery for vehicular ad hoc networks using modified lion algorithm," *Alexandria Engineering Journal*, vol. 57, no. 4, pp. 3075–3087, 2018.

[28] "Webpage, "OpenStreetMap"," https://www.openstreetmap.org/#map=18/30.32427/78.04188.

[29] S. Jain, S. Sharma, and R. Tomar, "Integration of wit API with python coded terminal bot," in *Emerging Technologies in Data Mining and Information Security*, pp. 397–406, Springer, Singapore, 2019.

[30] G. D. Singh, M. Prateek, and G. H. Sastry, "Methodology to perform simulation experiments for realistic VANET scenarios using open source software tools," *International Journal of Psychosocial Rehabilitation*, vol. 24, no. 6, pp. 10170–10175, 2020.

[31] P. Chithaluru, S. Kumar, A. Singh, A. Benslimane, and S. K. Jangir, "An energy-efficient routing scheduling based on fuzzy ranking scheme for internet of things (IoT)," *IEEE Internet of Things Journal*, 2021.

[32] P. P. Chatterjee, A. Deshpande, and A. Patel, "A discrete-event network simulator for internet systems," November 2020, https://www.nsnam.org/releases/ns-3-29/download/.

[33] "Dehradun clock tower|OpenStreetMap," November 2020, https://www.openstreetmap.org/search?query=dehradun clock tower#map=15/30.3321/78.0542&layers=N.

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 3400558, 16 pages
https://doi.org/10.1155/2021/3400558

Research Article

Secure Message Transmission for V2V Based on Mutual Authentication for VANETs

Jabar Mahmood,[1] **Zongtao Duan**,[1] **Heng Xue**,[1] **Yun Yang**,[1] **Michael Abebe Berwo**,[1] **Sajjad Ahmad Khan**,[2] **and Abd al Kader Ahmed Yassin**[3]

[1]*School of Information and Engineering, Chang'an University, Xi'an 710064, China*
[2]*Department of Computer Engineering, Istanbul Gelisim University (IGU), 34310 Istanbul, Turkey*
[3]*Hatay Mustafa Kemal University (MKU) Turkish-Hatay/Hassa-MYO Girne, 79. Sk., 31700, Turkey*

Correspondence should be addressed to Yun Yang; yangyun@chd.edu.cn

Received 25 September 2021; Revised 22 October 2021; Accepted 27 October 2021; Published 23 November 2021

Academic Editor: Muhammad Asghar Khan

The advancements in Vehicular Ad Hoc Networks (VANETs) require more intelligent security protocols that ultimately provide unbreakable security to vehicles and other components of VANETs. VANETs face various types of security pitfalls due to the openness characteristics of the VANET communication infrastructure. Researchers have recently proposed different mutual authentication schemes that address security and privacy issues in vehicle-to-vehicle (V2V) communication. However, some V2V security schemes suffer from inadequate design and are hard to implement practically. In addition, some schemes face vehicle traceability and lack anonymity. Hence, this paper's primary goal is to enhance privacy preservation through mutual authentication and to achieve better security and performance. Therefore, this article first describes the vulnerabilities of a very recent authentication scheme presented by Vasudev et al. Our analysis proves that the design of Vasudev et al.'s scheme is incorrect, and resultantly, the scheme does not provide mutual authentication between a vehicle and vehicle server when multiple vehicles are registered with the vehicle sever. Furthermore, this paper proposes a secure message transmission scheme for V2V in VANETs. The proposed scheme fulfills the security and performance requirements of VANETs. The security analysis of the proposed scheme using formal BAN and informal discussion on security features confirm that the proposed scheme fulfills the security requirements, and the performance comparisons show that the proposed scheme copes with the lightweightness requirements of VANETs.

1. Introduction

Recently, the use of transportation has increased in every aspect of our lives. Vehicles are used not only for traveling but also in various smart city applications (such as traffic lights, cameras, and street lights) [1]. Urban transportation faces various challenges such as traffic issues, parking challenges, poor connectivity, inefficient road safety, and traffic jamming [2]. Intelligent Transportation System (ITS) [3, 4] provides solutions to previously mentioned challenges in urban transportation [5].

Vehicular Ad Hoc Networks (VANETs) [6–9] play a vital role in the urban transportation system; they help to improve road safety and traffic management. VANETs communicate with various elements such as vehicles, Roadside Units (RSUs) [10–12], Onboard Wireless Units (OBUs), internet/network, and vehicle servers/vehicle authentication servers. Based on these elements, communication is divided into two categories, V2V and Vehicle to RSUs (V2R/V2I). V2V communicate through the Dedicated Short-Range Communication (DSRC) protocol [13], which is included in IEEE 802.11p [14, 15]. Figure 1 shows the VANET architecture.

The OBU is fixed inside the vehicle and integrated with a Global Positioning System (GPS), ITS-G5 IEEE 802.11p protocol, and various sensors [13]. The OBU function stores information such as vehicle location, speed, and traffic flow on the road during driving and permits disseminating the information to RSUs or other vehicles on the road. The RSUs are fixed on the road edges; RSUs collect all

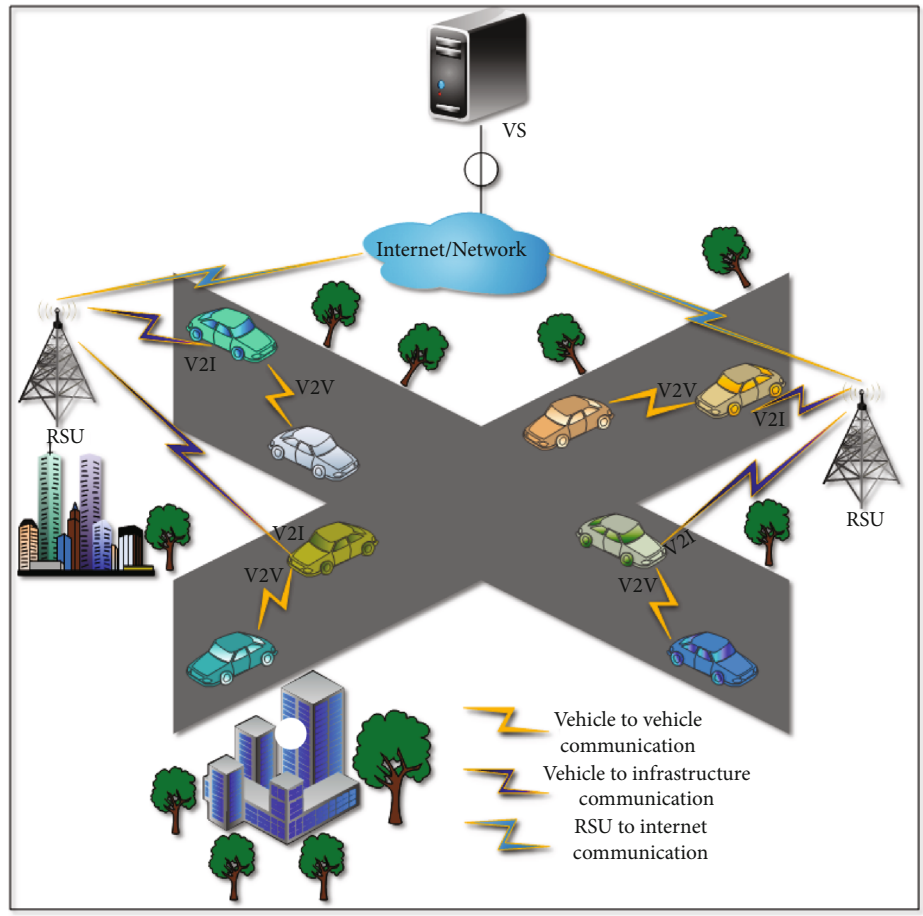


Figure 1: Structure of VANETs.

information from the vehicles/OBUs, save it, forward it to vehicles, and connect other RSUs for the network's security. That information is passed through a reliable communication channel from RSUs to OBUs and RSUs to RSUs. A vehicle server or vehicle authentication server ensures that all vehicles are trusted in-network and checks the vehicle ID and password when entering the network. If the vehicle fails to prove identity, an alert message is sent in the network through RSUs about a fake vehicle. Figure 2 provides complete details about V2V communication in VANETs. Usually, vehicles communicate with other vehicles, share information/data about the vehicle's current position, and share the keys. These data are confidential and sent through a secure communication channel with trusted vehicles part of the network. If confidential information is available, the adversary can use it in a way that is dangerous to vehicles and humans. In such a case, the adversary/attacker quickly gets a transmitted message and uses its advantages, such as altering the message and changing it according to its benefits or delaying the transmitted message making it unavailable to the original vehicle or devices within a specific time limit [16].

1.1. Motivation and Contributions. We observed that VANETs face various threats during communication, such as internal and external threats, as discussed previously. Every attacker hits the data packets, aiming to disturb the network and use its benefits. Due to these situations, we need a suitable protocol that provides strong user authentication and secures the data packet from attackers in V2V. This paper is aimed at analyzing the recent scheme, "A Lightweight Mutual Authentication Protocol V2V Communication on Internet of Vehicles," proposed by Vasudev et al. to present vital design faults. Specifically, LAMP-V2VCIoV cannot work when more than one registered vehicles are in the system. The working of LAMP-V2VCIoV can only be apprehended when there is only one vehicle registered. Moreover, this paper introduces a mutual authentication protocol for V2V communication in the VANETs (MAP-V2VCV). MAP-V2VCV is designed vigilantly to prevent any such incorrectness and provide an enhanced and secure message exchange.

The structure of the paper is organized as follows. The system model of the proposed scheme is presented in Section 2. The related works that have been done in recent years are presented in Section 3. In Section 4, we review Vasudev et al.'s authentication scheme. Section 5 points out the weakness of existing security scheme vulnerabilities. We propose a new and improved scheme in Section 6, while Section 7 describes the security analysis of the new scheme. Section 8 presents the security and performance analysis. At last, in Section 9, we provide the conclusion of the paper.

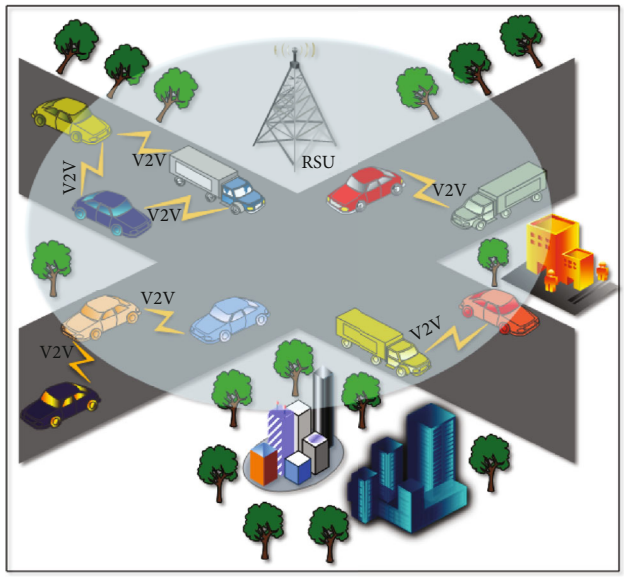


Figure 2: Typical structure of V2V communication.

2. System Models

This section presents the network and attack models and describes the working of both models on the contributed scheme.

2.1. Network Model. The network model is based on five entities, the vehicle/OBU, the RSU, registration authority (*RA*), trusted authority (*TA*), and vehicle server (*VS*); as shown in Figure 3, we describe each entity in detail.

The vehicle/OBU: an OBU installed inside each vehicle that receives messages from other vehicles/RSU/sensor verifies these messages and transmits them to other vehicles through the DSRC protocol. The secret information related to the message is kept secret in a tamper-proof device (TPD) inside the OBU. Every OBU in VANETs has a clock synchronized with the RSU communication range, also equipped with GPS and GUI interface that provide services such as the vehicle's location, the interaction of drivers to each other, and traffic information. Its computational power and storage capacity are more petite than RSU.

The RSU: the RSU is fixed on roadsides that acts as an intermediate entity between vehicles, *RA*, *TA*, and *VS*. The RSU is responsible for sharing traffic congestion, speed limits, and any threat information on the road. The RSU receives messages from the vehicle or RSUs, authenticates these messages, and then broadcasts these messages to other entities such as *VS*, via the secure communication channel.

Registration authority: in VANETs, *RA* is a trusted point to perform the registration procedure of every vehicle; this process is mandatory for each vehicle before moving to the communication phase. Generally, at the time of manufacture, the manufacturing company does this process; during the registration phase, vehicle users select required credentials, generate a key, and send some other information to *R A* for the registration. In the end, *RA*installs the OBU with the necessary parameters into the vehicle.

Trusted authority: *TA* is responsible for an authentication process that makes sure that the vehicle is trusted or authenticated and already registered with *RA*. *TA* first registers RSU and after that the vehicle and then generates anonymous identities to secure the privacy of the vehicle. *TA* also has the authority to identify the misbehaved vehicle's original identity and block it in the VANET network and inform other vehicles about that vehicle.

Vehicle server: the *VS* stores real-time information if any vehicle is requested to *VS* for the information that *VS* provides. When the vehicle wants that information, it first needs to register itself with the*TA*. If *TA* ensures the given vehicle is trusted, then credentials are sent to*VS*; after receiving this information from the trusted authority, the*VS*verifies that information again, and to ensure such information from*TA*,*VS*send some messages to*TA*; the purpose of this process is only for authenticity. After*TA*and*VS*, communication starts.

2.2. Attack Model. We choose the well-known Dolev-Yao threat model [17] for the security analysis of the proposed model. The Dolev-Yao threat model assumes and ensures a public channel for communication between vehicle to vehicle. A variety of proposals have been employed [18–21]; important points regarding the adopted attack model are given as follows:

(1) The attacker (*E*) properly controls the public channel. *E* is considered competent enough to listen, modify, delete, or jam any transmitted message between entities such as V_i, *TA*, and *VS*

(2) *E* can extract and analyze the parameter stored in a stolen smart card or capture the card's memory

(3) The vehicle and other entity are not trusted, which means any communicating authority or entity can try to impersonate on behalf of the other

(4) All parameters such as identities and the public keys of all the entities, including *TA*, are easily accessible to other systems and unauthorized users

(5) Private key (*PK*) of the participating entities, including *TA*, are secure and safe; no *E* is powerful enough to reveal the *PK* of any system entity

3. Related Work

The nature of VANETs is dynamic due to the Wireless Medium (WM) because of data transmission through WM to V2V, RSUs2V. Therefore, the chances of an attack are possible in the network every time. When attackers attack in the network during data transmission, stop, or delays, the original message can be tampered or discarded during this period [22]. A tampered or wrong message in VANETs becomes the reason for accidents or jamming of traffic. Xu et al. [22] proposed a security scheme to reduce the computation and storage cost and provide authentication to dense environments where vehicles receive multiple messages simultaneously, as well as to resist against the various attacks

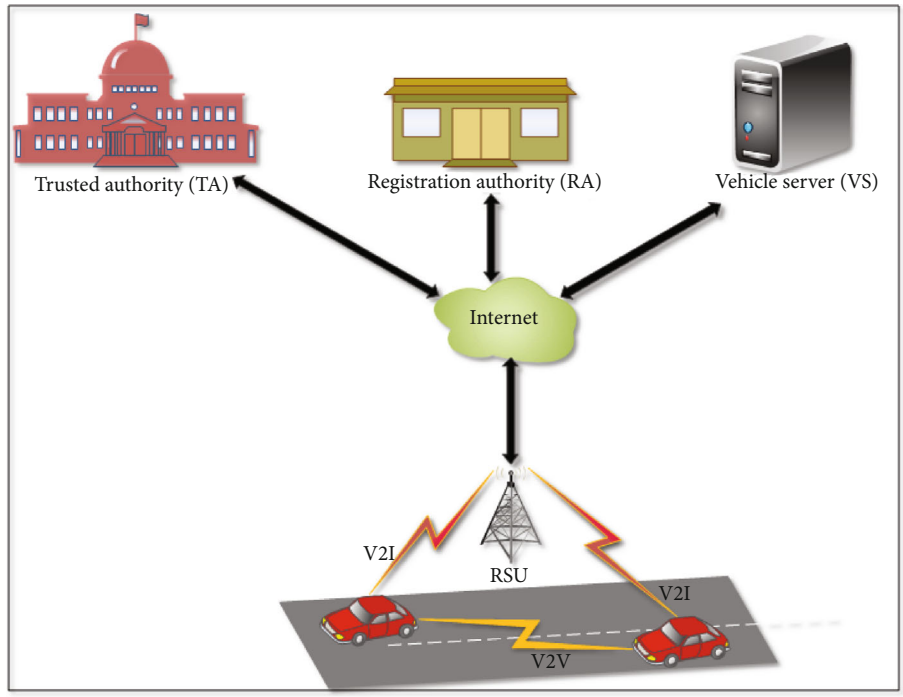


Figure 3: Network model of VANETs.

such as impersonation, modification, and replay attacks; however, the security analysis is not provided against remaining internal and external assaults [22].

VANET message transmissions from V2V or V2RSUs have many security threats. Vijayakumar et al. [23] proposed a dual authentication (DA) scheme that provides a high level of security to the vehicle inside the network and does not allow the entrance of any unauthorized vehicle in VANETS. It also provides a dual key management (DKM) security scheme for the user when joining or leaving which must be updated in the group. Nevertheless, the privacy of the vehicle's location is not provided in this scheme.

VANETs face various challenges due to dynamic topological conditions owing to speedily moving vehicles. Transmission of messages is in a limited area in VANETs, but security threats exist. Check of the authenticity of the message origin to the receiver in this environment is a big challenge. Chuang and Lee proposed a V2V communication security scheme called trust-extended authentication mechanism (TEAM) [24]. During analysis, Kumari et al. [25] find that TEAM is vulnerable to inside attacks, privacy breaches, impersonation attacks, and other challenges. Kumari et al. [25] proposed an enhanced trust extended authentication (ETEA) scheme for VANETs. ETEA proves that the analysis is better than TEAM and protects it from inside attacks. Also, computation load was reduced as compared to TEAM. Nevertheless, computational and storage cost is not discussed.

Various security protocols have been proposed for road safety applications in vehicle-to-everything (V2X) communication. These security protocols did not meet the lightweight (LW) preliminary requirements and fast processing integral parts of V2X; Hakeem et al. [26] proposed an LW authentication protocol for the privacy and protection of V2X. The protocol integrates with two hardware devices, biometrics devices and temper proof devices installed inside the vehicle. The proposed protocol is responsible for providing driver identity and private key security management. Decentralized certificateless authority generates a pseudoidentity of the driver, private key, secure privacy, and authentication V2V communication. They have also proposed an authentication signature protocol using the notation hash function. In [26], the scheme satisfies the security requirements and also reduces the message communication cost and computation time. Protection is provided against DoS, man-in-the-middle, modification, and replay assaults. However, storage cost was missing.

Chaudhry [27] states that the Internet of Vehicles (IoV) has become an integral part of our lives due to technological enhancement. Information is relevant to vehicles, including the position of the vehicle, information on the road, and the vehicle speed. This information is vital for selecting routes; without security, disseminating information between IoV entities is impossible. Many researchers proposed authentication schemes, but most security schemes did not perform as per claimed or communication cost or computation cost is very high. The authors in [27] proposed a secure message authentication protocol (SMEP-IoV); this protocol uses the symmetric lightweight hash function and encryption operation and provides a lightweight authentication process in 0.198 ms. SMEP-IoV resists various attacks such as stolen verifier, denial of service, replay, RSU impersonation, mutual authentication, and session key security. However, storage cost of the proposed is missing in their paper.

Recently, data transmission and protection of the user from various security attacks, the user authentication

protocol plays an integral role in ensuring security. Wang et al. [28] discovered two authentication security schemes that are not fully claimed and fail to provide secure communication, such as password guessing, session key disclosure, impersonation assaults, and user anonymity. In [28] eliminated the security threats from the existing scheme. The proposed improved authentication scheme based on the elliptic curve cryptosystem, performing analysis, proves that security scheme in [28] was better than existing schemes in terms of security, computation cost, and communication cost. However, storage cost was missing; also DoS and Sybil assaults were missing in the formal analysis.

In VANET, secure communication among neighbors, authentication, and trust establishment is an essential requirement of VANET. Many researchers proposed cryptography schemes that are claimed to overcome the inside assaults. However, they do not perform as per expectations. To reduce the inside attacks, researcher proposed a trust management scheme. Tangade and Manvi [29] proposed a neighbor trust management scheme (NTMS) for secure communication in VANET. NTMS employs an ID-based signature and HMAC [30]. NTMS provides various types of security during communication detection of malicious vehicles, the integrity of the message, and the level of trust among communication vehicles. However, formal security analysis was not provided, and also, computation cost and communication cost were missing.

Currently, the advancement of technologies has become a digital world, sharing information is not an issue. Hence, information must be secured; otherwise, the attacker may attack the information and use it for their own benefits and purposes. VANETs have become a more popular industry because vehicles share information among other vehicles speedily on the road. Limbasiya and Das [16] proposed a secure message exchange protocol using a public private key encryption and decryption approach in the computation of messages. In [16], the algorithm fulfills all security requirements on confidentiality, authenticity, and availability. This protocol also sends the current position of the vehicle to other vehicles within the network area. However, neither is formal security analysis provided nor are computation and communication costs discussed.

Vehicular sensor networks (VSNs) play a vital role in ITS and provide good driving experience, due to characteristics of VANETs facing different security threats. Researchers have proposed various authentication security schemes inappropriate to VSN applications due to high communication costs and high computation. Zhou et al. [30] improved the Chuang and Lee security scheme and eliminated the weakness of TEAM [24]. In [30], analysis was performed through the random oracle model and proved that this scheme was better than TEAM. Wu et al. [31] prove that Zhou et al. fail to provide identity guessing, impersonation assaults, and user anonymity and do not discuss DoS and Sybil attacks. Also, storage cost was missing.

For the last two decades, the mobile auto industry has been booming due to ITS, particularly the development of VANETs. It provides safety to the driver and passenger and a good experience. In VANETs, the mobility of vehicles is fast; due to this reason, privacy and security were a significant threat. Researchers have proposed an identity-based security scheme to overcome this issue but failed to provide the claimed solution. Wu et al. [31] improved Zhou et al.'s [30] scheme that failed to prove identity guessing and impersonation attack using elliptic curve encryption technology. Wu et al. [31] have proposed a new security scheme, V2V secure communication. However, computation cost and storage cost are missing. Table 1 provides the bird's eye view of the previous related works such as cryptography techniques, and their advantages and disadvantages/weaknesses are listed.

4. Summary of Vasudev et al.'s Authentication Scheme

This section provides a brief review of the scheme of Vasudev et al. [2]. The scheme is divided into four phases, and four entities are involved in these phases. First of all, we explain the entities and then the phases. The first entity vehicle V_i acts as a vehicle/user or node that wants to communicate with other vehicles or RSUs. Secondly, the registration authority (RA) is responsible for registering all vehicles; without RA registration, the vehicle cannot participate in VANET communication. The third entity is the trusted authority (TA), responsible for authentication between vehicle to vehicle and vehicle to a server. The fourth entity is the vehicle server (VS) that stores information about the network, such as vehicle position, weather condition, and congestion control. These four entities performed activity in four phases such as (1) registration, (2) login, (3) authentication, and (4) communication phases. For better understanding, the notations are given in Table 2.

4.1. Vehicle Registration. The vehicle driver/host (D_i) selects a vehicle ID and password (ID_i, PW_i) with random nonce Y_i. The V_i computes a cloaked ID and password such as $DVID_i = h(VID_i \| Y_i)$, $DPW_i = hh(PW_i \| Y_i)$ and sends to the registration authority through a secure channel. A secure channel means that the channel must ensure the integrity and confidentiality of information transferred via the channel. A secure channel is created using various cryptography security protocols such as SSH or TLS, or data or information is shared with the trusted user.

After receiving the data from a vehicle, RA calculates two parameters a_1 and b_1, which are unique for every vehicle or user. The value of a_1 is calculated such as $a_1 = h(DVID_i \| K_s)$, K_s is a private key that is shared by TA, and $b_1 = a_1 \oplus h(DVID_i \| DPW_i)$. The registration authority stores a_1 and b_1 parameters in SC and forwards to TA immediately. After receiving SC, it is sent to the driver/user via a secure channel.

After receiving the SC, $D_i$again computes the parameter C_i such as $C_i = VID_i \oplus PW_i \oplus Y_i$. Then, D_i stores the C_i and SC parameters for future communication.

4.2. Vasudev et al.'s Login, Authentication, and Communication. When a vehicle/user is registered successfully at RA, it must be logged in and authenticate itself with a trusted authority if D_i gets some information from the

Table 1: Summary of previous authentication schemes.

Paper	Cryptography technique	Advantage	Disadvantage
Xu et al. [22]	One-way hash function h(.) XOR (MD5)	Achieve lightweight certification; reduce storage and computation cost; less storage space; resist against impersonation, modification, and replay assaults	Does not resist reaming internal and external assaults such as DoS and man-in-the-middle, respectively
Vijayakumar et al. [23]	Hash code Finger print	Provide security to the vehicle and preventing unauthorized users, DKM for the user; unauthorized user does not enter the network; resist against replay, masquerading, Sybil, and message alteration assaults	Does not protect the vehicle location privacy
Kumari et al. [25]	One-way hash function XOR operation	Fast authentication process; low computational load; protect against impersonation, stolen verifier, modification, replay, and insider assaults	Computation cost and storage costs are missing
Hakeem et al. [26]	Hash chain key generation Elliptic curve	Enhances security level to protect anonymous identities; 20% ~ 85% communication overhead is compared to previous protocols; reduces the message communication cost and computation time; protects DoS, man-in-the-middle, modification, and replay assaults	Storage cost is missing
Chaudhry [27]	Symmetric lightweight hash functions and encryption	Provides sufficient security; provide SEMP-IoV best security requirement of the fast mobility vehicle IoV scenario; protects stolen verifier, denial of services, replay, RSU impersonation, mutual authentication, and session key security; authentication process takes 0.198 ms	Storage cost is missing
Wang et al. [28]	Elliptic curve cryptosystem	Protects session key exposure, forward scary assaults; low computation cost	Storage cost is missing; DoS and Sybil assaults were missing in formal analysis
Tangade and Manvi [29]	ID-based signatures HMAC techniques	Detection of malicious nodes; the integrity of the message is maintained; the proposed protocol fulfills the security requirements such as confidentiality, authenticity, and availability	Does not provide formal security analysis and lacks explanation of computation and communication costs
Limbasiya and Das [16]	One-way hash functions Bitwise XOR operation Low-cost cryptographic functions	Protects various assaults such as modification assault, man-in-the-middle assault, impersonation assault, concatenation, replay assault, stolen OBU, and password guessing assault	Formal security analysis is missing; computation cost and communication costs are missing
Zhou et al. [30]	Elliptic curve discrete logarithm problem	Resists internal assaults; low computation cost; secures the identity of driver and location privacy, and only authentication users get it	Storage cost is missing; does not discuss DoS and Sybil attacks
Wu et al. [31]	Hash functions XOR operation Elliptic curve encryption	Improves weaknesses of Zhou et al.'s security scheme such as guessing assaults and impersonation assaults	Computation and storages cost are missing

vehicle server. The purpose of authentication is to ensure D_i validity and protect impersonation assault from third-party vehicles or devices. The authentication process is also mandatory to verify that VS is not impersonated and that the vehicle gets accurate information. For normal execution of this phase, Figure 4 explains the process of login, authentication, and communication. The processes are described as follows.

4.2.1. Step VA1: $V_i \longrightarrow TA : \{MSG_1, X_1, T_u, SID\}$. Two parameters are required for login. The first one is the vehicle's identification number, and the second one is the password. It is not possible to login without these parameters. The vehicle computes the value of b_1, which is received from RA to cross-verify VID_i and PW_i. The vehicles (V_i) produce a nonce N_u and current timestamp T_u. Next, the vehicle computes three parameters such as MSG_1, Z_1, and X_1 for the communication with TA, $MSG_1 = h(a_1 \| T_u \| DPW_i \| N_u)$, $Z_1 = h(b_1 \| DPW_i)$, and $X_1 = N_u \oplus Z_1$, which are used for authentication of D_i. After that, the (MSG_1, X_1, T_u, SID) are sent to TA through an insecure channel.

4.2.2. Step VA2: $TA \longrightarrow VS : \{MSG_2, X_2, T_c, DCID\}$. When TA receives a message from the vehicle, the (MSG_1, X_1, T_u, SID) calculates the Z_1 and X_1 such as $Z_1^* = h(b_1 \| DPW_i)$ and $N_u^* = X_1 \oplus Z_1$. Also, it computes MSG_1

Table 2: Notation guide.

Notation symbols	Detail of notations
VS, D_i	Vehicle server, vehicle/host
VID_i	Identification number of the i^{th} vehicle
PW_i	The password of i^{th} vehicle
RA, TA	Registration authority, trusted authority
CID	The identification number of TA
SID_k	The identification number of $k^{th} VS$
Y_i	Random number (RN) generate vehicle
K_s	Secret key shared between VS and TA
N_{u_i}	Nonce produced by VID_i
N_{s_k}	Nonce produced by SID_k
N_s	Nonce produced by VS
Y_{ta}	Random number produced by RA
T_u, T_c, T_s	Timestamp of V_i, TA, VS
$EVID_i$	Pseudo identity of vehicle
E_{k_s}	Encryption using K_s
D_{k_s}	Decryption using K_s
$h(.)$	One-way cryptography hash function
$\oplus$	XOR operation
$\|\|$	Concatenation operation

$=^{?} h(a_1 \| T_u \| DPW_i \| N_u^*)$ to verify the same message which is received through an insecure channel from the vehicle. After calculation, the received information also ensures the integrity of the received message. The TA calculates $DCID$ such as $DCID = h(DVID_i \| CID \| SID)$. After that, it computes MSG_2 and X_2 as $MSG_2 = h(DCID \| K_s \| T_c \| N_u)$ and $X_2 = N_u \oplus h(K_s)$, respectively. T_c represents the timestamp that generated TAat the time when the message was computed. Finally, the $(MSG_2, X_2, T_c, DCID)$ is sent to the vehicle sever.

4.2.3. Step VA3: $VS \longrightarrow TA : \{MSG_3, X_3, T_s\}$. After receiving the information fromTA, $(MSG_2, X_2, T_c, DCID)$ calculates the information to verify whether it is correct or not, such as$N_u^* = X_2 \oplus h(K_s)$,$MSG_2 =^{?} h(DCID \| K_s \| T_c \| N_u^*)$. The VS produces random nonce N_s and timestamp T_s. The VS also generates secret key S_k, $S_k = h(DCID \| N_s \| N_u)$, that is shared with the vehicle for future communication. The VS also computes $X_3 = h(N_u \| N_s \| T_s \| K_s)$ and $MSG_3 = N_s \oplus N_u$; these parameters are $(MSG3, X_3, T_s)$ sent back to TA.

4.2.4. Step VA4: $TA \longrightarrow V_i : \{X_4, W\}$. At this phase, the trusted authority calculates the MSG_3 and X_3 as $N_s^* = MSG_3 \oplus N_u$, $X_3 =^{?} h(N_u \| N_s^* \| T_s \| K_s)$. After verification of information, TA computes $W = N_s \oplus DPW_i$, $X_4 = h(N_u \| N_s \| DPW_i)$ and sends (X_4, w) to the vehicle/user. The vehicle computes W and X_4 such as $N_s^* = W \oplus DWP_i$, $X_4 =^{?} h(N_u \| N_s^* \| DPW_i)$; after that, the secret key $S_k = h(DCID \| N_s \| N_u)$ is calculated.

4.2.5. Step VA5: Communication. The secret key S_k is used for V2V communication in the future. The vehicle server stores the vehicle/host identity and key after this communication. If vehicle A wants to communicate with other vehicles or devices, the message is encrypted with the help of a key and sent. After receiving a message from vehicle A, vehicle B sends it to VS to check the identity of vehicle A. The VS checks the legitimacy of vehicle B and vehicle A. If VS ensures that both are authorized vehicles, then the keys are sent to vehicle A and vehicle B through a secure channel. Then, vehicle B decrypts the request using this key that is received from VS.

5. Weaknesses of Vasudev et al.'s Scheme

This section highlights the weaknesses of Vasudev et al.'s scheme. The following subsections present the security scheme proposed in [2]. The scheme has some flaws and does not provide anonymity. The authenticated vehicle sends a request to TA for login approval through an insecure channel and also sends parameters $\{MSG_1, X_1, T_u, SID\}$. The TA does not recognize the specific identity of the vehicle where further communication is not possible between vehicles, TA and VS. To better understand Vasudev et al.'s scheme on that basis, the details of the scheme's incorrectness are mentioned below.

(1) V_i calculates following parameters after completing the login phase:

$$\begin{aligned} MSG_1 &= h(a_1 \| T_u \| DPW_i \| N_u), \\ Z_1 &= h(b_1 \| DPW_i), \\ X_1 &= N_u \oplus Z_1. \end{aligned} \tag{1}$$

V_i send $\{MSG_1, X_1, T_u, SID\}$

(2) After verifying the correctness of T_u, TA calculates the following:

$$Z_1^* = h(b_1 \| DPW_i), \tag{2}$$

$$N_u^* = X_1 \oplus Z_1^*, \tag{3}$$

$$MSG_1 \stackrel{?}{=} h(a_1 \| T_u \| DPW_i \| N_u^*). \tag{4}$$

(3) TA calculates Z_1 through Equation (2), where TA requires $h(b_1 \| DPW_i)$. TA receives the T_u and maintains the database that contains the records in the form of tuple$\{a_1, b_1\}$. Therefore, to extract $h(b_1 \| DPW_i)$, TA needs to know the $DVID_i$. Nevertheless, TA does not know about the identity of the vehicle. Moreover, to calculate N_u^* through Equation (3), it needs the value of Z_1^*; that is not possible because several vehicles send requests to TA at the same time where every vehicle has its own parameter values such as a_1, b_1, Z_i.

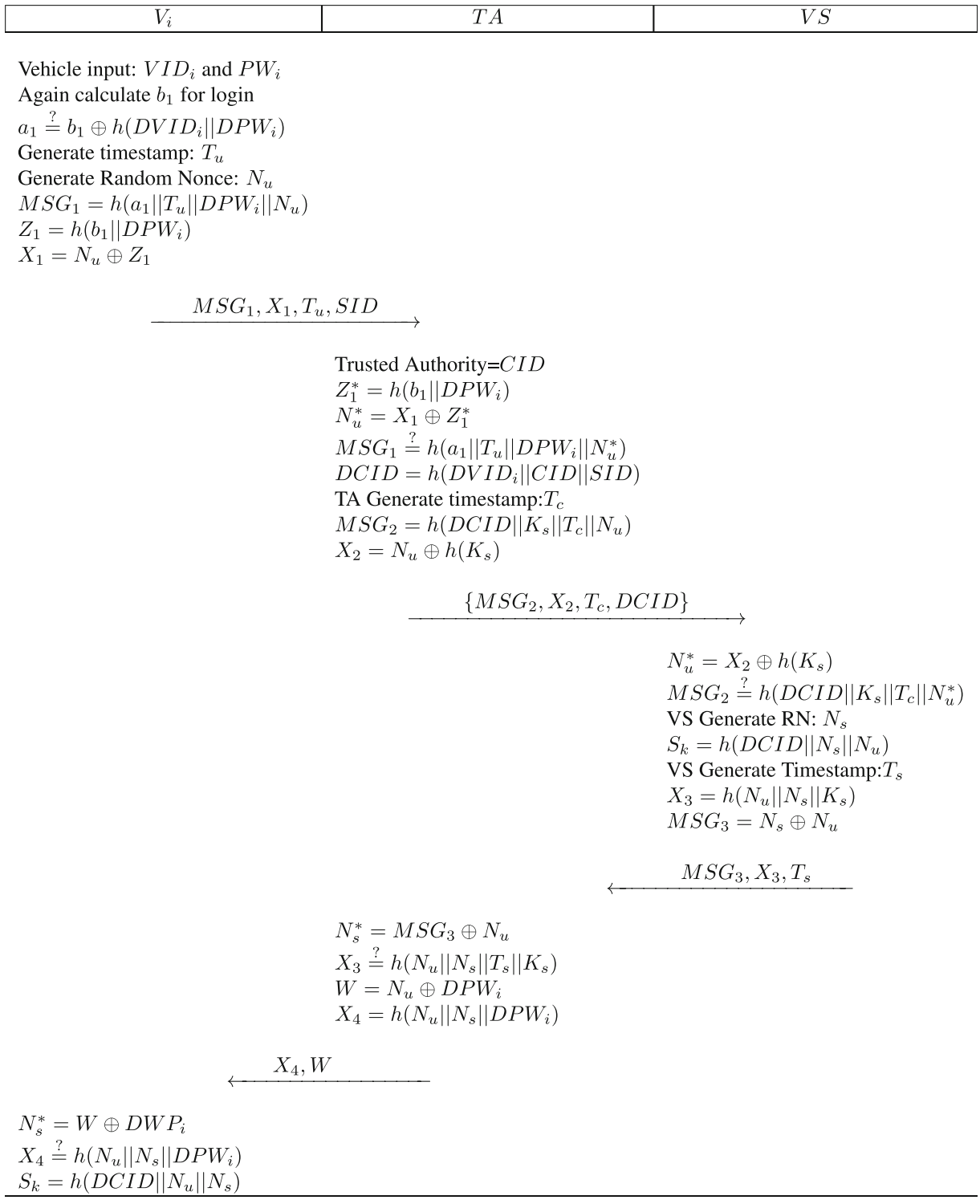


FIGURE 4: Vasudev et al.'s scheme.

Therefore, it is not possible for TA to identify the vehicle identity because TA does not know about Z_i. Similarly, in order to compute the originality of the message, Equation (4) needs the value of Z_1^*. So, TA does not calculate any parameters, and the authentication process may be suspended, irrespectively

(4) Similarly, the reply message from TA sends $\{X_4, W\}$ to the requesting vehicleV_i, without recognizing $V_i$as the information of the requesting vehicle is unknown for TA. Moreover, the message $\{MSG_2, X_2, T_c, DCID\}$ from TA to VS has not carried information about V_i; rather, TA itself is not able to recognize the

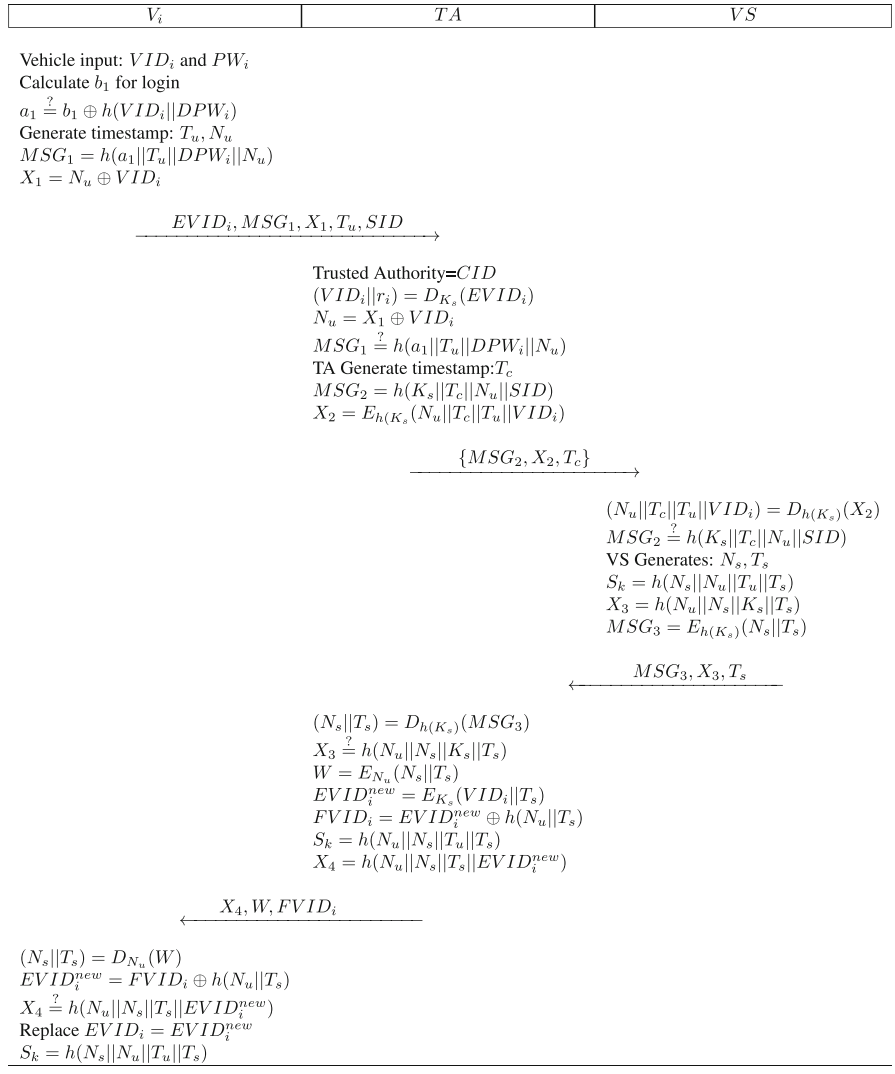


Figure 5: Proposed scheme.

identity of specific vehicles. Hence, TA does not send any message to V_i. Thus, this scheme is incorrect.

6. Proposed Scheme

In the following subsections, the main phases of the proposed scheme are explained:

6.1. Vehicle Registration. The driver of the vehicle/host (D_i) selects a vehicle ID and password (VID_i, PW_i) with random nonce Y_i. The V_i computes $DPW_i = h(PW_i \| Y_i)$ and sends $\{VID_i, DPW_i\}$ to the registration authority through a secure channel. After receiving data from the vehicle, RA generates $Y_{ta} \in Z_p^*$ and calculates the following parameters: a_1, b_1, and $EVID_i$, which are unique for every vehicle or user, where $a_1 = h(VID_i \| K_s)$, $b_1 = a_1 \oplus h(VID_i \| DPW_i)$, and $EVID_i = E_{K_s}(VID_i \| Y_{ta})$. The registration authority stores a_1, b_1, and $EVID_i$ in SC and immediately forwards to TA. After receiving SC, the information is sent to the driver/user via a secure channel.

When the SC information is received, D_i computes the parameter C_i as $C_i = VID_i \oplus PW_i \oplus Y_i$. Then, D_i stores C_i and SC parameters for future communication.

6.2. Proposed Login, Authentication, and Communication. When vehicles successfully register to the registration authority, they must be logged in and prove their authentication with a TA if the vehicle wants to obtain data from VS. The whole process is aimed at ensuring D_i validity and protecting against impersonation assaults from an intruder or third-party vehicle/device.

The authentication processes can also be done by the vehicle server to verify the impersonation of VS and send accurate information to the vehicle. Figure 5 describes the whole process of login, authentication, and communication. The explanation is given as follows.

6.2.1. Step PA1: $V_i \longrightarrow TA : \{EVID_i, MSG_1, X_1, T_u, SID\}$. Two parameters are required for the login process, i.e., the vehicle's identification number and the password. Login is not possible without these two parameters. After login, the

vehicle computes the value of b_1 which is received from RA to cross-verify VID_i and PW_i. The vehicle (V_i) produces a nonce N_u and current timestamp T_u. Then, the vehicle computes the other two parameters MSG_1 and X_1 for the communication with TA, $MSG_1 = h(a_1 \| T_u \| DPW_i \| N_u)$ and $X_1 = N_u \oplus VID_i$, respectively, which are used for authentication of D_i. After that, $(EVID_i, MSG_1, X_1, T_u, SID)$ sends the information to the TAthrough an insecure channel.

6.2.2. Step PA2: $TA \longrightarrow VS : \{MSG_2, X_2, T_c\}$. When TA receives a message from vehicle $(EVID_i, MSG_1, X_1, T_u, SID)$ to calculate the $EVID_i$, MSG_1, and X_1 such as $(VID_i \| r_i) = D_{K_s}(EVID_i)$, $MSG_1 = ^{?} h(a_1 \| T_u \| DPW_i \| N_u)$ also computes $N_u = X_1 \oplus VID_i$ to confirm the same message received on the channel from the vehicle. The above calculation ensures the integrity of the received message. The TA calculates MSG_2 and X_2 as $MSG_2 = h(K_s \| T_c \| N_u \| SID)$ and $X_2 = E_{h(K_s}(N_u \| T_c \| T_u \| VID_i)$, respectively. T_c represents the timestamp that is generated from T_A at the time when the message was computed. Finally, (MSG_2, X_2, T_c) is sent to the vehicle sever.

6.2.3. Step PA3: $VS \longrightarrow TA : \{MSG_3, X_3, T_s\}$. After receiving the information from TA in which (MSG_2, X_2, T_c), VS calculates the information to verify whether it is correct or not, such as $(N_u \| T_c \| T_u \| VID_i) = D_{h(K_s)}(X_2)$ and $MSG_2 = ^{?} h(K_s \| T_c \| N_u \| SID)$. The VS produces random nonce N_s and timestamp T_s. The VS also generates a secret key S_k, $S_k = h(N_s \| N_u \| T_u \| T_s)$, that is shared with the vehicle for future communication. The VS also computes $X_3 = h(N_u \| N_s \| K_s \| T_s)$ and $MSG_3 = E_{h(K_s)}(N_s \| T_s)$; these parameters $(MSG3, X_3, T_s)$ are sent back to TA.

6.2.4. Step PA4: $TA \longrightarrow V_i : \{X_4, W, FVID_i\}$. The trusted authority calculated MSG_3 and X_3 such as $(N_s \| T_s) = D_{h(K_s)}(MSG_3)$ and $X_3 = ^{?} h(N_u \| N_s \| K_s \| T_s)$. After verification of information, TA computes $W = E_{N_u}(N_s \| T_s)$, $EVID_i^{\text{new}} = E_{K_s}(VID_i \| T_s)$, $FVID_i = EVID_i^{\text{new}} \oplus h(N_u \| T_s)$, $S_k = h(N_u \| N_s \| T_u \| T_s)$, and $X_4 = h(N_u \| N_s \| T_s \| EVID_i^{\text{new}})$ to the vehicle/user.

The vehicle again computes W, X_4, and $FVID_i$ such as $(N_s \| T_s) = D_{N_u}(W)$, $EVID_i^{\text{new}} = FVID_i \oplus h(N_u \| T_s)$, and $X_4 = ^{?} h(N_u \| N_s \| T_s \| EVID_i^{\text{new}})$; after that, the $EVID_i$ is replaced with $EVID_i^{\text{new}}$ and the secret key $S_k = h(N_s \| N_u \| T_u \| T_s)$ is calculated.

6.2.5. Step PA5: Communication. The secret key S_k is used for V2V communication in the future. The vehicle server stores the vehicle/host identity and key after this communication. If vehicle A wants to communicate with other vehicles or devices, the message is encrypted with the help of a key and sent. After receiving a message from vehicle A, vehicle B sends it to VS to check the identity of vehicle A. The VS checks the legitimacy of vehicle B and vehicle A. If VS ensures that both are authorized vehicles, then a key is sent to vehicle A and vehicle B through a secure channel. Then, the vehicle B decrypts the request using this key which is received from VS.

7. Security Analysis

This section performs formal security analysis through the BAN-logic method and discusses how the proposed scheme protects it from various security attacks.

7.1. Formal Security Analysis through BAN-Logic. In this subsection, the detailed security analysis is provided of the proposed scheme using BAN-logic [35]. Firstly, some basic notations are presented that are used to analyze the proposed scheme. Here, the L and M are used as participators, and X is used as a formula.

(i) $(\#X)$: X is fresh

(ii) $L \mid \equiv X$: L believes the trustworthiness of X

(iii) $L \mid \sim X$: L once said X

(iv) $L \triangleleft X$: L sees X

(v) $L \mid X$: L has jurisdiction over X

(vi) $L \leftrightarrow^{K} M$: between L and M, K is shared key

(vii) $\{X, Y\}_k$: X and Y are encrypted with the help of K

(viii) $(X)_Y$:X combined with Y

The following BAN-logic rules are used to verify the security features:

(i) Rule 1: message meaning rule

If L sees a statement X encrypted with key K and L believes K is a shared secret key between L and M, then L believes M once said X.

$$\frac{L \mid \equiv \overset{K}{\leftrightarrow} M, L \triangleleft \{X\}_K}{L \mid \equiv M \mid \sim X}. \tag{5}$$

(ii) Rule 2: nonce verification rule

If L believes that the statement X is updated and L also believes that M once said X, then L believes M is the statement of X.

$$\frac{L \mid \equiv \#X, L \mid \equiv M \mid \sim X}{L \mid \equiv M \mid \equiv X}. \tag{6}$$

(iii) Rule 3: jurisdiction rule

If L believes M has jurisdiction over the statement X and L believes M is the statement X, then L believes the statement of X.

$$\frac{L \mid \equiv M \Rightarrow X, L \mid \equiv M \mid \equiv X}{L \mid \equiv X}. \tag{7}$$

(iv) Rule 4: freshness rule

If L believes that the part of the statement X is updated, then L believes that the statement $\{X, Y\}$ is updated.

$$\frac{L|\equiv\#(X)}{L|\equiv\#(X,Y)}. \tag{8}$$

(v) Rule 5: belief rule

If L believes that M believes in the statement of $\{X, Y\}$, then L believes that M believes in the part of statement X.

$$\frac{L|\equiv M|\equiv\{X,Y\}}{L|\equiv M|\equiv X}. \tag{9}$$

The main goals of the proposed security scheme are proven under the BAN-logic analytic procedure:

(i) $G1: V_i \mid \equiv V_i \leftrightarrow^{S_K} TA$

(ii) $G2: V_i \mid \equiv TA \mid \equiv V_i \leftrightarrow^{S_K} TA$

(iii) $G3: TA \mid \equiv V_i \leftrightarrow^{S_K} TA$

(iv) $G4: TA \mid \equiv V_i \mid \equiv V_i \leftrightarrow^{S_K} TA$

(v) $G5: VS \mid \equiv VS \leftrightarrow^{S_K} TA$

(vi) $G6: VS|\equiv TA| \equiv VS \leftrightarrow^{S_K} TA$

(vii) $G7: TA \mid \equiv VS \leftrightarrow^{S_K} TA$

(viii) $G8: TA|\equiv VS| \equiv VS \leftrightarrow^{S_K} TA$

In the proposed scheme, when a message is sent over an unsafe communication channel, the details of the message are mentioned below:

(i) $M1: V_i \longrightarrow TA: EVID_i, MSG_1X_1, T_u, SID : \{N_u, EVID_i\}_{VID_i}$

(ii) $M2: TA \longrightarrow VS: MSG_2, X_2, T_c : \{h(K_s\|T_c\|N_u\|SID), N_u\}_{K_s}$

(iii) $M3: VS \longrightarrow TA: MSG_3, X_3, T_s : \{N_s\}_{k_s}$

(iv) $M4: TA \longrightarrow V_i: X_4, W, FVID_i : \{N_u, N_s\}_{VID_i}$

Furthermore, the following assumptions are given as proof of the proposed security scheme:

(i) $A1: TA \mid \equiv\#(N_u)$

(ii) $A2: TA \mid \equiv\#(N_s)$

(iii) $A3: VS \mid \equiv\#h(K_s\|T_c\|N_u\|SID)$

(iv) $A4: V_i \mid \equiv\#(N_u)$

(v) $A5: V_i \mid \equiv TA(V_i \leftrightarrow^{S_k} TA)$

(vi) $A6: TA \mid \equiv V_i(V_i \leftrightarrow^{S_k} TA)$

(vii) $A7: VS \mid \equiv TA(VS \leftrightarrow^{S_k} TA)$

(viii) $A8: TA \mid \equiv VS \mid (VS \leftrightarrow^{S_k} TA)$

(ix) $A9: V_i \mid \equiv V_i \leftrightarrow^{VID_i} TA$

(x) $A10: TA \mid \equiv V_i \leftrightarrow^{VID_i} TA$

(xi) $A11: VS \mid \equiv VS \leftrightarrow^{S_k} TA$

(xii) $A12: TA \mid \equiv VS \leftrightarrow^{S_k} TA$

(xiii) $A13: VS \mid \equiv TA \mid \sim h(K_s\|T_c\|N_u\|SID), N_u$

7.1.1. BAN-Logic Proof. The BAN-logic is conducted to analyze the proposed scheme:

Step 1. S_1 can be acquired from M_1.

$$S_1: TA \triangleleft \left\{N_u, EVID_{iVID_i}\right\}. \tag{10}$$

Step 2. S_2 can be persuaded by applying rule 1, using S_1 and A_{10}.

$$S_2: TA|\equiv V_i| \sim (N_u, EVID_i). \tag{11}$$

Step 3. S_3 can be persuaded by applying rule 4, using S_2 and A_1.

$$S_3: TA| \equiv \#(N_u, EVID_i). \tag{12}$$

Step 4. S_4 can be persuaded by applying rule 2, using S_2 and S_3.

$$S_4: TA|\equiv V_i| \equiv (N_u, EVID_i). \tag{13}$$

Step 5. S_5 can be persuaded by S_4 and applying rule 5

$$S_5: TA|\equiv V_i| \equiv (N_u). \tag{14}$$

Step 6. S_6 obtained from M_2.

$$S_6: VS \triangleleft \left\{h(K_s||T_c||N_u||SID)_{K_s}\right\}. \tag{15}$$

Step 7. S_7 can be persuaded by applying rule 1, using S_6 and A_{13}.

$$S_7: VS|\equiv TA| \sim h(K_s||T_c||N_u||SID). \tag{16}$$

Step 8. S_8 can be persuaded by applying rule 5, using S_7 and A_3.

$$S_8: VS| \equiv \#h(K_s||T_c||N_u||SID), N_u. \tag{17}$$

Step 9. S_9 can be persuaded by applying rule 2, using S_7 and S_8.

$$S_9: VS|\equiv TA| \equiv h(K_s||T_c||N_u||SID), N_u. \tag{18}$$

Step 10. S_{10} obtained from M_3.

$$S_1 0 : TA \triangleleft \{N_U\}_{S_k}. \tag{19}$$

Step 11. $S_1 1$ can be persuaded by applying rule 1, using A_5 and S_8.

$$S_{11} : TA| \equiv VS| \sim (N_s). \tag{20}$$

Step 12. S_{12} can be persuaded by applying rule 2, using S_9 and S_{10}.

$$S_{12} : TA| \equiv VS| \equiv (N_s). \tag{21}$$

Step 13. S_{13} can be persuaded by S_9 and S_{12}, VS. TA can be calculated by session key $S_k = h(N_s \| N_u \| T_u \| T_s)$.

$$\begin{aligned} S_{13} : TA| \equiv VS| &\equiv \left(VS \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G8), \\ S_{14} : VS| \equiv TA| &\equiv \left(VS \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G6). \end{aligned} \tag{22}$$

Step 14. S_{15} and S_{16} can be persuaded by applying rule 3, using S_{13} and A_8 and S_{14} and A_7.

$$\begin{aligned} S_{15} : TA| &\equiv \left(VS \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G7), \\ S_{16} : VS| &\equiv \left(VS \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G5). \end{aligned} \tag{23}$$

Step 15. S_{17} obtained from M_4.

$$S_{17} : V_i \triangleleft \{N_s, N_U\}_{VID_i}. \tag{24}$$

Step 16. S_{18} can be persuaded by applying rule 1, using A_9 and S_{17}.

$$S_{18} : V_i| \equiv TA| \sim (N_u, N_s). \tag{25}$$

Step 17. S_{19} can be persuaded by applying rule 5, using S_{18} and A_4.

$$S_{19} : V_i| \equiv \#(N_u, N_s). \tag{26}$$

Step 18. S_{20} can be persuaded by applying rule 2, using S_{16} and S_{17}.

$$S_{20} : V_i| \equiv TA| \equiv (N_u, N_s). \tag{27}$$

Step 19. S_{21} and S_{22} can be persuaded by S_5, S_{18}, and V_i. TA can be calculated by session key $S_k = h(N_s \| N_u \| T_u \| T_s)$.

$$\begin{aligned} S_{21} : V_i| \equiv TA| &\equiv \left(V_i \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G2), \\ S_{22} : TA| \equiv V_i| &\equiv \left(V_i \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G4). \end{aligned} \tag{28}$$

Step 20. S_{23} and S_{24} can be persuaded by applying rule 3, using S_{21}, A_5, S_{22}, and A_6.

$$\begin{aligned} S_{23} : V_i| &\equiv \left(V_i \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G1), \\ S_{24} : TA| &\equiv \left(V_i \overset{S_k}{\leftrightarrow} TA \right) \longrightarrow (G3). \end{aligned} \tag{29}$$

7.2. Security Discussion. This subsection explains how the proposed security scheme can resist against various security attacks; details are given as follows.

7.2.1. Correctness. The proposed scheme completes the authentication process correctly between V_i and VS with the help of TA. The proposed scheme is designed and provides intuition to the common mistakes. It also provides supports for correctness issues in the future work. In the vehicle registration phase of the proposed scheme, a random and dynamic identity $EVID_i$ is generated by the RA and is stored in the memory of vehicle SC. This identity is used in the process of the login and authentication request on both SC in possession of the vehicle and TA. Furthermore, every vehicle has a different random number and unique identity. Thus, TA easily identifies the vehicle identity at the time of authentication when the vehicle requests TA for login. Therefore, the proposed scheme eliminates the correctness issues.

7.2.2. Impersonation Attack. Here, the defense of the proposed security scheme against the vehicle such as TA, and the VS impersonation assault are described.

(1) *Vehicle impersonation attack*: if E tries to launch the impersonation assault on the behalf of the vehicle, it needs to construct an original login request message M_1' such as $M_1' = MSG_1', EVID_i', T_u', X_1', SID'$, where $MSG_1' = h(a_1 \| T_u \| DPW_i \| N_u)$, $X_1' = N_u \oplus VID_i$, $EVID_i' = E_{K_s}(VID_i \| Y_{ta})$ with updated nonce N_u' and timestamp T_u'. However, it is seen at the start that it is very difficult to recover T_u, VID_i, and DWP_i for constructing $M' = MSG_1', EVID_i', T_u', X_1', SID'$. Thus, the proposed protocol provides security against the vehicle impersonation assault.

(2) *TA impersonation attack*: similarly, an E tries to instigate a forgery toward VS on the behalf of TA. For this purpose, E needs to construct the M_2' such as $M_2' = MSG_2, X_2$ with updated nonce N_u' and timestamp T_c' and also requires some confidential parameters such as T_c, N_u, T_u, and K_s secret keys. It is a computationally hard problem to compute these parameters from previously intercepted message MSG_2 and X_2. Thus, the proposed protocol also provides security against TA impersonation assault.

(3) *VS impersonation attack*: in the case of VS impersonation assault, when E launches an assault on VS toward TA, it also needs to design the message M_3'

with an updated nonce N_u' and new timestamp T_c', where $M_3' = MSG_3', X_3', T_s'$, $MSG_3' = E_h(N_s \| T_s)$, and $X_3' = h(N_u' \| N_s' \| K_s' \| T_s')$. However, the attacker may not be able to construct the valid message parameters in M_3', until granted the valid secret key K_s. Thus, E cannot impersonate the VS, and the proposed scheme provides security to VS impersonation assault.

7.2.3. Stolen SC Attack. Suppose if E steals the smart card and obtains all confidential credentials $\{a_1, b_1, EVID_i\}$ using a power analysis attack (PWA) [33]. E tries to compute MSG_1, X_1, and $EVID_i$. However, E requires the knowledge of $DPW_i = h(PW_i \| Y_i)$, whereas the E does not hold a hash function, which is not convertible. Thus, E cannot recover the password, and the stolen smart card cannot be accessible.

7.2.4. Session Key Security. The trusted authority and vehicle server both verify the value of nonce N_s, T_u, T_s, and N_u that are used to compute the secret key value $S_k = h(N_s \| N_u \| T_u \| T_s)$. This process ensures the originality of the session key. Thus, session key security is ensured.

7.2.5. Anonymity and Untraceability. In the phase of mutual authentication, the proposed security scheme utilizes random nonce N_u, r_i, and T_u, as well as timestamp T_u, T_c, and T_s in communication messages MSG_1–MSG_3. In the communication scenario, E may not differentiate among the messages of the different sessions, which publicly render the proposed scheme untraceable. At the same time, the E may not identify the vehicle identity, since the messages employ pseudoidentities, i.e., $EVID_i$, $EVID_i^{\text{new}}$, and $FVID_i$ and again replace $EVID_i^{\text{new}}$ into $EVID_i$ in the messages instead of original identities, that are enclosed under the rigidity of a one-way hash function-bearing collision resistance characteristic. Thus, the proposed scheme maintains the untraceability and anonymity characteristics.

7.2.6. Man-in-the-Middle Attack. If E want to launch the man-in-the-middle assault, it is required to build the message M' i.e., $M_1' = MSG_1, EVID_i, T_u, X_1, SID$ where $MSG_1 = h(a_1 \| T_u \| DPW_i \| N_u)$, $X_1 = N_u \oplus VID_i$, and $EVID_i = E_{K_s}(VID_i \| Y_{ta})$. However, to meet the goal, the attacker needs to build those message parameters with updated nonce N_u and timestamp T_u, which are not possible until E has access to K_s, $EVID_i$, and DPW_i. Likewise, E is not able to rebuild other messages such as MSG_1–MSG_3 in the protocol with updated nonce and timestamp without having access to important parameters in possession with those participating entities. Therefore, the proposed scheme provides security against the man-in-the-middle assault.

7.2.7. Off-Line Password Guessing Attack. It is proven that the proposed scheme is infeasible for E to get the identity of D_i, even after extracting the parameters. Suppose if E has access to a smart card, which contains $\{EVID_i, a_1, b_1, h(.), Y_i\}$, the parameters can be obtained by using the PWA [33]. However, assaults cannot compute the K_s and, ultimately, PW_i from DWP_i. The E has only one way to acquire the PW_i from MSG_1 without breaching the noninvertible characteristics of the cryptography hash function.

7.2.8. Replay Attack. In the proposed security scheme, various entities such as V_i, TA, and VS exchange the messages from MSG_1 to MSG_3 and utilize the timestamp T_u, T_c, and T_s to encounter the possible replay assault. At the same time, mutual authentication is required for communication. The messages need to be replied to in a short period of timestamp T to abolish the possibility of E manipulating the messages and initiating replay assault. Without updating the parameters MSG_1, X_1, $EVID_i$, MSG_2, X_2, MSG_3, X_3, W, X_4, and $FVID_i$, the updated timestamp cannot be utilized. At the same time, the parameters need to be updated with the new timestamp, whereas the E requires access to VID_i identity and password, and other shared parameters between V_i, TA, and VS. Thus, the replay assault does not happen in the proposed scheme.

7.2.9. Denial of Service (DoS) Attack. The proposed scheme provides security against DoS assault as the SC in the start authenticate V_i such as $EVID_i = H(VID_i \| Y_{ta})$. This condition will only be legal if V_i enters the correct identity VID_i and password DPW_i; after the insertion of the valid identity and password, the parameters are computed in SC $(VID_i \| Y_{ta}) = E_{ks}(EVID_i)$. The authentication of V_i is done locally at the vehicle's side. After that, a request is sent to TA for authentication. The same process is followed in the password and update phases to protect the incorrect modification of these parameters. Thus, the scheme prevents DoS assault.

8. Security and Performance Analysis

Under this section, the security features, computation cost, and communication cost of the proposed scheme with relation to other schemes are described [2, 25, 30, 34].

8.1. Security Features. Table 3 provides a detailed overview of security comparisons of our proposed scheme in relation to other schemes [2, 25, 30, 34]. In Table 3, the proposed scheme acquires the required attributes associated with pragmatic security under the DY model described in Section 2.2. At the same time, Vasudev et al.'s scheme [2] is incorrect and cannot fulfill the authentication as evinced in Section 5. In Vasudev et al.'s scheme [2], TA cannot identify the vehicle identity if more than one vehicle communicates to TA. This scheme also only works when one registered vehicle is in the system. Vasudev et al.'s scheme [2] is insecure against the man-in-the-middle attack. Additionally, the scheme of Mohit et al. [34] also failed to provide security against man-in-the-middle and DoS attacks. Kumari et al.'s scheme [25] is also insecure against the man-in-the-middle, offline password guessing, and DoS attacks. Zhou et al.'s scheme [30] failed to provide security against the impersonation attack such as (V_i, TA, VS) and is also insecure against the man-in-the-middle, offline password guessing, replay, and DoS attacks.

Table 3: Security analysis.

Schemes	Ours	[2]	[34]	[25]	[30]
Correctness	✓	✗	✓	✓	✓
Vehicle impersonation attack	✓	✓	✓	✓	✗
Trusted authority impersonation attack	✓	✓	✓	✓	✗
Vehicle server impersonation attack	✓	✓	✓	✓	✗
Stolen SC attack	✓	✓	✓	✓	✓
Anonymity attack	✓	✓	✓	✓	✓
Untraceability attack	✓	✓	✓	✓	✓
Man-in-the-middle attack	✓	✗	✗	✗	✗
Off-line password guessing attack	✓	✓	✓	✗	✗
Replay attack	✓	✓	✓	✓	✗
Mutual authentication	✓	✓	✓	✓	✓
DoS attack	✓	✓	✗	✗	✗

Note: ✓: provides or resists; ✗: does not provide or does not resist.

Table 4: Performance comparisons.

Scheme	Computation cost	RT (ms)	ME	BE	SC
Ours	$14T_h + 14T_{be}$	0.266	4	1824	512
Vasudev et al. [2]	$16T_h$	0.096	4	1696	384
Mohit et al. [34]	$19T_h$	0.114	4	1760	864
Kumari et al. [25]	$12T_h$	0.072	3	1056	608
Zhou et al. [30]	$16T_h$	0.096	3	1604	544

Note: RT: running time; ME: no. of message exchanges; BE: bit exchange: SC: storage cost in bits.

8.2. Computation Cost. We adopted the running times computed in [35] over a Pi-3:B+64-bit-Cortes A5-3:ARM-v8, SoC:1.4 GHz processor, and 1 GB LPDDR2-SDRAM. We denote T_{be}, T_h, and $T_\oplus$ as the symbols representing symmetric block encryption, hash, and exclusive or operations, respectively. Implying the experiment conducted in [35], the T_{be} furnishes in 0.013 ms, the running time of T_h is 0.006, while $T_\oplus$ takes negligible time to complete its execution, and therefore, $T_\oplus$ is being ignored in the comparisons. We used AES-128-bit block for encryption, and each identity and random numbers are of 64-bit size. Therefore, an encryption block can convert two parameters (identity/random number) into cipher text. The proposed scheme executes $\{14T_h + 14T_{be}\}$ operations with a running time of 0.266 ms. Table 4 shows the computation cost comparisons of the proposed and related schemes [2, 25, 30, 34]. The proposed scheme has a slight extra computation cost as compared with the other schemes [2, 25, 30, 34].

8.3. Communication Cost. To calculate the fair and pragmatic communication cost comparisons of the proposed scheme with related other schemes, we adopted 160-bit SHA-1, timestamps, random numbers, and identities which are considered to be 64 bits of length. We simulated the AES block cipher with 128-bit output. Thus, in the proposed scheme, communication cost is computed following the previously mentioned parameter values. The authentication cycle of the proposed scheme finishes through the exchange of four messages. In message 1, $\{EVID_i, MSG_1, X_1, T_u, SID\} = \{128 + 160 + 160 + 64 + 64\} = 576$ bits are sent from V_i to TA. In message 2, $\{MSG_2, X_2, T_c\} = \{160 + 160 + 64\} = 384$ bits sent from TA to VS.

In message 3, $\{MSG_3, X_3, T_s\} = \{160 + 160 + 64\} = 384$ bits are directed from VS to TA, and the transmission of message 4 $\{X_4, W, FVID_i\}$ requires transmission of $\{160 + 160 + 160\} = 480$ bits from TA to V_i. Thus, total communication cost of the authentication phase of the proposed scheme is $\{576 + 384 + 384 + 480\} = 1824$ bits. Referring to Table 4, the communication cost of the proposed scheme is higher than other schemes [2, 25, 30, 34]; however, other scheme do not provide one or more security features.

8.4. Storage Cost. To calculate the storage cost of the proposed scheme, we took into account the parameters stored in the memory of the vehicle. The three parameters stored are the hash output, random numbers, and block-based symmetric encryption. Due to usage of SHA-1, the hash output value is 160 bits, the size of the random nonce is 64 bits, and the size of AES-128 encryption is 128 bits. Thus, the storage cost of the proposed scheme is $\{a_1 + b_1 + EVID_i + C_i\} = \{160 + 160 + 128 + 64\} = 512$ bits. Table 4 shows the storage cost of the proposed scheme and other schemes [2, 25, 30, 34]. The storage cost of the proposed scheme is lower than the schemes in [25, 30, 34]; however, the storage cost of the proposed scheme is a bit higher than the scheme in [2], and we proved that Vasudev et al.'s scheme design is incorrect and cannot work in practical environments.

9. Conclusion

Primarily, this study reviewed some of the recent V2V authentication schemes. The paper is aimed at openly discussing the faulty design of the V2V mutual authentication scheme of Vasudev et al. We proved that the design of the scheme of Vasudev et al. is incorrect, and it cannot work practically. Moreover, we introduced an improvement over the scheme of Vasudev et al. The robustness of the proposed

scheme is formally proven through BAN-logic. The proposed security scheme provides mutual authentication between a vehicle and the vehicle server through intermediation of a trusted authority. We also provided security discussion and proved that the proposed scheme provides resistance against various security assaults and provides essential security features. The execution time of a cycle of authentication of the proposed scheme is slightly over the execution time of Vasudev et al.'s scheme. The comparisons with some of the related and recently proposed schemes also show that the proposed scheme provides known security features and resistance to known attacks, while the compared schemes lack one or more security features.

Data Availability

The data used to support this study are already inside the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Conceptualization was handled by J.M. and Y.Y.; investigation was handled by J.M., Y.Y., and A.K.Y; original draft preparation was handled by J.M., M.A.B., and H.X.; review and editing were handled by Y.Y., J.M., S.A.K., and M.A.B.; supervision was handled by Z.D.; and funding acquisition was handled by Z.D. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

This work was supported by funds for the Key Research and Development Plan Project of Shaanxi Province, China, under grant nos. 2019ZDLGY17-08, 2019ZDLGY03-09-01, and 2020ZDLGY09-02; Funds for Science and Technology Innovation Leading Talent of Shaanxi Province, China, under grant no. TZ0336; and Key Research Item for the Industry of Shaanxi Province under grant no. 2018GY-136.

References

[1] T. Limbasiya and D. Das, "Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication," *IEEE Systems Journal*, vol. 14, no. 1, pp. 520–529, 2019.

[2] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A lightweight mutual authentication protocol for v2v communication in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6709–6717, 2020.

[3] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, "An efficient and provably secure ecc-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1278–1291, 2021.

[4] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: a survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 1, pp. 383–398, 2019.

[5] Y. Zhang, G. Zhang, R. Fierro, and Y. Yang, "Force-driven traffic simulation for a future connected autonomous vehicle-enabled smart transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2221–2233, 2018.

[6] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: challenges and countermeasures," *Security and Communication Networks*, vol. 2021, Article ID 9997771, 20 pages, 2021.

[7] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020.

[8] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, "A comprehensive review of authentication schemes in vehicular ad-hoc network," *IEEE Access*, vol. 9, pp. 31309–31321, 2021.

[9] O. S. al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020.

[10] D. Kim, Y. Velasco, W. Wang, R. N. Uma, R. Hussain, and S. Lee, "A new comprehensive RSU installation strategy for cost-efficient VANET deployment," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4200–4211, 2017.

[11] Z. Gao, D. Chen, S. Cai, and H.-C. Wu, "Optimal and greedy algorithms for the one-dimensional RSU deployment problem with new model," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7643–7657, 2018.

[12] H. Tan and I. Chung, "Secure authentication and key management with blockchain in VANETs," *IEEE Access*, vol. 8, pp. 2482–2498, 2020.

[13] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[14] C.-Y. Chang, H.-C. Yen, and D.-J. Deng, "V2V QoS guaranteed channel access in IEEE 802.11p VANETs," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 5–17, 2015.

[15] F. Arena, G. Pau, and A. Severino, "A review on IEEE 802.11p for intelligent transportation systems," *Journal of Sensor and Actuator Networks*, vol. 9, no. 2, p. 22, 2020.

[16] T. Limbasiya and D. Das, "Secure message transmission algorithm for vehicle to vehicle (V2V) communication," in *2016 IEEE Region 10 Conference (TENCON)*, pp. 2507–2512, Singapore, November 2016.

[17] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[18] K. Mahmood, X. Li, S. A. Chaudhry et al., "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Generation Computer Systems*, vol. 88, pp. 491–500, 2018.

[19] A. Irshad, S. A. Chaudhry, O. A. Alomari, K. Yahya, and N. Kumar, "A novel pairing-free lightweight authentication protocol for mobile cloud computing framework," *IEEE Systems Journal*, vol. 15, no. 3, pp. 3664–3672, 2020.

[20] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in internet of vehicles with

blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11815–11829, 2020.

[21] M. N. Aman, M. H. Basheer, S. Dash et al., "Hatt: hybrid remote attestation for the internet of things with high availability," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7220–7233, 2020.

[22] H. Xu, M. Zeng, W. Hu, and J. Wang, "Authentication-based vehicle-to-vehicle secure communication for VANETs," *Mobile Information Systems*, vol. 2019, Article ID 7016460, 9 pages, 2019.

[23] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2016.

[24] M.-C. Chuang and J.-F. Lee, "TEAM: trust-extended authentication mechanism for vehicular ad hoc networks," in *2011 International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 1758–1761, Xianning, China, April 2011.

[25] S. Kumari, M. Karuppiah, X. Li, F. Wu, A. K. Das, and V. Odelu, "An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks," *Security and Communication Networks*, vol. 9, no. 17, 4271 pages, 2016.

[26] S. A. Abdel Hakeem, M. A. Abd el-Gawad, and H. W. Kim, "A decentralized lightweight authentication and privacy protocol for vehicular networks," *IEEE Access*, vol. 7, pp. 119689–119705, 2019.

[27] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for internet of vehicles," *Security and Communication Networks*, vol. 2021, Article ID 5554318, 9 pages, 2021.

[28] F. Wang, G. Xu, and L. Gu, "A secure and efficient ECC-based anonymous authentication protocol," *Security and Communication Networks*, vol. 2019, Article ID 4656281, 13 pages, 2019.

[29] S. Tangade and S. S. Manvi, "Trust management scheme in VANET: neighbour communication based approach," in *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, pp. 741–744, Bengaluru, India, August 2017.

[30] Y. Zhou, X. Zhao, Y. Jiang, F. Shang, S. Deng, and X. Wang, "An enhanced privacy-preserving authentication scheme for vehicle sensor networks," *Sensors*, vol. 17, no. 12, p. 2854, 2017.

[31] L. Wu, Q. Sun, X. Wang et al., "An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network," *IEEE Access*, vol. 7, pp. 55050–55063, 2019.

[32] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[33] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[34] P. Mohit, R. Amin, and G. P. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Vehicular Communications*, vol. 9, pp. 64–71, 2017.

[35] S. A. Chaudhry, J. Nebhen, K. Yahya, and F. al-Turjman, "A privacy enhanced authentication scheme for securing smart grid infrastructure," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 4083199, 14 pages
https://doi.org/10.1155/2021/4083199

Research Article

Provably Secure Client-Server Key Management Scheme in 5G Networks

Lei Yang,[1] **Yeh-Cheng Chen**,[2] **and Tsu-Yang Wu**[1]

[1]*College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China*
[2]*Department of Computer Science, University of California, Davis, CA, USA*

Correspondence should be addressed to Tsu-Yang Wu; wutsuyang@gmail.com

Received 25 August 2021; Revised 5 October 2021; Accepted 7 October 2021; Published 22 October 2021

Academic Editor: Muhammad Asghar Khan

The increasing demand for real-time data transmission in wireless mobile communication networks has promoted the maturity of mobile communication technology. Fifth-generation (5G) mobile communication technology is combined with cloud computing, high-frequency signal transmission, and other technologies and perfectly fits with the client-server architecture. 5G has been applied in many fields, such as the interconnection of smart devices, virtual reality, and cloud-based life. To provide the security and availability of the required services, we proposed a key management scheme based on the multiserver architecture of the client-server mode in 5G networks, which uses bilinear pairings and elliptic curve cryptography. Through informal security analysis and formal analysis (under the random oracle model and ProVerif tool), we demonstrated that the proposed scheme can complete mutual authentication and resist common network attacks. Furthermore, after the performance analysis of our scheme and other related schemes, it was found that this scheme has relatively low communication and computation costs and better security performance.

1. Introduction

The growth of mobile data has promoted the development of fifth-generation (5G) and sixth-generation (6G) mobile networks [1–4]. The data flow in mobile communication networks is soaring, and early mobile networks cannot meet the needs of users. The 5G network integrates 4G, WiFi, and other networks, providing richer communication modes and a better user experience. Specifically, in the 2G network era, users can only read words; in the 3G network era, users can view pictures; in the 4G network era, users can watch videos; in the 5G network era, users can engage in virtual reality interaction, cloud storage, and smart device interconnection. A content delivery network (CDN), as one of the key technologies of 5G networks, adds an intelligent virtual network based on the traditional network, which can build multiple proxy servers between the users and the source server. This requires the use of the benefits of the multiserver architecture and cloud computing technology to distribute information to users. As an extension of 5G, 6G can connect terrestrial wireless and satellite communications to achieve global coverage and the interconnection of everything. In other words, 5G/6G networks have a high transmission rate, low power consumption, low time delay, and other properties, allowing them to accommodate a large number of Internet of Things (IoT) devices and mobile users.

The increase in the electromagnetic wave frequency in 5G/6G networks results in high transmission rates, but it also leads to a reduction in the coverage distance and the deployment of more base stations. Furthermore, the deployment of base stations is related to the scope of network management, in which network security management is the fundamental guarantee for users to use a good network. In addition, as an emerging mobile communication, 5G/6G networks will involve many fields, such as mobile phones, smart homes, automatic driving, and telemedicine. In applications involving IoT [5–9], security has always been a weak link in the network. The management of stored and transmitted information is important. Once the information is disclosed, tampered with, or forged, it will lead to serious consequences. In addition, the client-server-based multiserver architecture overcomes the shortage of resources and long response time

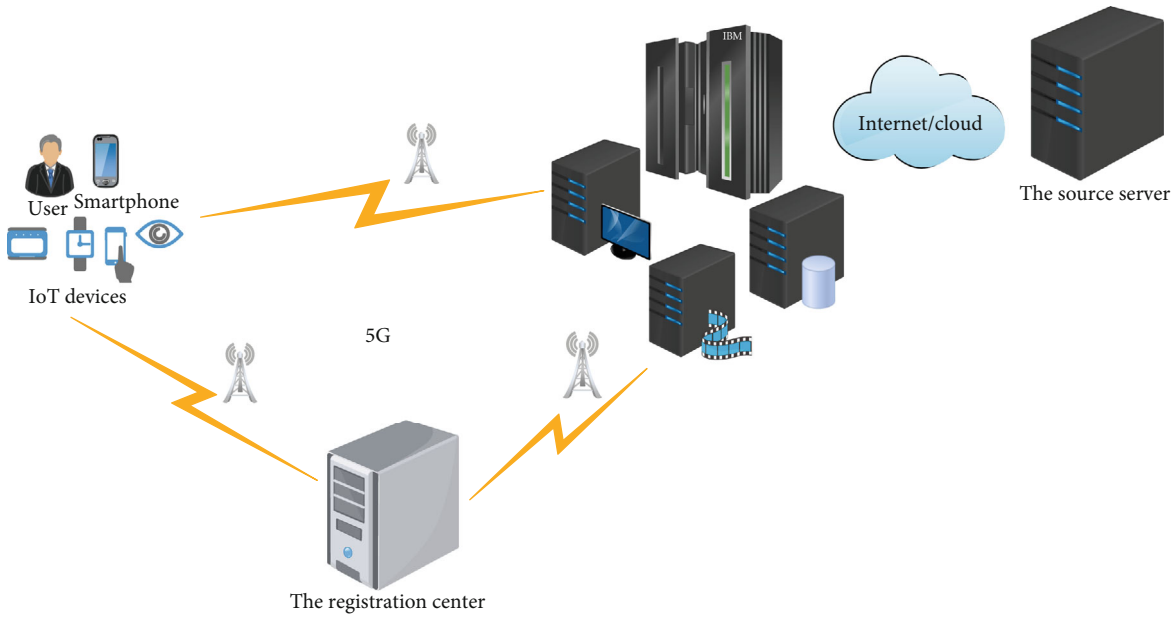


Figure 1: The client-server communication construction in 5G.

of a single server and can provide powerful network data processing capability. Therefore, to solve the security difficulties in network communication and improve user experience, secure authentication schemes for key management and storage based on the multiserver architecture in mobile networks have been proposed. The client-server communication construction in 5G is shown in Figure 1.

In Figure 1, every client and server must register with the registration center to obtain a legal identity to communicate in the network. Note that the clients include users and IoT devices. Owing to the powerful storage function of cloud computing technology, each proxy server will have the corresponding backup of the transmitted information. Therefore, in the authentication phase, a legitimate client directly authenticates and confirms the session key with a proxy server without the participation of the third-party source server.

In recent years, 5G has gradually developed into the core of mobile communication systems, and its distributed service mechanism is consistent with the multiserver architecture of the client-server mode. Therefore, some researchers have started working on mutual authentication protocols based on multiserver 5G networks. In 2019, Ying and Nayak [10] introduced an anonymous multiserver authentication scheme (MSAS) using self-certified public key cryptography in 5G and declared that their scheme was secure. Unfortunately, Haq et al. [11] found that [10] did not provide untraceability and two-factor security and could not resist offline identity, password guessing attacks, or user impersonation attacks. They then proposed an enhanced MSAS in 5G networks.

In this study, we introduced a key management scheme based on the multiserver architecture of the client-server mode in 5G networks. The scheme uses passwords, smart cards, and biometric authentication to provide users with more comprehensive security. Each IoT device has a unique media access control (MAC) address, which we enter as the biometric information of the user:

Table 1: Abbreviations.

5G	Fifth-generation
CDN	Content delivery network
IoT	Internet of Things
MSAS	Multiserver authentication scheme
MAC	Media access control
ROR	Real-Oracle-Random

(i) The research shows that our scheme can guarantee anonymity, perfect forward security, and anti-impersonation attacks, and the smart card is a stolen attack in a multiserver architecture

(ii) In our scheme, users and servers can complete mutual authentication without passing the registration center to avoid the communication load caused by excessive user traffic

(iii) In the random oracle model, we proposed a hypothesis based on the elliptic curve discrete logarithm problem. This reveals that the proposed scheme has a secure mutual authentication process. The informal security analysis and ProVerif tool proof reveal that the proposed scheme can resist common network attacks and has a secure and complete process of generating the session key

(iv) Our protocol has better performance. In a series of related schemes, the proposed scheme has relatively low communication and computation costs. This scheme is more suitable for servers in 5G communication to provide services to users

Some abbreviations used in this paper are shown in Table 1. The remainder of this paper is organized as follows.

Section 2 introduces the related work. A detailed description of the proposed scheme is provided in Section 3. Section 4 provides a formal and informal security analysis of the proposed scheme. Performance analysis of the schemes is presented in Section 5, and the study is concluded in Section 6.

2. Related Work

The earliest MSAS [12] was aimed at neural networks. Because of the time consumption of training neural networks, numerous enhanced MSASs have been proposed. In the process of remote authentication, it is not realistic to use only passwords. Using a smart card is a particularly effective resolution for user authentication and key management [13–15]. Lin et al. [16] introduced a remote MSAS without a verification table in 2003. Cao and Zhong [17] pointed out that [16] is insecure and exposed to serious user impersonation attacks. In addition, in 2004, Juang [18] pointed out that each user in [16] needs to use a large memory to store relevant parameters, which is not suitable for applications using the smart card. Moreover, [12, 16] do not generate a session key; therefore, there is a certain security risk in the communication process. Therefore, they designed an MSAS using a smart card and password. In the same year, Chang and Lee [19] thought that Juang's scheme [18] performed significant computation in smart cards; therefore, they proposed an efficient MSAS based on the smart card. In a multiserver environment, multiple servers are required to provide services to users, and providing strong anonymity is more secure for users. In 2009, Liao and Wang [20] introduced a scheme using dynamic identity and smart card authentication and concluded that their scheme met all requirements in an MS environment. However, Hsiang and Shih [21] discovered that [20] cannot resist insider attacks and spoofing attacks. To address the above security loopholes, they submitted an enhanced MSAS using smart cards and dynamic identity.

Because passwords and smart cards may be forgotten or lost, human biometrics are added to the design of key management and authentication protocols [22], such as fingerprint, face, and iris. In 2010, Li and Hwang [23] introduced a remote MSAS based on biometrics and smart cards and declared that their scheme can resist masquerade attacks, replay attacks, and smart card stolen attacks and present mutual authentication and nonrepudiation. In 2011, Li et al. [24] found that [23] had some security flaws; that is, they did not provide correct authentication and could not resist man-in-the-middle attacks and impersonation attacks. Further, they submitted an advanced remote MSAS using smart cards and biometrics. To ensure perfect forward security and reduce the computation consumption of smart cards, Yoon and Yoo [25] proposed a distributed MSAS without a verification table based on biometrics and smart cards in 2013. Liao and Hsiao [26] introduced a remote MSAS based on pairing. However, Kim et al. [27] found that [25] could not resist offline password guessing attacks; therefore, an enhanced solution was proposed to overcome this vulnerability. Hsieh and Leu [28] pointed out that [26] would be subject to tracking attacks, and there was no preverification phase. Therefore, they improved the MSAS for mobile users using a self-certified public key. In 2014, Chuang and Chen [29] proposed a lightweight MSAS that guarantees anonymity and claimed that it can resist a variety of attacks. Mishra et al. [30] showed that [29] could not resist impersonation attacks, smart card stolen attacks, and denial of service attacks. They then submitted an enhanced MSAS based on [29]. However, Lu et al. [31] proved that [30] is vulnerable to server impersonation attacks and lacks perfect forward security in 2015. Therefore, they proposed an MSAS based on three factors. In 2016, He et al. [32] introduced an anonymous MSAS using self-certified public key encryption. Li et al. [33] pointed out that [32] would be subject to offline password guessing attacks and impersonation attacks in 2019. Furthermore, they designed a secure MSAS for key management in a cloud computing environment. It is worth noting that Chuang and Tseng [34] proposed a compatible cross-species authentication and key exchange protocol and realized independent authentication and member revocation. To solve the performance problem of low-power clients, Tseng et al. [35] proposed a lightweight identity-based mutual authentication and key exchange protocol for resource-constrained devices. Some important related works are summarized in Table 2.

3. Background and Scheme

3.1. Preliminaries

3.1.1. Hash Function. In this section, we will introduce the basics of hash functions. The hash function $H(\cdot)$ takes the variable-length data block M as the input to generate a fixed-length hash value $h = H(M)$ and satisfies the following conditions:

(1) *One-Way*. Given h, it is difficult to compute M such that $h = H(M)$.

(2) *Weak Collision Resistance*. Given M_1, it is difficult to find $M_2 \neq M_1$ so that $H(M_1) = H(M_2)$.

(3) *Strong Collision Resistance*. It is difficult to find $M_1 \neq M_2$ so that $H(M_1) = H(M_2)$.

3.1.2. Bilinear Pairing. Suppose F_n^* is a finite field on an elliptic curve and n is a large prime number. G_1 is an additive cyclic subgroup with P as a generator on F_n^*, and G_2 is a multiplication group with n as order. For points $P, Q \in G_1$, the bilinear pairing [33–35] is a mapping, $e : G_1 \times G_1 \longrightarrow G_2$, which has the following properties:

(1) *Bilinear*. $e(aP, bQ) = e(P, Q)^{ab}$, where $a, b \in F_n^*$.

(2) *Nondegenerate*. $e(P, Q) \neq 1$.

(3) *Computability*. There is an efficient algorithm to compute $e(P, Q)$.

3.2. Proposed Scheme. We describe a client-server key management scheme in which the client can be a user or an IoT device. The scheme is divided into four phases:

Table 2: Cryptographic techniques and limitations.

Scheme	Cryptographic techniques	Limitations
Ying and Nayak [10]	(i) Utilized ECC (ii) Utilized a self-certified public key (iii) Based on the Diffie–Hellman problem	(i) Does not provide untraceability (ii) Does not provide two-factor security (iii) Does not resist offline identity guessing attacks (iv) Does not resist offline password guessing attacks (v) Does not resist user impersonation attacks
Yoon and Yoo [25]	(i) Based on biometrics (ii) Utilized ECC (iii) Based on a smart card	(i) Does not resist offline password guessing attacks
Liao and Hsiao [26]	(i) Based on bilinear pairings (ii) Utilized a self-certified public key (iii) Based on the Diffie–Hellman problem	(i) Does not resist tracking attacks (ii) Does not provide preverification
Chuang and Chen [29]	(i) Utilized a one-way hash function (ii) Based on biometrics (iii) Based on a smart card	(i) Does not resist impersonation attacks (ii) Does not resist smart card stolen attacks (iii) Does not resist denial of service attacks
Mishra et al. [30]	(i) Utilized a one-way hash function (ii) Based on biometrics (iii) Based on a smart card	(i) Does not resist server impersonation attacks (ii) Does not provide perfect forward security
He et al. [32]	(i) Based on bilinear pairings (ii) Utilized a self-certified public key (iii) Based on the Diffie–Hellman problem	(i) Does not resist offline password guessing attacks (ii) Does not resist impersonation attacks
Li et al. [33]	(i) Based on bilinear pairings (ii) Based on the Diffie–Hellman problem (iii) Utilized a one-way hash function	—
Chuang and Tseng [34]	(i) Based on bilinear pairings (ii) Based on the Diffie–Hellman problem (iii) Utilized a one-way hash function	—
Tseng et al. [35]	(i) Based on bilinear pairings (ii) Based on the Diffie–Hellman problem (iii) Utilized a one-way hash function	—

initialization, registration phase, time key update phase, and key management phase. The symbols and descriptions of the scheme are listed in Table 3.

3.2.1. Initialization. The RC sets up an elliptic curve and chooses the parameters. RC selects two elliptic curve groups G_1 and G_2 with the same order q. Subsequently, RC defines a bilinear pairing $e : G_1 \times G_1 \longrightarrow G_2$ and computes $g = e(P, P)$, where P is a generator of G_1. RC chooses a random number x as its private key, and $P_{pub} = x \cdot P$ is the corresponding public key. Finally, RC generates two hash functions, $HG(\cdot)$ and $H(\cdot)$, and publicizes $\{G_1, G_2, q, P, P_{pub}, g, HG(\cdot), H(\cdot)\}$.

3.2.2. Registration Phase. To join the system, both U_i and S_j must register with the RC to verify their legality. This phase includes the U_i and S_j registration.

(1) Server Registration Phase. The registration steps of S_j are shown as follows:

(1) Server S_j chooses its identity SID_{S_j} and a random number r_{sj} and computes the public key $P_{sj} = g^{r_{sj}}$. Thereafter, S_j sends $\{P_{sj}, SID_{S_j}\}$ to RC via a secure channel

(2) After receipt, RC computes $d_{sj} = x \cdot HG(SID_{S_j})$ and $P_{rsj} = (P_{sj})^x \oplus d_{sj}$ and then sends $\{P_{rsj}\}$ back to S_j

(3) S_j computes $d_{sj} = P_{rsj} \oplus (P_{pub})^{r_{sj}}$ as its private key and then checks if $e(d_{sj}, P) = ^{?} e(HG(SID_{S_j}), P_{pub})$. If not equal, S_j rejects messages. If equal, S_j accepts d_{sj} and stores $\{d_{sj}, r_{sj}\}$

(4) RC stores all servers' status and identities SID_{S_j} in a table Tab_{S_j}

(2) User Registration Phase. The registration steps of U_i are shown as follows:

(1) U_i selects identity ID_{U_i}, password PW_{U_i}, and biometric BIO_{U_i}. Note that the MAC address of an IoT device is the BIO_{U_i}. Thereafter, U_i generates a random number r_{ui} and computes $Gen(BIO_{ui}) = (\theta_{ui}, \sigma_{ui})$, $VID_{ui} = H(ID_{U_i} \| r_{ui})$, $FVID_{ui} = VID_{ui} \oplus (P_{pub})^{r_{ui}}$, $VPW_{ui} = H(PW_{U_i} \| VID_{ui} \| r_{ui})$, $FVPW_{ui} = VPW_{ui} \oplus (P_{pub})^{r_{ui}}$, $VBI_{ui} = H(\sigma_{ui} \| r_{ui})$, $FVBI_{ui} = VBI_{ui} \oplus$

Table 3: Symbols and descriptions.

Symbol	Description
U_i	User and IoT device
S_j	Server
RC	Registration center
$\mathscr{A}$	Adversary
SC	Smart card
SK_{U_i}	The session key of U_i
SK_{S_j}	The session key of S_j
x	The private key of the RC
d_{sj}	The private key of S_j
BIO_{U_i}	The biometrics of U_i
$Gen(\cdot)/Rep(\cdot)$	Fuzzy generator/reproduction function
$H(\cdot)$	Hash function
$HG(\cdot)$	Map-to-point hash function
$\|$	Connect operation
$\oplus$	Exclusive or operation
Π_U^x	The x-th communication of user U_i
Π_S^y	The y-th communication of server S_j
Π_{RC}^z	The z-th communication of registry RC
q_{hash}	The number of times to make the *Hash* query
q_{send}	The number of times to make the *Send* query
GM_m	The m-th game
$Succ_{\mathscr{A}}^{GM_m}(\xi)$	The event that $\mathscr{A}$ succeeds in the game GM_m
$\Pr\left[Succ_{\mathscr{A}}^{GM_m}(\xi)\right]$	The probability of the event $Succ_{\mathscr{A}}^{GM_m}(\xi)$

$(P_{pub})^{r_{ui}}$, and $P_{ui} = g^{r_{ui}}$ and sends $\{ID_{U_i}, FVID_{ui}, P_{ui}, FVPW_{ui}, FVBI_{ui}\}$ to RC

(2) Upon receiving, RC computes $VPW_{ui} = FVPW_{ui} \oplus (P_{ui})^x$, $VBI_{ui} = FVBI_{ui} \oplus (P_{ui})^x$, $VID_{ui} = FVID_{ui} \oplus (P_{ui})^x$, $d_{ui} = x \cdot HG(VID_{ui})$, $V_{ui} = H(VPW_{ui} \| VBI_{ui} \| VID_{ui})$, and $R_{sj} = e(d_{ui}, HG(SID_{S_j})) \oplus VBI_{ui} \oplus VPW_{ui}$. Further, RC creates table Tab_{U_i}, which includes all servers' SID_{S_j}, R_{sj}, P_{sj}, and Table $Tab_{S_{U_i}}$, which includes all users' $H(ID_{U_i})$, P_{ui}, and *status*. Subsequently, RC injects $\{Tab_{U_i}, V_{ui}\}$ to the smart card SC and sends it to U_i

(3) After receiving, U_i computes $E_{ui} = r_{ui} \oplus H(\sigma_{ui})$. Finally, U_i stores $\{E_{ui}, \theta_{ui}, P_{ui}\}$ into SC and deletes the other parameters

In other words, if a new client (including users and IoT devices) wants to join the client-server communication construction in 5G, they need to register with the RC according to the above steps in the user registration phase. After registration, the client can obtain the legal identity and corresponding information and communicate with the server.

3.2.3. Time Key Update Phase. In this phase, the RC checks the *status* of users in $Tab_{S_{U_i}}$ and dynamically distributes time keys to legitimate users. Communication in this phase occurs in public channels. The details are as follows:

(1) RC queries the *status* of the user's $H(ID_{U_i})$ in $Tab_{S_{U_i}}$. When *status* is "OK," RC selects a random number b_{ui} and adds b_{ui} into $Tab_{S_{U_i}}$. Thereafter, RC chooses a time-valid period t and computes $B_{ui} = g^{b_{ui}}$, $C_{ui} = (P_{ui})^{b_{ui}}$, and $T_{ui} = H(B_{ui} \| C_{ui} \| t)$. Further, RC sends $\{B_{ui}, T_{ui}, t\}$ to U_i via a public channel

(2) After receiving, U_i inserts their SC, inputs ID_{U_i} andBIO_{U_i}, and computes $\sigma_{ui} = Rep(BIO_{U_i}, \theta_{ui})$, $r_{ui} = E_{ui} \oplus H(\sigma_{ui})$, and $C_{ui} = (B_{ui})^{r_{ui}}$. Subsequently, U_i checks if $T_{ui} \stackrel{?}{=} H(B_{ui} \| C_{ui} \| t)$. If the equation holds, U_i accepts the time key and stores $\{C_{ui}, t\}$ into SC

3.2.4. Key Management Phase. U_i inserts SC to log into the system. Subsequently, U_i can authenticate and establish a session key using S_j. The detailed steps are as follows:

(1) U_i inputs ID_{U_i}, PW_{U_i}, and BIO_{U_i} and inserts their SC. U_i then computes $\sigma_{ui} = Rep(BIO_{ui}, \theta_{ui})$, $r_{ui} = E_{ui} \oplus H(\sigma_{ui})$, $VID_{ui} = H(ID_{U_i} \| r_{ui})$, $VPW_{ui} = H(PW_{U_i} \| VID_{ui} \| r_{ui})$, and $VBI_{ui} = H(\sigma_{ui} \| r_{ui})$ and checks if $V_{ui} \stackrel{?}{=} H(VPW_{ui} \| VBI_{ui} \| VID_{ui})$. The authorized user U_i logs into the system. Thereafter, the card reader queries Tab_{U_i} and displays all the server identities SID_{S_j}. U_i selects a server's SID_{S_j} and chooses a random number α. Further, U_i computes $Y_{ui} = g^{\alpha}$, $Q_{ui} = (P_{sj})^{r_{ui}}$, $F_{ui} = VID_{ui} \oplus H(Y_{ui} \| SID_{S_j} \| Q_{ui})$, and $V_1 = H(F_{ui} \| Y_{ui} \| P_{ui} \| VID_{ui} \| C_{ui})$ and sends $\{F_{ui}, Y_{ui}, P_{ui}, V_1\}$ to S_j

(2) Upon receiving, server S_j computes $Q_{sj} = (P_{ui})^{r_{sj}}$, $C_{ui} = (P_{ui})^{b_{ui}}$, and $VID'_{ui} = F_{ui} \oplus H(Y_{ui} \| SID_{S_j} \| Q_{sj})$ and checks if $V_1 \stackrel{?}{=} H(F_{ui} \| Y_{ui} \| P_{ui} \| VID'_{ui} \| C_{ui})$. When the equation holds, S_j generates a random number β and computes $e_{sj} = e(d_{sj}, HG(VID_{ui}))$, $Y_{sj} = g^{\beta}$, and $V_2 = H(e_{sj} \| Y_{sj} \| Y_{ui} \| VID_{ui} \| SID_{S_j} \| Q_{sj})$ and sends $\{V_2, Y_{sj}\}$ to U_i

(3) Upon receiving, U_i computes $e_{ui} = R_{sj} \oplus VPW_{ui} \oplus VBI_{ui}$. Subsequently, U_i checks if $V_2 \stackrel{?}{=} H(e_{sj} \| Y_{sj} \| Y_{ui} \| VID_{ui} \| SID_{S_j} \| Q_{sj})$ holds. When the equation holds, U_i computes $key_{ui} = (Y_{sj})^{\alpha}$ and establishes the session key $SK_{U_i} = H(key_{ui} \| Q_{ui} \| VID_{ui} \| SID_{S_j})$. Further, U_i computes $V_3 = H(SK_{U_i} \| VID_{ui} \| SID_{S_j})$ and sends it to S_j

(4) After receipt, S_j computes $key_{sj} = (key_{ui})^{\beta}$ and session key $SK_{S_j} = H(key_{sj} \| Q_{sj} \| VID_{ui} \| SID_{S_j})$. Finally,

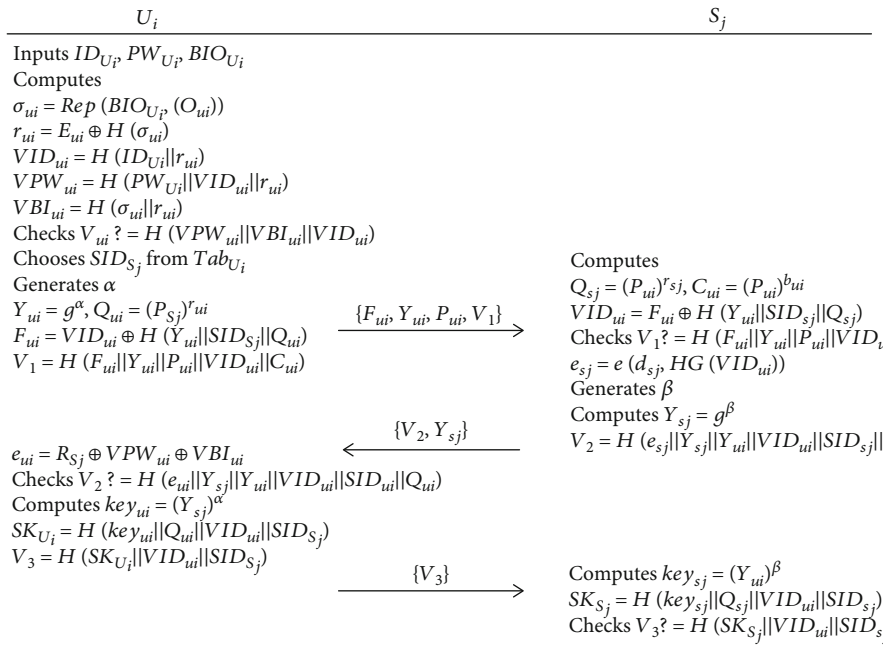


Figure 2: Key management phase.

S_j verifies whether $V_3 = ^{?} H(SK_{S_j}||VID_{ui}||SID_{S_j})$ and accepts the session key when the equation holds

The key management phase is shown in Figure 2.

4. Security Analysis

4.1. Formal Security Analysis Based on Real-Oracle-Random. We conducted a formal security analysis of the scheme under the Real-Oracle-Random (ROR) model [30, 32, 33, 36, 37]. The ROR model is used to simulate ideal hash functions. We assume that ideal hash functions are random and uniformly distributed. Suppose Π_U^x, Π_S^y, and Π_{RC}^z represent the x-th communication of user U_i, the y-th communication of server S_j, and the z-th communication of registry RC, respectively. The Π_U^x, Π_S^y, and Π_{RC}^z act to simulate the real communications of U_i, S_j, and RC. Note that $\mathcal{O} = \{\Pi_U^x, \Pi_S^y, \Pi_{RC}^z\}$.

4.1.1. Queries. Subsequently, adversary $\mathcal{A}$ verifies the security of the protocol with the following query:

(1) $Execute(\mathcal{O})$. Starting the query, $\mathcal{A}$ obtains message records of transmission in the public channel. The execution of this query is a passive attack.

(2) $Hash(string)$. Starting the query, $\mathcal{A}$ can enter a *string* and then obtain the corresponding hash value.

(3) $Send(\mathcal{O}, M)$. Starting the query, $\mathcal{A}$ sends M to $\mathcal{O}$ and receives a response from $\mathcal{O}$.

(4) $Corrupt(\mathcal{O})$. Starting the query, $\mathcal{A}$ obtains one of the private values from $\mathcal{O}$.

(5) $Test(\mathcal{O})$. Starting the query, $\mathcal{A}$ flips coin $\mathcal{C}$ and attempts to determine the correctness of the session key. There are only two results for flipping $\mathcal{C}$: $\mathcal{C}$ = 1 or $\mathcal{C} = 0$. The former means that $\mathcal{A}$ receives the session key, and the latter means that $\mathcal{A}$ receives a random string.

4.1.2. Definitions. The proposed scheme involves the discrete logarithm problem on an elliptic curve (ECDLP) over a finite field F_n^*, which is defined by the following. On the elliptic curve E, given the points H and Q of order n, and $H = aQ$, where H and Q belong to E and a to F_n^*, in the polynomial time ξ, the probability that $\mathcal{A}$ obtains a that satisfies $H = aQ$ is $Adv_{\mathcal{A}}^{ECDLP}(\xi) = \Pr[\mathcal{A}(Q, aQ) = a : a \in F_n^*, Q \in E]$. Furthermore, for a sufficiently small η, we have the following results: $Adv_{\mathcal{A}}^{ECDLP}(\xi) < \eta$.

4.1.3. Theorem. If $\mathcal{A}$ queries in polynomial time ξ, the advantage of breaking scheme S is $Adv_{\mathcal{A}}^{S}(\xi) \le 2 \max\{C' \cdot q_{send}^{s'}, q_{send}/2^l\} + 2q_{hash}Adv_{\mathcal{A}}^{ECDLP}(\xi) + q_{hash}^2/2^l + (q_{send} + q_{hash})/2^{l-1}$, where q_{hash} is the number of times to achieve the *Hash* query, q_{send} is the number of times to achieve the *Send* query, l is the length of the password, and C' and s' are constants.

Proof. We define the game sequence $GM_m (m = 0, 1, 2, 3, 4, 5, 6)$ to prove the theorem. $Succ_{\mathcal{A}}^{GM_m}(\xi)$ is the event that $\mathcal{A}$ succeeds in the game GM_m. □

(1) GM_0. GM_0 means starting the game without queries. At this time, the advantage of $\mathcal{A}$ breaking S is

$$Adv_{\mathcal{A}}^{S}(\xi) = \left|2 \Pr\left[Succ_{\mathcal{A}}^{GM_0}(\xi)\right] - 1\right|. \quad (1)$$

(2) GM_1. GM_1 starts executing the *Execute* query. Because the *Execute* query can only receive messages $\{B_{ui}, T_{ui}, t\}$, $\{F_{ui}, Y_{ui}, P_{ui}, V_1\}$, $\{V_2, Y_{sj}\}$, and $\{V_3\}$ transmitted through the public channel,

$$\Pr\left[Succ_{\mathscr{A}}^{GM_1}(\xi)\right] = \Pr\left[Succ_{\mathscr{A}}^{GM_0}(\xi)\right]. \tag{2}$$

(3) GM_2. GM_2 begins to achieve the *Send* query. Based on Zipf's law [38], we obtain

$$\left|\Pr\left[Succ_{\mathscr{A}}^{GM_2}(\xi)\right] - \Pr\left[Succ_{\mathscr{A}}^{GM_1}(\xi)\right]\right| \le \frac{q_{send}}{2^l}. \tag{3}$$

(4) GM_3. GM_3 begins to achieve the *Hash* query. Based on the birthday paradox, we obtain

$$\left|\Pr\left[Succ_{\mathscr{A}}^{GM_3}(\xi)\right] - \Pr\left[Succ_{\mathscr{A}}^{GM_2}(\xi)\right]\right| \le \frac{q_{hash}^2}{2^{l+1}}. \tag{4}$$

(5) GM_4. GM_4 starts to judge the security of the session key, mainly based on the following two attacks:

(i) *Perfect Forward Security*. $\mathscr{A}$ uses Π_{RC}^z to obtain x of RC and verify whether protocol S can provide perfect forward security.

(ii) *Known Session-Specific Temporary Information Attacks*. $\mathscr{A}$ uses Π_U^x or Π_S^y or Π_{RC}^z to obtain temporary information and verify whether protocol S can resist the attack.

In the above two cases, the ECDLP must be solved to calculate $SK_{U_i} = SK_{S_j}$. For $SK_{U_i} = H(key_{ui}\|Q_{ui}\|VID_{ui}\|SID_{S_j})$, in the first case, suppose $\mathscr{A}$ can calculate $d_{sj} = x \cdot HG(SID_{S_j})$ through x, but $key_{ui} = (Y_{sj})^{\alpha}andQ_{ui} = (P_{sj})^{r_{ui}}$ is unknown, which needs to solve ECDLP twice; in the second case, suppose $\mathscr{A}$ obtains the random number α of U_i and further calculates $key_{ui} = (Y_{sj})^{\alpha}$, but Q_{ui} and r_{ui} are still unknown. The above analysis is also true for $SK_{S_j} = H(key_{sj}\|Q_{sj}\|VID_{ui}\|SID_{S_j})$. Therefore,

$$\left|\Pr\left[Succ_{\mathscr{A}}^{GM_4}(\xi)\right] - \Pr\left[Succ_{\mathscr{A}}^{GM_3}(\xi)\right]\right| \le q_{hash}Adv_{\mathscr{A}}^{ECDLP}(\xi). \tag{5}$$

(6) GM_5. GM_5 uses Π_U^x to obtain the information $\{Tab_{U_i}, V_{ui}, E_{ui}, \theta_{ui}, P_{ui}, C_{ui}, t\}$ stored in SC. Subsequently, $\mathscr{A}$ uses the information to launch offline password guessing attacks or stolen smart card attacks. $\mathscr{A}$ calculates $V_{ui} = H(VPW_{ui}\|VBI_{ui}\|VID_{ui})$, where $VID_{ui} = H(ID_{U_i}\|r_{ui})$, $VPW_{ui} = H(PW_{U_i}\|VID_{ui}\|r_{ui})$, and $VBI_{ui} = H(\sigma_{ui}\|r_{ui})$. However, σ_{ui}, r_{ui}, ID_{U_i}, PW_{U_i}, and BIO_{U_i} are confidential. The probability that $\mathscr{A}$ can successfully guess the biological information of l-bit is $1/2^l$ [39], which is an extremely small value. Based on Zipf's law [38], we have

$$\begin{aligned}&\left|\Pr\left[Succ_{\mathscr{A}}^{GM_5}(\xi)\right] - \Pr\left[Succ_{\mathscr{A}}^{GM_4}(\xi)\right]\right| \\ &\le \max\left\{C' \cdot q_{send}^{s'}, \frac{q_{send}}{2^l}\right\},\end{aligned} \tag{6}$$

where C' and s' are constants.

(7) GM_6. GM_6 starts to execute query $H(key_{ui}\|Q_{ui}\|VID_{ui}\|SID_{S_j})$ or $H(key_{sj}\|Q_{sj}\|VID_{ui}\|SID_{S_j})$ to verify whether protocol S can resist the key compromise impersonation attacks. At this time, the advantage of $\mathscr{A}$ breaking S is

$$\left|\Pr\left[Succ_{\mathscr{A}}^{GM_6}(\xi)\right] - \Pr\left[Succ_{\mathscr{A}}^{GM_5}(\xi)\right]\right| \le \frac{q_{hash}}{2^l}. \tag{7}$$

Because the probability of success and failure of GM_6 is equal,

$$\Pr\left[Succ_{\mathscr{A}}^{GM_6}(\xi)\right] = \frac{1}{2}. \tag{8}$$

According to formulas (1)–(8), we have

$$\begin{aligned}\frac{1}{2}Adv_{\mathscr{A}}^{S}(\xi) &= \left|\Pr\left[Succ_{\mathscr{A}}^{GM_0}(\xi)\right] - \frac{1}{2}\right| \\ &= \left|\Pr\left[Succ_{\mathscr{A}}^{GM_0}(\xi)\right] - \Pr\left[Succ_{\mathscr{A}}^{GM_6}(\xi)\right]\right| \\ &= \left|\Pr\left[Succ_{\mathscr{A}}^{GM_1}(\xi)\right] - \Pr\left[Succ_{\mathscr{A}}^{GM_6}(\xi)\right]\right| \\ &\le \sum_{m=0}^{5}\left|\Pr\left[Succ_{\mathscr{A}}^{GM_{m+1}}(\xi)\right] - \Pr\left[Succ_{\mathscr{A}}^{GM_m}(\xi)\right]\right| \\ &= \max\left\{C' \cdot q_{send}^{s'}, \frac{q_{send}}{2^l}\right\} + q_{hash}Adv_{\mathscr{A}}^{ECDLP}(\xi) \\ &\quad + \frac{q_{hash}^2}{2^{l+1}} + \frac{(q_{send} + q_{hash})}{2^l}.\end{aligned} \tag{9}$$

Further, we have $Adv_{\mathscr{A}}^{S}(\xi) \le 2\max\{C' \cdot q_{send}^{s'}, q_{send}/2^l\} + 2q_{hash}Adv_{\mathscr{A}}^{ECDLP}(\xi) + q_{hash}^2/2^l + (q_{send} + q_{hash})/2^{l-1}$.

4.2. Formal Security Analysis Based on ProVerif. ProVerif, which is mainly used for the automatic verification of cryptographic-related security protocols, is a formal analysis tool based on the Dolev-Yao model [40] and computational model proposed by Abadi et al. and Blanchet et al. [41, 42]. The ProVerif tool [43] is based on the equivalence theory of function reduction, definition of terms and processes, structural equivalence between extended processes, and others and is applied to the security analysis of the real environment. Furthermore, the analysis and verification with ProVerif have security properties, such as confidentiality, authentication, and logic. Our proposed protocol was analyzed using ProVerif, as follows.

```
(**********channel**********)
free ch: channel.
free sch: channel [private].
(**********shared keys**********)
free SKUi: bitstring [private].
free SKSj: bitstring [private].
free IDUi: bitstring [private].
free SIDSj: bitstring [private].
(**********constants**********)
free x: bitstring [private].
free g: bitstring.
free P: bitstring.
free Ppub : bitstring.
(**********functions & reductions & equations*********)
fun H (bitstring): bitstring.
fun HG (bitstring): bitstring.
fun mult (bitstring, bitstring): bitstring.
fun bilinearmap (bitstring, bitstring): bitstring.
fun exp (bitstring, bitstring): bitstring.
fun con (bitstring, bitstring): bitstring.
reduc forall m: bitstring, n: bitstring; getmess (con (m, n)) = m.
```

Figure 3: Definitions.

```
(**********functions & reductions & equations*********)
fun xor (bitstring,bitstring): bitstring.
equation forall m: bitstring, n: bitstring; xor (xor (m, n), n) = m.
fun Gen (bitstring): bitstring.
fun Rep (bitstring, bitstring): bitstring.

(**********queries**********)
query attacker (SKUi).
query attacker (SKSj).
query attacker (IDUi).
query attacker (SIDSj).
query inj-event (UserAuthed ()) ==> inj-event (UserStarted ()).
query inj-event (UserAcServer ()) ==> inj-event (ServerAcUser ()).
query inj-event (ServerAcSK ()) ==> inj-event (UserAcServer ()).

(********** event**********)
event UserStarted ().
event UserAuthed ().
event ServerAcUser ().
event UserAcServer ().
event ServerAcSK ().
```

Figure 4: Queries and events.

Some constants and functions were defined as shown in Figure 3. Among them, *hash*, *concatenation*, and *xor* are common operations; *Bilinearmap*() is a bilinear pairing operation; exp (*bitstring*, *bitstring*) are exponential operations, with the first *bitstring* as the base and the last *bitstri ng* as the exponent. The anonymity and consistency of the protocol were analyzed using events and queries. As shown in Figure 4, the events *UserStarted*(), *UserAuthed*(), and *UserAcServer*(), respectively, indicate that the user starts authentication, completes login, and successfully authenticates the server; events *ServerAcUser*() and *ServerAcSK*(), respectively, indicate that the server successfully authenticates the user and completes the authentication of the session key.

Figures 5(a) and 5(b) show the specific operations of each entity and describe the authentication process between the user and the server. The results of the query using ProVerif are shown in Figure 6. The first and second results confirm that the session key is secure, and our scheme can resist key compromise impersonation attacks. The third and fourth results reveal that the proposed scheme can guarantee anonymity and resist offline password guessing attacks. The $inj-event(UserAuthed()) = \Rightarrow inj-event(UserStarted())$ indicates that the user logs in after authentication. The $inj-event(UserAcServer()) = \Rightarrow inj-event(ServerAcUser())$ indicates that user authentication is performed after the server completes authentication. The $inj-event(ServerAcSK()) = \Rightarrow inj-event(UserAcServer())$ indicates that the server verifies the session key after the user completes authentication. In other words, the proposed scheme maintains consistency.

4.3. Informal Analysis

4.3.1. Insider Attacks. In the proposed scheme, $\{ID_{U_i}, FVID_{ui}, P_{ui}, FVPW_{ui}, FVBI_{ui}\}$ are sent to RC when U_i is registered, where $FVID_{ui} = VID_{ui} \oplus (P_{pub})^{r_{ui}}$, $P_{ui} = g^{r_{ui}}$, $FVPW_{ui} = VPW_{ui} \oplus (P_{pub})^{r_{ui}}$, and $FVBI_{ui} = VBI_{ui} \oplus (P_{pub})^{r_{ui}}$. In this process, U_i does not directly transmit passwords or biometrics. Insiders in RC cannot compute real PW_{ui} and BIO_{ui}. Therefore, the proposed scheme can resist insider attacks.

4.3.2. User Impersonation Attacks. Malicious adversary $\mathcal{A}$ attempts to impersonate legitimate users in communicating with S_j. (1) $\mathcal{A}$ intercepts $\{F_{ui}, Y_{ui}, P_{ui}, V_1\}$, selects α', and computes $Y'_{ui} = g^{\alpha'}$, $Q_{ui} = (P_{sj})^{r_{ui}}$, $F'_{ui} = VID_{ui} \oplus H(Y'_{ui} \| SID_{S_j} \| Q_{ui})$, and $V_1 = H(F'_{ui} \| Y'_{ui} \| P_{ui} \| VID_{ui} \| C_{ui})$, where $VID_{ui} = H(ID_{U_i} \| r_{ui})$ and $C_{ui} = (B_{ui})^{r_{ui}}$. However, ID_{U_i} and r_{ui} are confidential to $\mathcal{A}$. Therefore, when S_j verifies V_1, it will reject $\mathcal{A}$. (2) If $\mathcal{A}$ intercepts $\{V_2, Y_{sj}\}$ and forges $\{V_3\}$, it attempts to pass S_j's validation for SK_{U_i}. However, $SK_{U_i} = H(key_{ui} \| Q_{ui} \| VID_{ui} \| SID_{S_j})$, where key_{ui}, Q_{ui}, and VID_{ui} are all confidential to $\mathcal{A}$. Therefore, S_j declines to generate a session key with $\mathcal{A}$. The above analysis indicates that the proposed scheme can resist user impersonation attacks.

4.3.3. Server Impersonation Attacks. Malicious adversary $\mathcal{A}$ attempts to impersonate S_j to communicate with legitimate users. $\mathcal{A}$ intercepts $\{F_{ui}, Y_{ui}, P_{ui}, V_1\}$ and $\{V_2, Y_{sj}\}$, selects β', and computes $Y'_{sj} = g^{\beta'}$ and $V'_2 = H(e_{sj} \| Y'_{sj} \| Y_{ui} \| VID_{ui} \| SID_{S_j} \| Q_{sj})$, where $e_{sj} = e(d_{sj}, HG(VID_{ui}))$, $VID_{ui} = H(ID_{U_i} \| r_{ui})$, and $Q_{sj} = (P_{ui})^{r_{sj}}$ are unknown to $\mathcal{A}$. Therefore, $\mathcal{A}$ cannot be forged as the S_j to communicate with U_i. In other words, our scheme can resist server impersonation attacks.

4.3.4. Replay Attacks. In our scheme, whenever U_i starts a new session with S_j, new α and β will participate in the session. $Y_{ui} = g^{\alpha}$, $Y_{sj} = g^{\beta}$, $key_{ui} = (Y_{sj})^{\alpha}$, and $key_{sj} = (key_{ui})^{\beta}$ are updated in each round, where Y_{ui} and Y_{sj} are used for

```
(*************User's process************)
let ProcessUser =
new IDUi: bitstring;
new PWUi: bitstring;
new BIOUi: bitstring;
new rui: bitstring;
let (a: bitstring, b: bitstring) = Gen (BIOUi) in
let VIDui = H (con (IDUi, rui)) in
let FVIDui = xor (VIDui, exp (Ppub, rui)) in
let VPWui = H (con (PWUi, con (VIDui, rui))) in
let FVPWui = xor (VPWui, exp (Ppub, rui)) in
let VBIui = H (con (b, rui)) in
let FVBIui = xor (VBIui, exp (Ppub,rui)) in
let Pui = exp (g, rui) in
out(sch, (IDUi, FVIDui, Pui, FVPWui, FVBIui));
in (sch, (xTabUi: bitstring, xVui: bitstring));
let Eui = xor (rui, H (b)) in
! (in (ch, (xBui: bitstring, xTui: bitstring, xt: bitstring));
let Cui = exp (xBui, rui) in
event UserStarted ();
let b' = Rep (BIOUi,a) in
let rui = xor (Eui, H(b')) in
let VIDui = H (con (IDUi, rui)) in
let VPWui = H (con (PWUi, con (VIDui, rui))) in
let VBIui = H (con (b', rui)) in
let Vui' = H (con (VPWui, con (VBIui, VIDui))) in
if Vui' = xVui then event UserAuthed (); (***authentication***)
new xSIDSj: bitstring;
new xPsj: bitstring;
new A: bitstring;
let Yui = exp (g, A) in
let Qui = exp (xPsj, rui) in
let Fui = xor (VIDui, H (con (Yui, con (xSIDSj, Qui)))) in
let V1 = H (con (Fui, con (Yui, con (Pui, con (VIDui, Cui))))) in
out (ch, (Fui, Yui, Pui, V1));
in (ch, (xV2: bitstring, xYsj: bitstring));
new xRsj: bitstring;
let eui = xor (xRsj, xor (VPWui, VBIui)) in
let V2' = H (con (Qui, con (econ (xYsj, VIDui), econ (Yui, eui)))) in
if V2' = xV2 then event UserAcServer ();
let keyui = exp (xYsj, A) in
let SKUi = H (con (keyui, con (Qui, con (VIDui, xSIDSj)))) in
let V3 = H (con (SKUi, con (VIDui, xSIDSj))) in
out (ch, (V3));
0).
(*************Server's process************)
let ProcessServer =
new SIDSj: bitstring; (* the Server's identity *)
new rsj: bitstring;
let Psj = exp (g, rsj) in
out (sch, (Psj, SIDSj));
in (sch, (yPrsj: bitstring));
let dsj = xor (yPrsj, exp (Ppub, rsj)) in
if bilinearmap (dsj, P) = bilinearmap (HG(SIDSj), mult (x, P)) then
```

(a) Process

```
! (in (ch, (yFui: bitstring, yYui: bitstring, yPui: bitstring, yV1: bitstring));
new ybui: bitstring;
let Qsj = exp (yPui, rsj) in
let Cui = exp (yPui, ybui) in
let VIDui = xor (yFui, H (con (yYui, con (SIDSj, Qsj)))) in
let V1' = H (con (yFui, con (yYui, con (yPui, con (VIDui, Cui))))) in
if V1' = yV1 then event ServerAcUser ();
new B: bitstring;
let esj = bilinearmap (dsj, HG (VIDui)) in
let Ysj = exp (g, B) in
let V2 = H (con (esj, con (Ysj, con (yYui, con (VIDui, con (SIDSj, Qsj)))))) in
out (ch, (V2, Ysj));
in (ch, (yV3: bitstring));
let keysj = exp (yYui, B) in
let SKSj = H (con (keysj, con (Qsj, con (VIDui, SIDSj)))) in
let V3' = H (con (SKSj, con (VIDui, SIDSj))) in
if V3' = yV3 then event ServerAcSK ();
0).
(*************RC's process************)
let UserReg =
in (sch, (zIDUi: bitstring, zFVIDui: bitstring, zPui: bitstring, zFVPWui: bi
tstring, zFVBIui: bitstring));
let VPWui = xor (zFVPWui, exp (zPui, x)) in
let VBIui = xor (zFVBIui, exp (zPui, x)) in
let VIDui = xor (zFVIDui, exp (zPui, x)) in
let dui = mult (x, HG (VIDui)) in
let Vui = H (con (VPWui, con (VBIui, VIDui))) in
let Rsj = xor (bilinearmap (dui, HG(SIDSj)), xor (VBIui, VPWui)) in
new Tabui: bitstring;
out (sch, (Tabui, Vui));
0.
let ServerReg =
in (sch, (zPsj: bitstring, zSIDSj: bitstring));
let dsj = mult (x, HG (zSIDSj)) in
let Prsj = xor (exp (zPsj, x), dsj) in
out (sch, (Prsj));
0.
let RCAuth =
new zPui: bitstring;
new zFVPWui: bitstring;
let VPWui = xor (zFVPWui, exp (zPui,x)) in
new bui: bitstring;
new t: bitstring;
let Bui = exp (g, bui) in
let Cui = exp (zPui, bui) in
let Tui = H (con (Bui, con (Cui, t))) in
out (ch, (Bui, Cui, t));
0.
let ProcessRC = UserReg | ServerReg | RCAuth.

(*---------main----------*)
process
        (!ProcessUser | !ProcessServer | !ProcessRC)
```

(b) Process

Figure 5: Processes.

validation and key_{ui} and key_{sj} constitute the session key. Therefore, the proposed scheme can resist replay attacks.

4.3.5. User Anonymity. In the key management phase, the user passes the virtual identity $VID_{ui} = H(ID_{U_i} \| r_{ui})$ to the server, and each round of session is protected by a new random number α. Accordingly, the server verifies the user's pseudonym $VID'_{ui} = F_{ui} \oplus H(Y_{ui} \| SID_{S_j} \| Q_{sj})$. Therefore, $\mathcal{A}$ cannot extract the real identity ID_{U_i} of the user. The proposed scheme achieves user anonymity.

5. Performance Analysis

The proposed scheme is evaluated with those of [32–35] in terms of security, computation cost, communication cost, and storage cost. These five protocols all use bilinear pairing operations. Considering the practical application value, we

```
(**********results**********)
1-- RESULT not attacker (SKUi[]) is true.
2-- RESULT not attacker (SKSj[]) is true.
3-- RESULT not attacker (IDUi[]) is true.
4-- RESULT not attacker (SIDSj[]) is true.
5-- RESULT inj-event (UserAuthed) ==> inj-event (UserStarted) is true.
6-- RESULT inj-event (UserAcServer) ==> inj-event (ServerAcUser) is true.
7-- RESULT inj-event (ServerAcSK) ==> inj-event (UserAcServer) is true.
```

Figure 6: Results.

Table 4: Security comparison.

	[32]	[33]	[34]	[35]	Ours
K1	χ [33]	√	√	√	√
K2	√	√	√	√	√
K3	√	√	√	√	√
K4	χ [33]	√	√	√	√
K5	√	√	√	√	√
K6	√	√	√	√	√
K7	χ [33]	√	√	√	√
K8	χ [33]	√	√	√	√

analyzed the consumption of the login and authentication phase for computation cost and communication cost and the consumption of the registration phase for storage cost.

5.1. Security Comparison. In Table 4, we conducted a security evaluation. Let K1, K2, K3, K4, K5, K6, K7, and K8 represent user anonymity, perfect forward security, session key agreement, offline password guessing attacks, insider attacks, preverification, server impersonation attacks, and user impersonation attacks, respectively. Note that preverification means that the user needs to pass the verification of the smart card before communicating with the server. Session key agreement means that the session key needs to be established by two participants. "√" indicates that the protocol can resist attacks. "χ" symbolizes that the protocol cannot resist the attack. Table 4 shows that the scheme in [32] is subject to server impersonation attacks and user impersonation attacks, which is a significant security hazard for the entire protocol. In addition, [32] cannot provide user anonymity and cannot resist offline password guessing attacks. The schemes in [33–35] and our scheme have strong security.

5.2. Computation Cost Comparison. In Table 5, we counted and compared the number of operations and computation time in the schemes of [32–35] and ours. T_{map} denotes the time of bilinear pairing operation, T_{mtp} denotes the time of hash operation from the map to point, T_{ex} represents the time consumption of exponential operation, T_f represents the time consumption of fuzzy extraction function, T_m represents the time consumption of scalar multiplication in G_1, T_a represents the time of point addition in G_1, T_{mg} represents the time of multiplication in G_2, and T_h represents the time consumption of general hash operation. The XOR and join operations were ignored. According to [32], the approximate time consumptions of T_{map}, T_{mtp}, T_{ex}, T_m, T_a, T_{mg}, and T_h are 32.713 ms, 33.582 ms, 2.249 ms, 13.405 ms, 0.081 ms, 0.008 ms, and 0.056 ms for the end-user, respectively. Note that we assume $T_f = T_m$. On the server-side, the approximate time consumptions of T_{map}, T_{mtp}, T_{ex}, T_m, T_a, T_{mg}, and T_h were 5.427 ms, 5.493 ms, 0.339 ms, 2.165 ms, 0.013 ms, 0.001 ms, and 0.007 ms, respectively. The consumption of the proposed scheme on the user-side was slightly higher than that of [33], but on the server-side, it is lower than that of their scheme. In addition, the total computation cost of the proposed scheme was slightly higher than that of [33]. In practical applications, it can cause almost the same online experience for the user. Figure 7 more intuitively shows the comparison of computation cost between our scheme and [32–35].

5.3. Communication and Storage Cost Comparison. We chose $q = 160$ bits and $n = 512$ bits. The output length in G_1 and G_2 is 1024 bits, and the output length for general hash operation and identity is 160 bits. The specific analysis is as follows.

In He et al.'s scheme [32], the transmitted messages are $\{R_{U_i}\}$, $\{y, \alpha_{S_j}\}$, and $\{C_{U_i}\}$, where $\{R_{U_i}, y\}$ belong to G_1 and $\{\alpha_{S_j}, C_{U_i}\}$ belong to F_n^*. The communication cost was 2368 bits. The stored messages are $\{g_{U_i}, \psi_{U_i}, v_{U_i}, b_{U_i}\}$ and $\{D_{S_j}\}$, where $\{g_{U_i}, b_{U_i}, D_{S_j}\}$ belong to G_1 and $\{\psi_{U_i}, v_{U_i}\}$ belong to F_n^*. The storage cost was 3392 bits.

In Li et al.'s scheme [33], the transmitted messages are $\{F_{ui}, k_{ui}, B_{ui}, d_{tui}, t\}$, $\{D_{sj}, k_{sj}\}$, and $\{D_{U_i}\}$, where $\{k_{ui}, B_{ui}, k_{sj}\}$ belong to $G_1$and $\{F_{ui}, d_{tui}, t, D_{sj}, D_{U_i}\}$ belong to F_n^*. The communication cost is 3872 bits. The stored messages are $\{T_{ui}, G_{ui}, V_{ui}, h_1, \theta_{ui}, W_{ui}, H_i(i = 00, 01, 1, \cdots, 7), g_{pub}\}$ and $\{B_{ui}, d_{tui}, t\}$, where $\{H_i(i = 00, 01), g_{pub}, B_{ui}, d_{tui}\}$ belong to G_1 and $\{T_{ui}, G_{ui}, V_{ui}, h_1, \theta_{ui}, W_{ui}, H_i(i = 1, \cdots, 7), t\}$ belong to F_n^*. The storage cost was 7360 bits.

In Chuang and Tseng's scheme [34], the transmitted messages are $\{AID, N_i, ACAKE\}$, $\{N_B, v_B\}$, and $\{v_i\}$, where $\{AID, N_i, ACAKE, N_B\}$ belong to G_1 and $\{v_B, v_i\}$ belong to F_n^*. The communication cost is 4416 bits. The stored messages are $\{ID_i, t, Q_i, MPK_t, HLP_i\}$, $\{ID_j, t, Q_j, MPK_t\}$, and $\{ID_l, t, Q_l, MPK_t, HLP_l\}$, where $\{Q_i, MPK_t, Q_j, MPK_t, Q_l, MPK_t\}$ belong to G_1 and $\{ID_i, t, HLP_i, ID_j, t, ID_l, t, HLP_l\}$ belong to F_n^*. The storage cost was 7424 bits.

Table 5: Computation cost comparison.

	[32]	[33]	[34]	[35]	Ours
User	$2T_m + T_a + T_{ex} + 8T_h \approx 31.837$ ms	$T_f + 2T_{ex} + 10T_h \approx 18.463$ ms	$2T_{map} + 2T_{mtp} + 3T_m + 4T_h \approx 173.029$ ms	$T_{map} + T_{mtp} + 2T_m + 5T_h \approx 93.385$ ms	$T_f + 3T_{ex} + 10T_h \approx 20.712$ ms
Server	$2T_{map} + 4T_{ex} + 2T_m + 5T_h \approx 16.575$ ms	$T_{map} + T_{mtp} + 4T_{ex} + T_m + 6T_h \approx 14.483$ ms	$T_{map} + T_{mtp} + 2T_m + 5T_h \approx 15.285$ ms	$5T_{map} + 8T_{ex} + 6T_m + 2T_h \approx 42.851$ ms	$T_{map} + T_{mtp} + 4T_{ex} + 5T_h \approx 12.311$ ms
Total	48.412 ms	32.946 ms	188.314 ms	136.236 ms	33.023 ms

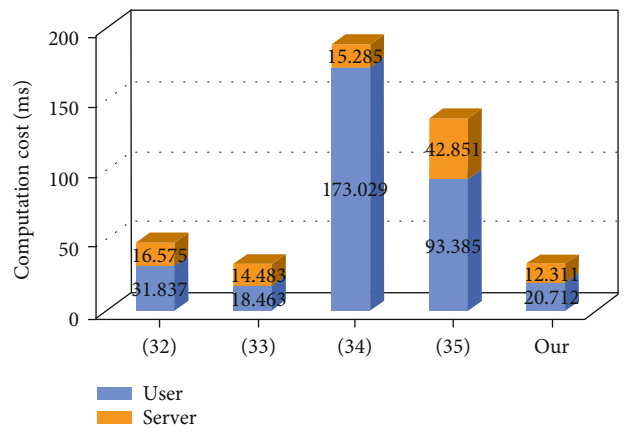


Figure 7: Computation cost comparison.

Table 6: Communication and storage cost comparison.

	Rounds	Communication cost (bits)	Storage cost (bits)
[32]	3	2368	3392
[33]	3	3872	7360
[34]	3	4416	7424
[35]	3	6944	8192
Our	3	3712	2848

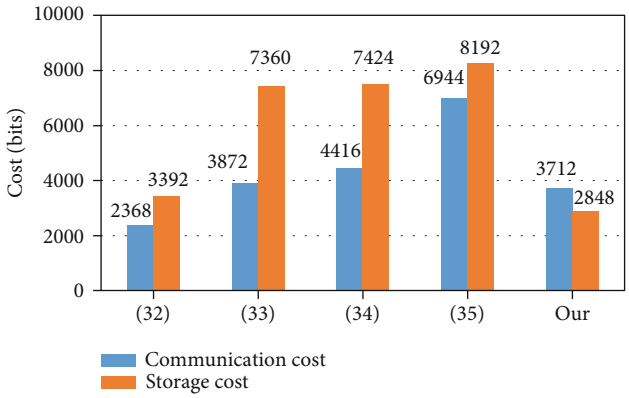


Figure 8: Communication and storage cost comparison.

In Tseng et al.'s scheme [35], the transmitted messages are $\{ID_c, QT_c, QU_c, X, n_c, Sig_c\}$, $\{Y_1, Y_2, Auth_s, n_s\}$, and $\{Auth_c\}$, where $\{X, n_c, Sig_c, Y_1, Y_2, n_s\}$ belong to G_1 and $\{ID_c, QT_c, QU_c, Auth_s Auth_c\}$ belong to F_n^*. The communication cost is 3872 bits. The stored messages are $\{SU_{c,0,1}, SU_{c,0,2}\}$, $\{XU_{c,0,1}, XU_{c,0,2}\}$, $\{SU_{s,0,1}, SU_{s,0,2}\}$, and $\{XU_{s,0,1}, XU_{s,0,2}\}$, where $\{SU_{c,0,1}, SU_{c,0,2}, XU_{c,0,1}, XU_{c,0,2}, SU_{s,0,1}, SU_{s,0,2}, XU_{s,0,1}, XU_{s,0,2}\}$ belong to G_1. The storage cost was 8192 bits.

In the proposed scheme, the transmitted messages are $\{F_{ui}, Y_{ui}, P_{ui}, V_1\}$, $\{V_2, Y_{sj}\}$, and $\{V_2\}$, where $\{Y_{ui}, P_{ui}, Y_{sj}\}$ belong to G_1 and $\{F_{ui}, V_1, V_2, V_3\}$ belong to F_n^*. The communication cost is 3712 bits. The stored messages are $\{Tab_{U_i}, V_{ui}, E_{ui}, \theta_{ui}, P_{ui}\}$ and $\{C_{ui}, t\}$, where $\{Tab_{U_i}, V_{ui}, E_{ui}, \theta_{ui}, t\}$ belong to G_1 and $\{P_{ui}, C_{ui}\}$ belong to F_n^*. The storage cost was 2848 bits.

Table 6 summarizes the communication and storage costs of the five schemes. It can be noticed that the communication cost of the proposed scheme is lower than that of [33–35] but slightly higher than that of [32]. However, [32] is subject to offline identity guessing and impersonation attacks. Furthermore, our scheme has the lowest storage cost. Figure 8 more intuitively shows the comparison of communication and storage costs between our scheme and [32–35].

6. Conclusion

Many researchers have proposed solutions for authentication in the multiserver architecture of the client-server mode, but most of them have some security vulnerabilities. In addition, the development of 5G technology has gradually matured, which can bring users a superfast online experience. Therefore, we proposed a secure key management protocol to protect user anonymity based on the multiserver architecture of the client-server mode in 5G. Through formal and informal analyses, we proved that our scheme has better security. Furthermore, the performance estimate confirms that the proposed scheme has higher advantages than similar schemes. Therefore, the proposed scheme is more suitable for the client-server mode of the multiserver in 5G.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1383–1396, Toronto, Canada, 2018.

[2] H. Viswanathan and P. E. Mogensen, "Communications in the 6G era," *IEEE Access*, vol. 8, pp. 57063–57074, 2020.

[3] E. K. Wang, X. Liu, C.-M. Chen, S. Kumari, M. Shojafar, and M. S. Hossain, "Voice-transfer attacking on industrial voice control systems in 5G-aided IIoT domain," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 7085–7092, 2020.

[4] P. Wang, C.-M. Chen, S. Kumari, M. Shojafar, R. Tafazolli, and Y.-N. Liu, "HDMA: hybrid D2D message authentication scheme for 5G-enabled VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5071–5080, 2021.

[5] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6428–6453, 2018.

[6] H. Xiong, Y. Wu, C. Jin, and S. Kumari, "Efficient and privacy-preserving authentication protocol for heterogeneous systems in IIoT," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11713–11724, 2020.

[7] H. Xiong, Y. Zhao, Y. Hou et al., "Heterogeneous signcryption with equality test for IIoT environment," *IEEE Internet of Things Journal*, 2020.

[8] M. A. Khan, I. Ullah, S. Nisar et al., "Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Information Systems*, vol. 2020, Article ID 8861947, 15 pages, 2020.

[9] M. Asghar Khan, I. Ullah, A. Alkhalifah et al., "A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

[10] B. Ying and A. Nayak, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography," *Journal of Network and Computer Applications*, vol. 131, pp. 66–74, 2019.

[11] I.-U. Haq, J. Wang, and Y. Zhu, "Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks," *Journal of Network and Computer Applications*, vol. 161, article 102660, 2020.

[12] L.-H. Li, L.-C. Lin, and M.-S. Hwang, "A remote password authentication scheme for multiserver architecture using neural networks," *IEEE Transactions on Neural Networks*, vol. 12, no. 6, pp. 1498–1504, 2001.

[13] X. Li, J. Liao, J. Zhang, J. Niu, and S. Kumari, "A secure remote user mutual authentication scheme using smart cards," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 89–92, Beijing, China, 2014.

[14] M. Karuppiah, "Remote user authentication scheme using smart card: a review," *International Journal of Internet Protocol Technology*, vol. 9, no. 2/3, pp. 107–120, 2016.

[15] T.-Y. Wu, Z. Lee, M. S. Obaidat, S. Kumari, S. Kumar, and C.-M. Chen, "An authenticated key exchange protocol for multi-server architecture in 5G networks," *IEEE Access*, vol. 8, pp. 28096–28108, 2020.

[16] I.-C. Lin, M.-S. Hwang, and L.-H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13–22, 2003.

[17] Xiang Cao and Sheng Zhong, "Breaking a remote user authentication scheme for multi-server architecture," *IEEE Communications Letters*, vol. 10, no. 8, pp. 580-581, 2006.

[18] W.-S. Juang, "Efficient multi-server password authenticated key agreement using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 251–255, 2004.

[19] C.-C. Chang and J.-S. Lee, "An efficient and secure multi-server password authentication scheme using smart cards," in *2004 international conference on cyberworlds*, pp. 417–422, Tokyo, Japan, 2004.

[20] Y.-P. Liao and S.-S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 24–29, 2009.

[21] H.-C. Hsiang and W.-K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, vol. 31, no. 6, pp. 1118–1123, 2009.

[22] Y. Luo, W.-M. Zheng, and Y.-C. Chen, "An anonymous authentication and key exchange protocol in smart grid," *Journal of Network Intelligence*, vol. 6, no. 2, pp. 206–215, 2021.

[23] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, 2010.

[24] X. Li, J.-W. Niu, J. Ma, W.-D. Wang, and C.-L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 73–79, 2011.

[25] E.-J. Yoon and K.-Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *The Journal of Supercomputing*, vol. 63, no. 1, pp. 235–255, 2013.

[26] Y.-P. Liao and C.-M. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients," *Future Generation Computer Systems*, vol. 29, no. 3, pp. 886–900, 2013.

[27] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, "Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme," in *Computational Science and Its Applications – ICCSA 2012*, pp. 391–406, Springer, 2012.

[28] W.-B. Hsieh and J.-S. Leu, "An anonymous mobile user authentication protocol using self-certified public keys based on multi-server architectures," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 133–148, 2014.

[29] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1411–1418, 2014.

[30] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards," *Expert Systems with Applications*, vol. 41, no. 18, pp. 8129–8143, 2014.

[31] Y. Lu, L. Li, H. Peng, and Y. Yang, "A biometrics and smart cards-based authentication scheme for multi-server environments," *Security and Communication Networks*, vol. 8, no. 17, 3228 pages, 2015.

[32] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2052–2064, 2016.

[33] W. Li, L. Xuelian, J. Gao, and H. Y. Wang, "Design of secure authenticated key management protocol for cloud computing environments," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2019.

[34] Y. H. Chuang and Y. M. Tseng, "CAKE: compatible authentication and key exchange protocol for a smart city in 5G networks," *Symmetry*, vol. 13, no. 4, p. 698, 2021.

[35] Y. M. Tseng, J. L. Chen, and S. S. Huang, "A lightweight leakage-resilient identity-based mutual authentication and key exchange protocol for resource-limited devices," *Computer Networks*, vol. 196, article 108246, 2021.

[36] Y.-S. Jheng, R. Tso, C.-M. Chen, and M.-E. Wu, "Password-based authenticated key exchange from lattices for client/server model," in *Advances in Computer Science and Ubiquitous Computing*, pp. 315–319, Springer, 2017.

[37] T.-Y. Wu, L. Yang, Z. Lee, C.-M. Chen, J.-S. Pan, and S. Islam, "Improved ECC-based three-factor multiserver authentication scheme," *Security and Communication Networks*, vol. 2021, Article ID 6627956, 14 pages, 2021.

[38] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.

[39] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1953–1966, 2015.

[40] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[41] M. Abadi and C. Fournet, "Mobile values, new names, and secure communication," *ACM SIGPLAN Notices*, vol. 36, no. 3, pp. 104–115, 2001.

[42] B. Blanchet, "A computationally sound mechanized prover for security protocols," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 4, pp. 193–207, 2008.

[43] T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian, and N. A. Al-Nabhan, "An enhanced pairing-based authentication scheme for smart grid communications," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–13, 2021.

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 1717585, 10 pages
https://doi.org/10.1155/2021/1717585

Research Article

Relay Selection-and-Jamming Scheme with Nonlinear Energy Harvesting

Triet Pham-Minh,[1] **Khuong Ho-Van**,[2,3] **Hoa Nguyen-Minh**,[1] **and Khanh Nghi-Vinh**[1]

[1]*Tra Vinh University, Vietnam*
[2]*Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City, Vietnam*
[3]*Vietnam National University Ho Chi Minh City, Linh Trung Ward, Thu Duc District, Ho Chi Minh City, Vietnam*

Correspondence should be addressed to Khuong Ho-Van; hvkhuong@hcmut.edu.vn

Received 19 August 2021; Revised 15 September 2021; Accepted 25 September 2021; Published 11 October 2021

Academic Editor: Muhammad Asghar Khan

When direct source-destination communications are in outage, relay selection is a preferable solution to improve reliability for this communications. However, such a relay selection makes the eavesdropper better overhear source data through both source-relay and relay-destination communication hops, losing data security. To improve both reliability and security, this paper proposes a relay selection-and-jamming (RaJ) scheme to select one intermediate node as a conventional relay and another node as a jammer. To enhance energy efficiency, all intermediate nodes harvest radio frequency energy in source signals for their operations with nonlinear energy harvesting (NL-EH). The security and reliability of the RaJ scheme are assessed through suggested rigorous/asymptotic expressions and are significantly better than two benchmark schemes without neither jamming nor both relay selection and jamming. Additionally, they can be optimized with reasonable selection of specifications. Moreover, the NL property of the energy harvesters dramatically affects the reliability but negligibly degrades the security for the RaJ scheme. Furthermore, the linear EH (L-EH) is more reliable but less secure than the NL-EH.

1. Introduction

1.1. Background. Radio frequency energy harvesting (RF EH), which exploits available RF signals to power communication devices, can solve problems of energy efficiency, energy shortage, and green communications in modern wireless systems [1–4]. RF EH is efficiently implemented through power-splitting (PS) and time-switching (TS) protocols in which the former carries out EH and data decoding in the same duration while the latter performs them separately in different durations (i.e., the latter requires lower circuitry implementation than the former) [5]. For performance analysis, EH has been modelled as linear (L) [6] or NL [7]. The linear EH (L-EH) model represents the linear increase of the scavenged energy with the input RF power. Nonetheless, nonlinear (NL) behaviors of EH circuit elements (e.g., diodes and inductors) induce the NL-EH model more realistic and precise than the L-EH one. As such, this paper is interested in the NL-EH model for practical-and-exact performance analysis.

When direct source-destination communications are in outage due to severe propagation conditions (strong path-loss, heavy shadowing, and deep fading), relay selection in which only one intermediate node among all available nodes between the source-destination pair is selected to satisfy a preset criterion is regarded as a technique that is efficient in improving communication reliability and reducing complexity as well as economical in bandwidth and power [8]. Nonetheless, such a relay selection offers the eavesdropper more chances to overhear source message through both source-relay and relay-destination communication hops instead of merely one hop in direct source-destination communications, threatening data security. To conceal

legitimate data, the jamming technique where jamming signals (or artificial noises) are purposively generated to impair solely the eavesdropper has been popularly exploited [9].

This paper assumes two intermediate nodes, which are self-powered by scavenging RF energy in source signals with the practical NL-EH, are willing to ameliorate both reliability and security for data transmission between the source-destination pair. The question is which node plays a role as a traditional relay to enhance communication reliability and as a jammer to protect secret data over both hops. Our solution, relay selection-and-jamming (RaJ) scheme, solves this question.

1.2. Previous Works. Our proposed RaJ scheme differs [7, 10–22] which investigated problems of security and/or reliability for the NL-EH (References which studied the L-EH with/without relaying (e.g., [5, 6, 9]) or the NL-EH without relaying (e.g., [23–35]) must not be surveyed because this paper considers simultaneously the NL-EH, relaying, and jamming.) with relaying. More specifically, [7, 10] analyzed the reliability of the pure relaying (namely, the nonrelay selection nonjamming (nRnJ)) scheme in terms of outage probability (OP). In the nRnJ scheme in [7, 10], the relay performs the amplify-and-forward (AF) operation on source signals with energy harvested by the TS protocol. Reconsidering the nRnJ scheme and the AF relay in [7, 10], the authors in [11, 12] analyzed and simulated the reliability in terms of bit error rate and throughput, respectively. Additionally, both [11, 12] utilized the PS protocol for scavenging energy in source signals. Secrecy performance quantified by secrecy outage probability was simulated in [13], and the OP was analyzed in [14–20] for the same nRnJ scheme as [7]. Notwithstanding, all the works in [13–20] investigated the decode-and-forward (DF) relay, which is also a research object of this paper. As compared to the AF relay, the DF relay is advantageous in preventing noise enhancement, probably improving the overall system performance. In [21], the throughput was simulated for the nonrelay selection-and-jamming (nRaJ) scheme where one relay capable of EH is appointed as a conventional relay and another user is dedicated as an energy supplier as well as a jammer. Instead of dedicating an intermediate node as a jammer in [21], the authors in [22] availed the destination as a jammer. Further, [22] considered the AF relay and the energy harvesting based on the PS protocol. However, the performance analysis on the ergodic secrecy capacity and the total harvested energy was not included in [22].

1.3. Contributions. Beside proposing the RaJ scheme with the NL-EH, this paper suggests the rigourous/asymptotic formulas of the OP and the intercept probability (IP) to quickly assess both reliability and security. These expressions are then simplified to obtain the OP/IP of the nRnJ and RnJ (relay selection nonjamming) schemes for performance comparison and highlighting the efficacy of simultaneous relay selection and jamming. Moreover, the OP/IP of the RaJ scheme with the L-EH is derived. Monte-Carlo simulations validate these analyses and shed insights into the reliability/security of the considered schemes and the feature of the NL-EH in comparison to the L-EH.

1.4. Structure. The remainder of this paper is structured as follows. Part 2 describes the investigated system. Next, part 3 provides detailed derivations of reliability and security of the proposed RaJ scheme. Then, two (nRnJ and RnJ) benchmark schemes are discussed in part 4. Subsequently, some useful remarks are withdrawn in part 5, especially the remark on the L-EH. Finally, part 6 presents simulated/theoretical results, and part 7 closes the paper.

2. System Description

Figure 1 sketches the considered RaJ scheme where the source S fails to convey secret messages directly to the destination D owing to bad propagation conditions (e.g., severe fading and strong shadowing). Therefore, two intermediate nodes, R_0 and R_1, are exploited with different roles as a traditional relay R to heal $S \longrightarrow D$ communications and as a jammer J to protect secret data against the eavesdropper E. To improve energy efficiency, R_0 and R_1 scavenge RF energy in source signals through the TS protocol and utilize scavenged energy for relaying and jamming operations. Accordingly, secret data reaches D in three stages with an entire duration of T.

In stage I with (Stage I is just for energy harvesting. Consequently, S transmits an arbitrary signal, which carries RF energy, not necessarily the secret information or a deterministic signal.) a duration of αT, the nonlinear energy harvester of R_i, $i = \{0, 1\}$, generates the power [7]:

$$P_{r_i} = \begin{cases} A_i P_s g_{sr_i} & , P_s g_{sr_i} \le \zeta_{\text{th}}, \\ A_i \zeta_{th} & , P_s g_{sr_i} > \zeta_{\text{th}}, \end{cases} \quad (1)$$

where $A_i = 2\vartheta_i\alpha/(1-\alpha)$; ϑ_i is energy converting efficiency; α is a time fraction; P_s is the transmission power of S; ζ_{th} is the saturation threshold; $g_{sr_i} = |h_{sr_i}|^2$ is the $S \longrightarrow R_i$ channel gain. Flat block Rayleigh fading channels are considered, and hence, h_{sr_i} is modelled ($h_{xy} \sim \mathcal{CN}(0, \lambda_{xy})$ notates a zero-mean λ_{xy}-variance complex Gaussian random variable. Therefore, $g_{xy} = |h_{xy}|^2$ obeys exponential distribution with mean λ_{xy}, shortly denoted as $g_{xy} \sim \mathcal{E}(\lambda_{xy})$, resulting in its cumulative distribution function (CDF) and the probability density function (PDF) as $F_{g_{xy}}(w) = 1 - e^{-w/\lambda_{xy}}$ and $f_{g_{xy}}(w) = e^{-w/\lambda_{xy}}/\lambda_{xy}$, respectively, where $w \ge 0$.) as $h_{sr_i} \sim \mathcal{CN}(0, \lambda_{sr_i})$ and is unchanged during T but changes independently in the next T. To guarantee S's messages to be restored correctly at the intermediate nodes with the highest possibility, ultimately limiting error propagation as much as possible, R_i and R_j with $j = 1 - i$ are selected as the conventional relay and the jammer, respectively, if $g_{sr_i} > g_{sr_j}$ (i.e., the $S - R_i$ channel is better than the $S \longrightarrow R_j$ channel).

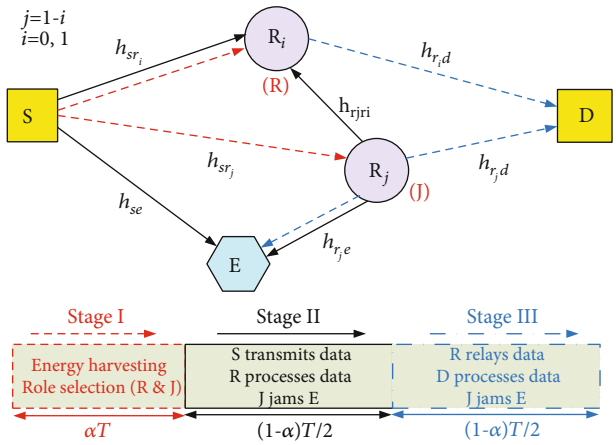


Figure 1: System model.

In stage II with a duration of $(1-\alpha)T/2$, S transmits secret data while R_j jams E for securing S's data. Therefore, signals received at E and R_i have an unique form as

$$y_m^{\mathrm{II}} = h_{sm}\sqrt{P_s}x_s + h_{r_jm}\sqrt{P_{r_j}}x_{r_j} + n_m, \tag{2}$$

where $m \in \{r_i, e\}$; x_s and x_{r_j} are the unit-power transmit symbols of S and R_j, correspondingly; $g_{sm} = |h_{sm}|^2 \sim \mathscr{E}(\lambda_{sm})$ and $g_{r_jm} = |h_{r_jm}|^2 \sim \mathscr{E}(\lambda_{r_jm})$ are the $S \longrightarrow m$ and $R_j \longrightarrow m$ channel gains, respectively; $n_m \sim \mathscr{CN}(0, \sigma^2)$ is the additive noise at the receiver m.

The jamming signal x_{r_j} created by R_j is deliberate to impair solely the wire-tapping of E without degrading signal reception of desired users (R_i and D). Such a special characteristic of x_{r_j} can come from pseudo-random signal generators whose seeds are securely shared only among D, R_j, and R_i [9, 21, 36–44]. Consequently, R_i and D can regenerate exactly x_{r_j} and entirely eliminate it, ultimately creating the signal received at R_i in stage II as

$$\tilde{y}_{r_i}^{\mathrm{II}} = h_{sr_i}\sqrt{P_s}x_s + n_{r_i}, \tag{3}$$

from which the signal-to-noise ratio (SNR) at R_i is established as

$$\Omega_{sr_i} = \frac{P_s g_{sr_i}}{\sigma^2}. \tag{4}$$

Generating x_{r_j} is solely known at D, R_i, and R_j for hiding x_s but E is blind with it. As such, the signal-to-interference plus noise ratio (SINR) which E obtains for restoring x_s in stage II is calculated from (2) to be

$$\Omega_{se} = \frac{P_s g_{se}}{P_{r_j} g_{r_je} + \sigma^2}. \tag{5}$$

In stage III with a duration of $(1-\alpha)T/2$, R_i decodes and forwards S's data while R_j interrupts E for securing R_i's transmission. Accordingly, signals received at D and E have an unique form as

$$y_w^{\mathrm{III}} = h_{r_iw}\sqrt{P_{r_i}}x_{r_i} + h_{r_jw}\sqrt{P_{r_j}}x_{r_j} + n_w, \tag{6}$$

where $w \in \{d, e\}$; x_{r_i} is the unit-power transmit symbol of R_i; $g_{r_jw} = |h_{r_jw}|^2 \sim \mathscr{E}(\lambda_{r_jw})$ and $g_{r_iw} = |h_{r_iw}|^2 \sim \mathscr{E}(\lambda_{r_iw})$ are the $R_j \longrightarrow w$ and $R_i \longrightarrow w$ channel gains, correspondingly; $n_w \sim \mathscr{CN}(0, \sigma^2)$ is the additive noise at the receiver w.

Thanks to the property of the jamming signal x_{r_j} and processing it similarly as stage II, the SNR at D and the SINR at E in stage III are correspondingly given by

$$\Omega_{r_id} = \frac{P_{r_i} g_{r_id}}{\sigma^2}, \tag{7}$$

$$\Omega_{r_ie} = \frac{P_{r_i} g_{r_ie}}{P_{r_j} g_{r_je} + \sigma^2}. \tag{8}$$

The decode-and-forward operation of R_i results in aggregated SINR at D for restoring x_s as

$$\Omega_d = \min\left(\Omega_{sr_i}, \Omega_{r_id}\right). \tag{9}$$

Since E receives signals in both stages, it can perform selection-combining them for higher intercept possibility [45], yielding the aggregated SINR as

$$\Omega_e = \max\left(\Omega_{se}, \Omega_{r_ie}\right). \tag{10}$$

The channel capacity available at w for restoring x_s is represented to be

$$\mathbb{C}_w = \frac{1-\alpha}{2}\log_2(1+\Omega_w). \tag{11}$$

3. The Proposed RaJ Scheme

Communication reliability and data security can be measured through the OP at D and the IP at E, respectively. These probability expressions of the proposed RaJ scheme are first derived in this part to quickly evaluate both reliability and security without exhaustive simulations. Then, by simplifying them, the OP and the IP of two benchmark RnJ and nRnJ schemes are inferred in the next part to facilitate performance comparison and show the efficacy of simultaneous relay selection and jamming.

3.1. Intercept Probability. The IP is addressed as the probability which E restores x_s successfully. According to information theory, given a preset transmission rate $\mathbb{R}$, the IP is the probability that $\mathbb{R}$ is smaller than $\mathbb{C}_e$, namely,

$$I^{\mathrm{RaJ}} = \mathbb{P}\{\mathbb{C}_e \geq \mathbb{R}\} = \mathbb{P}\{\Omega_e \geq \bar{\Omega}\}, \tag{12}$$

where $\bar{\Omega} = 2^{2\mathbb{R}/(1-\alpha)} - 1$ and $\mathbb{P}\{\cdot\}$ is the probability operator.

Inserting (10) into (12), one obtains

$$\begin{aligned} I^{\mathrm{RaJ}} &= \mathbb{P}\left\{\max\left(\Omega_{se}, \Omega_{r_i e}\right) \geq \bar{\Omega}\right\} \\ &= 1 - \mathbb{P}\left\{\max\left(\Omega_{se}, \Omega_{r_i e}\right) < \bar{\Omega}\right\} \overset{(a)}{=} 1 \\ &\quad - \sum_{i=0}^{1} \underbrace{\mathbb{P}\left\{\Omega_{se} < \bar{\Omega}, \Omega_{r_i e} < \bar{\Omega}, g_{sr_i} > g_{sr_j}\right\}}_{\bar{I}}, \end{aligned} \tag{13}$$

where $=^{(a)}$ follows the total probability law and the event $\{g_{sr_i} > g_{sr_j}\}$ means R_i as a conventional relay while R_j as a jammer.

Let $X = g_{sr_i}$, $Y = g_{sr_j}$, and $Z = P_{r_j} g_{r_j e} + \sigma^2$. Then, plugging (5) and (8) into $\bar{I}$ in (13) results in

$$\bar{I} = \Xi_{X,Y}\left\{ \underbrace{\mathbb{P}\left\{P_s g_{se} < \bar{\Omega} Z, P_{r_i} g_{r_i e} < \bar{\Omega} Z\right\}}_{\tilde{I}} \middle| X > Y \right\}, \tag{14}$$

where $\Xi\{\cdot\}$ is the expectation operator.

$\tilde{I}$ in (14) is expressed in closed-form as

$$\begin{aligned} \tilde{I} &= \Xi_Z\left\{ F_{g_{se}}\left(\frac{\bar{\Omega} Z}{P_s}\right) F_{g_{r_i e}}\left(\frac{\bar{\Omega} Z}{P_{r_i}}\right) \right\} \\ &= \int_0^{\infty} \left(1 - e^{-\bar{\Omega}\left(P_{r_j} x + \sigma^2\right)/P_s \lambda_{se}}\right) \left(1 - e^{-\bar{\Omega}\left(P_{r_j} x + \sigma^2\right)/P_{r_i} \lambda_{r_i e}}\right) \frac{e^{-x/\lambda_{r_j e}}}{\lambda_{r_j e}} dx \\ &= 1 - \frac{e^{-\bar{\Omega}\sigma^2/P_s \lambda_{se}}}{\bar{\Omega} P_{r_j} \lambda_{r_j e}/P_s \lambda_{se} + 1} - \frac{e^{-\bar{\Omega}\sigma^2/P_{r_i} \lambda_{r_i e}}}{\bar{\Omega} P_{r_j} \lambda_{r_j e}/P_{r_i} \lambda_{r_i e} + 1} \\ &\quad + \frac{e^{-\bar{\Omega}\sigma^2/P_s \lambda_{se} - \bar{\Omega}\sigma^2/P_{r_i} \lambda_{r_i e}}}{\bar{\Omega} P_{r_j} \lambda_{r_j e}/P_s \lambda_{se} + \bar{\Omega} P_{r_j} \lambda_{r_j e}/P_{r_i} \lambda_{r_i e} + 1}. \end{aligned} \tag{15}$$

Based on (1), four combinations of (P_{r_i}, P_{r_j}) are considered when deriving (14) as follows.

Combination 1: $(P_{r_i}, P_{r_j}) = (A_i P_s g_{sr_i}, A_j P_s g_{sr_j})$

This combination holds when $X \leq \zeta_{\mathrm{th}}/P_s$ and $Y \leq \zeta_{\mathrm{th}}/P_s$. Incorporating these conditions with $X > Y$ in (14) results in existence region of (X, Y) as $Y \leq X$ and $X \leq \zeta_{\mathrm{th}}/P_s$. By averaging $\tilde{I}$ in (15) over this region, one obtains $\bar{I}$ for this combination as

$$\bar{I}_1 = \frac{1}{\lambda_{sr_i}} \int_0^{\zeta_{\mathrm{th}}/P_s} I_1 e^{-x/\lambda_{sr_i}} dx, \tag{16}$$

where

$$I_1 = \frac{1}{\lambda_{sr_j}} \int_0^{X} \tilde{I} e^{-y/\lambda_{sr_j}} dy. \tag{17}$$

Invoking $\tilde{I}$ in (15) with $(P_{r_i}, P_{r_j}) = (A_i P_s X, A_j P_s Y)$ and after some simplifications, the integral in (17) is solved as

$$\begin{aligned} I_1 &= 1 - e^{-X/\lambda_{sr_j}} - \frac{\lambda_{se} e^{-\bar{\Omega}\sigma^2/P_s \lambda_{se}}}{\bar{\Omega} A_j \lambda_{r_j e} \lambda_{sr_j}} \\ &\quad \cdot \left[\Theta\left(X, \frac{1}{\lambda_{sr_j}}, \frac{\lambda_{se}}{\bar{\Omega} A_j \lambda_{r_j e}}\right) + \frac{A_i \lambda_{r_i e} X}{\lambda_{se}} e^{\bar{\Omega}\sigma^2/P_s \lambda_{se} - \frac{\bar{\Omega}\sigma^2}{A_i P_s \lambda_{r_i e} X}} \Theta \right. \\ &\quad \cdot \left(X, \frac{1}{\lambda_{sr_j}}, \frac{A_i \lambda_{r_i e} X}{\bar{\Omega} A_j \lambda_{r_j e}}\right) - \frac{e^{-\bar{\Omega}\sigma^2/A_i P_s \lambda_{r_i e} X}}{1 + \lambda_{se}/A_i \lambda_{r_i e} X} \Theta \\ &\quad \left. \cdot \left(X, \frac{1}{\lambda_{sr_j}}, \frac{1}{\bar{\Omega} A_j \lambda_{r_j e}/\lambda_{se} + \bar{\Omega} A_j \lambda_{r_j e}/A_i \lambda_{r_i e} X}\right) \right], \end{aligned} \tag{18}$$

where $\Theta(a, b, c) = \int_0^a e^{-bx}/(x + c) dx = e^{bc}[\mathrm{E}i(-ab - bc) - Ei(-bc)]$ with $Ei\{\cdot\}$ is the exponential integral [46].

Combination 2: $(P_{r_i}, P_{r_j}) = (A_i P_s g_{sr_i}, A_j \zeta_{\mathrm{th}})$

This combination holds when $X \leq \zeta_{\mathrm{th}}/P_s$ and $Y > \zeta_{\mathrm{th}}/P_s$. Incorporating these conditions with $X > Y$ in (14) results in empty region of (X, Y). Therefore, one obtains $\bar{I}$ for this combination as

$$\bar{I}_2 = 0. \tag{19}$$

Combination 3: $(P_{r_i}, P_{r_j}) = (A_i \zeta_{\mathrm{th}}, A_j P_s g_{sr_j})$

This combination holds when $X > \zeta_{\mathrm{th}}/P_s$ and $Y \leq \zeta_{\mathrm{th}}/P_s$. Incorporating these conditions with $X > Y$ in (14) results in existence region of (X, Y) as $X > \zeta_{\mathrm{th}}/P_s$ and $Y \leq \zeta_{\mathrm{th}}/P_s$. By averaging $\tilde{I}$ in (15) over this region, one obtains $\bar{I}$ for this combination as

$$\bar{I}_3 = \underbrace{\int_{\zeta_{\mathrm{th}}/P_s}^{\infty} f_X(x) dx}_{\bar{I}_{31}} \underbrace{\int_0^{\zeta_{\mathrm{th}}/P_s} \tilde{I} f_Y(y) dy}_{\bar{I}_{32}}, \tag{20}$$

where $\bar{I}_{31} = e^{-\zeta_{\mathrm{th}}/P_s \lambda_{sr_i}}$ and $\bar{I}_{32}$ is expressed in closed-form as follows after invoking $\tilde{I}$ in (15), substituting (P_{r_i}, P_{r_j}) with $(A_i \zeta_{\mathrm{th}}, A_j P_s Y)$ and executing simplifications:

$$\begin{aligned} \bar{I}_{32} &= 1 - e^{-\zeta_{\mathrm{th}}/P_s \lambda_{sr_j}} - \frac{\lambda_{se} e^{-\bar{\Omega}\sigma^2/P_s \lambda_{se}}}{\bar{\Omega} A_j \lambda_{sr_j} \lambda_{r_j e}} \left[\Theta\left(\frac{\zeta_{\mathrm{th}}}{P_s}, \frac{1}{\lambda_{sr_j}}, \frac{\lambda_{se}}{\bar{\Omega} A_j \lambda_{r_j e}}\right) \right. \\ &\quad + \frac{A_i \lambda_{r_i e} \zeta_{\mathrm{th}}}{\lambda_{se} P_s} e^{\bar{\Omega}\sigma^2/P_s \lambda_{se} - \bar{\Omega}\sigma^2/A_i \lambda_{r_i e} \zeta_{\mathrm{th}}} \Theta \\ &\quad \cdot \left(\frac{\zeta_{\mathrm{th}}}{P_s}, \frac{1}{\lambda_{sr_j}}, \frac{A_i \lambda_{r_i e} \zeta_{\mathrm{th}}}{\bar{\Omega} A_j \lambda_{r_j e} P_s}\right) - \frac{e^{-\bar{\Omega}\sigma^2/A_i \lambda_{r_i e} \zeta_{\mathrm{th}}}}{1 + \lambda_{se} P_s/A_i \lambda_{r_i e} \zeta_{\mathrm{th}}} \Theta \\ &\quad \left. \cdot \left(\frac{\zeta_{\mathrm{th}}}{P_s}, \frac{1}{\lambda_{sr_j}}, \frac{1}{\bar{\Omega} A_j \lambda_{r_j e}/\lambda_{se} + \bar{\Omega} A_j \lambda_{r_j e} P_s/A_i \lambda_{r_i e} \zeta_{\mathrm{th}}}\right) \right]. \end{aligned} \tag{21}$$

Combination 4: $(P_{r_i}, P_{r_j}) = (A_i \zeta_{\mathrm{th}}, A_j \zeta_{\mathrm{th}})$

This combination holds when $X > \zeta_{\mathrm{th}}/P_s$ and $Y > \zeta_{\mathrm{th}}/P_s$. Incorporating these conditions with $X > Y$ in (14) results

in existence region of (X, Y) as $X > Y$ and $Y > \zeta_{\text{th}}/P_s$. By averaging $\tilde{I}$ in (15) over this region, one obtains $\bar{I}$ for this combination as

$$\bar{I}_4 = \int_{\zeta_{\text{th}}/P_s}^{\infty} \left[\int_{y}^{\infty} \tilde{I}_4 f_X(x) dx \right] f_Y(y) dy = \frac{e^{-\left(\lambda_{sr_i} + \lambda_{sr_j}\right)\zeta_{\text{th}}/\lambda_{sr_i}\lambda_{sr_j}P_s}}{1 + \lambda_{sr_j}/\lambda_{sr_i}} \tilde{I}_4, \tag{22}$$

where $\tilde{I}_4$ is $\tilde{I}$ in (15) with $(P_{r_i}, P_{r_j}) = (A_i\zeta_{\text{th}}, A_j\zeta_{\text{th}})$, which is a constant.

Now it is ready to simplify (13) using the total probability law as

$$I^{\text{RaJ}} = 1 - \sum_{i=0}^{1} \sum_{k=1}^{4} \bar{I}_k = 1 - \sum_{i=0}^{1} \left(\bar{I}_1 + \bar{I}_{31}\bar{I}_{32} + \bar{I}_4 \right). \tag{23}$$

The asymptotic IP, $I_{\text{asym}}^{\text{RaJ}}$, is obtained when P_s approaches infinity. In the asymptotic region, only the combination 4 happens and hence,

$$I_{\text{asym}}^{\text{RaJ}} = 1 - \lim_{P_s \longrightarrow \infty} \bar{I}_4 = 1, \tag{24}$$

which indicates a complete insecurity.

3.2. Outage Probability. The OP is addressed as the probability which E restores x_s unsuccessfully. Consequently, the OP is the probability that $\mathbb{R}$ is greater than $\mathbb{C}_d$, namely,

$$O^{\text{RaJ}} = \mathbb{P}\{\mathbb{C}_d \le \mathbb{R}\} = \mathbb{P}\{\Omega_d \le \bar{\Omega}\}. \tag{25}$$

Given Ω_d in (9), one rewrites (25) as

$$\begin{aligned} O^{\text{RaJ}} &= \mathbb{P}\{\min\left(\Omega_{sr_i}, \Omega_{r_i d}\right) < \bar{\Omega}\} \\ &= 1 - \mathbb{P}\{\min\left(\Omega_{sr_i}, \Omega_{r_i d}\right) > \bar{\Omega}\} \\ &= 1 - \sum_{i=0}^{1} \underbrace{\mathbb{P}\{\Omega_{sr_i} > \bar{\Omega}, \Omega_{r_i d} > \bar{\Omega}, X > Y\}}_{\bar{O}}. \end{aligned} \tag{26}$$

Plugging (4) and (7) into $\bar{O}$ in (26) results in

$$\begin{aligned} \bar{O} &= \Xi_{X,Y}\left\{ \mathbb{P}\left\{ g_{r_i d} > \frac{\bar{\Omega}\sigma^2}{P_{r_i}} \right\} \middle| X > Y, X > \frac{\bar{\Omega}\sigma^2}{P_s} \right\} \\ &= \Xi_{X,Y}\left\{ e^{-\bar{\Omega}\sigma^2/P_{r_i}\lambda_{r_i d}} \middle| X > Y, X > \frac{\bar{\Omega}\sigma^2}{P_s} \right\}. \end{aligned} \tag{27}$$

Based on (1), two cases of P_{r_i} are considered when deriving (27) as follows.

Case 1. $P_{r_i} = A_i P_s X$

This case holds when $X \le \zeta_{\text{th}}/P_s$. Incorporating this condition with $X > Y$ and $X > \bar{\Omega}\sigma^2/P_s$ in (27) results in existence region of (X, Y). More specifically, if $\bar{\Omega}\sigma^2 > \zeta_{\text{th}}$, then the existence region is empty and hence, $\bar{O}$ in (27) becomes $\bar{O}_1 = 0$. Otherwise, the existence region is $Y < X$ and $\bar{\Omega}\sigma^2/P_s < X \le \zeta_{\text{th}}/P_s$. By averaging $e^{-\bar{\Omega}\sigma^2/A_i P_s \lambda_{r_i d} x}$ in (27) over this region, one obtains $\bar{O}$ for this case as

$$\begin{aligned} \bar{O}_1 &= \int_{\bar{\Omega}\sigma^2/P_s}^{\zeta_{\text{th}}/P_s} e^{-\bar{\Omega}\sigma^2/A_i P_s \lambda_{r_i d} x} \left[\int_0^X f_Y(y) dy \right] f_X(x) dx \\ &= \frac{1}{\lambda_{sr_i}} \left[\Psi\left(\frac{\bar{\Omega}\sigma^2}{P_s}, \frac{\zeta_{\text{th}}}{P_s}, \frac{1}{\lambda_{sr_i}}, \frac{\bar{\Omega}\sigma^2}{A_i P_s \lambda_{r_i d}} \right) \right. \\ &\quad \left. - \Psi\left(\frac{\bar{\Omega}\sigma^2}{P_s}, \frac{\zeta_{\text{th}}}{P_s}, \frac{1}{\lambda_{sr_i}} + \frac{1}{\lambda_{sr_j}}, \frac{\bar{\Omega}\sigma^2}{A_i P_s \lambda_{r_i d}} \right) \right], \end{aligned} \tag{28}$$

where $\Psi(u, v, k, l)$ is given in (A.1) in Appendix A.

Case 2. $P_{r_i} = A_i\zeta_{\text{th}}$

This case holds when $X > \zeta_{\text{th}}/P_s$. Incorporating this condition with $X > Y$ and $X > \bar{\Omega}\sigma^2/P_s$ in (27) results in existence region of (X, Y) as $Y < X$ and $X > B$ where $B = \max(\bar{\Omega}\sigma^2, \zeta_{\text{th}})/P_s$. By averaging $e^{-\bar{\Omega}\sigma^2/A_i\lambda_{r_i d}\zeta_{\text{th}}}$ in (27) over this region, one obtains $\bar{O}$ for this case as

$$\begin{aligned} \bar{O}_2 &= e^{-\bar{\Omega}\sigma^2/A_i\lambda_{r_i d}\zeta_{\text{th}}} \int_B^{\infty} \left[\int_0^X \mathrm{f}_Y(y) dy \right] f_X(x) dx \\ &= e^{-\bar{\Omega}\sigma^2/A_i\lambda_{r_i d}\zeta_{\text{th}} - B/\lambda_{sr_i}} \left(1 - \frac{\lambda_{sr_j} e^{-B/\lambda_{sr_j}}}{\lambda_{sr_i} + \lambda_{sr_j}} \right). \end{aligned} \tag{29}$$

Now it is ready to simplify (26) using the total probability law as

$$O^{\text{RaJ}} = 1 - \sum_{i=0}^{1} \left(\bar{O}_1 + \bar{O}_2 \right). \tag{30}$$

The asymptotic OP, $O_{\text{asym}}^{\text{RaJ}}$, is obtained when P_s approaches infinity. In the asymptotic region, only the case 2 happens and hence,

$$O_{\text{asym}}^{\text{RaJ}} = 1 - \sum_{i=0}^{1} \lim_{P_s \longrightarrow \infty} \bar{O}_2 = 1 - \sum_{i=0}^{1} \frac{\lambda_{sr_i} e^{-\bar{\Omega}\sigma_d^2/A_i\lambda_{r_i d}\zeta_{\text{th}}}}{\lambda_{sr_i} + \lambda_{sr_j}}, \tag{31}$$

which indicates joint impact of three involved channels (λ_{sr_i}, λ_{sr_j}, and $\lambda_{r_i d}$) on communication reliability.

3.3. Comment. Both I^{RaJ} and O^{RaJ} in (23) and (30) are expressed in novel-and-exact forms, facilitating in evaluating swiftly both security and reliability of the proposed RaJ scheme with the NL-EH without exhaustive simulations. In addition, they are leveraged to derive performance measures for benchmark schemes as well as linear energy harvesters.

4. Benchmark Schemes (RnJ and nRnJ)

4.1. The RnJ Scheme. To evaluate the efficacy of the jamming operation in our scheme, we compare it with the only relay selection scheme (e.g., [6, 47]) which lets R_j be idle in our scheme, namely, the RnJ scheme. The OP of the RnJ scheme is the same as that of ours (i.e., $O^{\mathrm{RnJ}} = O^{\mathrm{RaJ}}$) but the IP of the former is different from that of the latter. Following the derivation of O^{RaJ} in (30) with the note that $P_{r_j} = 0$, one obtains the IP of the RnJ scheme as

$$\begin{aligned} I^{\mathrm{RnJ}} = 1 - \left(1 - e^{-\bar{\Omega}\sigma^2/P_s\lambda_{se}}\right) \sum_{i=0}^{1} \\ \cdot \left[\frac{\lambda_{sr_i}}{\lambda_{sr_i}+\lambda_{sr_j}} - \frac{1}{\lambda_{sr_i}}\Phi\left(\frac{\zeta_{\mathrm{th}}}{P_s}, \frac{1}{\lambda_{sr_i}}, \frac{\bar{\Omega}\sigma^2}{A_iP_s\lambda_{r_ie}}\right)\right. \\ + \frac{1}{\lambda_{sr_i}}\Phi\left(\frac{\zeta_{\mathrm{th}}}{P_s}, \frac{1}{\lambda_{sr_i}} + \frac{1}{\lambda_{sr_j}}, \frac{\bar{\Omega}\sigma^2}{A_iP_s\lambda_{r_ie}}\right) \\ \left. - e^{-\zeta_{\mathrm{th}}/P_s\lambda_{sr_i} - \bar{\Omega}\sigma^2/A_i\lambda_{r_ie}\zeta_{\mathrm{th}}}\left(1 - \frac{\lambda_{sr_j}e^{-\zeta_{\mathrm{th}}/P_s\lambda_{sr_j}}}{\lambda_{sr_i}+\lambda_{sr_j}}\right)\right], \end{aligned} \tag{32}$$

where $\Phi(v, k, l)$ is given in (B.1) in Appendix B.

The asymptotic OP of the RnJ scheme is

$$I^{\mathrm{RnJ}}_{\mathrm{asym}} = \lim_{P_s \longrightarrow \infty} I^{\mathrm{RnJ}} = 1, \tag{33}$$

which indicates a complete insecurity.

4.2. The nRnJ Scheme. To evaluate the efficacy of simultaneous relay selection and jamming in our scheme, we compare it with the nRnJ scheme (e.g., [7]) which lets R_i always relay the source data and R_j be idle in our scheme (i.e., pure relaying). Then, the IP of the nRnJ scheme is

$$\begin{aligned} I^{\mathrm{nRnJ}} &= 1 - \mathbb{P}\left\{\Omega_{se} < \bar{\Omega}, \Omega_{r_ie} < \bar{\Omega}\right\} \\ &= 1 - \mathbb{P}\left\{P_s g_{se} < \bar{\Omega}\sigma^2, P_{r_i} g_{r_ie} < \bar{\Omega}\sigma^2\right\}. \end{aligned} \tag{34}$$

By considering two cases of P_{r_i} as for deriving O^{RaJ} in (30), one obtains the IP of the nRnJ scheme as

$$\begin{aligned} I^{\mathrm{nRnJ}} = 1 - \left(1 - e^{-\bar{\Omega}\sigma^2/P_s\lambda_{se}}\right) \\ \cdot \left[1 - e^{-\zeta_{\mathrm{th}}/P_s\lambda_{sr_i} - \bar{\Omega}\sigma^2/A_i\lambda_{r_ie}\zeta_{\mathrm{th}}} - \frac{1}{\lambda_{sr_i}}\Phi\left(\frac{\zeta_{\mathrm{th}}}{P_s}, \frac{1}{\lambda_{sr_i}}, \frac{\bar{\Omega}\sigma^2}{A_iP_s\lambda_{r_ie}}\right)\right], \end{aligned} \tag{35}$$

from which the asymptotic IP of the nRnJ scheme is given by

$$I^{\mathrm{nRnJ}}_{\mathrm{asym}} = \lim_{P_s \longrightarrow \infty} I^{\mathrm{nRnJ}} = 1, \tag{36}$$

which indicates a complete insecurity.

The OP of the nRnJ scheme is expressed to be

$$\begin{aligned} O^{\mathrm{nRnJ}} &= 1 - \mathbb{P}\left\{\Omega_{sr_i} > \bar{\Omega}, \Omega_{r_id} > \bar{\Omega}\right\} \\ &= 1 - \mathbb{P}\left\{P_s g_{sr_i} > \bar{\Omega}\sigma^2, P_{r_i} g_{r_id} > \bar{\Omega}\sigma^2\right\}. \end{aligned} \tag{37}$$

By considering two cases of P_{r_i} as for deriving O^{RaJ} in (30), one obtains the OP of the nRnJ scheme as

$$O^{\mathrm{nRnJ}} = \begin{cases} 1 - e^{-\bar{\Omega}\sigma^2/A_i\zeta_{\mathrm{th}}\lambda_{r_id} - B/\lambda_{sr_i}} - \dfrac{1}{\lambda_{sr_i}}\Psi\left(\dfrac{\bar{\Omega}\sigma^2}{P_s}, \dfrac{\zeta_{\mathrm{th}}}{P_s}, \dfrac{1}{\lambda_{sr_i}}, \dfrac{\bar{\Omega}\sigma^2}{A_iP_s\lambda_{r_id}}\right) & , \bar{\Omega}\sigma^2 < \zeta_{\mathrm{th}}, \\ 1 - e^{-\bar{\Omega}\sigma^2/A_i\zeta_{\mathrm{th}}\lambda_{r_id} - B/\lambda_{sr_i}} & , \bar{\Omega}\sigma^2 > \zeta_{\mathrm{th}}, \end{cases} \tag{38}$$

from which the asymptotic OP of the nRnJ scheme is given by

$$O^{\mathrm{nRnJ}}_{\mathrm{asym}} = \lim_{P_s \longrightarrow \infty} O^{\mathrm{nRnJ}} = 1 - e^{-\bar{\Omega}\sigma^2/A_i\zeta_{\mathrm{th}}\lambda_{r_id}}, \tag{39}$$

which indicates the dependence of communication reliability on only the $R_i \longrightarrow D$ channel.

5. Remarks

Remark 1. Three (RaJ, RnJ, and nRnJ) schemes are completely insecure as $P_s \longrightarrow \infty$ (please refer to (24), (33), and (36)). This is reasonable since E receives strong signals from S as $P_s \longrightarrow \infty$, making E decode successfully source data.

Remark 2. For the L-EH (i.e., ζ_{th} in (1) is infinite), the IP and the OP of the RaJ scheme are, respectively, addressed as

$$I^{\mathrm{RaJ}}_{\mathrm{Lin}} = \lim_{\zeta_{\mathrm{th}} \longrightarrow \infty} I^{\mathrm{RaJ}} = 1 - \frac{1}{\lambda_{sr_i}} \sum_{i=0}^{1} \int_0^{\infty} I_1 e^{-x/\lambda_{sr_i}} dx, \tag{40}$$

$$\begin{aligned} O^{\mathrm{RaJ}}_{\mathrm{Lin}} &= \lim_{\zeta_{th} \longrightarrow \infty} O^{\mathrm{RaJ}} \\ &= 1 - \frac{1}{\lambda_{sr_i}} \sum_{i=0}^{1} \left[\Lambda\left(\frac{\bar{\Omega}\sigma^2}{P_s}, \frac{1}{\lambda_{sr_i}}, \frac{\bar{\Omega}\sigma^2}{A_iP_s\lambda_{r_id}}\right)\right. \\ &\quad \left. - \Lambda\left(\frac{\bar{\Omega}\sigma^2}{P_s}, \frac{1}{\lambda_{sr_i}} + \frac{1}{\lambda_{sr_j}}, \frac{\bar{\Omega}\sigma^2}{A_iP_s\lambda_{r_id}}\right)\right], \end{aligned} \tag{41}$$

where $\Lambda(\cdot, \cdot, \cdot)$ is expressed in (A.4) in Appendix B.

6. Demonstrative Results

This part illustrates theoretical/simulated results to evaluate both reliability and security of the considered schemes via pivotal parameters. Monte-Carlo simulations produce simulated results while the derived expressions in parts 3–5 are calculated to achieve theoretical ones. Path-loss is accounted by modelling fading power of $x \longrightarrow y$ channel as $\lambda_{xy} = d_{xy}^{-3}$ where d_{xy} is the $x \longrightarrow y$ distance. For illustration purpose, users are located on a 2-dimension plane

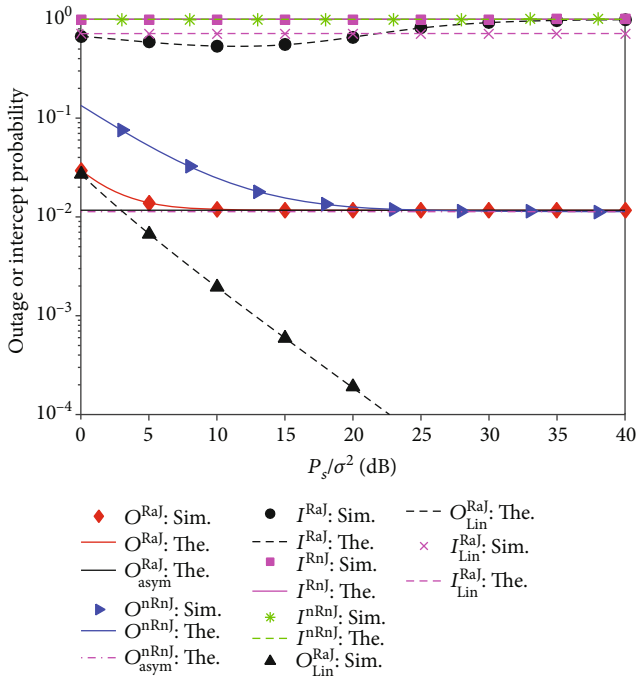


FIGURE 2: IP or OP versus P_s/σ^2. "The." and "Sim." represent the theoretical and the simulated results, correspondingly.

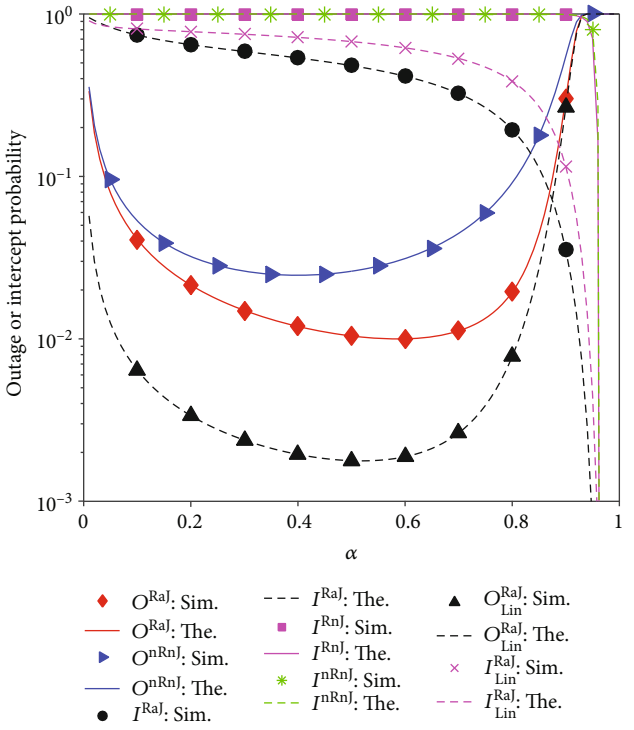


FIGURE 3: IP or OP versus α.

where S at (0.0,0.0), D at (1.0,0.0), E at (0.5,0.3), R_0 at (0.4877,0.0503), and R_1 at (0.4763,−0.0490); $\vartheta_i = 0.9$, $i \in \{0, 1\}$; $\mathbb{R} = 0.3$ bits/s/Hz. Since both RaJ and RnJ schemes achieve the same OP (i.e., $O^{RnJ} = O^{RaJ}$), the following results only expose O^{RaJ}.

Results in Figures 2–4 show coincidences between theory and simulation and between asymptote and theory at large P_s, validating both rigorous and asymptotic analyses. Moreover, these figures demonstrate that without jamming, two (RnJ and nRnJ) benchmark schemes suffer a complete insecurity ($I^{RnJ} = I^{nRnJ} = 1$) since secret data is not protected in both stages (II and III) as in the proposed RaJ scheme which is drastically secured (i.e., $I^{RaJ} < 1$). Furthermore, with relay selection, both (RaJ and RnJ) schemes achieve significantly better reliability than the nRnJ scheme (i.e., $O^{RaJ} = O^{RnJ} < O^{nRnJ}$). Therefore, the proposed RaJ scheme, which exploits simultaneous jamming and relay selection, considerably outperforms the (RnJ and nRnJ) benchmark schemes in terms of security as well as reliability.

Figure 2 unveils the OP/IP via P_s/σ^2 for $\zeta_{th}/\sigma^2 = 10$ dB and $\alpha = 0.4$. It is observed that O^{RaJ} decreases with increasing P_s, which makes senses because of increasing the harvested energy. Nevertheless, I^{RaJ} is minimum (i.e., the security reaches the peak) at a certain value of P_s. This implies that increasing P_s does not always improve security because E also benefits from receiving strong signals from S and R_i, eventually wire-tapping more source data. Interestingly, the minimum I^{RaJ} happens at the asymptotic OP O^{RaJ}_{asym}, and hence, P_s can be optimized to obtain the best reliability and security performances. Compared to the NL-EH, the L-EH apparently

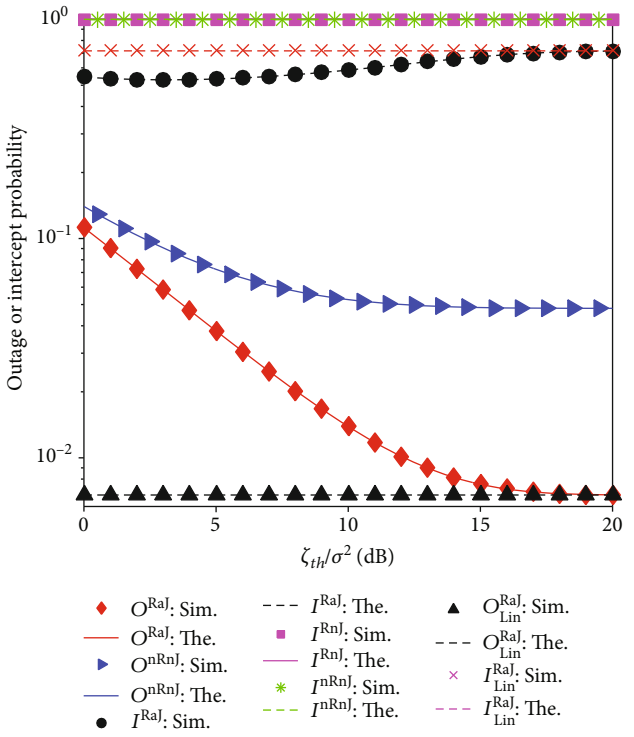


FIGURE 4: IP or OP versus ζ_{th}/σ^2.

offers considerably better reliability ($O^{RaJ}_{Lin} < O^{RaJ}$). However, the security of the former (I^{RaJ}) fluctuates around that of the latter (I^{RaJ}_{Lin}) with increasing P_s.

Figure 3 plots the IP/OP versus α for $P_s/\sigma^2 = \zeta_{\text{th}}/\sigma^2 = 10$ dB. It is noted that α is proportional to the EH time but inversely proportional to the signal processing time (stages II and III). Accordingly, α should be optimally adopted to balance these times for optimum reliability. Figure 3 shows that the RaJ and nRnJ schemes reach the lowest OP at $\alpha = 0.6$ and $\alpha = 0.4$, respectively. Interestingly, the security of the proposed RaJ scheme is considerably enhanced (i.e., I^{RaJ} significantly decreases) with increasing α. Some reasons lead to this observation as follows. Firstly, increasing α reduces the channel capacity at E because of the factor $(1-\alpha)/2$ before the logarithm in (11), causing the decrease of I^{RaJ}. Secondly, although increasing α helps R_i and R_j collect more energy, E suffers the increase of the jamming power from R_j, eventually reducing I^{RaJ}. Compared to the NL-EH, the L-EH is drastically more reliable ($O^{\text{RaJ}}_{\text{Lin}} < O^{\text{RaJ}}$) but less secure ($I^{\text{RaJ}}_{\text{Lin}} > I^{\text{RaJ}}$).

Figure 4 exposes the IP/OP versus $\zeta_{\text{th}}/\sigma^2$ for $P_s/\sigma^2 = 5$ dB and $\alpha = 0.4$. The reliability-and-security trade-off of the proposed RaJ scheme is observed in this figure. Nonetheless, the reliability gain increases faster than the security loss with increasing the saturation threshold of the NL energy scavenger ζ_{th}, exposing the advantage of both relay selection and jamming in our scheme in ensuring high reliability with affordable security threat. Such a trade-off with increasing ζ_{th} is reasonable since the NL-EH operates in the linear mode with higher harvested energy more frequently in the range of large ζ_{th}. Indeed, the performances of the NL-EH, I^{RaJ} and O^{RaJ}, reach those of the L-EH, $I^{\text{RaJ}}_{\text{Lin}}$ and $O^{\text{RaJ}}_{\text{Lin}}$, at large ζ_{th}.

7. Conclusions

The current paper recommended the relay selection-and-jamming scheme for radio frequency energy harvesting networks with the nonlinear energy harvester. Its security and reliability were also analyzed via the intercept and outage probabilities. Thanks to selecting the relay with the highest probability of decoding the source data and jamming the eavesdropper in both signal transmission stages, the proposed RaJ scheme achieved better reliability and security than the (RnJ and nRnJ) benchmark schemes without neither jamming nor both relay selection and jamming. Additionally, the best performance of the recommended scheme is achievable with choosing properly the source power and the time fraction, respectively. Moreover, the nonlinearity property of the energy harvesters significantly affects the reliability yet slightly degrades the security for the proposed scheme. Furthermore, the nonlinear energy harvester is less reliable yet more secure than the linear energy harvester.

Appendix

A. Derivation of $\Psi(u, v, k, l)$ in (28)

$\Psi(u, v, k, l)$ in (28) is

$$\Psi(u, v, k, \mathrm{l}) = \int_u^v e^{-kx-l/x} dx = \Lambda(u, k, l) - \Lambda(v, k, l), \tag{A.1}$$

where

$$\Lambda(c, k, l) = \int_c^\infty e^{-kx-l/x} dx. \tag{A.2}$$

Invoking the series expansion for $e^{-l/x}$, one rewrites (A.2) as

$$\begin{aligned}\Lambda(c, k, l) &= \int_c^\infty e^{-kx} \left(\sum_{m=0}^{\infty} \frac{1}{m!} \left[-\frac{l}{x} \right]^m \right) dx \\ &= \sum_{m=0}^{\infty} \frac{(-l)^m}{m!} \int_c^\infty \frac{e^{-kx}}{x^m} dx \overset{y=kx}{=} \sum_{m=0}^{\infty} \frac{(-kl)^m}{m!k} \int_{kc}^\infty \frac{e^{-y}}{y^m} dy.\end{aligned} \tag{A.3}$$

Using [46] (Equation (3.381.6)), the last integral in (A.3) is numerically evaluated as $(kc)^{-m/2} e^{-kc/2} W_{-m/2,(1-m)/2}(kc)$ where $W_{k,l}(z)$ is the Whittaker's function. Plugging this result into (A.3), one obtains

$$\Lambda(c, k, l) = \sum_{m=0}^{\infty} \frac{(-l)^m}{m!} k^{m/2-1} c^{-m/2} e^{-kc/2} W_{-m/2,(1-m)/2}(kc). \tag{A.4}$$

By plugging (A.4) into (A.1), one represents $\Psi(u, v, k, l)$ in (28) in a precise closed form.

B. Derivation of $\Phi(v, k, l)$ in (32)

$\Phi(v, k, l)$ in (32) is

$$\Phi(v, k, l) = \int_0^v e^{-kz-l/z} dz = \int_0^\infty e^{-kz-l/z} dz - \underbrace{\int_v^\infty e^{-kz-l/z} dz}_{\Lambda(v,k,l)}, \tag{B.1}$$

where $\Lambda(\cdot, \cdot, \cdot)$ is expressed in (A.4).

Availing [46] (Equation (3.471.9)), $\int_0^\infty e^{-kz-l/z} dz$ in (B.1) is solved as $2\sqrt{l/k} K_1(2\sqrt{kl})$ where $K_1(z)$ is the modified Bessel function of the second kind. Plugging this result into (B.1), one obtains

$$\Phi(v, k, l) = 2\sqrt{\frac{l}{k}} K_1\left(2\sqrt{kl}\right) - \Lambda(v, k, l). \tag{B.2}$$

Data Availability

The authors declare that all data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study/work/research was fully funded by the Tra Vinh University under grant contract number 181/HD.HDKH&DT-DHTV. The other supports Khuong Ho-Van who would like to thank Ho Chi Minh City University of Technology (HCMUT), VNU-HCM for the support of time and facilities for this study.

References

[1] T. N. Tran, T. P. Vo, P. Fazio, and M. Voznak, "SWIPT model adopting a PS framework to aid IoT networks inspired by the emerging cooperative NOMA technique," *IEEE Access*, vol. 9, pp. 61489–61512, 2021.

[2] D. Xu and H. Zhu, "Sum-rate maximization of wireless powered primary users for cooperative CRNs: NOMA or TDMA at cognitive users?," *IEEE Transactions on Communications*, vol. 69, no. 7, pp. 4862–4876, 2021.

[3] D. Dash, "Geometric algorithm for finding time-sensitive data gathering path in energy harvesting sensor networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.

[4] Y. Xu, H. Xie, C. Liang, and F. R. Yu, "Robust secure energy efficiency optimization in SWIPT-aided heterogeneous networks with a non-linear energy harvesting model," *IEEE IoT Journal*, vol. 8, no. 19, pp. 14908–14919, 2021.

[5] L. Ge, G. Chen, Y. Zhang, J. Tang, J. Wang, and J. A. Chambers, "Performance analysis for multihop cognitive radio networks with energy harvesting by using stochastic geometry," *IEEE IoT Journal*, vol. 7, no. 2, pp. 1154–1163, 2020.

[6] K. Ho-van and T. Do-Dac, "Security enhancement for energy harvesting cognitive networks with relay selection," *Wireless Communications and Mobile Computing*, vol. 2020, 13 pages, 2020.

[7] S. Solanki, P. K. Upadhyay, D. B. D. Costa, H. Ding, and J. M. Moualeu, "Performance analysis of piece-wise linear model of energy harvesting-based multiuser overlay spectrum sharing networks," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1820–1836, 2020.

[8] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE Journal on selected areas in communications*, vol. 24, no. 3, pp. 659–672, 2006.

[9] D. Wang, F. Zhou, and V. C. M. Leung, "Primary privacy preserving with joint wireless power and information transfer for cognitive radio networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 683–693, 2020.

[10] S. A. A. Kazmi and S. Coleri, "Optimization of full-duplex relaying system with non-linear energy harvester," *IEEE Access*, vol. 8, pp. 201566–201576, 2020.

[11] M. Babaei, U. Aygolu, M. Basaran, and L. Durak-Ata, "BER performance of full-duplex cognitive radio network with non-linear energy harvesting," *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 2, pp. 448–460, 2020.

[12] A. Anwar, S. T. Shah, S. F. Hasan, and D. R. Shin, "SWIPT-based three-step multiplicative amplify-and-forward two-way relay networks with non-linear energy conversion model," in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pp. 152–157, China, 2018.

[13] P. Maji, S. D. Roy, and S. Kundu, "Physical layer security with non-linear energy harvesting relay," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–6, India, 2019.

[14] K. Agrawal, M. F. Flanagan, and S. Prakriya, "NOMA with battery-assisted energy harvesting full-duplex relay," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13952–13957, 2020.

[15] A. Hakimi, M. Mohammadi, Z. Mobini, and Z. Ding, "Full-duplex non-orthogonal multiple access cooperative spectrum-sharing networks with non-linear energy harvesting," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 10925–10936, 2020.

[16] P. Raut, P. K. Sharma, T. A. Tsiftsis, and Y. Zou, "Power-time splitting-based non-linear energy harvesting in FD short-packet communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9146–9151, 2020.

[17] Y. Liu, Y. Ye, H. Ding, F. Gao, and H. Yang, "Outage performance analysis for SWIPT-based incremental cooperative NOMA networks with non-linear harvester," *IEEE Communications Letters*, vol. 24, no. 2, pp. 287–291, 2020.

[18] L. Shi, W. Cheng, Y. Ye, H. Zhang, and R. Q. Hu, "Heterogeneous power-splitting based two-way DF relaying with non-linear energy harvesting," in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, United Arab Emirates, 2018.

[19] X. Xie, J. Chen, and Y. Fu, "Outage performance and QoS optimization in full-duplex system with non-linear energy harvesting model," *IEEE Access*, vol. 6, pp. 44281–44290, 2018.

[20] Y. Liu, F. Gao, X. Deng, T. Wu, and X. Zhang, "Performance analysis for incremental DF relaying networks with non-linear energy harvesting," in *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, pp. 354–360, China, 2020.

[21] F. Wang and X. Zhang, "Secure resource allocation for polarization-based non-linear energy harvesting over 5G cooperative CRNs," *IEEE Wireless Communications Letters*, p. 1, 2020.

[22] Y. Zhang, X. Q. Jiang, H. Hai, J. Hau, and K. Peng, "Generalized non-linear energy harvesting protocol for enhancing security of AF multi-antenna relaying systems," in *2019 IEEE 2nd International Conference on Electronics and Communication Engineering (ICECE)*, pp. 195–201, China, 2019.

[23] D. Wang and S. Men, "Secure energy efficiency for NOMA based cognitive radio networks with nonlinear energy harvesting," *IEEE Access*, vol. 6, pp. 62707–62716, 2018.

[24] L. Ni, X. da, H. Hu, M. Zhang, and K. Cumanan, "Outage constrained robust secrecy energy efficiency maximization for EH cognitive radio networks," *IEEE Wireless Communications Letters*, vol. 9, no. 3, pp. 363–366, 2020.

[25] N. Shanin, L. Cottatellucci, and R. Schober, "Markov decision process based design of SWIPT systems: non-linear EH circuits, memory, and impedance mismatch," *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 1259–1274, 2021.

[26] S. Bayat, A. Khalili, and Z. Han, "Resource allocation for MC MISO-NOMA SWIPT-enabled HetNets with non-linear energy harvesting," *IEEE Access*, vol. 8, pp. 192270–192281, 2020.

[27] D. Wang, F. Rezaei, and C. Tellambura, "Performance analysis and resource allocations for a WPCN with a new nonlinear energy harvester model," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1403–1424, 2020.

[28] G. Ma, J. Xu, Y. F. Liu, and M. R. V. Moghadam, "Time-division energy beamforming for multiuser wireless power transfer with non-linear energy harvesting," *IEEE Wireless Communications Letters*, vol. 10, no. 1, pp. 53–57, 2021.

[29] Z. Zhu, N. Wang, W. Hao, Z. Wang, and I. Lee, "Robust beamforming designs in secure MIMO SWIPT IoT networks with a non-linear channel model," *IEEE IoT Journal*, vol. 69, no. 2, pp. 1867–1878, 2020.

[30] T. X. Vu, S. Chatzinotas, S. Gautam, E. Lagunas, and B. Ottersten, "Joint optimization for PS-based SWIPT multiuser systems with non-linear energy harvesting," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Seoul, Korea (South), 2020.

[31] X. Liu, Y. Gao, M. Guo, and N. Sha, "Secrecy throughput optimization for the WPCNs with non-linear EH model," *IEEE Access*, vol. 7, pp. 59477–59490, 2019.

[32] Y. Lu, K. Xiong, P. Fan, Z. Ding, Z. Zhong, and K. B. Letaief, "Global energy efficiency in secure MISO SWIPT systems with non-linear power-splitting EH model," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 216–232, 2019.

[33] S. Gao, K. Xiong, R. Jiang, L. Zhou, and H. Tang, "Outage performance of wireless-powered SWIPT networks with non-linear EH model in Nakagami-m fading," in *2018 14th IEEE International Conference on Signal Processing (ICSP)*, pp. 668–671, China, 2018.

[34] F. Zhou, Z. Chu, Y. Wu, N. Al-Dhahir, and P. Xiao, "Enhancing PHY security of MISO NOMA SWIPT systems with a practical non-linear EH model," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, USA, 2018.

[35] E. Boshkovska, D. W. K. Ng, L. Dai, and R. Schober, "Power-efficient and secure WPCNs with hardware impairments and non-linear EH circuit," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2642–2657, 2018.

[36] P. Chakraborty and S. Prakriya, "Secrecy performance of an idle receiver assisted underlay secondary network," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9555–9560, 2017.

[37] R. Su, Y. Wang, and R. Sun, "Secure cooperative transmission in cognitive AF relay systems with destination-aided jamming and energy harvesting," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–5, Turkey, 2019.

[38] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1319–1329, 2017.

[39] X. Hu, X. Zhang, H. Huang, and Y. Li, "Secure transmission via jamming in cognitive radio networks with possion spatially distributed eavesdroppers," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–6, Spain, 2016.

[40] Z. Li, T. Jing, X. Cheng, Y. Huo, W. Zhou, and D. Chen, "Cooperative jamming for secure communications in MIMO cooperative cognitive radio networks," in *2015 IEEE International Conference on Communications (ICC)*, pp. 7609–7614, UK, 2015.

[41] Zhihui Shu, Yi Qian, and Song Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, 2013.

[42] Y. Wu, X. Chen, and X. Chen, "Secure beamforming for cognitive radio networks with artificial noise," in *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, pp. 1–5, China, 2015.

[43] B. Fang, Z. Qian, W. Shao, and W. Zhong, "Precoding and artificial noise design for cognitive MIMOME wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6753–6758, 2016.

[44] V. D. Nguyen, T. Q. Duong, O. A. Dobre, and O. S. Shin, "Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2609–2623, 2016.

[45] M. K. Simon and M. S. Alouini, *Digital Communication over Fading Channels*, John Wiley & Sons, Inc., Hoboken, New Jersey, Second edition, 2005.

[46] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, Academic Press, San Diego, CA, USA, 6th edition, 2000.

[47] J. Ye, Z. Liu, H. Zhao, G. Pan, Q. Ni, and M. S. Alouini, "Relay selections for cooperative underlay CR systems with energy harvesting," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 358–369, 2019.

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5986469, 14 pages
https://doi.org/10.1155/2021/5986469

Research Article

Securing Wireless Body Area Network with Efficient Secure Channel Free and Anonymous Certificateless Signcryption

Fazal Noor, Turki A. Kordy, Ahmad B. Alkhodre, Oussama Benrhouma, Adnan Nadeem, and Ali Alzahrani

Department of Computer and Information Systems, Islamic University of Madinah, Madinah 400411, Saudi Arabia

Correspondence should be addressed to Fazal Noor; mfnoor@gmail.com

Received 19 August 2021; Revised 7 September 2021; Accepted 9 September 2021; Published 7 October 2021

Academic Editor: Mohammed H. Alsharif

In the last few years, the wireless body area network (WBAN) has emerged as an appealing and viable option in the e-health application domain. WBAN technology is primarily used to offer continuous screening of health data to patients, independent of their location, time, or activity. A WBAN, on the other hand, is vulnerable to different cyberattacks due to the openness of the wireless environment and the privacy of people's physiological data. A highly efficient and secure cryptographic scheme that can fulfill the needs of resource-constrained WBAN sensors and devices is considered necessary. First, we take a look at the most up-to-date security solutions for WBANs. Then, we go through some of the underlying concerns and challenges with WBAN security. We propose a new framework called secure channel free certificateless signcryption scheme for WBANs based on a hyperelliptic curve that can meet security requirements such as confidentiality, anonymity, integrity, resistance against unauthorized users, unforgeability, public verifiability, forward secrecy, and antireplay attack, all of which can be achieved with low computation and communication costs. The computation cost of the proposed scheme is 3.36 ms, which is much better than its counterpart schemes.

1. Introduction

A Wireless Body Area Network (WBAN) is a revolutionary innovation that can deliver real-time preventative or proactive healthcare services at a lower cost [1]. Many low-power, intelligent, and tiny biomedical sensors are attached to, implanted in, or implanted around the human body in a WBAN without interfering with the individual's usual activities. Sensors continuously measure specific biological functions, such as temperature, blood pressure, heart rate, ElectroCardioGram (ECG), respiration, and others regardless of their current location or activity [2]. The physiological information collected is then transmitted over the wireless links to a remote processing unit without the need for complex and wired medical equipment. The ongoing miniaturization of sensors, actuators, and processors coupled with ubiquitous wireless connectivity has contributed to the emergence of WBANs. At the same time, advances in smartphones technology have also enhanced the mobility feature of WBAN technology. Today, WBAN can be connected through the Internet and other existing short-range wireless technologies (ZigBee, Bluetooth, Wi-Fi, and so on) and cellular networks. Wi-Fi may be considered the most favored options for wearable sensor nodes due to its low-cost and high-data-rate features [3].

As shown in Figure 1, the authors suggested a general communication architecture for a WBAN-based e-healthcare system [4]. A body control unit (BCU) and numerous wearable sensor/actuator nodes are included in the proposed design (e.g., a smartphone). Sensor nodes detect biological processes such as pulse, body temperature, blood pressure, glucose level, and electrocardiogram (ECG). According to the messages gathered from the sensors, actuators engage with a BCU (i.e., an insulin pump). The BCU collects biological data and sends it, together with the patient's profile, to a local/-remote medical server through networks. Medical staff offers medical treatments in a timely manner after obtaining and analyzing patient-related data. The BCU functions as a center node in a star topology in general. Additionally, sensor nodes

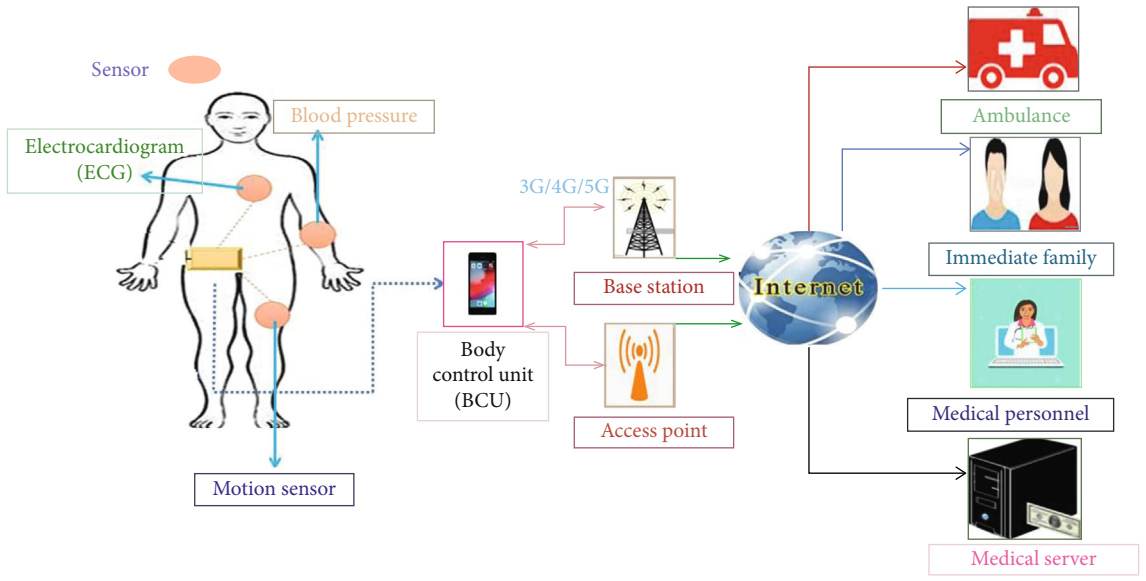


Figure 1: General architecture of a typical WBAN-based healthcare monitoring system [4].

upload data to a medical server or provide data directly to medical staff via the BCU. The medical personnel then issues the relevant instructions to the sensors via the BCU.

In a WBAN system, both patient-related information and medical messages are equally significant. WBAN, on the other hand, is vulnerable to a variety of cyberattacks owing to the open nature of wireless networks. As a result, to enable a safe WBAN system, an effective security architecture is necessary. Confidentiality and authentication are two key security problems in WBANs that must be addressed. Encryption and digital signatures, in general, are the answers to confidentiality and authenticity. The sign-then-encrypt technique is often employed when both procedures are required at the same time. Low-end WBAN sensor devices, on the other hand, have stringent constraints (such as limited on-board energy and processing resources) that prevent complicated cryptographic procedures. "Signcryption" [5] might be used to address these limitations. It is a public-key cryptosystem that performs both digital signature and encryption functions in a single logic step. It is far more efficient and cost-effective than the combination of encryption and digital signatures. Furthermore, it is considerably more suited for resource-constrained situations such as WBAN due to its reduced costs compared to techniques using signature followed by encryption.

As a result, a lightweight signcryption scheme that can fulfill the criteria of WBAN devices is required. Therefore, we offer a certificateless signcryption scheme in this paper. The scheme is based on the concept of a hyperelliptic curve and does not require a secure channel. The new scheme meets all of the previously specified security requirements while incurring low computation and communication costs, making it particularly appropriate for resource-constrained WBAN devices.

1.1. Signcryption for WBAN. Wireless body area network has received a lot of attention in the last decade especially as various technologies improve and devices keep getting smaller, more powerful, and cheaper. In a WBAN, different sensors are implanted in the human body for sensing and collecting data about different types of physiological information which are then sent to the application providers for further analysis and actions. As we have mentioned previously, communication takes place in the WBAN system while using an insecure network, i.e., the Internet, which requires two main security requirements, namely, authentication and confidentiality. Here, signcryption is the most suitable option because it combines both authentication and confidentiality in a single step, and it also requires low computational power making it suitable for resource-constrained devices such as sensors.

Figure 2 shows the generic signcryption model for WBAN which uses four entities, i.e., sensors, controller, trusted authority, and application providers. Normally, the trusted authority is a third party, which is responsible for providing the system parameters such as keys and certificates for different public-key cryptographic techniques. Sensor nodes are implanted into a person's body for sensing and collecting physiological data and then sending this data to the controller. Likewise, the controller applies the signcryption scheme to the data and transmits it to some application provider. Once the application provider receives the signcryption query, it verifies the authenticity of the sender. If the verification is successful, the application provider performs the decryption process and encrypts the requested data using some secret key (which is only known to the controller and the application provider) and sends it to the application provider. However, for access control, the same process can be repeated on the application provider side as shown in Figure 3. Here, the application provider generates the signcryption of the access control query by combining signature with encryption while using a single key pair in a single algorithm and transmits it to the controller. Once the controller receives the signcryption query, it verifies the

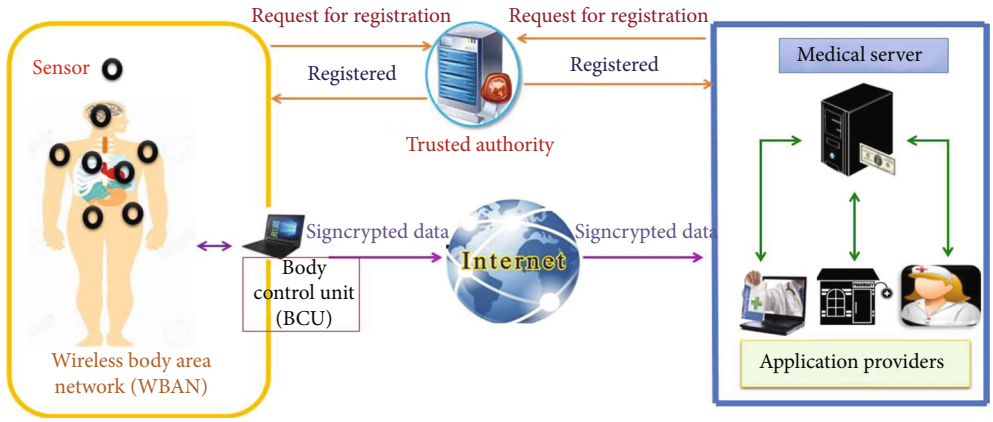


Figure 2: Signcryption performed by the controller.

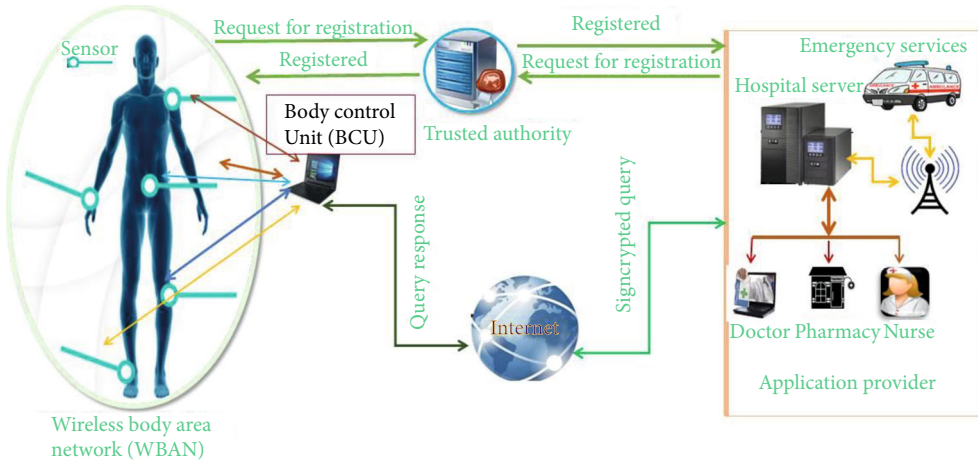


Figure 3: Signcryption performed by the application provider.

authenticity of the sender. If the verification is successful, the controller performs the decryption process and encrypts the requested data using some secret key (which is only known to the controller and the application provider) and sends it to the application provider.

1.2. Security Requirements for WBAN with Signcryption. In a WBAN, the communication process normally takes place through an open network. This means that the attacker can have unauthorized access to reveal the content of encrypted data, modify the original message, generate the forged signature, and so on. The basic security requirements for signcryption used in WBAN include (1) confidentiality: the attacker can compromise the confidentiality of the patient's sensitive data, if he/she gets access to the encryption or decryption keys. (2) Integrity: the attacker can modify the content of the original message only with the help of encryption or decryption keys. (3) Unauthorized access: the attacker can easily generate the authorized data access request if he/she has a valid digital signature. If the attacker cannot generate a valid then it is called an unauthorized access. (4) Unforgeability: the attacker can generate a forged signature as generated by the authorized user (I think that is what you mean here otherwise we mean the authorized user also generates a forged signature), if he/she gets access to the private key used for generating the digital signature. If the attacker fails to get access to this private key, then, it is called unforgeability. (5) Anonymity: the attacker can pretend to be the authorized user, if he/she can get the identity of the user from ciphertext. The inability of the attacker to access the users' identities is called anonymity. (6) Forward secrecy: the attacker cannot get access to the encryption/decryption keys, even, if he/she got access to the sender's private key. (7) Public verifiability: the attacker sends the false signcryption text instead of the authorized sender, and if it causes discrepancies between the sender and the receiver, then, the judge/third party can remove this dispute, which is called public verifiability. (8) Antireplay attack: the attacker cannot replay the existing messages if the sender and receiver use nonce and timestamp techniques for the freshness of messages.

1.3. Contributions of This Work. We summarize the main contributions of this work as follows:

(i) We present a comprehensive review of recently proposed signcryption schemes to improve security in the WBAN environment. To the best of our

knowledge, this is the first survey that focuses on signcryption for WBAN security

(ii) We identify the strengths and weaknesses of the previously proposed signcryption schemes for WBAN in terms of security requirements and their cost-efficiency

(iii) Based on the strengths and weaknesses identified for the past related works on signcryption schemes for WBAN, we propose a novel security architecture for the WBAN environment using secure channel free certificateless signcryption based on hyperelliptic curve. The new scheme satisfies all the security requirements identified earlier, and it incurs low computation and communication costs which make it particularly suitable for resource-constrained WBAN devices

The rest of the article is set out as follows. The related work is presented in Section 2, which also includes classification, security deficiencies, and cost requirements. The proposed scheme is provided in Section 3. In Section 4, we describe the construction of the proposed scheme. Section 5, on the other hand, provides the proposed scheme's security discussions. In addition, we discuss performance analysis in Section 6. The conclusion is presented in Section 7.

2. Related Works on Signcryption for WBAN

In this section, we review and analyze existing signcryption schemes for WBAN with respect to their research goals, security requirements, and computation and communication overheads. Amin et al. [6] proposed a hybrid key establishment technique for body area network (BANs) based on symmetric cryptography with signcryption. They make a cluster head selection with session key creation in one logical step and claimed reduced computation cost as well as communication overhead. They also claimed that their approach supports various security properties such as confidentiality, antireplay attack, integrity, and authentication. However, the scheme consumes high energy and increased bandwidth due to the elliptic curve cryptosystem (ECC). It suffers from certificate renewal and revocation problems. It does not support forward secrecy, public verifiability, mutual authentication, and nonrepudiation. Wang and Liu [7] proposed a ring signcryption method utilizing attribute-based cryptosystem for WBANs. The security hardiness and efficiency of this scheme are based on the computational Diffie-Hellman (CDH) assumption from bilinear pairing. Their method supports various security requirements, i.e., authenticity, nonrepudiation, and confidentiality. However, this method does not address the key escrow problem because the Hospital Authority (HA) performs the role of the Private Key Generation (PKG) center that generates the private keys for both the controller and data users (such as doctor, researchers, and emergency). Therefore, the HA can easily use the user's private key to forge the signature. Moreover, the scheme's efficiency is based on bilinear pairing which consumes high energy and uses high bandwidth. It does not support forward secrecy, public verifiability, mutual authentication, and antireplay attack.

Jothi and Srinivasan [8] proposed another method which combines the concept of attribute-based cryptosystem with ring signcryption. In this system, the sensors which are planted into the body use ant colony optimization with the concept of fuzzy ontology. They claimed better performance as compared to existing elliptic curve-based methods with respect to efficiency and feasibility. Further, their approach also supports various security services such as authentication, unforgeability, confidentiality, public verifiability, integrity, nonrepudiation, and forward secrecy. Unfortunately, this method suffers from two major weaknesses, i.e., the key escrow problem and private key distribution among users which needs a secure channel. Li and Hong [9] proposed a new signcryption method that uses the concept of certificateless cryptosystem (CC) with bilinear pairing. Further, they implemented this new method in WBANs and showed that it incurs low computation overhead and energy as compared to existing schemes for WBANs. Their approach supports authentication, confidentiality, nonrepudiation, public verifiability, integrity, and cipher-text authenticity. But this scheme suffers from a partial private key distribution among users which needs a secure channel. Additionally, since this method is based on bilinear pairing, it consumes high energy and increased network bandwidth. Iqbal et al. [10] proposed a new signcryption method with the public verifiability security requirement. They performed the cluster head selection process for this new method and claimed better efficiency due to the hyperelliptic curve, which is suitable for resource hungry environments of WBANs. Their proposed method supports security services such as confidentiality, integrity, forward secrecy, and authentication. However, the network model fails to provide a central authority and suffers from certificate renewal and revocations problems. Further, this work focuses mainly on the public verifiability security property while the authors fail to explain this property. Moreover, this scheme does not provide nonrepudiation, mutual authentication, and protection against replay attack.

Saeed et al. [11] proposed a new method for the Internet of things based on heterogeneous online/offline signcryption, in which the sensor nodes (sender) utilize the functionality of a certificateless infrastructure (CLI), and the server (receiver) utilizes the services of public key infrastructure (PKI). They proved the scheme security requirement using a random oracle model and showed that it satisfies security requirements such as authentication, nonrepudiation, integrity, and confidentiality. Furthermore, they applied the scheme in WBAN. However, due to CLI and PKI, this scheme suffers from secret key distribution, and the certificate revocation and management problem. It also suffers from high consumption of and network bandwidth because it uses bilinear pairing. Also, it does not support mutual authentication, forward secrecy, public verifiability, and protection against replay attack. Lu et al. [12] proposed a scheme for a social network-based mobile health care system that uses attribute-based signcryption. They used a four-party model to protect patients' sensitive information. The scheme provides traceability, privacy, unforgeability, and

correctness. Using encryption and digital signature in a single step, they claimed better performance efficiency. However, due to the PKG concept, this scheme suffers from private key distribution and the key escrow problem. The scheme does not support forward secrecy, public verifiability, nonrepudiation, mutual authentication, and protection against replay attack. Moreover, it has high power consumption and network bandwidth due to of the use of bilinear pairing. Li et al. [13] developed a novel method using certificateless signcryption, and then, they practically deployed this scheme for access control services in WBAN. This method supports several security requirements that include authenticity, integrity, confidentiality, nonrepudiation, and anonymity. They also compare their scheme with existing schemes and demonstrated better results in terms of energy consumption and computational cost. However, due to the CLI concept, this scheme suffers from the partial private key distribution problem and incurs high power consumption. The method does not support public verifiability, forward secrecy, and mutual authentication.

Prameela [14] proposed an improved scheme that uses certificateless signcryption with anonymous mutual authentication for access control in WBANs. They used a chaos baker map scheme with XOR operation and a one-way hash chain function for secure authentication. The experimental results obtained with the proposed scheme yielded better results compared with existing ones in terms of energy consumption, end-to-end delay, coverage time, packet delivery ratio, and throughput. The scheme supports confidentiality, mutual authentication, nonrepudiation, and integrity. Conversely, because of the use of CLI, this scheme suffers from partial private key distribution difficulties and high power consumption and network bandwidth because it uses bilinear pairing. This scheme does not support forward secrecy, public verifiability, and protection against replay attack. Omala et al. [15] proposed a keyword search technique for WBAN based on heterogeneous signcryption, in which the data owner uses the concept of CLI, while the server and receiver utilize the PKI functionality. This heterogeneous signcryption generates the mathematical structure of bilinear pairing. The scheme supports security services such as confidentiality, unforgeability, nonrepudiations, and authenticity. However, the scheme suffers and incurs high power consumption and communication costs due to bilinear pairing. It suffers from weaknesses such as it needs a secure channel for the data owner's partial private key distribution and PKI certificate management at the server and receiver side. It does not provide public verifiability, forward secrecy, and mutual authentication.

Omala et al. [16] proposed an access control technique for WBAN based on heterogeneous signcryption, in which the controller uses the concept of CLI, while application providers utilize the concept of identity-based cryptography (IBC). The scheme's cost and security efficiency are based on the mathematical structure of elliptic curve cryptography. The technique is cost-efficient and supports security services such as anonymity, confidentiality, unforgeability, nonrepudiations, and authenticity. However, the scheme also suffers from high computational and communication costs due to elliptic curve cryptosystem. It also needs a secure channel for the application provider's partial private key distribution. It also suffers from the key escrow problem at the controller side. It does not support public verifiability, forward secrecy, and mutual authentication. Gao et al. [17] proposed an elliptic curve-based technique for access control of WBAN by using a certificateless signcryption. They claimed better cost efficiency, for the technique supports security services such as confidentiality, unforgeability, nonrepudiation, and authenticity. However, the scheme also suffers from high computation and communication costs due to the elliptic curve cryptosystem. It also needs a secure channel for the partial private key distribution. The techniques do not support forward secrecy, public verifiability, and mutual authentications. Ullah et al. [18] proposed an energy-efficient access control technique for WBAN with IoT using certificate-based signcryption. The scheme's cost and security efficiency are based on the mathematical structure of hyperelliptic curve cryptography. The authors of this technique claimed better cost-efficiency. The scheme supports security services that include confidentiality, unforgeability, antireplay attack, integrity, public verifiability, and forward security. However, since the scheme requires certificate management, the scheme may not scale well when the number of devices in the network increases. The scheme does not support mutual authentication and anonymity properties. Iqbal et al. [19] proposed a new scheme for body sensor network. This scheme uses attribute-based signcryption with blockchain technology. The security and efficiency of this scheme are based on bilinear pairing. The scheme has better power consumption and low communication overheads. The scheme supports security requirements such as confidentiality and unforgeability. The scheme provides protection against antireplay and man-in-the-middle attacks. However, the scheme can be suffering from more computational and communication cost due to bilinear pairing. As with other approaches, the scheme needs a secure channel for partial private key distribution and certificate management due to CLI and PKI. The scheme does not support mutual authentication, anonymity, public verifiability, and forward secrecy. Xiong et al. [20] presented a heterogeneous signcryption method for WBANs that transitions from an identity-based cryptosystem to a public key infrastructure (PKI) with an equality test (HSCIP-ET). The technique enables the IBC system's sensors to encrypt critical data using the management center's public key in the PKI system before uploading it to the cloud server. Based on the discussions above, Table 1 summarizes the results of our review.

2.1. Classification of Signcryption Schemes for WBAN regarding Public Key Cryptography. In this section, we classified the existing signcryption schemes for WBAN such as asymmetric cryptosystems and mathematically hard problems. In Table 2, we summarize the contributed schemes on the basis of public key cryptosystems that are attribute based, PKI based, certificateless, certificate based, and heterogeneous, respectively. The schemes in [7, 8, 12, 19] realized on the concept of attribute-based signcryption, while schemes in [7, 8, 12] at the same time utilizes the concept

Table 1: Strengths and weaknesses of signcryption schemes for WBANs.

Goal(s) of research	Strengths	Weaknesses
[6]	(i) They make a cluster head selection with session key creation in one logical step (ii) Claimed for reduced computational cost as well as communication overhead (iii) Claimed for various security properties such as confidentiality, antireplay attack, integrity, and authentication	(i) Suffering from certificate renewal and revocations problems (ii) Suffered from greater consumption of computational power (iii) Suffered increased nature of bandwidth (iv) Suffer from the lack of forward secrecy, public verifiability, and nonrepudiation
[7]	(i) Claimed for better efficiency (ii) Claimed for various security requirements, i.e., authenticity, nonrepudiation, and confidentiality	(i) Failed to remove the key escrow problem (ii) Suffered from greater computational power (iii) Suffered from increased nature of bandwidth (iv) Lack of forward secrecy, public verifiability, and antireplay attack
[8]	(i) Claimed for better performance with respect to efficiency and feasibility (ii) Claimed for various security services that are authentication, unforgeability, confidentiality, public verifiability, integrity, nonrepudiation, and forward secrecy	(i) Suffering from the key escrow problem (ii) Suffering from private key distribution problem (iii) Lack of antireplay attack
[9]	(i) Claimed for minimum consumptions of computation and energy (ii) Claimed for security services such as authentication, confidentiality, nonrepudiation, public verifiability, integrity, and ciphertext authenticity	(i) Suffering from a partial private key distribution problem (ii) Undergone from larger consumption of computational power (iii) Suffering from bigger nature of bandwidth (iv) Lack of forward security property
[10]	(i) Claimed for better efficiency (ii) Claimed for confidentiality, integrity, forward secrecy, and authentication	(i) Failing to provide the role of central authority (ii) Suffering from certificate renewal and revocations problems (iii) Suffered from public verifiability security property (iv) Lacking from nonrepudiation, and antireplay attack
[11]	(i) They prove the scheme security requirement using a random oracle model (ii) Claimed for security property such as authentication, nonrepudiation, integrity, and confidentiality	(i) Suffering from secret key distribution (ii) Suffering from certificate revocation and management problem (iii) Undergo from larger consumption of computational power (iv) Suffering from the bigger nature of bandwidth (v) Lack of forward secrecy, public verifiability, and antireplay attack
[12]	(i) Claimed for a number of analysis, i.e., traceability, privacy, unforgeability, and correctness (ii) Using encryption and digital signature in a single step (iii) Claimed for better performance regarding efficiency	(i) Suffering from private key distribution and the key escrow problem. (ii) Undergo from larger consumption of computational power (iii) Suffering from bigger nature of bandwidth (iv) Lack of forward secrecy, public verifiability, nonrepudiation, and antireplay attack
[13]	(i) Claimed for a series of security requirements, i.e., authenticity, integrity, confidentiality, nonrepudiation, and anonymity (ii) Claimed for better results regarding energy consumption and computational cost	(i) Suffering from partial private key distribution problem (ii) Underwent from loftier consumption of computational power and a larger nature of bandwidth (iii) Lack of public verifiability and forward secrecy
[14]	(i) Claimed for better results compared with existing ones regarding energy consumption, end-to-end delay, coverage time, packet delivery ratio, and throughput (ii) Claimed for confidentiality, mutual authentication, non-repudiation, and integrity, authentication	(i) Undergo from partial private key distribution difficulties (ii) Suffering from snootier consumption of computational power and a larger nature of bandwidth (iii) Lack of forward secrecy, public verifiability, and antireplay attack

Table 1: Continued.

Goal(s) of research	Strengths	Weaknesses
[15]	(i) Claimed for better efficiency (computational and communication cost) (ii) Claimed for confidentiality, unforgeability, nonrepudiations, and authenticity	(i) Suffering from more computational and communication cost (ii) Affected by needing the secure channel for the data owner partial private key distribution (iii) Suffering from certificate management at the server and receiver side (iv) Lack of public verifiability and forward secrecy
[16]	(i) Claimed for better cost-efficiency (ii) Claimed for security services that are anonymity, confidentiality, unforgeability, nonrepudiations, and authenticity	(i) Suffering from more computational and communication cost (ii) Affected by requiring the secure channel for the application provider partial private key distribution (iii) Suffering from key escrow problem at the controller side (iv) Lack of public verifiability and forward secrecy
[17]	(i) Claimed for better cost-efficiency (ii) Claimed for security services that are confidentiality, unforgeability, nonrepudiations, and authenticity	(i) Suffering from more computational and communication cost (ii) It can be affected by requiring the secure channel for the partial private key distribution (iii) Lack of forward secrecy and public verifiability
[18]	(i) Claimed for better cost efficiency (ii) Claimed for security services that are confidentiality, unforgeability, antireplay attack, integrity, public verifiability, and forward security	(i) Affected by requiring the certificate management in a network which consists a large number of devices (ii) It can also be affected by the lack of anonymity property
[19]	(i) Claimed for better utilization of energy, computational consumptions, and with less communication overhead (ii) Claimed for the security requirements like confidentiality, unforgeability, antireplay attack, and resist for man-in-the-middle attack	(i) Suffering from more computational and communication cost (ii) Affected by needing the secure channel for partial private key distribution (iii) Suffering from certificate management (iv) Affected by the lack of public verifiability and forward secrecy security requirements

Table 2: Classification of signcryption schemes W.r.t to asymmetric cryptosystem.

Attribute-based signcryption techniques for WBAN	[7, 8, 12, 19]
Identity-based signcryption techniques for WBAN	[7, 8, 12]
PKI-based signcryption techniques for WBAN	[6, 10]
Certificateless signcryption techniques for WBAN	[9, 13, 14, 17]
Certificate-based signcryption techniques for WBAN	[18]
Heterogeneous signcryption techniques for WBAN	[11, 15, 16, 19]

Table 3: Classification on the basis of hard problems.

Bilinear pairing cryptosystem	[7, 9, 11–15, 19]
Elliptic curve cryptosystem	[16, 17]
Fuzzy-based cryptosystem	[8]
Hyperelliptic curve cryptosystem	[10, 18]

of identity-based cryptosystem, and scheme in [19] uses the heterogeneous cryptosystem method. The techniques presented in [6, 10] are realized on PKI-based cryptography. The schemes proposed in [9, 13, 14, 17] used the concept of certificateless signcryption technique. The technique used in [18] is based on certificate-based signcryption, and the schemes in [11, 15, 16, 19] are on the basis of heterogeneous signcryption techniques.

2.2. Classification of Signcryption Schemes for WBAN with respect to Cryptographic Hard Problems. In this section, we classified the existing signcryption schemes for WBAN on the basis of hard problems that are shown in Table 3. The schemes presented in [7, 9, 11–15, 19] are based on the concept of bilinear pairing, while the schemes provided in [16, 17] utilize the concept of elliptic curve cryptography. The scheme proposed in [8] used the Fuzzy-based cryptosystem, while the schemes contributed in [10, 18] use the notion of hyperelliptic curve cryptography.

2.3. Security Deficiencies in Signcryption Techniques for WBAN. In this phase, on the basis of our analysis that is presented in Table 1, where each technique has its own pros and cons and it is difficult to differentiate the superiority of each technique on others. Further, each of those has its own security limitations on the basis of security properties such as confidentiality, unforgeability, integrity, anonymity, nonrepudiations, forward secrecy, antireplay attack, public verifiability, and preventing from unauthorized access, respectively. The scheme presented in [6] has been suffering from the lack of forward secrecy, public verifiability, and nonrepudiation. The scheme in [7] has the diffenciencies of forward secrecy, public verifiability, and antireplay attack. The scheme in [8] can be affected by the lack of antireplay attack. The technique used in [9] has the limitations of not providing the forward security. The method used in [10] is suffering from the absence of nonrepudiation and antireplay attack. The mechanism used in [11] has been suffering from the absence of forward secrecy, public verifiability, and antireplay attack. The presented scheme in [12] does not provide the security properties such as forward secrecy, public verifiability, nonrepudiation, mutual authentication, and antireplay attack. The mechanism used in [13] can be suffered from the absence of public verifiability and forward secrecy. Due to the absence of forward secrecy, public verifiability, and antireplay attack, the scheme used in [14] can affect. During communication, the schemes used in [15–17, 19] can be affected by the absence of public verifiability, forward secrecy, and mutual authentication security properties. The scheme used in [18] is affected by the absence of mutual authentication property.

2.4. Cost Requirements of Signcryption Technique for WBAN. We divide the cost requirements into two subcategories, i.e., computational cost and communication overhead. First of all, we investigate the computational cost of the signcryption mechanisms for WBAN. The computational cost is normally calculated by using some major operations. In signcryption schemes for WBAN, discussed in Table 1, the well-known technique, which is used for the cost efficiency, is bilinear pairing, elliptic curve, and the hyperelliptic curve. According to the experimental results, which is discussed in [21], regarding the major operations, the single pairing operation takes 14.90 milliseconds (ms), single exponential operation takes 1.25 ms, single elliptic scalar multiplication consumes 0.97 ms, and according to [22–26], single hyperelliptic curve needs 0.48 ms, respectively. Thus, from Table 3, we can easily choose the best scheme on the basis of computational cost. Likewise, the schemes [7, 9, 11–15, 19] are based on bilinear pairing, which can be required 14.90 ms for single pairing operations; and the mechanisms used in [16, 17] are based on elliptic curve, which requires 0.97 ms, while the schemes of [10, 18] requiring 0.48 ms due to hyperelliptic curve. Based on the aforementioned discussion, we can conclude that the hyperelliptic curve is the most favorable option while designing signcryption scheme for WBAN. Further, for communication overhead, the assumption observed from [18] bilinear pairing, elliptic curve, and the hyperelliptic uses 1024 bits, 160 bits, and 80 bits key sizes, respectively. We can conclude that the hyperelliptic curve will be the best option in terms of communication overhead for such types of WBAN, which have a low bandwidth capacity.

3. Proposed Secured Channel Free Certificateless Signcryption for WBAN

From Table 1, it is very clear that all the existing signcryption schemes for WBAN are suffering from certain flaws such as key escrow, certificate management, and secure channel needs. Further, these schemes are also suffering from the lack of one or more security requirements, and some of the schemes are suffering from high computational communication cost. To remove the key escrow, certificate management, and the need of secure channel problem and to provide all the claimed security requirements as discussed in related work section (3) with low computational and communication cost, we proposed a new framework called secured channel free certificateless signcryption for WBAN. For this new scheme, we adopt the secured channel free concept from [27], certificateless signcryption from [13], and the security and efficiency of the particular scheme based on a hyperelliptic curve [18]. Here, the secure channel free means that this scheme does not require any secure channel for the distributions of partial private key among the participated users. In Figure 4, we show the flow of secured channel-free certificateless signcryption for WBAN. This new ecosystem contains four entities, i.e., the smart sensor nodes, controller, application provider, and key generation center (KGC), respectively. The following substeps can be more helpful while clarifying the working flow of this new ecosystem.

3.1. Key Generation Center. The key generation center generates the public parameter set, master private, and public key. Then, KGC published publicly the public parameter set and master public key. After this, upon receiving the identity from application provider and controller, KGC generates the pseudorandom partial private key (PRPPK) for each user and transmits it to each user through open network.

3.2. Application Providers. Application providers are the run time service providers (SP), i.e., doctors, nurses, smart pharmacy, and emergency services, which monitor the patient's condition. For the monitoring purpose, the SP can request for patient data, while for privacy and authorization, SP perform signcryption on access control query and then transmit it to the controller. For the signcryption process, the application providers first send his identity to KGC for accessing of PRPPK. The KGC then produces PRPPK and sends it to the application providers through open network. The application providers then extract the partial private key from the PRPPK and generate the full public and private key. Further, the application providers generate secret session key for the encryption of patient data. At the end, the application providers produce the signcryption on patient data by using all the aforementioned parameters and transmit it to the controller by using internet.

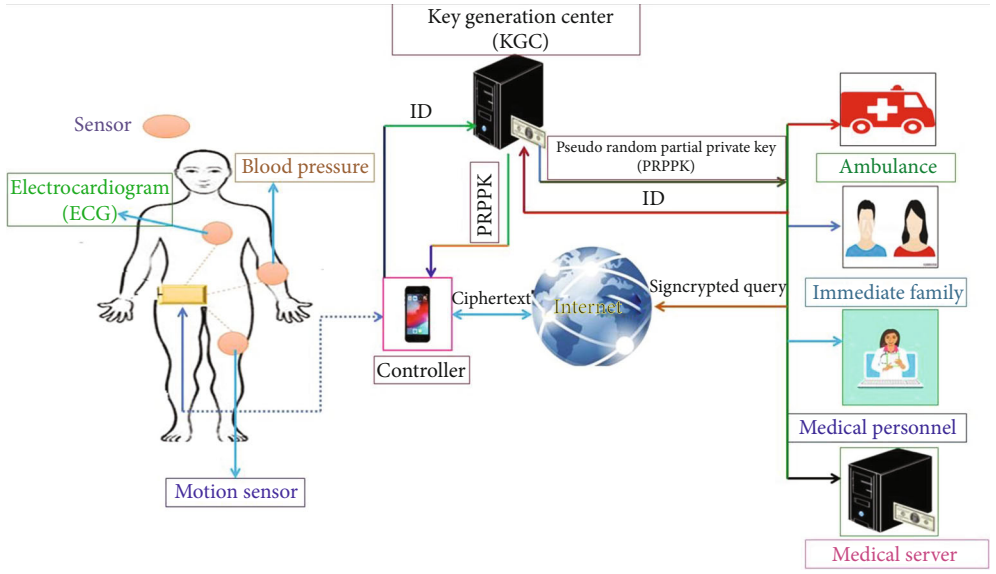


Figure 4: Secure channel free certificateless signcryption for WBAN.

Table 4: Symbols used in the proposed scheme.

S. no	Symbol	Description
1	KGC	Key generation center
2	$\mathscr{L}$	Selected input security parameter from hyperelliptic curve
3	$\mathcal{Q}$	It is a prime number with size $\mathcal{Q} \cong 2^{80}$
4	$F_{\mathcal{Q}}$	A finite field of its order is $\mathcal{Q}$
5	$\mathcal{H}\mathcal{E}^{\circ}C$	A hyperelliptic curve on $F_{\mathcal{Q}}$
6	D	A divisor from $F_{\mathcal{Q}}$
7	$\square$	Master private key of KGC
8	$W = \square.D$	Master public key of KGC
9	$\mathcal{H}_I$, $\mathcal{H}_{II}$, $\mathcal{H}_{III}$, and $\mathcal{H}_{IV}$	Four irreversible hash functions
10	Φ	Public parameter set
11	ID_s, ID_r	Identity of sender and receiver
12	U_s, U_r	Secret value of sender and receiver
13	$\mathcal{O}_s$, $\mathcal{O}_r$	Private key of sender and receiver
14	Y_s, Y_r	Public key of sender and receiver
15	G_r, R_r	Partial private key pair of receiver
16	G_s, R_s	Partial private key pair of sender
17	E_σ	Represents encryption through a secret key σ
18	D_σ	Represents decryption through a secret key σ
19	M	Eptimized plaintext
20	N_s	A fresh nonce which is used to safeguards replay attack
21	$\|\|$	Used for concatinations
22	Z^*_q	A group from hyper elliptic curve of order $\mathcal{Q}$

3.3. Smart Sensor Nodes. These are the small sensors, which are generally implanted within the patient's body for monitoring data regarding the nature of different diseases and then hand over to the controller on demand basis.

3.4. Controller. The controller is a smart device that can be a laptop, mobile phone, and personal digital assistant, etc., which is normally used to receive data from sensors and also the access control signcrypted query from application

Table 5: Computational cost comparisons on the basis of major operations.

Schemes	Signcryption	Unsigncryption	Total
Saeed et al. [11]	5 PBM + 1 E	1 PBM + 2 P	6 PBM + 1 E + 2 P
Lu et al. [12]	11 E + 2 PBM + 1P	6P + 1E	12 E + 2 PBM + 7P
Li et al. [13]	1 E + 4 PBM	2P + 1 E + 2 PBM	2P + 2 E + 6 PBM
Prameela [14]	2 E	3E	5E
Omala et al. [15]	3 PBM	3P + 1PBM	3P + 4PBM
Omala et al. [16]	3 ESM	3 ESM	6 ESM
Gao et al. [17]	3 ESM	4 ESM	7 ESM
Ullah et al. [18]	4 HEM	4 HEM	8 HEM
Iqbal et al. [19]	5 PBM + 1E	1 PBM + 2P	6 PBM + 1E + 2P
Proposed	4 HEM	3 HEM	7 HEM

Table 6: Comparative analysis in terms of ms.

Schemes	Signcryption	Unsigncryption	Total
Saeed et al. [11]	23.52	34.11	57.63
Lu et al. [12]	45.19	91.37	136.56
Li et al. [13]	19.21	40.39	59.6
Prameela [14]	3.94	5.91	9.85
Omala et al. [15]	12.93	49.01	61.94
Omala et al. [16]	2.91	2.91	5.82
Gao et al. [17]	2.91	3.88	6.79
Ullah et al. [18]	1.92	1.92	3.84
Iqbal et al. [19]	23.52	34.11	57.63
Proposed	1.92	1.44	3.36

Table 7: Computation cost improvement in percentage.

Schemes	Computation cost of (A)	Computation cost of (B)	Cost reduction (C)
Saeed et al. [11]	57.63	3.36	94.16
Lu et al. [12]	136.56	3.36	97.53
Li et al. [13]	59.6	3.36	94.36
Prameela [14]	9.85	3.36	65.88
Omala et al. [15]	61.94	3.36	94.57
Omala et al. [16]	5.82	3.36	42.26
Gao et al. [17]	6.79	3.36	50.51
Ullah et al. [18]	3.84	3.36	12.5
Iqbal et al. [19]	57.63	3.36	94.16

Percentage change: $C = (A - B/A) * 100$.

providers. In our case, on receipting the signcrypted query from application providers, the controller then performs the unsigncryption process on it and then verifies and decrypts it. For this process, the controller first sends his identity to the KGC for accessing of PRPPK. The KGC then produces PRPPK and sends it to the controller through open network. The controller extracts the partial private key from the PRPPK and generates the full public and private key. Further, the application providers recover the secret session key for the decryption of access control query. At the end, the controller performs the unsigncryption process upon the signcrypted access control query, if the verification process is done, then, controller decrypts the query and encrypts the requested patient data through secret key and send back to the application providers.

Note: this scheme provides the security services of confidentiality and integrity because it encrypts the patient data through secret key, which is only known to the application providers and the controller. It also resists against the unauthorized user access because if the attacker wants to access the data then he/she must generate a forged signature for it. Therefore, the controller does not generate the forged signature because for this purpose he/she must have the private key of application providers. Even if the private key of application providers/controller is known to the attacker, still this scheme has resisted against to break the confidentiality, because for encryption and decryption purpose, it uses the secret key, which means the new scheme provides the forward secrecy property. Further, this scheme hides the identity of the controller and application providers; it means that it cannot send the identity of the controller and application provider openly with ciphertext, which provides the anonymity property. It also used a technique for the discrepancy resolving among the application providers and controller, if happen, which is called public verifiability security requirement. The new scheme generates a fresh nonce, encrypts it, and sends along with every access control query for the resistance of replay attack. What is more in this new scheme, it is based on a hyperelliptic curve, which is the generalized form elliptic curve which provides the same level of security with 80 bits key in contrast to 160 bits key of elliptic curves. Thus, due to the hyperelliptic curve, our new scheme has the capacity of low computational cost and decrease communication overhead. If we look into the literature section of this paper, only two signcryption schemes [10, 18] for WBAN on the basis of the hyperelliptic curve are available, but the schemes in [10] have the limitations of failing to provide the role of central authority, suffering from certificate renewal and revocations problems, lacking of public verifiability, nonrepudiation, and antireplay attack. The scheme used in [18] can be affected by requiring the certificate

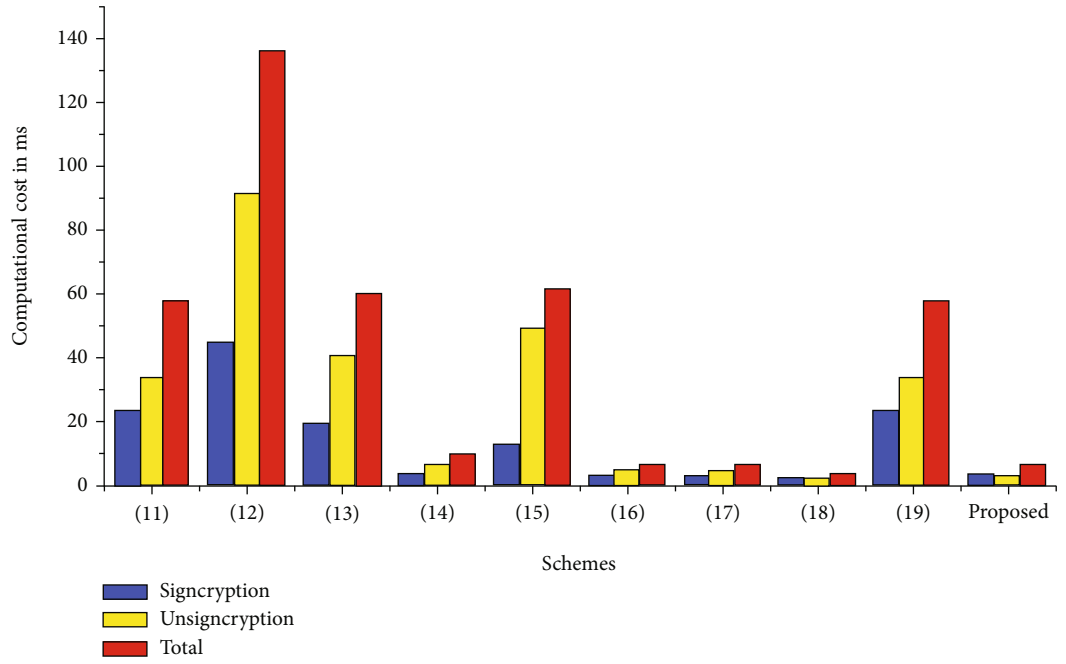


Figure 5: Computational cost.

Table 8: Communication cost improvement in percentage.

Schemes	Computation cost of (A)	Computation cost of (B)	Cost reduction (C)
Saeed et al. [11]	3072	1184	61.45
Lu et al. [12]	4096	1184	71.09
Li et al. [13]	4096	1184	71.09
Prameela [14]	3072	1184	61.45
Omala et al. [15]	3072	1184	61.45
Omala et al. [16]	1504	1184	21.27
Gao et al. [17]	1984	1184	40.32
Ullah et al. [18]	1184	1184	0
Iqbal et al. [19]	3072	1184	61.45

Percentage change: $C = (A - B/A) * 100$.

management in a network which consists a large number of devices, and it can also be affected by the lack of anonymity property. So, our scheme also removes all these disadvantages which are discussed above.

4. Constructions of the Proposed Scheme

It includes the substeps that are setup, actor key setting, actor partial private key setting, actor private key generation, actor public key setting, CLSC-signcrypt, and CL-unsigncrypt, respectively.

Here, first of all, we provide the symbols used in the proposed scheme in Table 4 and the whole process of the construction towards a new scheme in the following steps.

4.1. Setup. The setup phase is executed by KGC to make a system parameter set and master key. The following are the steps which show how to compose a system parameter set and master key.

(1) Given a security parameter $\mathscr{L}$, the KGC chooses a prime number $\mathscr{Q}$ and makes a finite field $F_{\mathscr{Q}}$, where its order is $\mathscr{Q}$ such that $\mathscr{Q} \cong 2^{80}$. Select a hyperelliptic curve $(\mathscr{H}\mathscr{E}^{\circ}C)$ on $F_{\mathscr{Q}}$ and pick a divisor D from $F_{\mathscr{Q}}$

(2) Uniformly select $\square \in Z^*_{\mathscr{q}}$ as the master private key and calculate its public key as $W = .D$, further, it saves $\square$ at his memory and enables W publicly to the network

(3) It also choice the hash functions that are $\mathscr{H}_{\mathrm{I}}$, $\mathscr{H}_{\mathrm{II}}$, $\mathscr{H}_{\mathrm{III}}$, and $\mathscr{H}_{\mathrm{IV}}$

(4) Produce parameter set $\wp = \{\mathscr{H}_{\mathrm{I}}, \mathscr{H}_{\mathrm{II}}, \mathscr{H}_{\mathrm{III}}, \mathscr{H}_{\mathrm{IV}}, \mathscr{Q}, \mathscr{H}\mathscr{E}^{\circ}C, F_{\mathscr{Q}}, W, D\}$ and publish it to the network

4.2. Actor Key Setting. An actor with ID_a uniformly chooses $U_a \in Z^*_{\mathscr{q}}$ as his/her secret value, calculates $V_a = U_a.D$, and sends (V_a, ID_a) to KGC.

4.3. Actor Partial Private Key Setting. After receipting (V_a, ID_a), the KGC then uniformly chooses $P_a \in Z^*_{\mathscr{q}}$, calculates $R_a = P_a.D$, calculates the pseudopartial private key $G_a = P_a + \square\mathscr{H}_I(V_a, R_a, ID_a) + \mathscr{H}_I(V_a.\square, ID_a)$, and sends (G_a, R_a) to an actor with ID_a utilizing an open network.

4.4. Actor Private Key Generation. After receipting (G_a, R_a), an actor with ID_a first verifies it by utilizing the equation $G_a.D = R_a + \mathscr{H}_I(V_a, R_a, ID_a).W + \mathscr{H}_I(U_a.W, ID_a).D$, if it is held, then it extracts the partial private key as $T_a = G_a - \mathscr{H}_I(U_a.W, \mathrm{ID}_a)$ and produces the private key as $\mathscr{O}_a = U_a + T_a$.

4.5. Actor Public Key Setting. An actor with ID_a computes his/her public key as $Y_a = V_a + R_a$ and sends it to the KGC through open network.

Table 9: Comparative analysis in terms of bits.

Schemes	Ciphertext size
Saeed et al. [11]	$\|m\| + 2\|G\|$
Lu et al. [12]	$\|m\| + 8\|G\|$
Li et al. [13]	$\|m\| + 3\|G\|$
Prameela [14]	$\|m\| + 2\|G\|$
Omala et al. [15]	$\|m\| + 2\|G\|$
Omala et al. [16]	$\|m\| + 3\|q\|$
Gao et al. [17]	$\|m\| + 6\|q\|$
Ullah et al. [18]	$\|m\| + 2\|n\|$
Iqbal et al. [19]	$\|m\| + 2\|G\|$
Proposed	$\|m\| + 2\|n\|$

4.6. CL-Signcrypt. With the sender and receiver identities $(\mathrm{ID_s}, \mathrm{ID_r})$ and a messages M, the sender performs the following steps by composing CGSWSC-signcrypt algorithm.

(1) Uniformly choose $\gamma \in Z^*_{\mathbb{Q}}$ and calculate $\beta = \gamma.D$

(2) Compute $\boldsymbol{d} = \gamma.(Y_\mathrm{r} + \mathscr{H}_\mathrm{I}(Y_\mathrm{r}, \mathrm{ID_r}).W)$ and $\eta = \mathscr{H}_\mathrm{II}(\beta, \mathrm{ID_r}, \delta)$

(3) Uniformly choose another number $\Phi \in Z^*_q$ and compute $\sigma = \mathscr{H}_\mathrm{III}(\beta, \Phi)$

(4) Generate the ciphertext as $\mathscr{K} = {}_\sigma(M[]\mathrm{N_s})$ and then calculate a digital signature as $\Delta = \mho_\mathrm{s} + \gamma.\varphi$, where $\varphi = \mathscr{H}_{IV}(M[]\mathrm{ID_s}, \beta, \Phi)$

(5) At the end, the sender transmits $\psi = (\Lambda, \Delta, \varphi, \beta)$ to the receiver

4.7. CL-Unsigncrypt. Upon receipting $\psi = (\Lambda, \Delta, \varphi, \beta)$, the receiver can verify it by composing the following steps.

(1) Calculate $\boldsymbol{d} = \mho_\mathrm{r}.\beta$ and $\eta = \mathscr{H}_\mathrm{II}(\beta, \mathrm{ID_r}, \delta)$

(2) Compute $\Phi = f(\eta)$ and calculate $\sigma = \mathscr{H}_\mathrm{III}(\beta, \Phi)$

(3) Recover the plain text as $(M[]N_\mathrm{s}) = D_\sigma(\Lambda)$ and compute $\varphi^{\exists} = \mathscr{H}_\mathrm{IV}(M[]\mathrm{ID_s}, \beta, \Phi)$

(4) Accept $(\mathrm{M}[]\mathrm{ID_s})$, if $\varphi^{\exists} = \boldsymbol{v}$ and $\Delta.D = Y_s + \mathscr{H}_\mathrm{I}(Y_\mathrm{s}, \mathrm{ID_s}).W + \varphi.\beta$ are holds

4.7.1. Correctness. Each actor with ID_a can verify the pseudopartial private key G_a by utilizing the following computations:

$$\begin{aligned} G_\mathrm{a}.D &= (R_\mathrm{a} + \mathscr{H}_I(V_\mathrm{a}, R_\mathrm{a}, \mathrm{ID_a}).W + \mathscr{H}_I(U_\mathrm{a}.W, \mathrm{ID_a}).D \\ &= G_\mathrm{a}.D = (P_\mathrm{a} + \square\mathscr{H}_I(V_\mathrm{a}, R_\mathrm{a}, \mathrm{ID_a}) \\ &\quad + \mathscr{H}_I(V_\mathrm{a}.\square, \mathrm{ID_a})).D \\ &= (P_\mathrm{a}.D + \square.D\mathscr{H}_I(V_\mathrm{a}, R_\mathrm{a}, \mathrm{ID_a}) + \mathscr{H}_I(V_\mathrm{a}.\square, \mathrm{ID_a}).D) \\ &= R_\mathrm{a} + \mathscr{H}_I(V_\mathrm{a}, R_\mathrm{a}, \mathrm{ID_a}).W + \mathscr{H}_I(V_\mathrm{a}.\square, \mathrm{ID_a}).D). \end{aligned} \tag{1}$$

The receiver can verify the signature as if $\Delta.D = Y_s + \mathscr{H}_\mathrm{I}(Y_\mathrm{s}, \mathrm{ID_s}).W + \varphi.\ \beta$ is held.

$$\begin{aligned} &= \Delta.D = (\mho_\mathrm{s} + \gamma.\varphi).D = (U_\mathrm{s} + \mathrm{T_s} + \gamma.\varphi).D \\ &= (U_\mathrm{s} + G_\mathrm{s} - \mathscr{H}_I(U_\mathrm{s}.W, \mathrm{ID_s}) + \gamma.\varphi).D \\ &= (U_\mathrm{s} + G_\mathrm{s} - \mathscr{H}_I(U_\mathrm{s}.\square.\mathrm{D}, \mathrm{ID_s}) + \gamma.\varphi).D \\ &= (U_\mathrm{s} + P_\mathrm{s} + \mathscr{H}_I(V_\mathrm{s} + R_\mathrm{s}, \mathrm{ID_s}) + \mathscr{H}_I(V_\mathrm{s}.,\mathrm{ID_s}) \\ &\quad - \mathscr{H}_I(V_\mathrm{a}.,\mathrm{ID_s}) + \gamma.\varphi).D = (U_\mathrm{s} + P_\mathrm{s} + \mathscr{H}_I(V_\mathrm{s} + R_\mathrm{s}, \mathrm{ID_s}) \\ &\quad + \gamma.\varphi).D = (U_\mathrm{s}.D + P_\mathrm{s}.D + D\mathscr{H}_I(V_\mathrm{s} + R_\mathrm{s}, \mathrm{ID_s}) + \gamma.D.\varphi) \\ &= (V_\mathrm{s} + R_\mathrm{a} + \mathscr{H}_I(V_\mathrm{s} + R_\mathrm{s}, \mathrm{ID_s})\mathrm{W} + \varphi.\beta \\ &= Y_\mathrm{s} + \mathscr{H}_\mathrm{I}(Y_\mathrm{s}, \mathrm{ID_s}).W + \varphi.\beta. \end{aligned} \tag{2}$$

5. Security Discussions

This scheme provides the security services of confidentiality and integrity because it encrypts the patient data through secret key, which is only known to the application providers and the controller. It also resists against the unauthorized user access because if the attacker wants to access the data then he/she must generate a forged signature for it. Therefore, the attacker does not generate the forged signature because for this purpose he/she must have the private key of application providers. Even if the private key of application providers/controller is known to the attacker, still this scheme has resisted against to break the confidentiality, because, for encryption and decryption purposes, it uses the secret key, which means the new scheme provides the forward secrecy property. Further, this scheme hides the identity of the controller and application providers; it means that it cannot send the identity of the controller and application provider openly with ciphertext, which provides the anonymity property. It also used a technique for the discrepancy resolving among the application providers and controller, if happen, which is called public verifiability security requirement. The new scheme generates a fresh nonce, encrypts it, and sends along with every access control query for the resistance of replay attack. What is more in this new scheme, it is based on a hyperelliptic curve, which is the generalized form elliptic curve which provides the same level of security with 80 bits key in contrast to 160 bits key of elliptic curves. Thus, due to the hyperelliptic curve, our new scheme has the capacity of low computational cost and decrease communication overhead. If we look into the literature section of this paper, only two signcryption schemes [10, 18] for WBAN on the basis of the hyperelliptic curve are available, but the schemes in [10] have the limitations of failing to provide the role of central authority, suffering from certificate renewal and revocations problems, lacking of public verifiability, nonrepudiation, and antireplay attack. The scheme used in [18] can be affected by requiring the certificate management in a network which consists a large number of devices, and it can also be affected by the lack of anonymity property. So, our scheme also removes all these disadvantages which are discussed above.

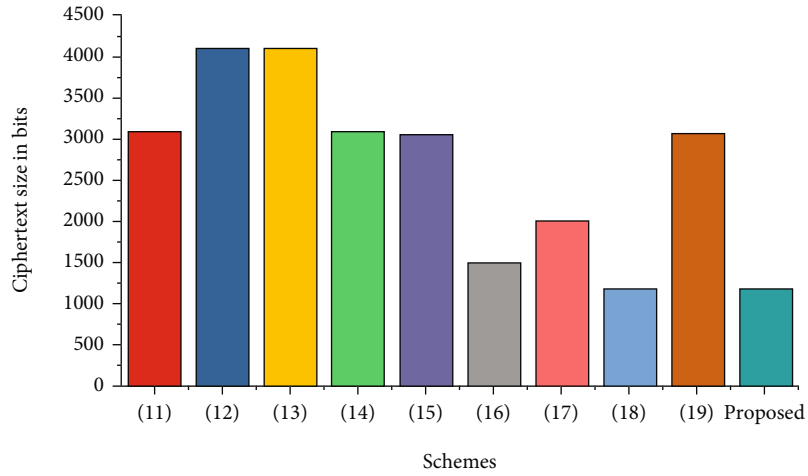


Figure 6: Communication cost.

6. Performance Analysis

This section includes performances analysis in terms of computational and communication costs.

6.1. Computational Cost. In Table 5, we give the computational cost comparison among our designed secure channel free certificateless signcryption and the existing ones, i.e., Saeed et al. [11], Lu et al. [12], Li et al. [13], Prameela [14], Omala et al. [15], Omala et al. [16], Gao et al. [17], Ullah et al. [18], and Iqbal et al. [19] on the basis of major operations. We consider the major operation, i.e., bilinear pairing, pairing-based scalar multiplication, exponential, hyperelliptic divisor multiplication, and elliptic curve scalar multiplication in the proposed one and in Saeed et al. [11], Lu et al. [12], Li et al. [13], Prameela [14], Omala et al. [15], Omala et al. [16], Gao et al. [17], Ullah et al. [18], and Iqbal et al. [19]. Further, P, PBM, E, HEM, and ESM signify one pairing operation, one pairing-based scalar multiplication operation, one exponential operation, one hyperelliptic curve divisor multiplication operation, and one elliptic curve scalar multiplication operation, respectively. Additionally, we create comparisons among the proposed one and Saeed et al. [11], Lu et al. [12], Li et al. [13], Prameela [14], Omala et al. [15], Omala et al. [16], Gao et al. [17], Ullah et al. [18], and Iqbal et al. [19] on the basis of milliseconds (ms), which is shown in Table 6. We observed from [21] that the single ESM consumes 0.97 ms, P needs 14.90 ms, PBM consumes 4.31 ms, E needs 1.97 ms, and it is also assumed that HEM earnings consume 0.48 ms [22–26]. Moreover, a computation cost reduction is shown in Table 7 and Figure 5, respectively.

6.2. Communication Overhead. Sending additional bits along with the actual ciphertext is called communication overhead. If the additional bits are smaller in size, then, the communication will be fast; otherwise, delays will occur in communications. In this phase, we compare our designed CB-PS with existing ones, i.e., Saeed et al. [11], Lu et al. [12], Li et al. [13], Prameela [14], Omala et al. [15], Omala et al. [16], Gao et al. [17], Ullah et al. [18], and Iqbal et al. [19] on the basis of communication overhead as shown in Table 8. To make these comparisons, we suppose that $|H| \cong |ID| \cong |q| \cong 2160$ bits, $|h| \cong |ID| \cong |n| \cong 280$ bits, $|G|$, and $|\mathscr{mW}| \cong |\mathscr{m}| \cong 1024$ bits. Besides, a communication cost reduction is shown in Tables 9 and 8 and Figure 6, respectively.

7. Conclusion

A detailed review of the currently available signcryption schemes that might be used in the WBAN system is presented in this article. Then, each scheme is subjected to a critical review in terms of security requirements, as well as the need for computational and communication expenses. The research revealed that the majority of existing WBAN signcryption schemes failed to meet one or more security requirements, as well as had high computational and communication costs. Then, for WBAN applications, we presented a new framework called secure channel free certificateless signcryption scheme, which is based on the notion of a hyperelliptic curve. The proposed scheme removes all the limitations of existing signcryption schemes for WBAN, because it does not suffer from the certificate management problem, key escrow problem, and does not require any secure channel for the distribution of partial private key. In addition, the scheme is lightweight in terms of computational and communication costs. Furthermore, the new scheme has the capability of providing the security requirements, such as confidentiality, integrity, resist against the unauthorized user, unforgeability, public verifiability, forward secrecy, and antireplay attack, respectively. In the future, we are intended to apply the same scheme to the multimessage and multireceiver environment.

Data Availability

All data generated or analyzed during this study are included in this article.

Conflicts of Interest

The authors declare no conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

[1] A. Meharouech, J. Elias, and A. Mehaoua, "Moving towards body-to-body sensor networks for ubiquitous applications: a survey," *Journal of Sensor and Actuator Networks*, vol. 8, no. 2, p. 27, 2019.

[2] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: a survey," *IEEE Communication Surveys and Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[3] M. A. Khan, I. M. Qureshi, and F. Khanzada, "A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (FANET)," *Drones*, vol. 3, no. 1, p. 16, 2019.

[4] Y. Chen and F. Zhao, "A hybrid half-duplex/full-duplex transmission scheme in relay-aided cellular networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, Article ID 795, 15 pages, 2017.

[5] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption)," in *Annual international cryptology conference*, pp. 165–179, Berlin, Heidelberg, 1997.

[6] N. U. Amin, J. Iqbal, and A. R. Abbasi, "Secure key establishment and cluster head selection for body area networks based on signcryption," *Journal of Applied Environmental and Biological Sciences*, vol. 4, pp. 210–216, 2014.

[7] C. Wang and J. Liu, "Attribute-based ring signcryption scheme and its application in wireless body area networks," in *International Conference on Algorithms and Architectures for Parallel Processing*, pp. 521–530, Cham, 2015.

[8] A. Arul Jothi and B. Srinivasan, "Security analysis in body area networks using attribute-based ring signcryption scheme," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 13, no. 1, pp. 48–56, 2016.

[9] F. Li and J. Hong, "Efficient certificateless access control for wireless body area networks," *IEEE Sensors Journal*, vol. 16, no. 13, pp. 5389–5396, 2016.

[10] J. Iqbal, N. U. Amin, and A. I. Umar, "Nizamuddin, public verifiable signcryption and cluster head selection for body sensor networks," *Journal of Applied Environmental and Biological Sciences*, vol. 6, pp. 64–72, 2016.

[11] M. E. S. Saeed, Q. Liu, G. Tian, B. Gao, and F. Li, "HOOSC: heterogeneous online/offline signcryption for the internet of things," *Wirel. Networks*, vol. 24, no. 8, pp. 3141–3160, 2018.

[12] Y. Lu, X. Wang, C. Hu, H. Li, and Y. Huo, "A traceable threshold attribute-based signcryption for mHealthcare social network," *International Journal of Sensor Networks*, vol. 26, no. 1, pp. 43–53, 2018.

[13] F. Li, Y. Han, and C. Jin, "Cost-effective and anonymous access control for wireless body area networks," *IEEE Systems Journal*, vol. 12, no. 1, pp. 747–758, 2018.

[14] S. Prameela, "Enhanced certificateless security improved anonymous access control with obfuscated quality-aware confidential data discovery and dissemination protocol in WBAN," *International Journal of Pure and Applied Mathematics*, vol. 118, pp. 2627–2635, 2018.

[15] A. A. Omala, I. Ali, and F. Li, "Heterogeneous signcryption with keyword search for wireless body area network," *Security and Privacy*, vol. 1, no. 5, article e25, 2018.

[16] A. A. Omala, A. S. Mbandu, K. D. Mutiria, C. Jin, and F. Li, "Provably secure heterogeneous access control scheme for wireless body area network," *Journal of Medical Systems*, vol. 42, no. 6, p. 108, 2018.

[17] G. Gao, X. Peng, and L. Jin, "Efficient access control scheme with certificateless signcryption for wireless body area networks," *International Journal of Network Security*, vol. 21, pp. 428–437, 2019.

[18] I. Ullah, A. Alomari, N. Ul Amin, M. A. Khan, and H. Khattak, "An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the internet of things," *Electronics*, vol. 8, no. 10, p. 1171, 2019.

[19] J. Iqbal, A. I. Umar, N. Amin, and A. Waheed, "Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019.

[20] H. Xiong, Y. Hou, X. Huang, Y. Zhao, and C. -M. Chen, "Heterogeneous signcryption scheme from IBC to PKI with equality test for WBANs," *IEEE Systems Journal*, pp. 1–10, 2021.

[21] I. Ullah, N. U. Amin, J. Khan et al., "A novel provable secured signcryption scheme: a hyper-elliptic curve-based approach," *Mathematics*, vol. 7, no. 8, p. 686, 2019.

[22] M. Asghar Khan, I. Ullah, A. Alkhalifah et al., "A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

[23] M. A. Khan, I. Ullah, N. Kumar et al., "An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4839–4851, 2021.

[24] M. A. Khan, I. Ullah, S. Nisar et al., "Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Information Systems*, vol. 2020, Article ID 8861947, 15 pages, 2020.

[25] M. A. Khan, H. Shah, S. U. Rehman et al., "Securing internet of drones with identity-based proxy signcryption," *IEEE Access*, vol. 9, pp. 89133–89142, 2021.

[26] M. A. Khan, S. U. Rehman, M. I. Uddin et al., "An online-offline certificateless signature scheme for internet of health things," *Journal of Healthcare Engineering*, vol. 2020, Article ID 6654063, 10 pages, 2020.

[27] L. Pang, M. Kou, M. Wei, and H. Li, "Anonymous certificateless multi-receiver signcryption scheme without secure channel," *IEEE Access*, vol. 7, pp. 84091–84106, 2019.