Hindawi
Journal of Sensors
Volume 2023, Article ID 4237198, 16 pages
https://doi.org/10.1155/2023/4237198

Research Article

Stochastic Bat Optimization Model for Secured WSN with Energy-Aware Quantized Indexive Clustering

J. Paruvathavardhini and B. Sargunam

Department of Electronics and Communication Engineering, School of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India

Correspondence should be addressed to J. Paruvathavardhini; vardhini.jpv@gmail.com

Received 23 January 2023; Revised 11 May 2023; Accepted 13 May 2023; Published 26 May 2023

Academic Editor: Giovanni Diraco

The wireless sensor networks (WSNs) with dynamic topology communication among the sensor nodes is vulnerable to numerous attacks. As they have limited power, there arises a conflict between the complex security scheme and the consumption of energy which are inversely proportional to each other. Hence, a trade-off should be accomplished between the implemented scheme and energy. A novel secure and energy-aware routing technique quantized indexive energy-aware clustering-based combinatorial stochastic sampled bat optimization (QIEAC-CSSBO) is proposed which consists of clustering, optimal route path identification, and route maintenance. The clustering process and selection of cluster head (CH) with high residual energy is done using the quantized Schutz indexive Linde–Buzo–Gray algorithm (QIEAC). Optimal route identification is done using CSSBO (combinatorial stochastic sampled Prevosti's bat optimization), and fitness of every bat is measured on combinatorial functions, namely, distance, energy, trust, and link stability among nodes. Stochastic universal sampling selection procedure is applied to select the global best optimal path for secure data transmission. Lastly, route maintenance process is performed to identify alternative route while link failure occurs among nodes. Experimental assessment is performed using various performance metrics, namely, energy consumption, packet delivery ratio, packet drop rate, throughput, and delay. The proposed method QIEAC-CSSBO enhances the performance of packet delivery ratio by 4%, throughput by 26%, and packet drop rate by 27% and reduces energy consumption by 11%, as well as delay by 16% as compared to existing techniques.

1. Introduction

Wireless sensor networks (WSN) have imprinted its inevitable need in all the fields like environmental monitoring, health monitoring, precision agriculture, industrial monitoring, smart home (IoT-based WSN), traffic monitoring, and military applications. WSN is a network area which includes large number of nodes and ability of wireless transmission, but it has inadequate battery power and minimal storage capacity. A sensor node in WSN monitors and collects the data from the various environments. The collected data is sent from one location to another by means of wireless spontaneous connectivity [1, 2]. These nodes comprise of small components like transceivers, microprocessor, and controller to process and communicate the sensed data to the desired destination, and there is a battery to support all these operations. Hence, the battery plays a vital role in the performance of a sensor network as its lifetime is based on the same as it is very difficult to change the battery in the case of deployed sensors. The performance of a WSN diminishes as the nodes die without energy, so it is remarkably important to extend the lifetime of the nodes by efficiently using the energy [3–5]. Several works were proposed to improve the lifetime of the network, and most of the proposed works focus on improved routing protocols based on the cluster. The performance of the network requires a trade-off between the energy constraint and the resource limitations of the sensors. However, when there are many nodes in the network, the standard direct routing uses more energy and may significantly shorten the network lifetime [6]. In WSN, the whole network is divided into subnetworks called clusters controlled by a node within that family called cluster

head (CH). Hence, in this type of routing, the intracluster and intercluster communications may behave in a multihop fashion. In order to conserve its remaining energy and avoid wasting it trying to communicate with a neighbor who is far away, a sensor node only interacts with its nearest neighbor. This was the method that was initially developed in the name of LEACH [7], and later, many routing protocols were developed with many other techniques in such a way to preserve the energy of the nodes in the network [8, 9]. A very sensitive and adaptive method of clustering should be developed to extend the lifetime of a WSN.

One of the key concerns with WSNs is secure data transmission. Due to the open communication channel between the sensor nodes, the network is susceptible to many attacks, and additionally, the central communication is relatively complex owing to the dynamic topology structure. Wireless communication networks are more susceptible to physical layer, link layer, and network layer threats such as congestion attack, forgery attack, and collision attack than wired communication networks [10]. For some applications, such as those in the military and sensing jobs in unreliable situations, many WSNs are deployed in harsh, unpredictable, and frequently hostile physical environments. In many of these actual WSNs, secure data transfer is very important and desired. Security and privacy are therefore of the utmost importance for the development of WSNs and sensor network applications [11, 12]. This lead to the development of various encryption-based algorithms for data security and image security in different application like military, environmental monitoring, healthcare, and IoT [13, 14]. Implementation of security algorithm in the WSN may reduce the performance and energy, so there should be a trade-off between the security implemented and usage of the battery power [15–17]. So, an efficient routing protocol should be proposed to manage both the complexity and the usage of power.

The development of WSN in a huge number of applications is done in common. The enhancement of system lifetime is achieved by managing the usage of energy. But, the management of energy still remains a challenge as when the complexity of algorithm increases used to achieve better transmission or to enhance the level of security. So, the scope of this research is to reduce the energy consumption and efficiently use the available energy and thus propose an integrated method of cluster formation and CH selection, to enhance energy efficiency as well as secure routing within WSN, thus achieving a trade-off between the security algorithm implemented and energy consumption. With respect to the aforementioned case, a better technique, QIEAC-CSSBO (quantized indexive energy-aware clustering-based combinatorial stochastic sampled bat optimization), is proposed. First, the quantized Schutz indexive Linde–Buzo–Gray algorithm is applied to a QIEAC-CSSBO technique for clustering the sensor nodes. Secondly, the combinatorial stochastic sampled Prevosti's bat optimization algorithm is employed to find an efficient and secured route. Following this, a route maintenance is done to observe for a fault node or malicious node with the help of fitness value and fix it.

The paper is organized as follows: Section 2 discusses in detail about the various types of clustering-based routing protocols and different optimization methods to improve the network lifetime with some of the security methods, and it winds up with the research gaps identified along with the objectives of this research. The proposed system model for clustering and optimal path finding is discussed in Section 3. The performance analysis of the proposed system is discussed in Section 4, and Section 5 exemplifies the conclusion with future scope.

2. Related Work

Several works have been proposed which discusses about the effective usage of the energy, curtailing energy consumption, and security of the data transmitted in WSN. The network clustering can extend the life of sensor nodes by reducing their energy consumption. This is a crucial strategy for energy conservation. Similar to clustering, routing has a big impact on energy usage reduction. In WSN, clustering and routing are crucial factors in how much energy sensor nodes use. Therefore, various evolutionary and bioinspired optimization strategies are investigated and explored in this research in order to prolong the life of this network. Therefore, various evolutionary and bioinspired optimization strategies are investigated and explored in this research in order to prolong the life of this network [18].

Taylor C-SSA has been presented by [19] to achieve multihop routing using CH selection as well as data transmission. QEBSR is designed in [20] for energy-efficient data transmission and minimize delay. Here, better throughput was not achieved. LD^2 FA-PSO is proposed in [21], for energy-efficient data transmission through the optimal path and finding the attackers. E-ALWO is designed in [22] to route the data packets based on energy and trust.

Multiobjective-based clustering as well as sailfish optimizer (SFO) is proposed [23] for maintaining energy efficiency and prolong network lifetime. Distributed as well as optimized fuzzy clustering method is introduced in [24] for enhancing data transmission and reduce packet loss.

SEHR [25] has been proposed to identify the attacks and minimize the packet drop ratio in WSN. Lightweight as well as Secure Tree-based Routing protocol (LSTR) was introduced in [26], and an effective ID-based authenticated key-agreement mechanism is used to secure the data routing from sensor nodes to the base station (BS). LSTR limits the number of necessary keys to a single, preloaded permanent private key in sensor nodes. HMBCR method has been proposed in [27] for WSN to guarantee efficiency of energy as well as lifetime of network. An energy-efficient clustering is presented in [28], to collect and transmit data using a higher packet delivery ratio by minimal energy consumption. A hybrid WGWO-based clustering method was proposed in [29], which combines two metaheuristic algorithms whale and grey wolf for achieving better clustering mechanism (formation of clusters and selection of cluster head) in a dynamic manner with the help of relay nodes. A new technique, which considers both energy efficiency and security is designed in [30] for WSN, in order to protect against

internal threats LTMS (lightweight trust management scheme) based on binomial distribution, is proposed, MSCR (multidimensional secure clustered routing) is proposed for implementing the security scheme on considering the domains of distance, energy, security, and environment simultaneously.

User-independent as well as dynamical technique GSA (gravitational search algorithm) is proposed in [31] for measuring optimal number of clusters as well as establishing finest CH which improves the network lifetime. BOA (butterfly optimization algorithm) for selecting optimal CH by considering the residual energy, distance to and from the neighbor nodes and BS, node centrality and degree over collection of nodes, and ACO (ant colony optimization) for finding the optimal route to the base station is presented in [32]. SCEER (secure cluster-based efficient energy routing) is designed in [33] for achieving higher network lifetime for effective and secured packet transmission in two phases. The proposed system does not attain higher throughput. CEMT (A Cognitive Energy Efficient and Trusted Routing Model) for the security of wireless sensor networks is proposed in [34], by using trust calculation algorithm to secure the network environment with improved detection approaches based on nodes' increased coincidence rates to locate the malicious behaviour.

TBSIOP (Trust-Based Secure Intelligent Opportunistic Routing Protocol) is designed in [35] for enhancing performance of packet delivery ratio and delay by checking the genuineness of the relay nodes. The qualities used are genuineness in data forwarding, sending acknowledgements, and energy depletion. Grey wolf-updated whale optimization was implemented in [36] to cluster-based routing scheme for choosing optimal CH for providing better energy model, radio model, and security model considering the threshold value of the risk factors.eeTMFO/GA (energy efficient trusted moth flame optimization and genetic algorithm-based clustering algorithm) was designed in [37] for secure and energy-aware data transmission. Here, CH is selected using the moth flame algorithm by using attributes like average distance between the clusters, residual energy, node density, and delay. x Integration of GSO (glowworm swarm optimization) with ACO (ant colony optimization), i.e., GSO-ACO, is proposed in [38] to energy-efficient optimal cluster head selection considering the attributes like energy, delay, and distance. ACO has the benefits of being simple to search through in parallel, finding good solutions quickly, adapting to changes like new distances, and ensuring convergence. The fact that GSO does not require centralized control makes it easily scalable, and it also has the ability to learn quickly and is suitable for nonlinear modelling.

The energy consumption issue is improved by a new algorithm that clusters sensor nodes in wireless sensor networks using the bacterial foraging optimization algorithm [39]. By designating a few nodes as cluster heads, this technique encourages the emergence of useful clusters in the network. When communicating with the cluster head, which receives data packets from every node in the cluster, nodes employ a one-step routing protocol. The cluster head then sends the compiled data to the mobile sink node via a predetermined path. The ICCHR (improved chain-based clustering hierarchical routing) algorithm [40] uses a threshold-setting technique that is appropriate for environments with long direct deployment orchards. Here, the algorithm uses the greedy algorithm to form a chain of the elected CHs. Then, based on the distance, it is labelled and involved in communication. A source routing-based energy-efficient region routing protocol (ER-SR) was designed by [41], which uses a distributed energy region technique that is proposed to dynamically choose the network nodes with high residual energy as source routing nodes. It allows only the partial nodes to participate in the routing process and balance the energy consumption of sensor nodes, the source routing nodes, then chooses the best source routing path for every common node. Additionally, an efficient distance-based ant colony optimization technique is proposed to find the global ideal transmission channel for each node in order to reduce the energy consumption of data transmission. A HCSA (hybrid crow search algorithm) is proposed [42] for efficient data gathering from the CHs, therefore enhancing the network lifetime. A multiobjective-based weighted sum approach is then used to choose a precise data gathering node in the circular cell cluster region, considering factors like proximity, communication cost, residual energy, and coverage. To collect data from the cluster head, routing and dynamic mobile sink relocation methods are used. An examination of the LEACH protocol and how wormhole attacks affect energy dissipation, and affected network performance was done in [43]. The deployment of security protocols and when there are more than 5-8 cluster heads also affect the network's performance.

A secured DMHCET routing protocol based on the hierarchical clustering technique has been suggested by [44], and multilevel cluster zones exist in this; each zone collects data and shares it with the zone below it. The zonal head is changed for each transmission using the remaining energy in this manner, which offers a better-secured channel while consuming less energy. It guarantees a reliable next hop node and will promptly alter the route in the event of a deviation. The bat algorithm was reformed to improve the choice of cluster-head nodes from the traditional method LEACH, and a curve technique was developed using FTBA (FTBA-TC) [45]. FTBA-TC improved BA's global and local search capabilities while enhancing the local search functionality based on FTBA. Experiments were used to examine three alternative curve forms and six different parameter combinations. For the LEACH protocol, a unified heuristic bat algorithm (UHBA) is proposed [46]. To further optimize the cluster head of the LEACH, the unified heuristic technique is employed to balance the global search with the local search. As a result, the cluster, which is located not too far from the base station, has its cluster heads scattered quite evenly. A standard routing protocol for wireless sensor networks (WSN) with two main goals is proposed: on-demand- and node behaviour-(ODNB-) based routing [47]. The routing procedure is then started between any two nodes the user chooses. The cluster head nodes in the clustered network then collect, aggregate, and transmit data. Second, data routing is performed as needed, with the source and destination nodes chosen in accordance with the needs of the application.

There are various limitations in each method that was discussed, various protocols were proposed for energy aware and security on its way, but when security is implemented with precision, the energy becomes a challenge. Some of the critics (research gaps) are as follows:

(i) The authors have not achieved the expected time for packet delivery; hence, time delay got increased. End-to-end delay, delay aware routing, node authentication, and throughput are not achieved [20, 23, 26, 28, 29, 31–33, 39, 40, 42, 45]

(ii) The authors have not utilized the energy harvesting method efficiently to enhance network operation, and energy efficient routing was not established; also, efficient metaheuristic optimization with less complexity was not developed for identifying routing path [22, 25, 27, 36–38, 41, 43]

(iii) The node authenticity, energy consumption for individual attacks, energy-efficient-secured data transmission, optimized path for secured transmission, and the attacks within layered networked construction are not achieved by the works presented in the literature review [19, 21, 24, 34, 35, 44, 46, 47]

(iv) This method failed to consider basic parameters, and security is based on cluster head, and it does not bother about other nodes in the network [30].

Based on the purview to overcome the above limitations, this paper focuses on implementing the following contributions:

(i) To achieve an efficient data transmission; the node that uses the remaining residual energy in a better way is chosen as CH for every cluster

(ii) To propose a better optimization technique finds the best optimal path on multiple objective functions, namely, distance, energy, trust, and link stability between nodes

(iii) Applying the stochastic universal sampling selection procedure to the optimization algorithm to select the current best and position and velocity updates is used to find the global best solution for secure data transmission

(iv) To recognize the optimal route path for achieving data transmission which also aids to enhance packet delivery as well as minimize packet drop

(v) Finally, the route maintenance procedure improves transmission and minimizes the delay by detecting the alternative route when the link failure occurs between the nodes

An extensive simulation is carried out to estimate the performance of the proposed QIEAC-CSSBO technique and compared with the two existing works Taylor C-SSA [19] and QEBSR [20].

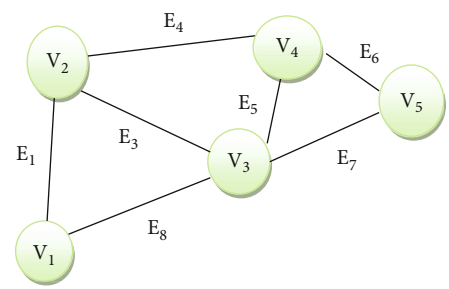


Figure 1: Directed graph.

3. System Model

In this section, the secured clustering scheme quantized indexive energy-aware clustering-based combinatorial stochastic sampled bat optimization (QIEAC-CSSBO) is proposed with the combination of the following algorithms: (i) quantized Schutz indexive Linde–Buzo–Gray clustering algorithm and (ii) combinatorial stochastic sampled Prevosti's bat optimization algorithm. The first section describes the process of cluster formation with cluster head selection using the quantized Schutz indexive Linde–Buzo–Gray clustering algorithm. The second section describes in detail about the optimal path selection and route maintenance using the Combinatorial Stochastic Sampled Prevosti's Bat Optimization algorithm. In this way, sensor nodes are grouped into smaller clusters. Hence, the optimal route is picked in the network, which makes the scheme consume low power. The network and energy model is explained in Section 3.1.

3.1. Network and Energy Model. The proposed QIEAC-CSSBO uses the directive graph for secure data transmission. The directed graph is a mathematical model used to determine the relationship between the two variables.

From Figure 1, a weighted undirected graph is formulated as

$$G = (V, E), \tag{1}$$

where "V" denotes the sensor nodes $Sn_i \in Sn_1, Sn_2, Sn_3 \cdots Sn_n$ (soldiers) deployed in a squared area "$n * n$," and "E" stands for the links (i.e., relationship) between the sensor nodes (soldiers). Figure 2 demonstrates the directive graph with five vertices (i.e., sensor nodes) V_1, V_2, V_3, V_4, V_5 and eight edges $E_1, E_2, E_3, E_4, E_5, E_6, E_7, E_8$ (i.e., links). Each sensor node in the network collects the information or sensitive data packets "$dp_i = dp_1, dp_2, \cdots, dp_n$." The deployed sensor nodes are partitioned into a number of clusters $C_1, C_2, \cdots C_k$. For each node in the network, we have to find the multicriteria (i.e., multiobjective) functions such as distance, energy, trust, and link stability between the nodes for secured data transmission. The energy (i.e., initial energy) of the sensor node is estimated based on the product of power and time. It is formulated as given below:

$$E_n = P_w * T_m. \tag{2}$$

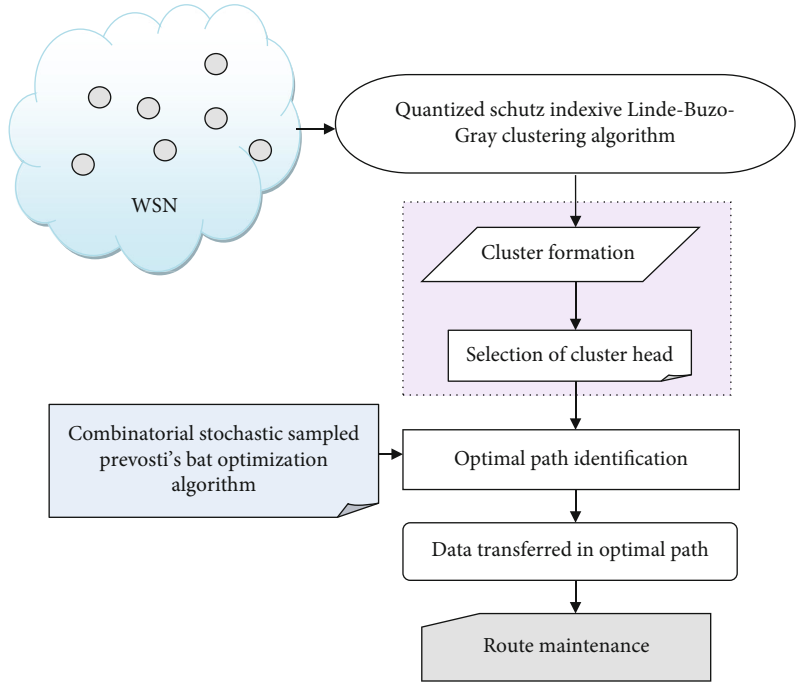


Figure 2: Architecture of the proposed QIEAC-CSSBO technique.

From (2), E_n denotes an energy level of the sensor nodes, P_w denotes power, and T_m indicates a time. The energy that is remaining back after each process is called residual energy and that is measured:

$$E_{res} = E_{\text{ini}} - E_{\text{cons}}. \tag{3}$$

In (3), E_{res} denotes residual energy, E_{ini} represents total energy and E_{cons} indicates energy consumption.

3.1.1. Proposed Framework. WSNs in the military application are typically confirmed to be a very cooperative technology on the entire battlefield. Hence, a novel quantized indexive energy-aware clustering-based combinatorial stochastic sampled bat optimization (QIEAC-CSSBO) is introduced. This QIEAC-CSSBO technique focuses on security as an important paradigm for performing energy-efficient data transmission. The QIEAC-CSSBO technique undergoes three stages for attaining energy efficiency and security of communication through clustering, optimal route path identification, and route maintenance.

Figure 2 illustrates QIEAC-CSSBO to perform secure and energy-efficient data transmission in WSN. Initially, the quantized Schutz indexive Linde–Buzo–Gray clustering algorithm chooses cluster head "C_h" on their energy level for efficient transmission along the optimal route path "P_{optimal}." An optimal path is identified using Combinatorial Stochastic Sampled Prevosti's Bat Optimization algorithm for secure data transmission. If any route fails, an alternative route is identified through the route maintenance mechanism. Brief discussions about three different processes are described in the following subsections.

3.2. Quantized Schutz Indexive Linde–Buzo–Gray Clustering Algorithm. In the first phase, QIEAC-CSSBO employs the quantized Schutz indexive Linde–Buzo–Gray algorithm for clustering the sensor nodes based on energy which supports to increase the lifetime of the network. The quantized Schutz indexive Linde–Buzo–Gray algorithm is a vector quantization algorithm that works based on dividing a large set of sensor nodes (i.e., vectors) into groups having a similar number of nodes closest to them. These nodes are identified based on the Schutz index which is a metric to compute the similarity between the energy level and centroid of clusters.

Figure 3 illustrates the flow process of clustering using the quantized Schutz indexive Linde–Buzo–Gray algorithm. First, the entire sensor nodes (soldiers) in the network (battlefield) are divided based on their energy.

In WSN, every sensor node has same energy levels during node deployment. Then, the node provides certain amount of energy for sensing, processing, and communication purposes. After sensing and monitoring, the sensor nodes' initial energy degrades, and then, the residual energy is measured. Next, "k" numbers of clusters $Cl_1, Cl_2, Cl_3, \cdots Cl_k$ as well as centroid $\vartheta_1, \vartheta_2, \vartheta_3, \cdots \vartheta_k$ are initialized. The Schutz index is used to calculate the similarity between each cluster's centroid and each node's residual energy and is given in Equation (4),

$$\beta_{\text{SI}} = 0.5 * \left[\frac{\sum_i \sum_j \left|E_{\text{res}}(Sn_i) - \vartheta_j\right|}{\sum_i E_{\text{res}}(Sn_i)}\right], \tag{4}$$

where "β_{SI}" (Equation (5)) indicates a Schutz index coefficient, $E_{\text{res}}(Sn_i)$ indicates testing residual energy of sensor nodes, and ϑ_j represents cluster centroid. Therefore, the

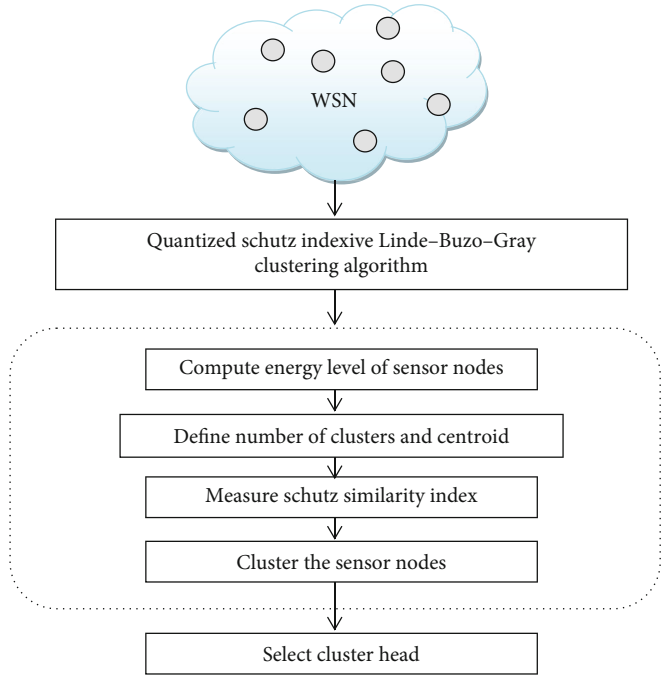


Figure 3: Flow process of the quantized Schutz indexive Linde–Buzo–Gray clustering algorithm.

Schutz index coefficient provides the outcomes in the ranges from 0 to +1.

$$\beta_{\mathrm{SI}} = \begin{cases} 1, & \text{highersimilarity} \\ 0, & \text{Lessersimilarity} \end{cases}. \quad (5)$$

The clusters are formed based on the energy level of the clusters compared with the centroid using the similarity index. The nodes with similar indices are formed into different clusters. The cluster head is chosen following the clustering procedure to provide effective data transfer with minimal delay. The proposed method identifies a cluster head from the cluster members that have higher energy.

Algorithm 1 explains clustering method. At first, residual energy is computed, then initializes the "b" number of clusters. Cluster centroid is initialized based on average energy level to every cluster. Then, the similarity between the cluster centroid and residual energy of is measured to group node into a particular cluster. The higher similarity indicates that the sensor nodes are gathered within the cluster. Next, cluster head is selected for improving data transmission as well as minimizing delay. Node using better residual energy among the cluster members is selected by CH. It collects information from additional members.

3.3. Combinatorial Stochastic Sampled Prevosti's Bat Optimization Algorithm for Secured Data Transmission. The second phase of the QIEAC-CSSBO algorithm is to find the secured path to transmit the data. WSN does not have centralized management or a static infrastructure and uses a broadcast transmission channel. Because of this, WSNs lack tamper protection, making them highly vulnerable to attacks. A hacker can therefore listen in on all traffic, send malicious packets, replay earlier messages, or take over a sensor node. Hence, security is of prime importance in applications like military communications, and two major concerning security issues are node authentication and privacy protection. Here in this paper, a novel Combinatorial Stochastic Sampled Prevosti's Bat Optimization algorithm for node authentication is processed with respect to the security requirements and security analysis against various attacks in military applications. The proposed algorithm is swarm-intelligence-based and finds good solutions automatically around the multidimensional search space. The bat is called a search agent that starts to find its food source at the current position and velocity and ends its movement at the location of prey. The prey is the best location for each bat. Here, the bats are related to the cluster heads, and the prey is related to multiple objective functions. Each bat that finds and catches its prey is said to be in the best location (i.e., best optimal path). An optimal route is found using the bat optimization technique [48], as it is effective at identifying globally optimal solutions. Additionally, bat optimization offers a very quick convergence rate (i.e., stable optimal path found at the end of a sequence of solutions). Hence, it aids the algorithm in determining the best route for enhancing data transmission and reducing delay.

The proposed technique initializes the populations of the cluster head (i.e., bats), C_{h1}, C_{h2}, $C_{h3,\ldots}C_{hk}$, that are stimulated around the search space (i.e., network) with initial position $\alpha_i(t)$ and velocity $\beta_i(t)$ followed by the fitness value that is calculated based on a number of objective functions, including the nodes' distance, energy, trust, and link stability.

Let us consider the two-dimensional space; distance among two nodes is expressed by Prevosti's distance. Prevosti's distance is a metric to find the nearest node for optimal route discovery.

Input: Sensor nodes $Sn_i \in Sn_1, Sn_2, Sn_3 \cdots Sn_n$,
Output: Number of clusters
Begin
1: for each sensor node Sn_i
2: **Measure** residual energy 'E_{res}'
3: Initialize the '$\boldsymbol{b}$' number of clusters $Cl_1, Cl_2, Cl_3, \cdots Cl_b$
4: **For each cluster** $\boldsymbol{Cl_k}$
5: Initialize the centroid '$\vartheta_1, \vartheta_2, \vartheta_3, \cdots \vartheta_b$'
6: **End for**
7: **For each cluster centroid** ϑ_k'
8: **For each** residual energy 'E_{res}' of node
9: Measure the similarity 'β_{SI}'
10: If ($\beta_{SI} = 1$) **then**
11: Group sensor nodes into particular clusters
12: **end if**
13: **End for**
14: **End for**
15: Obtain clustering results
16: **for each cluster** $\boldsymbol{C_k}$
17: Select cluster head 'C_h'
18: **end for**
19: End for
End

Algorithm 1: Quantized Schutz indexive Linde–Buzo–Gray clustering algorithm.

$$D = \frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{m}\left|sn_i - sn_j\right|, \tag{6}$$

where "D" represents a Prevosti's distance between the sensor nodes Sn_i and Sn_j. "n" indicates the number of sensor nodes. Energy of sensor node is measured using (6).

The sensor nodes surveil the neighboring nodes (as the trust of sensor nodes is an essential feature for identifying the most faithful node among different types of attacks such as blackhole, grayhole, flooding, and scheduling attacks) and apply the trust estimation as given below:

$$\mathrm{Tst} = \left[\frac{F\left(dp_{j\longrightarrow k}\right)}{S\left(dp_{i\longrightarrow j}\right)}\right]. \tag{7}$$

In (7), node trust (Tst) is evaluated from the data packets forwarded from node "j" to k's as well as data packets transferred from "i" to "j." The estimated trust value should be between 0 and 1.

Finally, the link stability factor helps to identify the stable link between the nodes for providing longer connectivity and reducing the packet drop. The link from one node i to node j (denoted by $i \longrightarrow j$) is connected at a time "t" and is measured as follows:

$$LC_{i\longrightarrow j}(t) = \left[\frac{Ts_r}{D}\right]. \tag{8}$$

From (8), $LC_{i\longrightarrow j}(t)$ denotes link connectivity by time "t," Ts_r denotes transmission range of sensor node, D indicates distance among two nodes i and j. Transmission range of node is higher compared with distance (i.e., $Ts_r > D$). If the link connectivity between node is maximum than threshold (T), then nodes i and j are connected, and the particular link is stable at a time "t." The threshold is the cut-off value of the function, and all test values which are equal to or greater than this value are considered as a positive result.

Based on multiple objective functions, the fitness is measured with the help of a combinatorial function that deals with both minimization problem as well as a maximization problem, depending on whether the given objective function (i.e., fitness function) is to be minimized or maximized.

$$\varphi_F = \arg\min\ (D)\&\&\arg\max\ (E_{\mathrm{res}}, \mathrm{Tst})\&\&\left(LC_{i\longrightarrow j}(t) > T\right). \tag{9}$$

In (9), φ_F denotes fitness function, "arg min" indicates the argument of minimum function, D is the distance, E_{res} denotes residual energy, Tst represents trust, $LC_{i\longrightarrow j}(t)$ symbolize link stability, and T denotes threshold. The "n" best bats are chosen with stochastic universal sampling selection process. This helps to minimize the complexity of the algorithm. A stochastic universal sampling selection procedure is a selection operator used to select the best individuals from a population-based on the fitness. The selection of individuals is carried out based on probability estimation as given:

$$p = \frac{\varphi_{Fi}}{\sum_{j=1}^{n}\varphi_{Fj}}. \tag{10}$$

From (10), selection probability (p) is estimated based on the ratio of every individual fitness "φ_{Fi}" to the average fitness

of the population in jth individual "φ_{Fj}." When population creation is varied, fitness value and selection probability are also changed. It means that the best individuals are selected with probability (p). Then, the second-best individual is selected with the probability as follows:

$$Sn_i(\text{sec}) = p * [1 - p]. \tag{11}$$

Similarly, the third-best individual "S" with probability is selected as

$$Sn_i(\text{th}) = p * [1 - p]^2. \tag{12}$$

Likewise, all the best individuals are selected, and others are removed for identifying the global best solution. After that, global best solutions are identified with the updating of current positions and velocities as given below. The current position of each individual depends on the fitness:

$$\alpha_i(t+1) = \alpha_i(t) + \beta_i(t+1), \tag{13}$$

$$\beta_i(t+1) = \beta_i(t) + \left|\alpha_i(t) - \varphi_{F\text{global}}\right|, \tag{14}$$

where $\alpha_i(t+1)$ denotes an updated position of the bat, $\alpha_i(t)$ denotes a current position of the bat, $\beta_i(t+1)$ indicates an updated velocity of the bat, $\beta_i(t)$ denotes current velocity of the bat, and $\varphi_{F\text{global}}$ indicates a global best solution. Therefore, current position of the individuals which is closer to the fitness of the global best solution is selected as an optimal. Based on the updated position of the bat, the global best route path is identified between the source and base station node for secure and energy-efficient data transmission. The flowchart which demonstrates Combinatorial Stochastic Sampled Prevosti's Bat optimization algorithm for detecting global best route path for increasing security of data delivery in WSN is as shown in Figure 4.

Figure 5 shows the optimal route path discovery to energy-efficient and secure data transmission. First, source node transfers data packets with CH, and it finds another optimal cluster head to establish the route path; following this, the path is established. In this way, the optimal route is identified. The algorithmic process of the proposed Combinatorial Stochastic Sampled Prevosti's Bat Optimization algorithm is described as follows.

Algorithm 2 provides optimal route path discovery using the combinatorial stochastic sampled Prevosti's bat Optimization technique. The proposed optimization technique first generates the population of bats. For each bat, compute the fitness on multiple objective functions between nodes. The stochastic universal sampling selection procedure is applied to select the current best bat based on fitness. Then, the global best is identified with the help of position and velocity updates. Finally, the optimal best route path between sources with base station is discovered through CH. Then, source nod starts to transfer sensitive data packets with base station. Finally, within case of any link between the nodes is broken, the alternative energy-efficient and secure neighboring

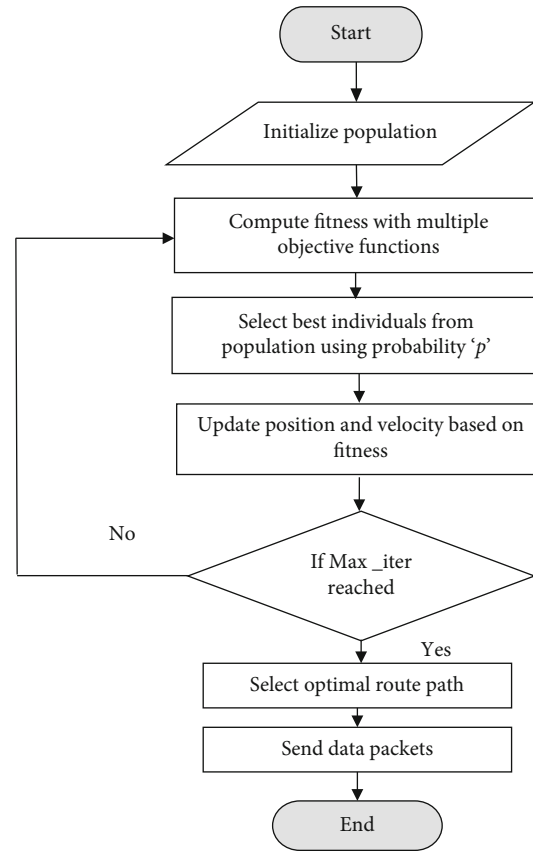


Figure 4: Flow chart of Combinatorial Stochastic Sampled Prevosti's Bat Optimization algorithm.

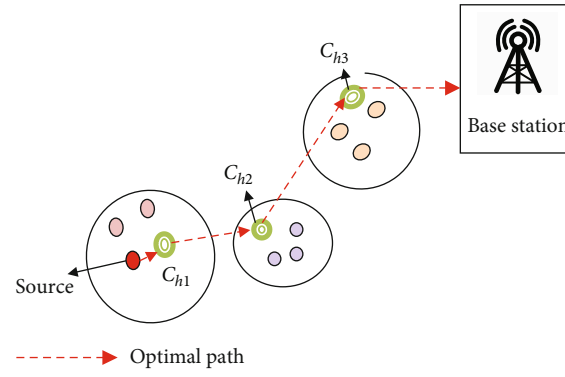


Figure 5: Optimal route path discovery.

nodes are detected for enhancing security of data as well as lesser delay.

Lastly, route maintenance is performed with QIEAC-CSSBO for identifying optimal route that the link failure occurs among nodes. This route maintenance is the phase where the link maintenance is protected when the distribution of data packets. Link breaks along active optimal path, and node finds quicker with break region (i.e., adjacent active node) for improving secure data transmission as well as minimizes the delay.

Input: Data packets $dp_1, dp_2, dp_3, \cdots .dp_n$, source node SN, cluster heads $C_{h1,}C_{h2} \cdots C_{hm}$, a base station ($BS$)
Output: Optimal route discovery
Begin
1. Initialize the population of Bats *i.e* cluster heads $C_{h1,}C_{h2} \cdots C_{hm}$
2. **for each** $C_{hi,}$
3. Measure the multi-objective functions D, E_{res}, Tst, $LC_{i \longrightarrow j}(t)$
4. Calculate the fitness 'φ_F'
5. Select current best 'n' individuals (i.e cluster heads) using () () ()
6. **If** $(\varphi_F(i) > \varphi_F(j))$ **then**
7. Update the position of $\alpha_i(t+1)$ and velocity $\beta_i(t+1)$
8. **End if**
9. **If** (Max_ iteration) **then**
10. Obtain the global best route path
11. **else**
12. Go to step 4
13. **End if**
14. End for
15. A source node (SN) sends data packets $dp_1, dp_2, dp_3, \cdots .dp_n$ to BS via optimal route path
16. **If** any link fails **then**
17. Select another optimal route and send data packets
18. End if
19. End
End

Algorithm 2: Combinatorial stochastic sampled Prevosti's bat optimization algorithm.

4. Performance Analysis and Discussion

The simulation is carried out using NS2.34 network simulator with WSN-DS. The network area considered for simulation is 1100 m ∗ 1100 m, where 500 sensor nodes are randomly deployed over the network area. DSR routing protocol is utilized for attack detection in WSN. Random waypoint is employed by mobility for achieving secure data transmission. Time is 300 seconds as well as sensor nodes' speeds are ranges of 0-20 m/s. The dataset used for intrusion detection for the proposed system is taken from https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds. The simulation of the proposed algorithm QIEAC-CSSBO is compared with the existing methods [19, 20]. The parameters used for simulation is given in Table 1.

4.1. Performance Metrics. The simulated data for the proposed and the existing methods are analyzed based on the following metrices like energy consumption, packet delivery ratio, packet drop rate, throughput, and end-to-end delay.

4.1.1. Energy Consumption. It is measured as the amount of energy consumed by the sensor nodes for sensing the data. The overall energy consumption is mathematically calculated as given below:

$$\text{Cons}_E = n * \text{Cons}_E(Sn), \tag{15}$$

where Cons_E indicates an energy consumption, n indicates a sensor node, and "$\text{Cons}_E(Sn)$" indicates the amount of energy consumed by the single sensor node (Sn). The energy consumption is measured in terms of joule (J).

4.1.2. Packet Delivery Ratio. It is measured as the ratio of the number of data packets successfully received at the base station from the total data packets being sent from the source node. The data packet delivery ratio is mathematically calculated as given below:

$$\text{Ratio}_{\text{PD}} = \frac{[\text{dp}_{\text{received}}]}{[\text{dp}_{\text{sent}}]} * 100, \tag{16}$$

where Ratio_{PD} denotes a packet delivery ratio, $\text{dp}_{\text{received}}$ is the data packets received, and dp_{sent} indicates data packet sent. The measurement of delivery ratio is performed in percentage (%). In the higher packet delivery ratio, the method achieves higher security.

4.1.3. Packet Drop Rate. It is defined as the ratio of the number of data packets dropped due to attacks from the total data packets being sent from the source node. The packet drop rate is computed as given below:

$$\text{Rate}_{\text{DR}} = \frac{\left[\text{dp}_{\text{dropped}}\right]}{[\text{dp}_{\text{sent}}]} * 100, \tag{17}$$

where Rate_{DR} indicates a packet drop rate, $\text{dp}_{\text{dropped}}$ indicates data packets dropped, and dp_{sent} indicates data packet sent. The packet drop rate is measured in percentage (%).

4.1.4. Throughput. It is referred to as the ratio of the number of data packets that a network successfully delivered per unit

Table 1: Simulation parameters.

Simulation parameter	Value
Simulator	NS2.34
Number of sensor nodes	50, 100, 150, 200, 250, 300, 350, 400, 500
Network area	1100 m ∗ 1100 m
Simulation time	300 s
Mobility model	Random way point
Routing protocol	DSR
Sensor node speed	0-20 m/s.
Data packets	100, 200, 300, 400, 500, 600, 700, 800, 900, 1000
Initial energy of each sensor node	0.5 J
Packet size for data	256-512 bytes
Transceiver energy	An ideal value for transmitter power is -6 dBm. But it could range between -1 and -7 dBm. For receiver power, the value could range between -1 and -9 dBm.
Number of runs	10

time. Mathematically, the throughput is estimated as given below:

$$\mathrm{TH}_{\mathrm{put}} = \left[\frac{\mathrm{dp\ delivered\ (bits)}}{T\,(\mathrm{s})}\right]. \tag{18}$$

From (18), $\mathrm{TH}_{\mathrm{put}}$ indicates a throughput, dp delivered indicates a data packet delivered in terms of bits, and $T(s)$ indicates a unit time in terms of seconds. The throughput is measured in terms of bits per second (bps).

4.1.5. End-to-End Delay. It is estimated as the difference between the expected arrival time of data packets at the destination and the observed arrival time. The end-to-end delay is mathematically formulated as given below:

$$D_{\mathrm{EE}} = T\,(\mathrm{dp})_{\mathrm{ex}} - T\,(\mathrm{dp})_{\mathrm{obs}}. \tag{19}$$

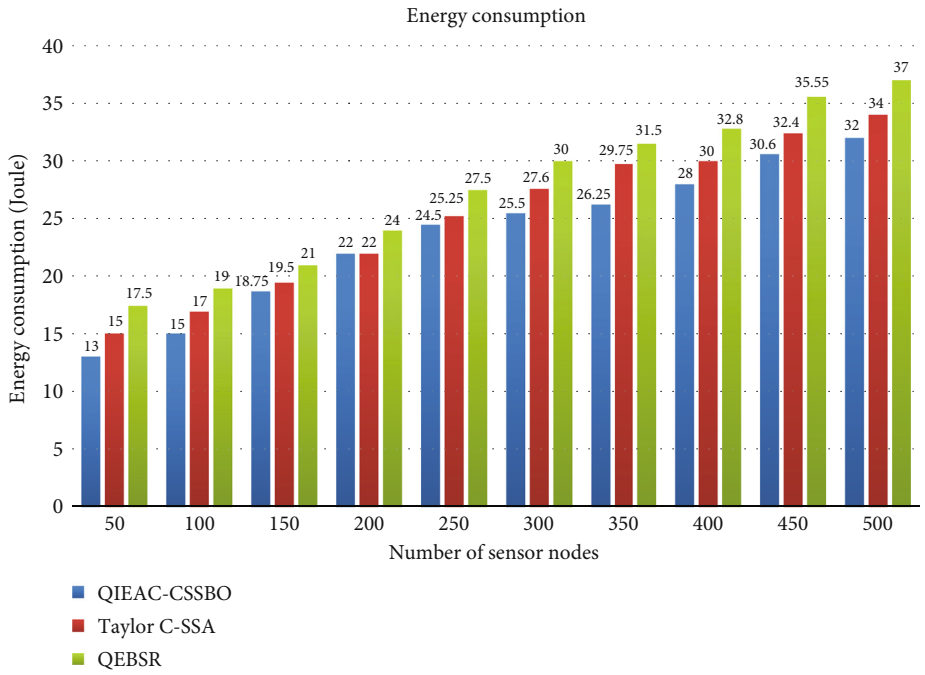
From (19), D_{EE} be the end-to-end delay, $T\,(\mathrm{dp})_{\mathrm{ex}}$ indicates a data packet expected time, and $T\,(\mathrm{dp})_{\mathrm{obs}}$ indicates a data packet arrives at the destination. The delay is measured in milliseconds (ms).

4.2. Simulation Results and Discussion. The simulation is performed based on the aforementioned parameters, and the results are evaluated by comparing the proposed method QIEAC-CSSBO with the existing methods Taylor C-SSA [19] and QEBSR [20]. The following tables and figures depict the measured metrices and its corresponding graphical representation.

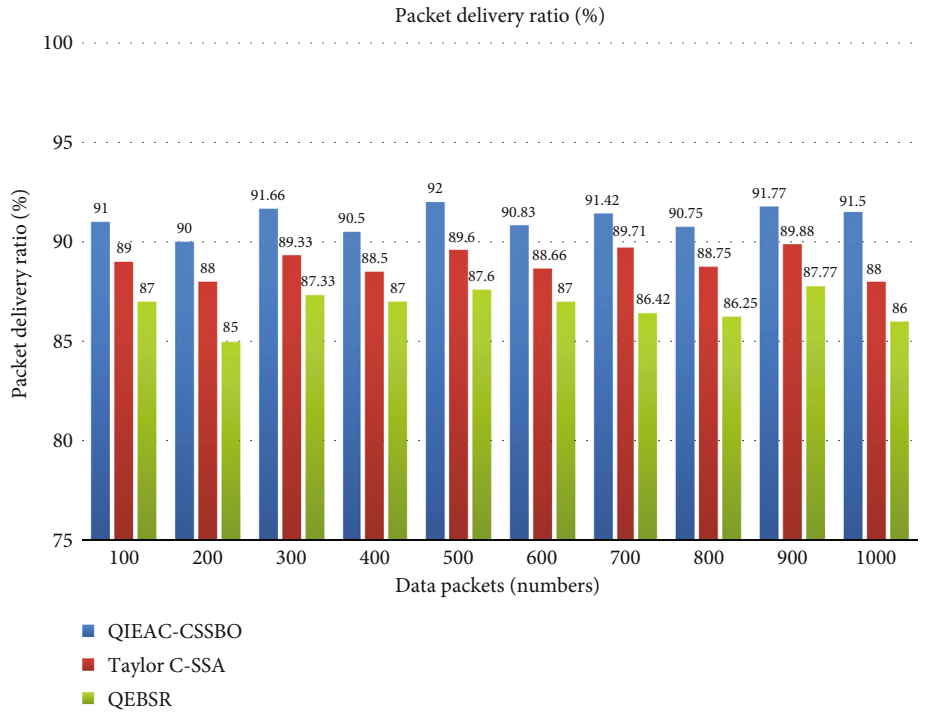
Figure 6(a) and Table 2 depict energy consumption against number of sensor nodes (i.e., soldiers). In the proposed method, the quantized Schutz indexive Linde–Buzo–Gray algorithm forms the cluster and selects the CH based on the energy level, and the bat optimization provides a quick convergence rate in which the fitness function value derived from the multiple objective functions motivates the QIEAC-CSSBO to find the optimal path with minimum time by using the stochastic universal sampling selection procedure. It finds the best individuals using probability estimation with less complexity (Equations (9)–(14)), thereby improving data transmission as well as minimizing energy consumption. It is clearly seen that the proposed QIEAC-CSSBO method gives better performance when compared with the other two existing techniques. Energy consumption of QIEAC-CSSBO is reduced as 7% and 15% when compared to [19, 20], respectively. Therefore, the lifetime of the node has been increased approximately by 11% which in-turn will support in extension of the entire network lifetime. Energy conservation is a significant aspect of WSN, as the battery cannot be changed often.

Figure 6(b) and Table 3 illustrate the performance of QIEAC-CSSBO and existing Taylor C-SSA [19] and QEBSR [20] techniques in terms of packet delivery ratio. The performance of a network will be estimated based on the number of packets delivered at the sink node. Hence, a network is said to perform high when its PDR is high. The bat optimization technique in the proposed algorithm optimizely selects neighboring CH that has closest distance, higher residual energy, higher trust, and better link stability based on the fitness function (Equation (9)) and selection probability (Equation (10)) for finding optimal route path to transfer data with great authenticity. The node with higher trust is used to transmit sensitive transmission continuously against the attacks. This process improves data transmission. The application of combinatorial stochastic sampled Prevosti's bat optimization technique for secure data transmission is robust to attackers within military network. For analysing the performance of the proposed technique with other two existing techniques, the packets sent varies from 100 to 1000 packets, and the result shows that packet delivery ratio of the proposed system is enhanced by 2% and 5% compared with [19, 20], respectively.

The impact of packet drop rate will reduce the network performance. This occurs due to multipath fading, intrusion of compromised nodes, and energy efficiency of the nodes. Hence, the aforementioned factors have to be controlled to avoid the packet drop loss. This is achieved in route discovery module, by finding the node trust Tst (Equation (7)) which determines the trustworthiness of a node and the link

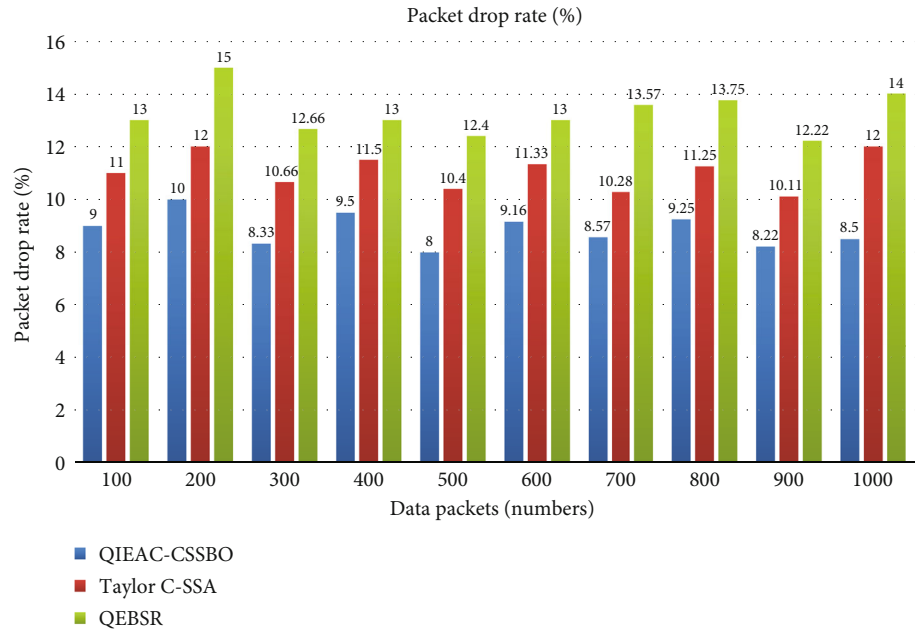


(a)

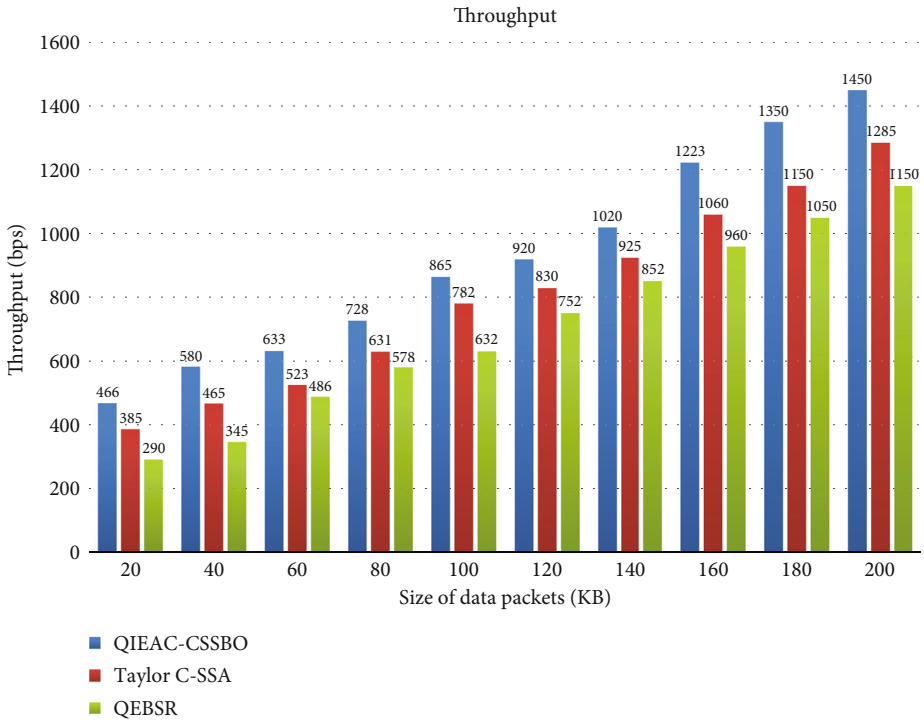


(b)

Figure 6: Continued.

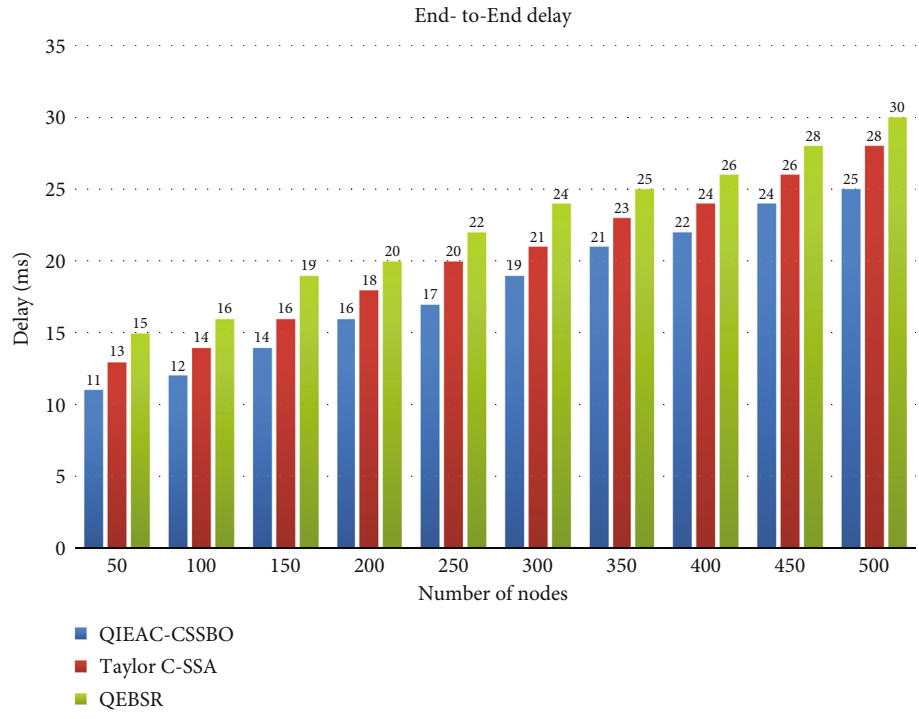


(c)



(d)

Figure 6: Continued.



(e)

Figure 6: (a) Evaluation of energy consumption of the simulated algorithms. (b) Evaluation of packet delivery ratio of the simulated algorithm. (c) Evaluation of packet drop rate comparison of the simulated algorithms. (d) Evaluation of throughput of the simulated algorithms. (e) Evaluation of end-to-end delay of the simulated algorithms.

Table 2: Comparison of energy consumption.

Sensor nodes (numbers)	Energy consumption (J)		
	QIEAC-CSSBO	Taylor C-SSA	QEBSR
50	13	15	17.5
100	15	17	19
150	18.75	19.5	21
200	22	22	24
250	24.5	25.25	27.5
300	25.5	27.6	30
350	26.25	29.75	31.5
400	28	30	32.8
450	30.6	32.4	35.55
500	32	34	37

Table 3: Comparison of packet delivery ratio.

Data packets (numbers)	Packet delivery ratio (%)		
	QIEAC-CSSBO	Taylor C-SSA	QEBSR
100	91	89	87
200	90	88	85
300	91.66	89.33	87.33
400	90.5	88.5	87
500	92	89.6	87.6
600	90.83	88.66	87
700	91.42	89.71	86.42
800	90.75	88.75	86.25
900	91.77	89.88	87.77
1000	91.5	88	86

stability factor $LC_{i\longrightarrow j}(t)$ (Equation (8)) which determines the stability of the node that avoids multipath fading. And the fitness function (Equation (9)) shows how efficient and optimal is a node to transmit the data in a secured manner. To analyze the performance of the proposed model with the reference models, packets ranging from 100 to 1000 is sent over the network, and the result obtained is presented in Table 4 and Figure 6(c). The above statistical measure demonstrates that the QIEAC-CSSBO comparatively performs well for higher packet drop rate. Packet drop rate is minimized as 20% and 33% when compared with [19, 20], respectively.

The throughput is the final performance parameter which shows the performance of a network which is obtained from a successful transmission with combined effort (i.e., the data transmission with higher packet delivery ratio and less packet drop). This is achieved when a high energy cluster head aggregates the data over cluster members and forwards it to the base station through the optimal path with the nodes with higher energy. Here, the

Table 4: Comparison of packet drop rate.

Data packets (numbers)	Packet drop rate (%)		
	QIEAC-CSSBO	Taylor C-SSA	QEBSR
100	9	11	13
200	10	12	15
300	8.33	10.66	12.66
400	9.5	11.5	13
500	8	10.4	12.4
600	9.16	11.33	13
700	8.57	10.28	13.57
800	9.25	11.25	13.75
900	8.22	10.11	12.22
1000	8.5	12	14

Table 5: Comparison of throughput.

Size of data packets (KB)	Throughput (bps)		
	QIEAC-CSSBO	Taylor C-SSA	QEBSR
20	466	385	290
40	580	465	345
60	633	523	486
80	728	631	578
100	865	782	632
120	920	830	752
140	1020	925	852
160	1223	1060	960
180	1350	1150	1050
200	1450	1285	1150

performance analysis between the proposed method and the existing methods is done by transmitting the data range varying from 20 to 200 KB. It is observed that the throughput of data transmission is enhanced as 16% and 35% when compared with Taylor C-SSA [19] and QEBSR [20], respectively, as shown in Table 5 and Figure 6(d). On the whole, the throughput has been increased by 26%. This is achieved when the nodes with minimum distance and higher energy are divided in the data transmission to increase the amount of data delivery per unit time.

The end-to-end delay in WSN is the total period taken for data packet to be transmitted from source to destination. Hence, if the delay is minimum, the performance of the netwrok seems to be better. The proposed combinatorial stochastic sampled Prevosti's bat optimization technique discovers an optimal route using higher link stability and detects the shortest path among neighboring soldiers (Equations (6)–(14)). The performance analysis is done by transmitting the data among the sensor nodes ranging from 50 nodes to 500 nodes, and the time is noted as shown in Table 6, and Figure 6(e) depicts it in graphical manner. It is observed that the delay in QIEAC-CSSBO is minimized as 11% and 20% when compared with [19, 20], respectively.

Table 6: Comparison of end-to-end delay.

Sensor nodes (numbers)	End-to-end delay (ms)		
	QIEAC-CSSBO	Taylor C-SSA	QEBSR
50	11	13	15
100	12	14	16
150	14	16	19
200	16	18	20
250	17	20	22
300	19	21	24
350	21	23	25
400	22	24	26
450	24	26	28
500	25	28	30

Moreover, if there is any link failure in the network, the QIEAC-CSSBO technique performs a route maintenance procedure to select an alternative optimal route path to deliver data packets. This helps to minimize the delay of data arrival at the destination.

5. Conclusion and Future Scope

The energy efficiency as well as protection is the main challenge within distributed WSN. To achieve this, clustering, route path discovery, and route maintenance are developed by QIEAC-CSSBO technique. First, the quantized Schutz indexive Linde–Buzo–Gray algorithm is applied to form many clusters. Followed by, the algorithm chooses CH with higher residual energy in the cluster. Node using better residual energy is selected as the cluster head and the data are forwarded over cluster member towards the base station. After that, optimal route path is identified for data transmission using combinatorial stochastic sampled Prevosti's bat optimization algorithm. The proposed optimization algorithm shows better convergence and activates based on the following constraints, namely, energy, distance, link stability, and trust. As a result, QIEAC-CSSBO improves secure data transmission and minimizes the delay. Experimental assessment is carried out with various performance metrics such as packet delivery ratio, throughput, energy consumption, packet drop, and delay compared with conventional techniques. The proposed technique gives 17% improvement in energy consumption and 3% in packet delivery ratio and reduces drop rate by 3%; throughput is improved by 27%, and the end-to-end delay is minimized by 10% when compared with the existing methods Taylor C-SSA [19] and QEBSR [20]. In the future, followed by the optimal route discovery, an efficient encryption algorithm would be developed for securing the data from various attacks.

In future, the proposed method can be further extended to a novel certificateless signcryption method by the optimal route discovery for securing energy-efficient data transmission. In addition, the computation overhead metric is considered to secure data transmission.

Data Availability

In WSN, dataset is used for intrusion detection systems taken from https://www.kaggle.com/datasets/bassamkasas beh1/wsnds. No other dataset was used in this work. The works that are taken as reference is cited in the article at appropriate places in the article. The complete work and implementation were done by me (J. Paruvathavardhini, under the guidance of Dr. B. Sargunam).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

I would like to extend my thanks to my supervisor Dr. B. Sargunam, who guided me in this research work. Furthermore, I am glad to extend my gratitude to Dr. R. Sudarmani, who provided her expertise in this research.

References

[1] T. Rault, A. Bouabdallah, and Y. Challal, "Energy efficiency in wireless sensor networks: a top-down survey," *Computer Networks*, vol. 67, pp. 104–122, 2014.

[2] R. Sudarmani and K. R. S. Kumar, "Particle swarm optimization-based routing protocol for clustered heterogeneous sensor networks with mobile sink," *American Journal of Applied Sciences*, vol. 10, no. 3, pp. 259–269, 2013.

[3] B. Kavya, V. Vani, and H. Roopa, "Efficient cluster head rotation based on residual energy to extend network lifetime," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 774–777, Coimbatore, India, July 2020.

[4] N. Shabbir and S. R. Hassan, "Routing protocols for wireless sensor networks (WSNs)," in *Wireless Sensor Networks-Insights and Innovations*, 2017.

[5] A. Chatap and S. Sirsikar, "Review on various routing protocols for heterogeneous wireless sensor network," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 440–444, Palladam, India, February 2017.

[6] K. Cengiz and T. Dag, "Energy aware multi-hop routing protocol for WSNs," *IEEE access*, vol. 6, pp. 2622–2633, 2018.

[7] S. C. V. Bhaskar and V. R. Rani, "Performance analysis of efficient routing protocols to improve quality of service in wireless sensor networks," in *2017 International Conference on Communication and Signal Processing (ICCSP)*, pp. 0006–0009, Chennai, India, April 2017.

[8] A. Aalavandhar and A. Arjunan, "A comparative study of different cluster mechanism for wireless sensor networks," in *2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 781–785, Coimbatore, India, June 2019.

[9] N. U. Sama, K. B. Zen, A. U. Rahman, B. BiBi, A. U. Rahman, and I. A. Chesti, "Energy efficient least edge computation LEACH in wireless sensor network," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, pp. 1–6, Sakaka, Saudi Arabia, October 2020.

[10] H. Hayouni, M. Hamdi, and T. H. Kim, "A survey on encryption schemes in wireless sensor networks," in *2014 7th International Conference on Advanced Software Engineering and Its Applications*, pp. 39–43, Hainan, China, December 2014.

[11] Z. Huanan, X. Suping, and W. Jiannan, "Security and application of wireless sensor network," *Procedia Computer Science*, vol. 183, pp. 486–492, 2021.

[12] S. A. Salehi, M. A. Razzaque, P. Naraei, and A. Farrokhtala, "Security in wireless sensor networks: issues and challanges," in *2013 IEEE International Conference on Space Science and Communication (IconSpace)*, pp. 356–360, Melaka, Malaysia, July 2013.

[13] J. Paruvathavardhini, S. Menaga, N. Gomathi, S. Karthikkumar, and S. Brindha, "A study depicting the advent of artificial intelligence in health care," *European Journal of Molecular Clinical Medicine*, vol. 7, no. 11, pp. 131–146, 2020.

[14] B. Y. Sovetov, T. M. Tatarnikova, and V. V. Cehanovsky, "Wireless sensor network security models," in *2020 9th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–4, Budva, Montenegro, June 2020.

[15] D. Rusinek, B. Ksiezopolski, and A. Wierzbicki, "Security trade-off and energy efficiency analysis in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 6, Article ID 943475, 2015.

[16] M. A. Al Sibahee, S. Lu, Z. A. Hussien, M. A. Hussain, K. A. A. Mutlaq, and Z. A. Abduljabbar, "The best performance evaluation of encryption algorithms to reduce power consumption in WSN," in *2017 International Conference on Computing Intelligence and Information System (CIIS)*, pp. 308–312, Nanjing, China, April 2017.

[17] K. J. S. R. Kommuru, K. K. Y. Kadari, and B. K. R. Alluri, "A novel approach to balance the trade-off between security and energy consumption in WSN," in *2018 2nd International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*, pp. 85–90, Ghaziabad, India, September 2018.

[18] Y. P. Makimaa and R. Sudarmani, "Survey on energy optimization techniques for clustering and routing in applications of wireless sensor networks," *Solid State Technology*, vol. 63, no. 6, pp. 20053–20065, 2020.

[19] A. Vinitha, M. S. S. Rukmini, and Dhirajsunehra, "Secure and energy aware multi-hop routing protocol in WSN using taylor-based hybrid optimization algorithm," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 5, pp. 1857–1868, 2022.

[20] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, and R. Patan, "Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks," *IEEE Transactions on Engineering Management*, vol. 68, no. 1, pp. 170–182, 2021.

[21] S. Prithi and S. Sumathi, "LD2FA-PSO: a novel learning dynamic deterministic finite automata with PSO algorithm for secured energy efficient routing in wireless sensor network," *Ad Hoc Networks*, vol. 97, article 102024, 2020.

[22] K. SureshKumar and P. Vimala, "Energy efficient routing protocol using exponentially-ant lion whale optimization algorithm in wireless sensor networks," *Computer Networks*, vol. 197, article 108250, 2021.

[23] D. Mehta and S. Saxena, "MCH-EOR: multi-objective cluster head based energy-aware optimized routing algorithm in wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 28, article 100406, 2020.

[24] K. K. Le-Ngoc, Q. T. Tho, T. H. Bui, A. M. Rahmani, and M. Hosseinzadeh, "Optimized fuzzy clustering in wireless sensor networks using improved squirrel search algorithm," *Fuzzy Sets and Systems*, vol. 438, pp. 121–147, 2022.

[25] K. Haseeb, K. M. Almustafa, Z. Jan, T. Saba, and U. Tariq, "Secure and energy-aware heuristic routing protocol for wireless sensor network," *IEEE Access*, vol. 8, pp. 163962–163974, 2020.

[26] K. Hamouid, S. Othmen, and A. Barkat, "LSTR: lightweight and secure tree-based routing for wireless sensor networks," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1479–1501, 2020.

[27] S. Al-Otaibi, A. Al-Rasheed, R. F. Mansour, E. Yang, G. P. Joshi, and W. Cho, "Hybridization of metaheuristic algorithm for dynamic cluster-based routing protocol in wireless sensor networksx," *IEEE Access*, vol. 9, pp. 83751–83761, 2021.

[28] S. Bharany, S. Sharma, S. Badotra et al., "Energy-efficient clustering scheme for flying ad-hoc networks using an optimized LEACH protocol," *Energies*, vol. 14, no. 19, p. 6016, 2021.

[29] R. S. Rathore, S. Sangwan, S. Prakash, K. Adhikari, R. Kharel, and Y. Cao, "Hybrid WGWO: whale grey wolf optimization-based novel energy-efficient clustering for EH-WSNs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, Article ID 101, 2020.

[30] W. Fang, W. Zhang, W. Chen, J. Liu, Y. Ni, and Y. Yang, "MSCR: multidimensional secure clustered routing scheme in hierarchical wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, Article ID 14, 2021.

[31] S. Ebrahimi Mood and M. M. Javidi, "Energy-efficient clustering method for wireless sensor networks using modified gravitational search algorithm," *Evolving Systems*, vol. 11, no. 4, pp. 575–587, 2020.

[32] P. Maheshwari, A. K. Sharma, and K. Verma, "Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization," *Ad Hoc Networks*, vol. 110, article 102317, 2021.

[33] S. Gopinath, K. V. Kumar, P. Elayaraja, A. Parameswari, S. Balakrishnan, and M. Thiruppathi, "Sceer: secure cluster based efficient energy routing scheme for wireless sensor networks," *Materials Today: Proceedings*, vol. 45, pp. 3579–3584, 2021.

[34] A. B. Feroz Khan and G. Anandharaj, "A cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT," *Wireless Personal Communications*, vol. 119, no. 4, pp. 3149–3159, 2021.

[35] D. K. Bangotra, Y. Singh, A. Selwal, N. Kumar, and P. K. Singh, "A trust based secure intelligent opportunistic routing protocol for wireless sensor networks," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1045–1066, 2022.

[36] D. L. Reddy, C. G. Puttamadappa, and H. N. G. Suresh, "Hybrid optimization algorithm for security aware cluster head selection process to aid hierarchical routing in wireless sensor network," *IET Communications*, vol. 15, no. 12, pp. 1561–1575, 2021.

[37] R. Sharma, V. Vashisht, and U. Singh, "eeTMFO/GA: a secure and energy efficient cluster head selection in wireless sensor networks," *Telecommunication Systems*, vol. 74, no. 3, pp. 253–268, 2020.

[38] D. L. Reddy, C. Puttamadappa, and H. N. Suresh, "Merged glowworm swarm with ant colony optimization for energy efficient clustering and routing in wireless sensor network," *Pervasive and Mobile Computing*, vol. 71, article 101338, 2021.

[39] S. Tabatabaei, "Provide energy-aware routing protocol in wireless sensor networks using bacterial foraging optimization algorithm and mobile sink," *PLoS One*, vol. 17, no. 3, article e0265113, 2022.

[40] H. Wu, H. Zhu, L. Zhang, and Y. Song, "Energy efficient chain based routing protocol for orchard wireless sensor network," *Journal of Electrical Engineering & Technology*, vol. 14, no. 5, pp. 2137–2146, 2019.

[41] C. Xu, Z. Xiong, G. Zhao, and S. Yu, "An energy-efficient region source routing protocol for lifetime maximization in WSN," *IEEE Access*, vol. 7, pp. 135277–135289, 2019.

[42] P. K. Kodoth and G. Edachana, "An energy efficient data gathering scheme for wireless sensor networks using hybrid crow search algorithm," *IET Communications*, vol. 15, no. 7, pp. 906–916, 2021.

[43] K. P. Sampoornam, S. Saranya, G. K. Mohanapriya, P. S. Devi, and S. Dhaarani, "Analysis of LEACH routing protocol in wireless sensor network with wormhole attack," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, pp. 147–152, Tirunelveli, India, February 2021.

[44] P. Manasa, K. Shaila, and K. R. Venugopal, "DMHCET: detection of malicious node for hierarchical clustering based on energy trust in wireless sensor network," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pp. 688–692, London, UK, July 2020.

[45] X. Cai, Y. Sun, Z. Cui, W. Zhang, and J. Chen, "Optimal LEACH protocol with improved bat algorithm in wireless sensor networks," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 13, no. 5, pp. 2469–2490, 2019.

[46] X. Cai, S. Geng, D. Wu, L. Wang, and Q. Wu, "A unified heuristic bat algorithm to optimize the LEACH protocol," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 9, article e5619, 2020.

[47] Y. P. Makimaa and R. Sudarmani, "Incorporating node behavioral analysis with on-demand secured routing of improving the efficiency of wireless sensor networks applications," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 6, pp. 1674–1686, 2021.

[48] S. P. Kaur and M. Sharma, "Radially optimized zone-divided energy-aware wireless sensor networks (WSN) protocol using BA (bat algorithm)," *IETE Journal of Research*, vol. 61, no. 2, pp. 170–179, 2015.