Wireless Communications and Mobile Computing

Green Internet of Things in 5G and Beyond

Lead Guest Editor: Samarendra Nath Sur
Guest Editors: Korhan Cengiz and Vinayakumar Ravi

Green Internet of Things in 5G and Beyond

Green Internet of Things in 5G and Beyond

Lead Guest Editor: Samarendra Nath Sur
Guest Editors: Korhan Cengiz and Vinayakumar Ravi

Contents

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9932652, 12 pages
https://doi.org/10.1155/2022/9932652

Research Article

Splitting Energy of Transmit Power Serving Grouping Users in Full-Duplex Networks under Imperfect Hardware

Nhan Duc Nguyen,[1] **Anh-Tu Le**,[2] **and Dinh-Thuan Do**[3]

[1]*Faculty of Mechanical-Electrical and Computer Engineering, School of Engineering and Technology, Van Lang University, 69/68 Dang Thuy Tram Street, Ward 13, Binh Thanh District, 70000 Ho Chi Minh City, Vietnam*
[2]*Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh City 700000, Vietnam*
[3]*Electrical Engineering Department, University of Colorado Denver, Denver, CO 80204, USA*

Correspondence should be addressed to Anh-Tu Le; leanhtu@iuh.edu.vn

Received 25 August 2021; Revised 11 March 2022; Accepted 31 March 2022; Published 25 April 2022

Academic Editor: Abdul Basit

In this paper, we consider a wireless system providing power allocation fairness for grouping users by conducting a non-orthogonal multiple access (NOMA). In particular, a rigorous analysis is performed to evaluate performance of destination in a downlink of wireless system. With advances of NOMA, the user grouping scheme allows users to be shared the same frequency/power domain, and hence, fairness is guaranteed. In this regard, we focus on evaluation of the performance of a cell-center user and a cell-edge user in dedicated group. To enable forwarding function at cell-center user, we require the assistance of a full-duplex– (FD–) based relay to serve the cell-edge user. These users are assigned a fixed power allocation scheme. To characterize system performance, the closed-form expressions of the outage probability are computed for two users. To generalize channels in such system, Nakagami-m fading channels could be adopted to achieve complete theoretical analysis. Furthermore, we provide some comparisons of such FD NOMA under the impact of hardware impairment. We find that a significant improvement of outage probability can be achieved when the signal-to-noise ratio (SNR) at the source is high. Numerical results illustrate that both the analytical outage probability of the central user and the cell-edge user match the simulation results.

1. Introduction

Recent advances in wireless communications provide a new method to better serve the larger number of users [1, 2]. As one of these promising techniques, the non-orthogonal multiple access (NOMA) could be implemented in wireless system by employing non-orthogonal signal transmission at the transceiver [3–5]. On the transmit side, the users' information is superimposed in the power domain. The system relies on the way to enhance spectrum efficiency. In the NOMA system, multiple terminals can be served over the same resource block, thus employing that the NOMA is the effective way to enhance both spectrum efficiency and the sum rate. At the receiver side, successive interference cancellation (SIC) is conducted to decode the users' signal [6, 7]. Regarding SIC operation, by treating other signals as interference, the user with the best channel condition is given higher priority to decode. These advances of NOMA are prominent compared with orthogonal multiple access (OMA).

In the work of [6], an intermediate node acts as a relay to forward a signal from a source to a destination. The relaying system along with device-to-device is designed to achieve better transmission range or to enhance reliability by leveraging spatial diversity [7]. Higher spectrum efficiency can be obtained by enabling cognitive radio in NOMA systems [8]. More benefits are reported in the joint NOMA and cooperative communications, where NOMA users with poor channel conditions can be improved in their performance [9]. One or more dedicated relays are designed in relay-aided NOMA transmission to achieve performance improvement [10–17]. By considering arbitrary and optimal power allocation mode with full-duplex (FD) users operating

as decode-and-forward (DF) relays, the work in [9] studied the outage probability (OP) and ergodic sum-rate (ESR). In [13], NOMA-aided cooperative network is studied by exploring the model of Nakagami-m channels. In this NOMA system, the closed-form expressions are derived to indicate the OP and the ergodic sum rate. In such a network, the source is required to serve simultaneously with multiple destinations through a relay using half duplex (HD). In similar studies [14–16], considering partial relay selection (PRS), a cooperative NOMA system with multiple relays can exhibit better performance in terms of and sum rate and OP. In [17], Nakagami-m channels with a single FD-amplify and forward (AF) relay was studied to evaluate the outage performance and the ESR. In such a NOMA-based cooperative system, a fading-free self-interference link is adopted at the relay.

Recent works have considered the impact of hardware impairment and imperfect channel estimation in FD/HD cooperative NOMA-aided relaying systems. The works in [18–26] and references therein discussed the harmful impact of hardware impairment noise in various wireless technologies. The work of [18] especially focused on hardware impairment of FD/HD NOMA-aided relaying systems in Internet-of-things (IoT). In particular, the authors were concerned with the impact of hardware impairments via low-cost devices in practical IoT deployment. The authors derived exact OP and ergodic capacity expressions for near and far users under Rayleigh fading channels. In [19], the authors investigated the OP of a cooperative simultaneous wireless information and power transfer (SWIPT) NOMA-assisted multiple-relay network. The energy harvesting (EH) relays are also responsible for the communication between the base station and users. The EH relays operate under hardware impairment and imperfect channel state information (iCSI). PRS is exploited to select an EH relay to transmit information from the base station to a near and far user. Closed-form OP expressions are derived to understand deeply the impact of hardware impairments and iCSI.

Similarly, in [20], the authors examined the joint influence of residual hardware impairment (RHI) and iCSI on power beacon aided cooperative NOMA multiple-relay systems. By this way, the communication is enabled by the multiple relays harvesting energy from the power beacon. The communication from the base station to the far users is achieved only via the relays, while near users can receive information from either the base station or the relays or both. In addition, there is a direct link between the base station and far users. The authors derived exact OP expressions for the system users. Simulation results showed the existences of error floors in the OP performance curves attributed to RHIs and iCSI. In [21], the authors investigated the impact of hardware impairment and imperfect channel estimation in SWIPT NOMA-aided massive IoT systems. Communication between the base station and NOMA IoT devices is achieved via a direct link and the aid of multiple relays with EH and storage capability. PRS is utilized to select the optimal relay among the multiple relays to transmit information from the base station to the NOMA IoT devices. The authors also derived closed-form OP expressions and investigated the energy efficiency of the proposed system. In addition, the authors obtained the optimal power allocation strategy to maximize the sum rate in the high signal-to-noise ratio (SNR) region. Simulation results showed that hardware impairment harms performance and channel estimation is good for OP.

In [22], the authors examined how maximum-ratio transmission (MRT)/maximum-ratio combining (MRC) performs in NOMA-aided FD relay systems suffering from RHIs as well as imperfect CSI and imperfect SIC. The base station uses MRT and the multiple users utilize MRC, and the two-antenna relay relies on AF mode in its operation. The authors derived closed-form OP expressions under Nakagami-m fading channels. The authors also obtained diversity and array gain tight lower bounds and asymptotic OP expressions. The simulation results demonstrated the necessity of loop-interference cancellation at the FD relay for the proposed system to outperform HD-NOMA systems. Moreover, the results proved that RHIs impact significant users with lower power coefficients but the diversity order is not affected. Also, imperfect CSI does not impact the system significantly.

1.1. Related Works. Considering the impact of hardware impairment, the authors in [23] investigated performance of all devices and self-interference at the FD relay on the detection performance of NOMA-assisted multiple-input multiple-output (MIMO) FD relaying system with MRT/MRC at the source and destination, respectively. The authors derived exact OP expressions, throughput, and symbol error rate (SER). Simulation results showed a significant impact of hardware impairment at high data rates on OP, throughput, and SER of the considered system when compared to the non-impaired version of the considered system. Furthermore, numerical results showed the introduction of error floors at the high SNR region of OP and SER performance curves. Fortunately, the introduction of MRT/MRC with more transmit antennas at the source than at the destination was found to enhance the OP and SER performance under hardware impairment conditions.

Moreover, in [24], the authors analyzed the performance of cooperative FD-NOMA relaying when in-phase and quadrature-phase imbalance (IQI) and imperfect SIC are considered. The authors derived exact OP and approximate analytical ESR expressions. Simulation results demonstrated that both NOMA-FD relaying and OMA-FD relaying are impacted in their OP and ESR performance in the moderate and high SNR region. However, OP of FD-NOMA relaying is impacted slightly than OMA-FD relaying. In addition, when FD-NOMA relaying is compared with the equivalent HD version, the far users of the FD-NOMA relaying suffer less from imperfect SIC. In [25], the authors considered the impact of hardware impairments on uplink FD-NOMA relaying in mobile edge computing (MEC) networks. The authors derived OP expressions of the proposed system. Numerical results showed the impact of hardware impairment on FD-NOMA relaying in MEC networks. In [26], the authors considered the impact of hardware impairment

on cooperative NOMA-FD system under Rician fading channels. The authors derived approximate analytical OP and ergodic rate expressions of the considered system. Numerical results highlight that NOMA-FD relaying enhances the ESR compared to the HD version of the proposed system.

1.2. Our Contributions. Motivated by the aforementioned papers, we deploy in this article an FD for performance improvement of two destinations in a NOMA-aided relay wireless system. Different from the aforementioned literature laid a solid foundation for the role of NOMA in Rayleigh fading to analyze system performance, the impact of FD-NOMA in general channel condition, namely, Nakagami-m fading, has not been well understood. Table 1 indicates some similar work. Based on the different parameter settings, the Nakagami-m fading channel can be reduce to how we analyze the system performance with multiple types of channel. Our main contribution is that the impact of hardware impairment is explored when we consider OP for the two destinations in our proposed system model. We also observe the benefits of the deployed relay in low transmit SNR regions in terms of optimal throughput performance at the cell edge user. Our paper provides several contributions compared with recent studies, shown in Table 1. Our contributions are listed as follows:

(i) We consider transmission in FD-NOMA system where a single antenna base station communicates with two devices arranged in a central and cell-edge positions. Communication between the base station and NOMA devices is achieved via a direct link between the cell-center device and the base station, while the single antenna FD relay with self-interference cancellation capability can forward signals to the cell-edge user. We study the outage and optimal throughput performance to determine the system performance under Nakagami-m fading channels and several practical hardware conditions

(ii) We then determine the signal-to-interference-plus-noise ratios (SINRs) of the two devices and use them to formulate exact OP and optimal throughput formulas. The derived expressions are validated by the Monte-Carlo simulations

(iii) We analyze and compare the OP and optimal throughput under various conditions. In particular, we find that hardware impairment, self-interference at the FD relay, the fixed rate, and the channel fading parameter are the main impacts on OP and optimal system throughput. The obtained numerical results demonstrate the impact of low-cost devices on OP and optimal throughput via many practical scenarios

1.3. Organization. The rest of this paper is organized as follows. Section 2 describes the downlink NOMA-aided FD relay system under Nakagami-m fading channels. In Section 3, we consider the scenario of NOMA in terms of outage performance. In Section 4, we consider optimal throughput performance. In Section 5, we provide extensive numerical simulations, and Section 6 concludes the paper.

2. System Model

We consider a cooperative Relay-aided NOMA system. In here, we assume a base station (S) and two destinations D_1 and D_2 with a help relay (R) in full-duple (FD) mode as in Figure 1. We consider D_2 as the central user, while the cell-edge user is D_1. In addition, all devices are equipped with a single antenna. We set g_{SR} as the channel between S and R, g_{SD_2} is the channel between S and D_2, g_{RD_1} is the channel between R and D_2, and g_R is the residual self-interference at R. Moreover, all the channels follows Nakagami-m channel fading. In addition, we consider the perfect CSI for all channels as [8].

The received signal from S to R is given by

$$y_R = \left(\sqrt{P_S\beta_2}x_2 + \sqrt{P_S\beta_1}x_1 + \varpi_{R,t}\right)g_{SR} + \varpi_{R,r} + \sqrt{P_R}\tau g_R x_1 + n_R, \tag{1}$$

where P_S is the transmit power at S, P_R is the transmit power at R, β_1 and β_2 are the power allocation coefficients, and $\varpi_{R,t}$ and $\varpi_{R,r}$ are the distortion noises with $CN(0, P_S\eta_{R,t}^2)$ and $CN(0, P_S|g_{SR}|^2\eta_{R,r}^2)$, respectively. $\eta_{R,t}^2$ and $\eta_{R,r}^2$ are the level of hardware impairments at S and R as in [27], $\tau(0 \le \tau \le 1)$ is the level of self-interference (SI), and n_R denotes the additive white Gaussian noise (AWGN) with $CN(0, \sigma^2)$. When the signal x_2 is detected at R, the signal to-interference plus noise ratio (SINR) at R is expressed as

$$\begin{aligned}\Gamma_{R,x_1} &= \frac{P_S\beta_1|g_{SR}|^2}{P_S\beta_2|g_{SR}|^2 + P_S|g_{SR}|^2\left(\eta_{R,t}^2 + \eta_{R,r}^2\right) + P_R\tau|g_R|^2 + \sigma_{SR}^2} \\ &= \frac{\mu_S\beta_1|g_{SR}|^2}{\mu_S\beta_2|g_{SR}|^2 + \mu_S|g_{SR}|^2\left(\eta_{R,t}^2 + \eta_{R,r}^2\right) + \mu_R\tau|g_R|^2 + 1},\end{aligned} \tag{2}$$

where $\mu_S = P_S/\sigma^2$ and $\mu_R = P_R/\sigma^2$. Then, R forwards the signal x_1 when detected successful. Therefore, the signal at D_1 is given by

$$y_{RD_1} = \left(\sqrt{P_R}x_1 + \varpi_{D_1,t}\right)g_{RD_1} + \varpi_{D_1,r} + n_{D_1}, \tag{3}$$

where $\varpi_{D_1,t}$ and $\varpi_{D_1,r}$ are the distortion noises with $CN(0, P_R\eta_{D_1,t}^2)$ and $CN(0, P_R|g_{RD_1}|^2\eta_{D_1,r}^2)$, respectively; $\eta_{D_1,t}^2$ and $\eta_{D_1,r}^2$ are the level of hardware impairments at R and D_1; and n_{D_1} is the AWGN. Then, the SINR when detecting x_1

Table 1: A comparison of existing works with our study on the impact of hardware impairment.

Scheme	Reference	Major contributions
Half/full-duplex-NOMA-IoT	[18]	Hardware impairment of FD/HD NOMA-aided relaying systems is investigated. The exact OP and ergodic capacity expressions can be achieved for near and far users under Rayleigh fading channels
EH-SWIPT-NOMA	[19]	The OP performance is evaluated for a cooperative SWIPT NOMA-assisted multiple-relay network. This system employs EH relays to enhance transmission from the base station to users. The degraded performance is considered under joint impact of hardware impairment and iCSI
Power beacon-NOMA	[20]	The joint influences of RHIs and iCSI on power beacon aided cooperative NOMA multiple-relay systems are examined since the multiple relays harvesting energy are enabled
FD-NOMA	[23]	The impact of hardware impairment at all devices and self-interference at the FD relay is studied for NOMA-assisted MIMO FD relaying system
FD-NOMA-MEC	[25]	The impact of hardware impairments is studied at uplink NOMA-aided FD relaying in mobile edge computing (MEC) networks
FD-NOMA	Our work	We consider transmission assisted by NOMA where a single antenna base station communicates with two devices arranged in a central and cell-edge position. The evaluations of outage and throughput performance are provided under Nakagami-m fading channels and several practical hardware conditions

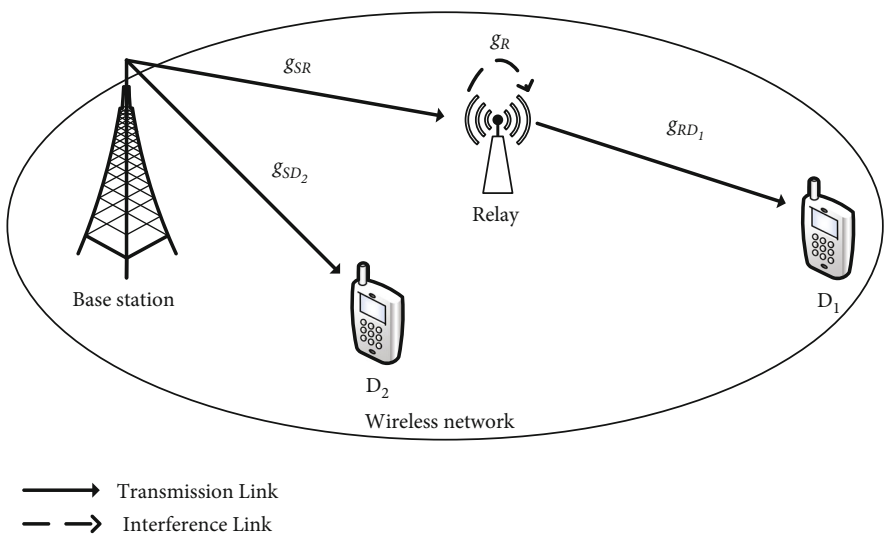

Figure 1: System model of NOMA relying on FD-assisted relay.

at D_1 is given by

$$\Gamma_{D_1,x_1} = \frac{P_R\left|g_{RD_1}\right|^2}{P_R\left|g_{RD_1}\right|^2\left(\eta_{D_1,t}^2+\eta_{D_1,r}^2\right)+\sigma^2} = \frac{\mu_R\left|g_{RD_1}\right|^2}{\mu_R\left|g_{RD_1}\right|^2\left(\eta_{D_1,t}^2+\eta_{D_1,r}^2\right)+1}. \tag{4}$$

Meanwhile, the received signal at D_2 can be expressed as

$$y_{SD_2} = \left(\sqrt{P_S\beta_1}x_1+\sqrt{P_S\beta_2}x_2+\varpi_{D_2,t}\right)g_{SD_2}+\varpi_{D_2,r}+n_{D_2}, \tag{5}$$

where $\varpi_{D_2,t}$ and $\varpi_{D_2,r}$ are the distortion noises with $CN(0, P_S\eta_{D_2,t}^2)$ and $CN(0, P_S|g_{RD_2}|^2\eta_{D_2,r}^2)$, respectively; $\eta_{D_2,t}$ and $\eta_{D_2,r}$ are the level of hardware impairments at S and D_2; and n_{D_2} is the AWGN. Thus, the SINR when detecting the signal x_1 at D_2 is given by

$$\begin{aligned}\Gamma_{D_2,x_1} &= \frac{P_S\beta_1\left|g_{SD_2}\right|^2}{P_S\beta_2\left|g_{SD_2}\right|^2+P_S\left|g_{SD_2}\right|^2\left(\eta_{D_2,t}^2+\eta_{D_2,r}^2\right)+\sigma^2}\\ &= \frac{\mu_S\beta_1\left|g_{SD_2}\right|^2}{\mu_S\beta_2\left|g_{SD_2}\right|^2+\mu_S\left|g_{SD_2}\right|^2\left(\eta_{D_2,t}^2+\eta_{D_2,r}^2\right)+1}.\end{aligned} \tag{6}$$

Moreover, by applying SIC, the SINR at D_2 to detect its own signal x_2 is given by

$$\Gamma_{D_2,x_2} = \frac{\mu_S\beta_2\left|g_{SD_2}\right|^2}{\mu_S\left|g_{SD_2}\right|^2\left(\eta_{D_2,t}^2+\eta_{D_2,r}^2\right)+1}. \tag{7}$$

3. Outage Performance

In this section, we analyze the outage probability of two users D_1 and D_2. The channel of g_k with $k \in SR, RD_1, SD_2, R$ is given as follows [8]:

$$f_{|g_k|^2}(\gamma) = \left(\frac{m_k}{\Omega_k}\right)^{m_k} \frac{\gamma^{m_k-1}}{\Gamma(m_k)} e^{-\frac{m_k}{\Omega_k}\gamma}, \tag{8}$$

where m_k is the fading severity parameter and Ω_k being the average power.

3.1. Outage Probability of D_2. The outage probability of the system is written as follows [28]:

$$P_{\text{out}}^{D2} = 1 - \Pr\left(\Gamma_{D_2,x_1} > \vartheta_1, \Gamma_{D_2,x_2} > \vartheta_2\right), \tag{9}$$

where $\vartheta_1 = 2^{\nu_1} - 1$, $\vartheta_2 = 2^{\nu_2} - 1$, ν_1, and ν_2 denotes the target rate. With the help of (6) and (7), (9) is expressed as

$$P_{\text{out}}^{D2} = 1 - \Pr\left(\left|g_{SD_2}\right|^2 > \frac{\chi}{\mu_S}\right) = 1 - \int_{\frac{\chi}{\mu_S}}^{\infty} f_{|g_{SD_2}|^2}(\gamma) d\gamma, \tag{10}$$

where $\kappa_{D_2,1} = \beta_1 - \vartheta_1\beta_2 - \vartheta_1(\eta_{D_2,t}^2 + \eta_{D_2,r}^2)$, $\kappa_{D_2,2} = \beta_2 - \vartheta_2(\eta_{D_2,t}^2 + \eta_{D_2,r}^2)$, and $\chi = \max\left((\vartheta_1/\kappa_{D_1,1}), (\vartheta_2/\kappa_{D_1,2})\right)$. Using (8) and ([29], 3.351.2), the closed-form expression of D_2 is given by

$$\begin{aligned} P_{\text{out}}^{D2} &= 1 - \int_{\frac{\chi}{\mu_S}}^{\infty} \left(\frac{m_{SD_2}}{\Omega_{SD_2}}\right)^{m_{SD_2}} \frac{\gamma^{m_{SD_2}-1}}{\Gamma\left(m_{SD_2}\right)} e^{-\frac{m_{SD_2}}{\Omega_{SD_2}}\gamma} d\gamma \\ &= 1 - \sum_{a=0}^{m_{SD_2}-1} \frac{1}{a!} \left(\frac{m_{SD_2}\chi}{\Omega_{SD_2}\mu_S}\right)^a e^{-\frac{m_{SD_2}\chi}{\Omega_{SD_2}\mu_S}}. \end{aligned} \tag{11}$$

3.2. Outage Probability of D_1. As the main result reported in [28], the outage probability of D_1 is expressed as

$$P_{\text{out}}^{D1} = 1 - \Pr\left(\Gamma_{R,x_1} > \vartheta_1, \Gamma_{D_1,x_1} > \vartheta_1\right). \tag{12}$$

Proposition 1. *The closed-form expression of D_1 can be expressed as*

$$\begin{aligned} P_{\text{out}}^{D1} = 1 - &\sum_{b=0}^{m_{\text{SR}}-1} \sum_{c=0}^{b} \sum_{n=0}^{m_{RD_1}-1} \binom{b}{c} \frac{\Gamma(m_R + c)(\mu_R)^c e^{-m_{\text{SR}}\vartheta_1/\Omega_{\text{SR}}\mu_S\kappa_R - m_{RD_1}\vartheta_1/\Omega_{RD_1}\mu_R\kappa_{D_1}}}{\Gamma(m_R) b! n!} \left(\frac{m_R}{\Omega_R}\right)^{m_R} \\ &\times \left(\frac{m_{\text{SR}}\vartheta_1}{\Omega_{\text{SR}}\mu_S\kappa_R}\right)^b \left(\frac{m_R}{\Omega_R} + \frac{m_{\text{SR}}\vartheta_1\mu_R}{\Omega_{\text{SR}}\mu_S\kappa_R}\right)^{-m_R-c} \left(\frac{m_{RD_1}\vartheta_1}{\Omega_{RD_1}\mu_R\kappa_{D_1}}\right)^n. \end{aligned} \tag{13}$$

Proof. See the appendix. □

4. Asymptotic Outage Probability Analysis

In this section, we derive an asymptotic OP expression at high-SNR $\mu_S = \mu_R \longrightarrow \infty$. Then, we apply the first-order Maclaurin series expansions $e^{-x} \simeq 1 - x$. Thus, the asymptotic OP of D_2 can be expressed by

$$P_{\text{out}}^{D2,\infty} = 1 - \sum_{a=0}^{m_{SD_2}-1} \frac{1}{a!} \left(\frac{m_{SD_2}\chi}{\Omega_{SD_2}\mu_S}\right)^a \left(1 - \frac{m_{SD_2}\chi}{\Omega_{SD_2}\mu_S}\right). \tag{14}$$

Similarly, the asymptotic OP of D_1 is given by

$$\begin{aligned} P_{\text{out}}^{D1} = 1 - &\sum_{b=0}^{m_{\text{SR}}-1} \sum_{c=0}^{b} \sum_{n=0}^{m_{RD_1}-1} \binom{b}{c} \left(\frac{m_R}{\Omega_R}\right)^{m_R} \frac{\Gamma(m_R + c)(\mu_R)^c}{\Gamma(m_R) b! n!} \left(\frac{m_{RD_1}\vartheta_1}{\Omega_{RD_1}\mu_R\kappa_{D_1}}\right)^n \\ &\times \left(\frac{m_{\text{SR}}\vartheta_1}{\Omega_{\text{SR}}\mu_S\kappa_R}\right)^b \left(\frac{m_R}{\Omega_R} + \frac{m_{\text{SR}}\vartheta_1\mu_R}{\Omega_{\text{SR}}\mu_S\kappa_R}\right)^{-m_R-c} \left(1 - \frac{m_{\text{SR}}\vartheta_1}{\Omega_{\text{SR}}\mu_S\kappa_R} - \frac{m_{RD_1}\vartheta_1}{\Omega_{RD_1}\mu_R\kappa_{D_1}}\right). \end{aligned} \tag{15}$$

5. Optimal Throughput Analysis

In this section, we carry out the optimal analysis of the throughput performance. More particularly, we offer a method for determining the best value of $T_{\text{out},i}^*$, which results in the system's maximum throughput.

Based on achievable outage probability, throughput is the ability to transmit signals at fixed rate ν_i. In particular, the throughput of each user is given by [8].

$$T_{\text{out},i} = \left(1 - P_{\text{out},i}^*\right)\nu_i. \tag{16}$$

The optimal points of such throughput as varying target rates of ν_i is expressed as

$$T_{\text{out},i}^* = \arg\max\left\{T_{\text{out},i}(\nu_i)\right\}. \tag{17}$$

Based on this algorithm, the optimal values of throughput can be obtained properly. We expect to verify such algorithm in next section.

Input: P_{out}^{Di}
OutPut: Optimal value $T_{\text{out},i*}^{*}$
Set $\nu_i^{\alpha} \longleftarrow [0 : 0.25 : 5]$ is used for the X-axis
Initialize $f \longleftarrow zeros(1, length(\nu_i^{\alpha}))$ and $T_{\text{out},i} \longleftarrow zeros(1, length(\nu_i^{\alpha}))$
for $k = 0$: $length(\nu_i^{\alpha})$ **do**
  $\nu_i \longleftarrow \nu_i^{\alpha}(k)$
  Compute $\phi_i(:,k) \longleftarrow P_{\text{out}}^{Di}(\nu_i)$
  $T_{\text{out},i}(:,k) \longleftarrow [1-\phi_i(:,k)]\nu_i$
end for
$[\sim, i] \longleftarrow \arg\max [T_{\text{out},i}(:,;)]$
Return $T_{\text{out},i}^{*} \longleftarrow T_{\text{out},i}(:,i)$

Algorithm 1: The algorithm of finding the optimal throughput coefficient $T_{\text{out},i}^{*}$.

Table 2: Table of parameters.

System parameters	Value
The power allocation	$\beta_1 = 0.7$ and $\beta_2 = 0.3$
The level of self-interference	$\tau = 0.1$
The target rate	$\nu_1 = 0.5$ and $\nu_2 = 1$ bit per channel use
The parameter of channel	$\Omega = \Omega_{SR} = \Omega_{RD_1} = \Omega_{SD_2} = \Omega_R = 1$
The level of hardware impairments	$\eta_t^2 = \eta_{R,t}^2 = \eta_{D_1,t}^2 = \eta_{D_2,t}^2$ and $\eta_r^2 = \eta_{R,r}^2 = \eta_{D_1,r}^2 = \eta_{D_2,r}^2$
The fading severity parameter	$m = m_{SR} = m_{RD_1} = m_{SD_2} = m_R$
Monte-Carlo simulations	10^6 iterations

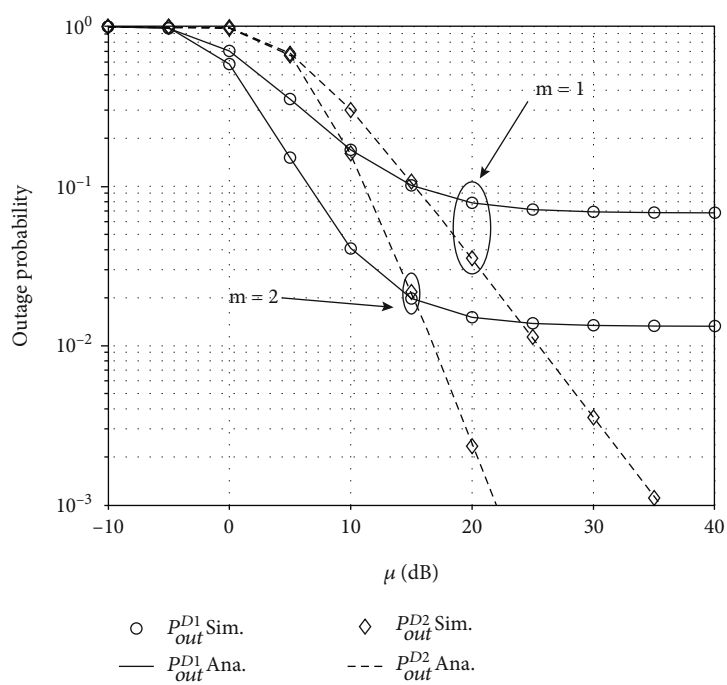

Figure 2: Outage performance vs μ (dB) varying m with $\eta_t^2 = \eta_r^2 = 0.01$.

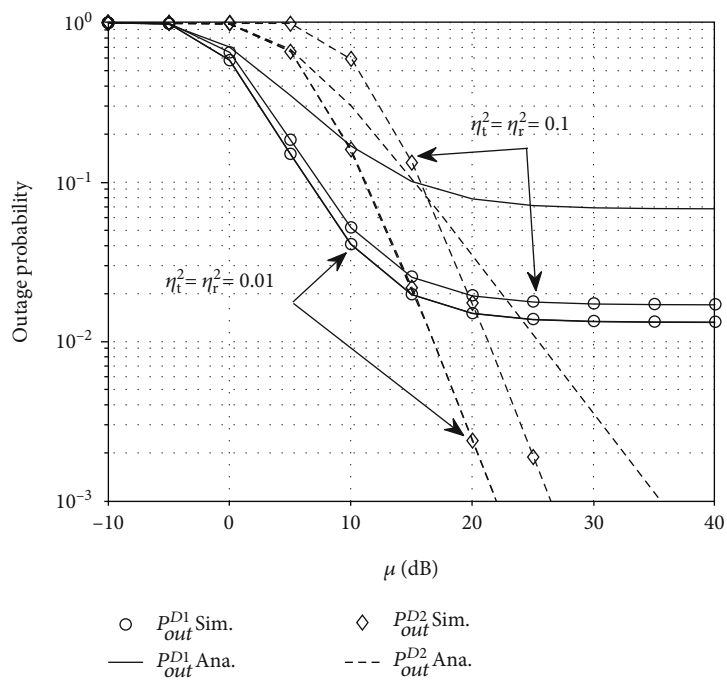

Figure 3: Outage performance vs μ (dB) varying $\eta_t^2 = \eta_r^2$ with $m = 2$.

6. Numerical Results

In this section, we want to illustrate system performance via simulations. In first step, we set $\mu = \mu_S = \mu_R$, and the simulation parameters can be shown in Table 2.

Figure 2 depicts the outage probability of two users versus the transmit SNR at source with two values of fading channel, $m = 1$ and $m = 2$. The exact outage probability curves match with Monte-Carlo simulation. Fortunately, this result confirms our correctness in term of computation of outage probability. We can see the performance gap of two users for the NOMA system over Nakagami-m fading. It can be explained that different signal decoding, number of hops for transmission, and different power allocation factors lead to the performance gap among the two users. We can see that the absence of SIC at D_1 results in the outage probability approaching an error floor and failing to go lower in moderate to high SNR regions. It can be concluded that the considered system has better outage behavior once channel condition is improved, i.e., coefficients of Nakagami-m fading are enhanced in specific situations.

We can observe the impact of hardware impairment in our proposed FD NOMA system, shown in Figure 3. By considering the two values of $\eta_t^2 = \eta_r^2$, we see that lower levels of hardware impairment lead to improvement in terms of outage performance. It is clear that $\eta_t^2 = \eta_r^2 = 0.01$ is the better case in terms of outage performance. However, D_1 still approaches an error floor in moderate to high SNR regions. It means that such system will work well if we improve signal at the base station. Further, by limiting impact of hardware impairment, such system retains its quality of transmission at downlink.

Figure 4 compares the system associated with FD and HD scenarios. The OP performance of D_1 versus transmit SNR is studied while varying values of SNR. The HD case is proven with more benefits in term of OP compared FD-NOMA system. The HD-NOMA system could be better outage compared FD-NOMA system at high SNR region. However, FD-NOMA system exhibits more spectrum efficiency as aforementioned.

In Figure 5, two users are affected by power allocation factors since the corresponding SINRs depend mostly on such allocation factors. Interestingly, the fairness among those users can be changed by such factors. To reduce the overhead in transmission, such factors are hold as fixed values to satisfy demands at users at specific situations. The other trends of OP performance can be seen similarly as previous figures.

In Figure 6, we observe the throughput of the system versus transmit SNR while varying m with $\eta_t^2 = \eta_r^2 = 0.01$. From Figure 6, we can observe different throughput curves depending on $T_{\text{out},i}$. The best throughput performance is achieved by $T_{\text{out},2}$ because destination 2 has a direct link to the base station and does not rely on the relay. Furthermore, depending on the value of i, the best throughput performance is achieved with higher values of fading parameter m. However, all the performance curves approach a ceiling at moderate to high SNR regions and fail to go higher, indicating that there are limits to the system determined by the fixed rate ν_1 in (16) and (17) as can also be seen in Figure 7.

In Figure 8, we observe throughput of the system versus transmit SNR while varying $\eta_t^2 = \eta_r^2$ with $m = 2$. Similar to Figure 6, the $T_{\text{out},2}$ obtains the best performance in the

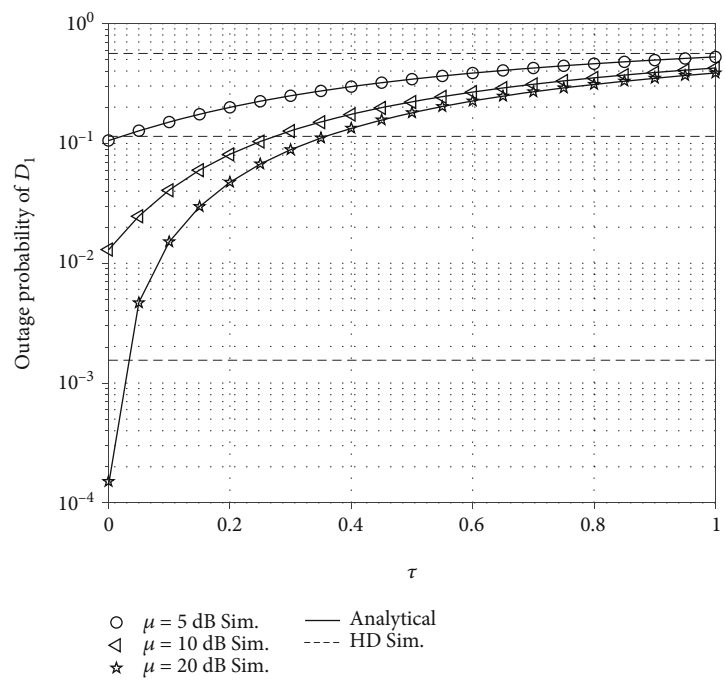

Figure 4: Outage performance of D_1 vs τ varying μ(dB) with $m = 2$ and $\eta_t^2 = \eta_r^2 = 0.01$.

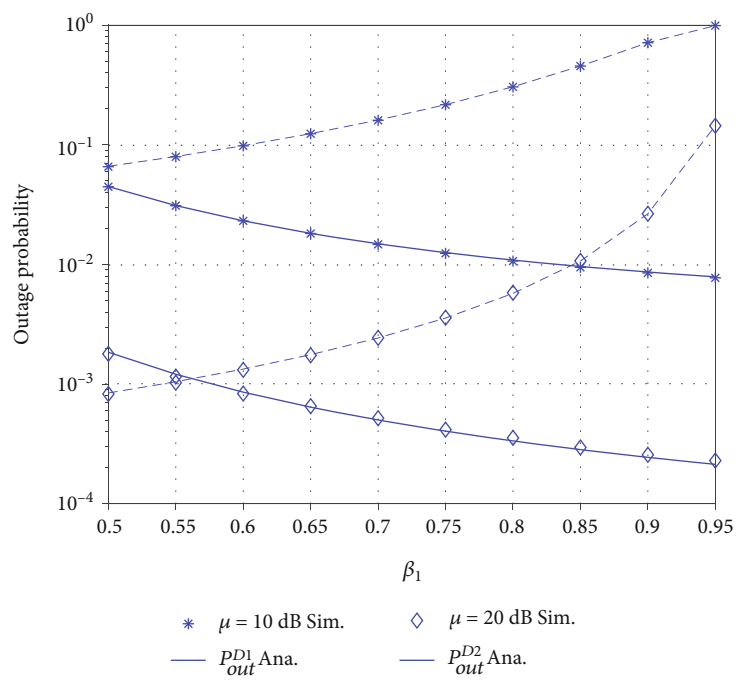

Figure 5: Outage performance vs β_1 varying μ with $m = 2$ and $\eta_t^2 = \eta_r^2 = 0.01$.

moderate to high SNR region under the considered hardware impairments, though all the performance curves converge at a ceiling at moderate to high SNR regions and fail to go higher despite the level of hardware impairments. It's important to note that at below 0 dB levels, destination 1 outperforms destination 2, this due to the relay, that amplifies and forwards the weak base station transmit signal to destination 2. Here, we can also see the benefits of the relay in the low SNR transmit regions on the cell edge user due to the lack of significant performance variations when $\eta_t^2 = \eta_r^2$ is varied unlike in the case of the centrally located user as can be seen in Figure 8.

The impact of self-interference related to the FD mode at R on throughput performance is studied in Figure 9. In this figure, we observe the impact of increasing τ on the system throughput performance. There is no significant difference

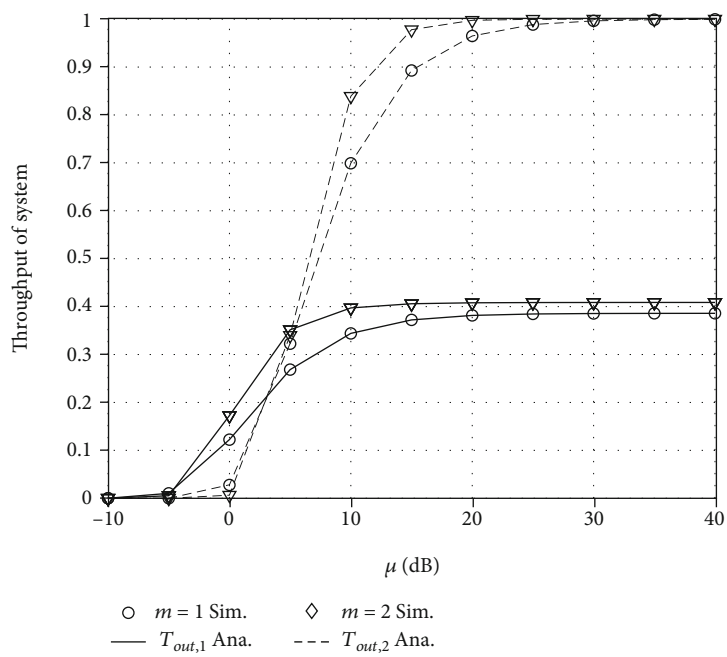

Figure 6: Throughput of system vs μ (dB) varying m with $\eta_t^2 = \eta_r^2 = 0.01$.

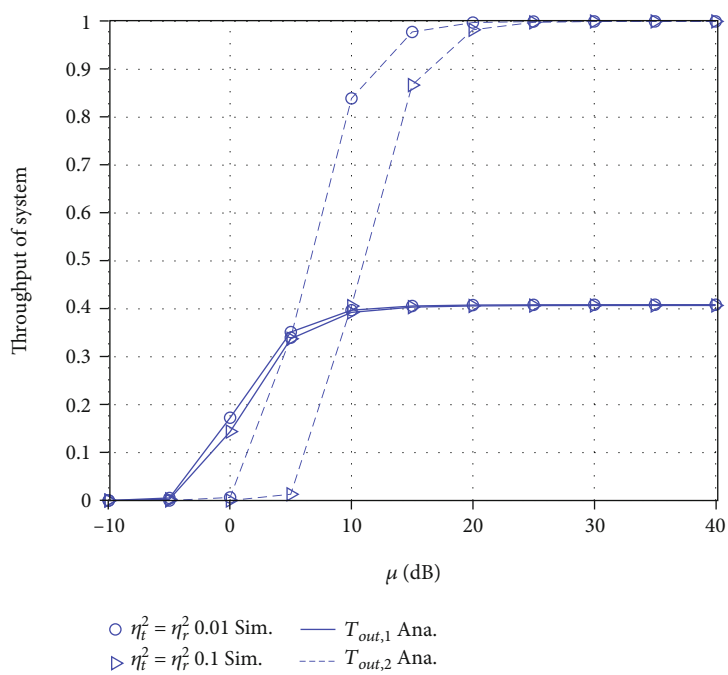

Figure 7: Throughput of system vs $\nu_1 = \nu_2$ with $\tau = 0.1$, $\beta_1 = 0.8$, $\beta_2 = 0.2$, and $\mu = 30$dB.

between $\tau = 0.01$ and $\tau = 0.1$ in terms of throughput performance. But, at higher levels of τ, the throughput performance starts to deteriorate. This result is helpful to network designers as they can deploy a suitable FD relay after having thoroughly considered the self-interference values based on the Figure 9.

In Figure 7, we observe that the optimal throughput can be achieved once we have the target rate $\nu_1 = \nu_2$ with $\tau = 0.1$, $\beta_1 = 0.8$, $\beta_2 = 0.2$, and $\mu = 30$dB. At rate $\nu_1 = \nu_2$ greater than 1 and less than about 2.3, the best performance is achieved by the central user. It can be explained that the FD contributes to improve links between the base station and cell-edge user. Figure 7 also depicts the maximum analytical value of each destination user on the y axis as well as the maximum $\nu_1 = \nu_2$ rate on the x axis. Figure 7 demonstrates the limits of throughput when $\nu_1 = \nu_2$ is varied. This result is helpful to network designers intending to deploy this system in practice.

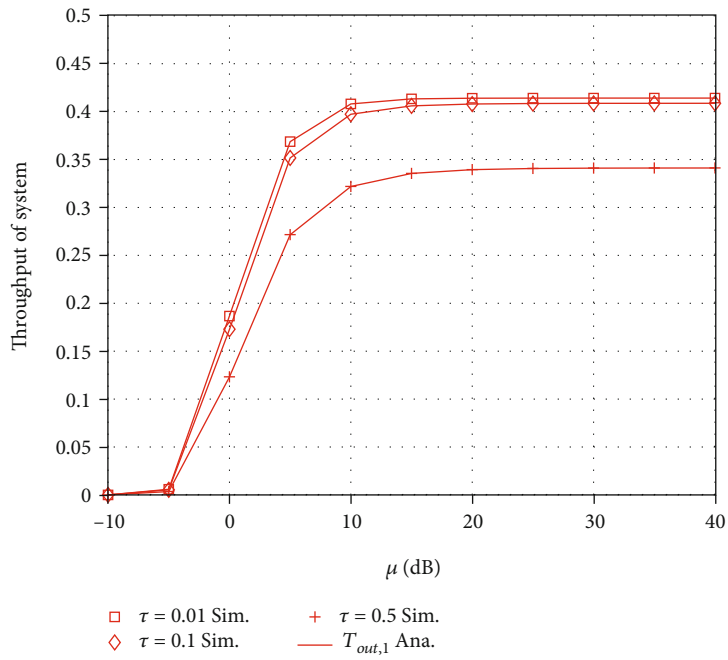

Figure 8: Throughput of system vs μ (dB) varying $\eta_t^2 = \eta_r^2$ with $m = 2$.

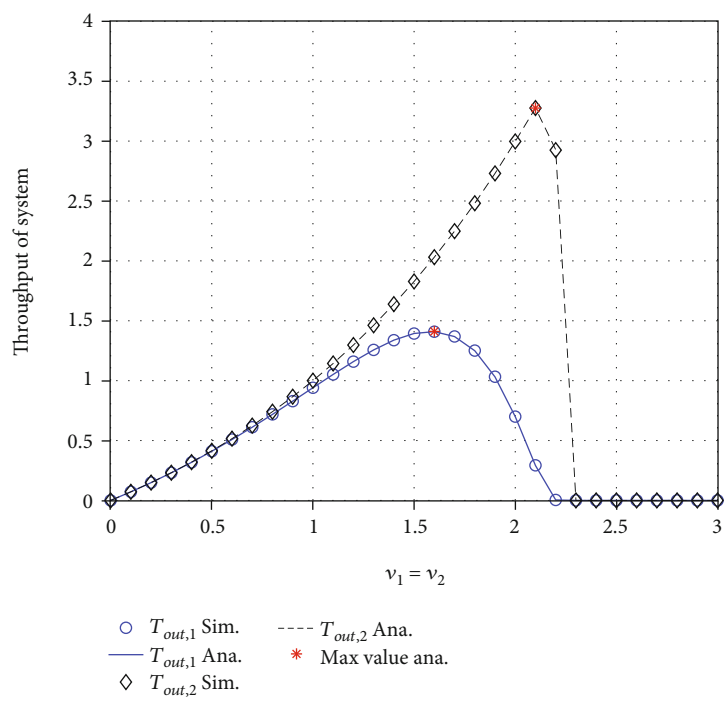

Figure 9: Throughput of system vs μ (dB) varying τ with $m = 2$ and $\eta_t^2 = \eta_r^2 = 0.01$.

In all the figures discussed so far, the analytical and simulated results closely match.

7. Conclusions

In this paper, we have studied the impact of hardware impairment on the outage performance of FD-NOMA over Nakagami-m fading channels. We characterize two kinds of users depending how far from the base station. The cell-edge user is serviced by the FD-assisted cell-center user. As the main result, new closed-form expressions for the outage probability are derived to evaluate the main factors affecting the system performance. Based on the obtained analytical results, we observed that lower levels of self-interference related to the FD mode and lower levels of hardware impairment can achieve enhancement of the system outage

performance. Finally, the performance gap of these two scenarios was compared in various situations to verify the main impacts on outage probability. In future work, we can deploy multiple antennas at both source and destinations to achieve a larger improvement of outage probability at the destinations.

Appendix

A. Proof of Proposition 1

First, (12) can be rewritten as

$$P_{\text{out}}^{D1} = 1 - \underbrace{\Pr\left(\Gamma_{R,x_1} > \vartheta_1\right)}_{\Lambda_1} \underbrace{\Pr\left(\Gamma_{D_1,x_1} > \vartheta_1\right)}_{\Lambda_2}. \tag{A.1}$$

Next, the first term Λ_1 can be calculated as

$$\begin{aligned}\Lambda_1 &= \Pr\left(|g_{SR}|^2 > \frac{\vartheta_1\left(\mu_R\tau|g_R|^2+1\right)}{\mu_S\kappa_R}\right)\\ &= \int_0^\infty f_{|g_R|^2}(z)\int_{\frac{\vartheta_1(\mu_R\tau z+1)}{\mu_S\kappa_R}}^\infty f_{|g_{SR}|^2}(\gamma)d\gamma dz,\end{aligned} \tag{A.2}$$

where $\kappa_R = \beta_1 - \vartheta_1\beta_1 - \vartheta_1(\eta_{R,t}^2 + \eta_{R,r}^2)$. Moreover, we can write (A.2) by

$$\begin{aligned}\Lambda_1 = &\sum_{b=0}^{m_{\text{SR}}-1}\frac{e^{-m_{\text{SR}}\vartheta_1/\Omega_{\text{SR}}\mu_S\kappa_R}}{\Gamma(m_R)b!}\left(\frac{m_R}{\Omega_R}\right)^{m_R}\left(\frac{m_{\text{SR}}\vartheta_1}{\Omega_{\text{SR}}\mu_S\kappa_R}\right)^b\int_0^\infty z^{m_R-1}\\ &(\mu_R\tau z+1)^b e^{-\left(\frac{m_R}{\Omega_R}+\frac{m_{\text{SR}}\vartheta_1\mu_R\tau}{\Omega_{\text{SR}}\mu_S\kappa_R}\right)z}dz.\end{aligned} \tag{A.3}$$

Based on ([29], 1.111), we can transform Λ_1 by

$$\begin{aligned}\Lambda_1 = &\sum_{b=0}^{m_{\text{SR}}-1}\sum_{c=0}^{b}\binom{b}{c}\frac{(\mu_R\tau)^c e^{-m_{\text{SR}}\vartheta_1/\Omega_{\text{SR}}\mu_S\kappa_R}}{\Gamma(m_R)b!}\left(\frac{m_R}{\Omega_R}\right)^{m_R}\\ &\left(\frac{m_{\text{SR}}\vartheta_1}{\Omega_{\text{SR}}\mu_S\kappa_R}\right)^b\int_0^\infty z^{m_R+c-1}e^{-\left(\frac{m_R}{\Omega_R}+\frac{m_{\text{SR}}\vartheta_1\mu_R\tau}{\Omega_{\text{SR}}\mu_S\kappa_R}\right)z}dz.\end{aligned} \tag{A.4}$$

Next, with the help of ([29], 3.351.3) we can obtain Λ_1 as

$$\begin{aligned}\Lambda_1 = &\sum_{b=0}^{m_{\text{SR}}-1}\sum_{c=0}^{b}\binom{b}{c}\frac{\Gamma(m_R+c)(\mu_R\tau)^c e^{-m_{\text{SR}}\vartheta_1/\Omega_{\text{SR}}\mu_S\kappa_R}}{\Gamma(m_R)b!}\left(\frac{m_R}{\Omega_R}\right)^{m_R}\\ &\left(\frac{m_{\text{SR}}\vartheta_1}{\Omega_{\text{SR}}\mu_S\kappa_R}\right)^b\left(\frac{m_R}{\Omega_R}+\frac{m_{\text{SR}}\vartheta_1\mu_R\tau}{\Omega_{\text{SR}}\mu_S\kappa_R}\right)^{-m_R-c}.\end{aligned} \tag{A.5}$$

The second term Λ_2 can be calculated as

$$\Lambda_2 = \Pr\left(\Gamma_{D_1,x_1} > \vartheta_1\right) = \Pr\left(\left|g_{RD_1}\right|^2 > \frac{\vartheta_1}{\mu_R\kappa_{D_1}}\right) = \int_{\frac{\vartheta_1}{\mu_R\kappa_{D_1}}}^\infty f_{|g_{RD_1}|^2}(x)dx, \tag{A.6}$$

where $\kappa_{D_1} = 1 - \vartheta_2(\eta_{D_1,t}^2 + \eta_{D_1,r}^2)$. Similarly, Λ_2 is obtained as

$$\Lambda_2 = e^{-\frac{m_{RD_1}\vartheta_1}{\Omega_{RD_1}\mu_R\kappa_{D_1}}}\sum_{n=0}^{m_{RD_1}-1}\frac{1}{n!}\left(\frac{m_{RD_1}\vartheta_1}{\Omega_{RD_1}\mu_R\kappa_{D_1}}\right)^n. \tag{A.7}$$

Putting (A.5) and (A.7) into (A.1), (13) is obtained. It completes the proof.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

We are greatly thankful to Van Lang University, Vietnam, for providing the budget for this study.

References

[1] S. Teodoro, A. Silva, R. Dinis, F. M. Barradas, P. M. Cabral, and A. Gameiro, "Theoretical analysis of nonlinear amplification effects in massive MIMO systems," *IEEE Access*, vol. 7, pp. 172277–172289, 2019.

[2] D. Castanheira, A. Silva, and A. Gameiro, "Retrospective interference alignment for the K -User M x N MIMO Interference Channel," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8368–8379, 2016.

[3] H. Zuo and X. Tao, "Power allocation optimization for uplink non-orthogonal multiple access systems," in *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–5, Nanjing, China, 2017.

[4] Z. Na, J. Lv, F. Jiang, M. Xiong, and N. Zhao, "Joint subcarrier and subsymbol allocation-based simultaneous wireless information and power transfer for multiuser GFDM in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5999–6006, 2019.

[5] D.-T. Do, M. -S. Van Nguyen, M. Voznak, A. Kwasinski, and J. N. de Souza, "Performance analysis of clustering car-following V2X system with wireless power transfer and massive connections," *IEEE Internet of Things Journal*, 2021.

[6] D.-T. Do, A.-T. Le, Y. Liu, and A. Jamalipour, "User grouping and energy harvesting in UAV-NOMA system with AF/DF relaying," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11855–11868, 2021.

[7] Z. Song, X. Wang, Y. Liu, and Z. Zhang, "Joint spectrum resource allocation in Noma-based cognitive radio network with SWIPT," *IEEE Access*, vol. 7, pp. 89594–89603, 2019.

[8] D.-T. Do, A. Le, and B. M. Lee, "NOMA in cooperative underlay cognitive radio networks under imperfect SIC," *IEEE Access*, vol. 8, pp. 86180–86195, 2020.

[9] L. Zhang, J. Liu, M. Xiao, G. Wu, Y. Liang, and S. Li, "Performance analysis and optimization in downlink NOMA systems with cooperative full-duplex relaying," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2398–2412, 2017.

[10] J. B. Kim and I. H. Lee, "Non-orthogonal multiple access in coordinated direct and relay transmission," *IEEE Communications Letters*, vol. 19, no. 11, pp. 2037–2040, 2015.

[11] C. Zhong and Z. Zhang, "Non-orthogonal multiple access with cooperative full-duplex relaying," *IEEE Communications Letters*, vol. 20, no. 12, pp. 2478–2481, 2016.

[12] R. Tang, J. Cheng, and Z. Cao, "Contract-based incentive mechanism for cooperative NOMA systems," *IEEE Communications Letters*, vol. 23, no. 1, pp. 172–175, 2019.

[13] J. Men, J. Ge, and C. Zhang, "Performance analysis of non-orthogonal multiple access for relaying networks over Nakagami-m fading channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1200–1208, 2017.

[14] S. Lee, D. B. da Costa, Q. T. Vien, T. Q. Duong, and R. T. de Sousa, "Non-orthogonal multiple access schemes with partial relay selection," *IET Communications*, vol. 11, no. 6, pp. 846–854, 2017.

[15] D. Deng, L. Fan, X. Lei, W. Tan, and D. Xie, "Joint user and relay selection for cooperative NOMA networks," *IEEE Access*, vol. 5, pp. 20220–20227, 2017.

[16] Y. Li, Y. Li, X. Chu, Y. Ye, and H. Zhang, "Performance analysis of relay selection in cooperative NOMA networks," *IEEE Communications Letters*, vol. 23, no. 4, pp. 760–763, 2019.

[17] N. Guo, J. Ge, C. Zhang, Q. Bu, and P. Tian, "Non-orthogonal multiple access in full-duplex relaying system with Nakagami-m fading," *IET Communications*, vol. 13, no. 3, pp. 271–280, 2019.

[18] C.-B. Le, D.-T. Do, and M. Voznak, "Exploiting impact of hardware impairments in NOMA: adaptive transmission mode in FD/HD and application in internet-of-things," *Sensors*, vol. 19, no. 6, p. 1293, 2019.

[19] X. Li, J. Li, P. T. Mathiopoulos, D. Zhang, L. Li, and J. Jin, "Joint impact of hardware impairments and imperfect CSI on cooperative SWIPT NOMA multi-relaying systems," in *2018 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 95–99, 2018.

[20] X. Li, M. Liu, D. Deng, J. Li, C. Deng, and Q. Yu, "Power beacon assisted wireless power cooperative relaying using NOMA with hardware impairments and imperfect CSI," *AEU-International Journal of Electronics and Communications*, vol. 108, pp. 275–286, 2019.

[21] X. Li, Q. Wang, M. Liu et al., "Cooperative wireless-powered NOMA relaying for B5G IoT networks with hardware impairments and channel estimation errors," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5453–5467, 2021.

[22] M. Toka, E. Guven, G. K. Kurt, and O. Kucur, "Performance analyses of MRT/MRC in dual-hop NOMA full-duplex AF relay networks with residual hardware impairments," 2021, https://arxiv.org/abs/2102.08464.

[23] B. C. Nguyen, T. Nguyen-Kieu, T. M. Hoang, P. T. Tran, and M. Vozňák, "Analysis of MRT/MRC diversity techniques to enhance the detection performance for MIMO signals in full-duplex wireless relay networks with transceiver hardware impairment," *Physical Communication*, vol. 42, article 101132, 2020.

[24] X. Li, M. Liu, C. Deng, P. T. Mathiopoulos, Z. Ding, and Y. Liu, "Full-duplex cooperative NOMA relaying systems with I/Q imbalance and imperfect SIC," *IEEE Wireless Communications Letters*, vol. 9, no. 1, pp. 17–20, 2020.

[25] M. S. Van Nguyen, D.-T. Do, Z. D. Zaharis, C. X. Mavromoustakis, G. Mastorakis, and E. Pallis, "Enabling full-duplex in MEC networks using uplink NOMA in presence of hardware impairments," *Wireless Personal Communications*, vol. 120, no. 3, pp. 1945–1973, 2021.

[26] C. Deng, M. Liu, X. Li, and Y. Liu, "Hardware impairments aware full-duplex NOMA networks over Rician fading channels," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2515–2518, 2021.

[27] D.-T. Do and A.-T. Le, "NOMA based cognitive relaying: transceiver hardware impairments, relay selection policies and outage performance comparison," *Computer Communications*, vol. 146, pp. 144–154, 2019.

[28] V. Aswathi and A. V. Babu, "Full/half duplex cooperative NOMA under imperfect successive interference cancellation and channel state estimation errors," *IEEE Access*, vol. 7, pp. 179961–179984, 2019.

[29] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, San Diego, CA, 2000.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1830497, 17 pages
https://doi.org/10.1155/2022/1830497

Research Article

5G Cognitive Radio Networks Using Reliable Hybrid Deep Learning Based on Spectrum Sensing

Vinodkumar Mohanakurup,[1] Vishwadeepak Singh Baghela,[2] Sarvesh Kumar,[3] Prabhat Kumar Srivastava,[4] Nitika Vats Doohan,[5] Mukesh Soni,[6] and Halifa Awal[7]

[1]*Bell Canada, Canada*
[2]*School of Computer Science & Engineering, Galgotias University, Greater Noida, India*
[3]*Department of Computer Science & Engineering, Babu Banarasi Das University, Lucknow, India*
[4]*Department of Computer Science and Engineering, Quantum University, Roorkee, Uttarakhand, India*
[5]*Department of Computer Science & Engineering, Medi-Caps University, Indore, India*
[6]*IEEE Senior Member, Bhopal, Madhya Pradesh, India*
[7]*Department of Electrical and Electronics Engineering, Tamale Technical University, Ghana*

Correspondence should be addressed to Halifa Awal; ahalifa@tatu.edu.gh

Received 3 December 2021; Revised 24 January 2022; Accepted 9 March 2022; Published 11 April 2022

Academic Editor: Samarendra Nath Sur

Spectrum sensing is critical in allowing the cognitive radio network, which will be used in the next generation of wireless communication systems. Several approaches, including cyclostationary process, energy detectors, and matching filters, have been suggested over the course of several decades. These strategies, on the other hand, have a number of disadvantages. Energy detectors have poor performance when the signal-to-noise ratio (SNR) is changing, cyclostationary detectors are very complicated, and matching filters need previous knowledge of the main user (PU) signals. Additionally, these strategies rely on thresholds under particular signal-noise model assumptions in addition to the thresholds, and as a result, the detection effectiveness of these techniques is wholly dependent on the accuracy of the sensor. In this way, one of the most sought-after difficulties among wireless researchers continues to be the development of a reliable and intelligent spectrum sensing technology. In contrast, multilayer learning models are not ideal for dealing with time-series data because of the large computational cost and high rate of misclassification associated with them. For this reason, the authors propose a hybrid combination of long short-term memory (LSTM) and extreme learning machines (ELM) to learn temporal features from spectral data and to exploit other environmental activity statistics such as energy, distance, and duty cycle duration for the improvement of sensing performance. The suggested system has been tested on a Raspberry Pi Model B+ and the GNU-radio experimental testbed, among other platforms.

1. Introduction

As wireless communication technology advances at a fast pace, and as new technologies such as 5G and the Internet of things (IoT) emerge, radio spectrum is becoming more scarce [1]. Because of the huge difference in overall band utilization indicated by the spectrum allocation and occupancy campaign [2–4], which ranges from 7 percent to 35 percent, it is clear that spectrum resources are underused. Cognitive radio has resolved the trade-off between spectrum availability and exponential growth, which was previously an issue (CR). It is feasible for these radios to detect and alter their settings to deliver the highest possible performance while causing no interference to the signals of other licensed users [5].

The licensed user is referred to as the principal user (PU) in the CR, while the unlicensed user is referred to as the secondary user (SU). The fundamental function of CR is to let SUs get access to vacant licensed bands in a probabilistic and noninterfering way while minimizing interference.

Spectrum sensing solutions that are both efficient and reliable are required to address this issue [6].

A number of sensing algorithms that have been developed for a variety of contexts have been proposed. There are several scenarios proposed, including the semiblind maximum eigenvalue detector (MED) [7], the generalized likelihood ratio test (GLRT)-based signal subspace eigenvalues detector (SSE) [8], which works on the known noise power, and the total blind scenario, which includes the maximum to average eigenvalue ratio (MAER) detector [9] and the arithmetic to geometric mean (AGM) [10] detector, which excludes the effect of noise power. These detectors are ineffective because they only detect samples from the live sensing timeslots, which are insufficient for determining the amount of PU [11]. These processes operate on the basis of the signal noise model, which assumes that the signal is spatially unequally distributed. Deep learning (DL) plays an important part in illuminating the study by eliminating the need for signal noise model conjecture; instead, it learns from the sensing data intelligently and precisely through quick computing, allowing for the detection of a trustworthy spectrum. Better spectrum sensing approaches are made possible via the use of deep learning models such as convolutional neural networks (CNN) and long short-term memory (LSTM). A hybrid mix of CNN and LSTM [12–18] is also presented as a solution for the signal categorization difficulties [19]. Despite the fact that DL-based spectrum sensing algorithms have higher performance, improvisation is still necessary for improving the spectrum sensing performance even in low SNR conditions, as shown in this paper. To overcome this constraint, the authors suggest a unique hybrid deep learning model, which combines the best features of both LSTM and extreme learning machines (ELM), for improving the spectrum sensing approach. The following is the paper's most significant contribution:

We suggested a hybrid deep learning model consisting of LSTM combined with ELM, in which the prior events are supplied together with the current events as a starting point for learning. High-speed training and behavior of the suggested method have resulted in significant performance improvements in terms of likelihood of detection and sensing accuracy, even while operating in low signal-to-noise ratio (SNR) regimes [20].

(1) Second, to provide a flexible and robust empirical hardware testbed to assess multiple learning models and to produce unbiased training datasets that comprise varied quantities of data under diverse signal-to-noise ratio (SNR) circumstances

(2) Finally, statistical aspects of PU activity such as duty cycle, distance, timestamps, and power being used as input data to improve the performance of the proposed model by including them into the model

A brief summary of the study is included in the following sections: Section 2 highlights relevant studies by other authors. Section 3 discusses the preliminary perspectives on long short-term memory and extreme learning machines that have been developed. After discussing the system model in Section 4, we will go on to Section 5, which will go into the dataset description, feature extraction, and operating principles of the proposed model in further depth. Detailed descriptions of empirical testbeds, as well as results of experiments and comparative analyses, are offered in Section 6. Finally, in Section 7, the study concludes with a discussion of possible future improvements.

2. Works Which Are Connected

Using DNN for spectrum sensing, Surendra and colleagues came up with a novel method of detection. This paper proposes "DLSenseNet," a DL-based model for spectrum sensing in which the structure information of received modulated signals is used for the purpose of spectrum sensing. The performance of the convolutional neural network (CNN) has been enhanced in order to recognize false alarms in CR users and lower the error rate. The suggested DNN-based spectrum detector [21] has a disadvantage in that it requires a large amount of training.

Using SVM, CNN, and reinforcement learning algorithms for cooperative spectrum sensing, Wang and Liu [22] examined the supervised and unsupervised learning techniques for cooperative spectrum sensing [23]. Similarly, Sundous and Halawani [24] investigated the difficulties associated with implementing machine learning algorithms in real time for spectrum sensing applications. The study examined a number of supervised and unsupervised reinforcement models for the extraction of energy detection-based features, cyclostationary-based feature extraction, and signal processing-based feature extraction [25].

Artificial neural network (ANN), support vector machine (SVM), decision trees (TREE), and KNN learning models" are all used in the detection of signals, according to Saber et al. (2020). According to [26], the performance of the classifiers was evaluated in order to establish which approach for spectrum sensing was the most effective among the three ways.

Those severe challenges were addressed by Cheng et al. [27], who created a stacked autoencoder-based spectrum sensing technology to overcome them (SAE-SS). This architecture is very effective in sifting through incoming signals to extract the most crucial and least obvious pieces of information possible. Furthermore, it is more resistant to temporal delays in noise than previous sensing systems. The suggested methodology does not need the usage of past knowledge or specific characteristics of present users [28]. Furthermore, it does not need the usage of any third-party feature extraction techniques.

Data-driven detectors with test statistics that are automatically generated from signal samples have been suggested by Xie et al. (2020) and are described in detail below. DL-based detectors that are currently available always need a substantial quantity of labelled training data in order to achieve good detection performance. UDSS is a "unsupervised deep spectrum sensing technique (UDSS)" created by the author to solve this problem. It is based on unsupervised deep learning (DL). Neither previous knowledge of the signal's noise level nor its statistical covariance matrix was

necessary for this strategy to be successful [29]. Furthermore, in the absence of PU signals, it simply necessitates a modest number of samples to be gathered [30]. Since semi-automatic algorithms require both labelled and unlabeled data in order to train, this approach has the disadvantage of lowering automation while also lowering the overall performance [31].

When determining the state of PU transmission, Cheng et al. (2019) used an SAE (stacked autoencoder) in the time domain to preprocess the raw signal samples and a logistic regression classifier to determine the status of PU transmission. While other DL spectrum sensing algorithms achieve great detection performance, the SAE outperforms them due to its remarkable ability to learn critical aspects of signals [32].

This work, conducted by Shah and Koo [33], describes a reliable spectrum sensing system that makes use of the K-nearest neighbor machine learning technique to detect interference. As part of the training phase, the fusion centre pools the local choices of CR users and a global decision is provided to each CR user by means of a majority vote. In the classification phase, each CR user compares their current sensing report to existing sensing classes and distance vectors are calculated as a result of this comparison [34]. In order to determine the quantitative variables that will be utilized in computing the posterior probability, the K-nearest neighbor technique is used. This collection of local choices is then combined at the fusion centre using a new decision combining strategy that takes into consideration the dependability of each CR user. The suggested KNN classifier has a drawback that makes it inefficient for a large number of users [22].

Due to the fact that the great majority of contemporary spectrum sensing detectors are designed using specific signal-noise model assumptions, the detection performance of these detectors is heavily reliant on the validity of the assumed models [35]. The upshot is that much of the present research in the area of spectrum sensing has been concentrated on deep learning, which is not restricted by any model assumptions and is thus more flexible. Be mindful of the fact that deep learning techniques such as convolutional neural networks (CNN) and long short-term memory (LSTM) networks, both of which are employed in deep learning, are very effective in extracting spatial and temporal properties from their respective input datasets [36]. Specifically, in this paper, we propose a CNNLSTM detector that first employs a CNN to extract energy correlation features from the covariance matrices generated by the sensing data and then feeds a series of energy correlation features corresponding to multiple sensing periods into an LSTM to learn the pattern of PU activity. In order to maximize the possibility of detection in the future, it is necessary to understand PU activity patterns in order to do so. The superiority of the CNN-LSTM detector in both conditions with and without noise uncertainty has been shown by a large number of simulations in both situations [33]. The suggested study, on the other hand, explains that the methods rely on thresholds under certain signal-noise model assumptions in addition to the thresholds, and as a consequence, the detection efficacy of these approaches is completely reliant on the accuracy of the sensor in question. As a result, the development of a dependable and intelligent spectrum sensing technology continues to be one of the most sought-after challenges among wireless researchers today [37]. ML and DL algorithms, which are used in the construction of extremely accurate spectrum sensing models for wireless communications, have recently been forced into the limelight of the study in the field of machine and deep learning. A multilayer learning model, on the other hand, is not appropriate for dealing with time-series data because of its enormous computational cost and high rate of misclassification, which makes it unsuitable for dealing with time-series data [38]. Consequently, to improve sensing performance, the authors propose a hybrid combination of long short-term memory (LSTM) and extreme learning machines (ELM) to learn temporal features from spectral data and to exploit other environmental activity statistics such as energy, distance, and duty cycle duration. The proposed system has been tested on a variety of systems, including a Raspberry Pi Model B+ and the GNU-radio experimental testbed. A comparison is then conducted to assess the performance of the proposed LSTM-ELM-based spectrum sensing strategy in comparison to that of other already existing approaches. It has been discovered via experiments that the proposed spectrum sensing strategy surpasses other strategies in terms of detection time and classification accuracy, with the proposed technique requiring less time to detect and more time to classify than the other techniques [39].

3. Preliminary Overview

Here, we will go through the long short-term memory (LSTM) and the extreme learning machines (ELM) frameworks, which are both very important.

3.1. Long Short-Term Memory: An Overview. In contrast to conventional neural networks, which are described in [14], artificial neural networks have no memory components and are thus unable to retain data. Furthermore, when the size of the datasets grows, it has certain gradient difficulties. Thus, it is necessary for the structural alteration to receive feedback between subsequent timestamps in order for it to work. This widely used learning model is known as LSTM, and its flexibility in memory and ability to handle large databases make it a good fit for a variety of diverse applications. Figure 1 depicts the proposed LSTM model, which is made up of LSTM cells.

LSTM is a "memory-based NN" which comprises 4 gates, namely, "input gate (IG), output gate (OG), forget gate (FG), and cell input (CI)". For each iteration, the LSTM network has the ability to remember the values. Let X_t be the input, then, the hidden layer output is represented as h_t, and its former output is represented as h_{t-1}. The CI state is $\rightarrow C_t$, then, the cell output state is represented as G_t, and its former state is represented as G_{t-1}. The 3 gate states are j_t, T_f, and T_0.

The LSTM can resemble both G_t and h_t which are able to communicate in RNN. In the LSTM network, the current

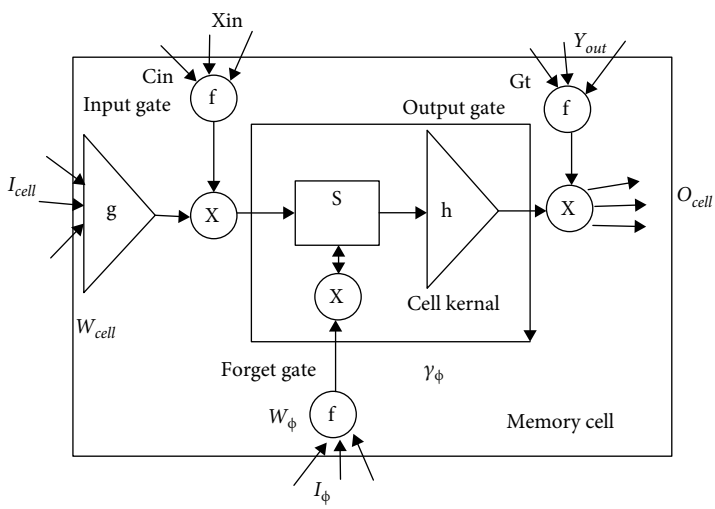

Figure 1: LSTM structure.

input state is merged with the output of the previous unit. The OG and FG play important role to update the memory.

The following mathematical expressions are utilized to determine G_t and h_t,

$$\begin{aligned} I.G &: j_t = \theta\left(G_l^i.O_t + G_h^i.e_{t-1} + s_i\right), \\ F.G &: T_f = \theta\left(G_l^f.O_t + G_h^f.e_{t-1} + s_f\right), \\ O.G &: T_o = \theta\left(G_l^0.O_t + G_h^o.e_{t-1} + s_o\right), \\ C.I &: \widetilde{T_C} = \tan h\left(G_l^C.O_t + G_h^C.e_{t-1} + s_C\right), \end{aligned} \tag{1}$$

where $G_l^0, G_l^f, G_l^i, G_l^C$ indicates the weight matrices between IG and output layers and $G_h^i, G_h^f, G_h^o, G_h^C$ denotes the weight conditions generated between hidden and input layers. The s_i, s_f, s_o, s_C are the bias vectors and tan h is considered to be hyperbolic function. The following mathematical expression is utilized to determine the cell output state.

$$\begin{aligned} T_c &= k_t * \widetilde{T_C} + T_f * T_{t-1}, \\ e_t &= T_o * \tan h(T_C). \end{aligned} \tag{2}$$

The final output score is obtained using equation (2). This final output score is used to predict the presence of PU signals based on the power levels.

3.2. Extreme Learning Machines: An Overview. The traditional fully connected classification layers are designed based on the principle of extreme learning machines. Extreme learning machines are a category of the neural network proposed by Huang et al. [36]. This kind of neural network utilizes the single hidden layers in which the hidden layers do not require the tuning mandatorily. Compared with the other learning algorithms such as "support vector machines (SVM) and random forest (RF)," ELM exhibits the better performance, high speed, and less computational overhead [40].

Based on machine learning, we developed a trustworthy spectrum sensing method, in which the FC applies a weighted decision combination rule to make decisions about which channels to use. Spectrum sensing is carried out by CR users during the training phase, and the sensing report is assigned to a sensing class based on the receipt of an acknowledgment signal (ACK) and the outcome of an overall decision. A CR user's behavior in a changing environment is triggered by the changing activity of a PU, which is represented by the sensing class, and is referred to as "adaptive response." Both the activity of the PU and the behavior of the CR user in response to that activity are correctly represented by these sensing classes. The categorization process may be initiated once adequate information about the surrounding environment has been gathered. As part of the training process, users of the CR may choose between two options on a local level. The local decision is made in the quantized-hard form, which is a quantized-hard form. Users' local selections are sent to the FC, which then makes a global decision based on the information received. CR users may choose whether to stay silent or broadcast in line with the general decision made by the CR committee. If wireless communications and mobile computing (Wi-Fi and mobile computing).

The detailed working mechanism of ELM is discussed in [27, 41]. In ELM, kernel function is utilized to obtain high accuracy. The ELM has minimum training error and better approximation. ELM is utilized for both classification as well as prediction because it uses nonzero activation function and autotuning of weight biases. In ELM, "L" neurons in the hidden layer are required to work with an activation function, so the output layer is "linear." It is unnecessary to tweak these hidden layers consistently [42]. Generally, hidden layer nodes are arbitrarily appointed. In ELM, the single hidden layer output is expressed in equation (3) as follows:

$$f_L(x) = \sum_{i=1}^{L} \beta_i h_i(x) = h(x)\beta, \tag{3}$$

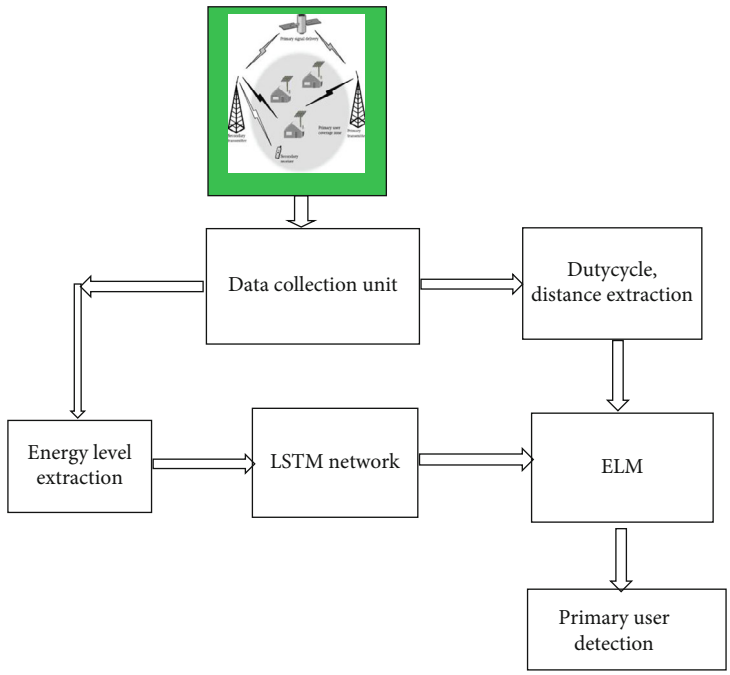

Figure 2: System model for the proposed architecture.

```
Procedure Create Datasets (Energy, Distance, Duty-Cycles, Time Period)
    For SNR =-20 dB to +20 Db
        Create PU_SNR_Signal= AWGN+ data signal
End
For i=1 to N do//where N = size of the data
        PU_Signal(i) = Data
End for
Return (PU_signal(i)
```

Algorithm 1: Data Collection Process for training the proposed learning model.

where x➔input, β➔output weight vector, and it is mathematically expressed as follows:

$$\beta = [\beta_1, \beta_2, \cdots, \beta_L]^T. \tag{4}$$

$H(x)$➔output hidden layer is mathematically expressed as follows:

$$h(x) = [h_1(x), h_2(x), \cdots, h_L(x). \tag{5}$$

To determine "output vector O" which is called as the "target vector," the hidden layers are mathematically expressed in equation (6) as follows:

$$H = \begin{bmatrix} h(x_1) \\ h(x_2) \\ \vdots \\ h(x_N) \end{bmatrix}. \tag{6}$$

The minimal nonlinear least square methods are significantly utilized for the basic implementation of the ELM and it is represented in equation (7) as follows:

$$\beta' = H^* O = H^T \left(HH^T\right)^{-1} O, \tag{7}$$

where $H*$ ➔inverse of H known as Moore–Penrose generalized inverse.

The above expression is also written as follows:

$$\beta' = H^T \left(\frac{1}{C} HH^T\right)^{-1} O. \tag{8}$$

By using the above expression, the output function is given as follows:

$$f_L(x) = h(x)\beta = h(x) H^T \left(\frac{1}{C} HH^T\right)^{-1} O. \tag{9}$$

Equation (9) is used for better classification of signals based on the PU characteristics.

Table 1: Statistical features and its mathematical expression.

Sl. no.	Statistical features	Mathematical expression	Descriptions
01	Power levels	$[ET^{\mathrm{PU}}(\mathrm{data}) + TxE_x^{\mathrm{PU}}]$	The power levels are calculated by adding the power required for transmitting the signals, and the energy of the detector is used
02	Duty cycle	$D = T_{\mathrm{on}}/(T_{\mathrm{on}} + T_{\mathrm{off}})$	T_{on}: on-time intervals; T_{off}: off-time intervals
03	Distance	$10\left[\frac{\rho_o - \sigma_m - \rho_r - 10n\log(f) + 30n - 32.44}{10n}\right]$	Distance is calculated ; $'\rho_o{}'$ indicates power of the signal (dBm) in the zero distance, $'\rho_r{}'$ indicates signal power (dBm) in the distance d, $'f'$ indicates the signal frequency (MHz), $'\sigma_m{}'$ indicates fade margin, and $'n'$ refers to the path-loss exponent

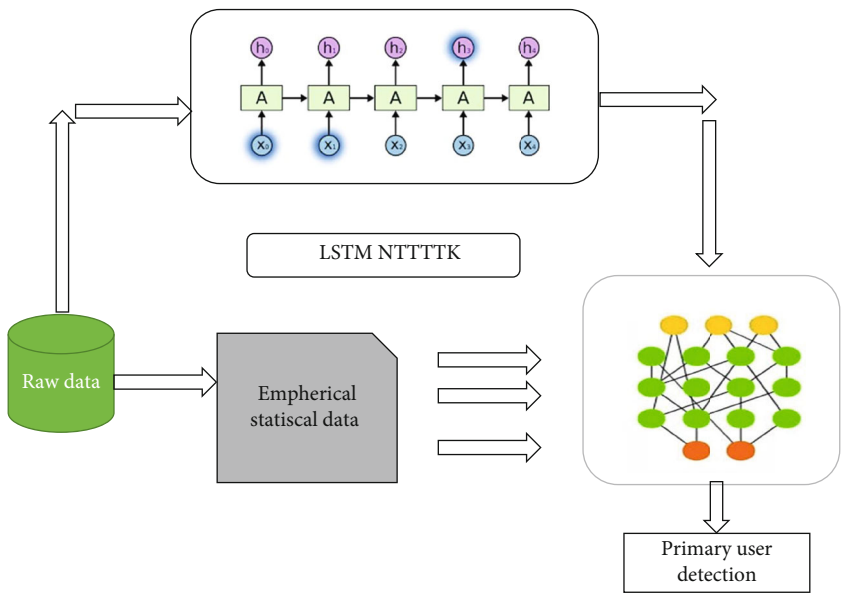

Figure 3: Schematic diagram for the proposed architecture.

4. System Model

The system model considered the multiuser cognitive radio scenario. Figure 1 represents the proposed dynamic resource allocation network (DRAIN-NETS) for an effective spectrum sensing. A PU transmitter is used for transmitting the PU signals. The primary signal users are collected and sampled [43]. These sampled signals are used to train and test the proposed model in such a way that the architecture can take the decision to determine the unknown samples in the network.

Consider $X(n) = \{Xx1(n), x2(n), x3(n), \cdots, x(k)n\}t$, where k represents the number of user and n denotes the received signals from k users. $X(n)$ indicates the discrete time sample present at k^{th} users. The paper uses the binary hypothesis testing process for spectrum sensing as mentioned in [42].

$$\begin{aligned} H1 &: X(n) = R_{N(n)} + Y(n), \\ H0 &: X(n) = Y(n). \end{aligned} \tag{10}$$

Table 2: Learning parameters.

Sl. no.	Hyperparameters	Values
1	Learning rate	0.001
2	Batch size	30
3	Number of epochs	250
4	Hidden layers	4
5	Optimizer	Adam
6	Activation function used	ReLU
7	Loss function	MSE

Here, $R\_N(n)$ indicates the signal vectors which suffers from channel fading and path loss. $Y(n)$ indicates the different noise vector with zero mean. Hence, by [42], hypothesis $H1$ indicates the presence of PU and $H0$ indicates its absence. These signal parameters are separated into real and imaginary components used to train and test the proposed architecture.

```
Procedure Evaluate the model (Energy, Duty Cycle, Distance, Time Period)
Output: Presence of PUs
Feature Extraction Phase (Energy, Duty-cycle, Distance, Time period)
For i =1 to N// where N refers to data size
            Predicted output (P(o)) is calculated using equation(4) &(6)
        ELM _Output=ELM(P(o), Distance, Duty-cycle, Tn) using Equation (9)
    PU presence = Elm_Output
        End
End
End
```

Algorithm 2: Overall training method for the Proposed Framework.

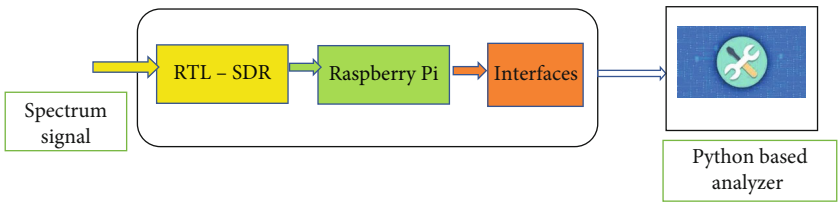

Figure 4: Empirical experimentation setup for validating the proposed sensing algorithm.

Table 3: Specifications for the RTL_SDR for different frequency bands.

Tuner	Frequency range
Elonics E4000	52–2200 MHz with a gap from 1100 MHz to 1250 MHz (varies)
Rafael Micro R820T	24–1766 MHz
Rafael Micro R828D	24–1766 MHz
Fitipower FC0013	22–1100 MHz (FC0013B/C, FC0013G has a separate L-band input, which is unconnected on most sticks)
Fitipower FC0012	22–948.6 MHz
FCI FC2580	146–308 MHz and 438–924 MHz

5. Proposed Framework

As in the proposed work, 5G communication indicates that it is possible to avoid interfering with other users by using a variety of conventional multiple-access techniques, such as time division multiple access (TDMA), orthogonal frequency division multiple access (OFDMA), and code division multiple access (CDMA). However, because of the fast increase in the number of mobile devices, these approaches may not be sufficient to meet the needs of users who demand access to wireless communication networks. NOMA is becoming more important in 5G networks for building multiaccess schemes as a result, since it enables several users to simultaneously use the same frequency resources. There are two basic kinds of NOMA techniques: code domain and power domain, which are both discussed here. In this study, we concentrate on the power domain, in which numerous users are allocated to utilize the same frequency and time resources for their data transmissions, as described before. Specific to this method of transmission, the signals of several users are superposed to transmit over the same resources and successive interference cancellation (SIC) is performed to decode the users' intended signals and eliminate interference at the receiver. In many various communication systems, such as the industrial Internet of things, machine-to-machine communications, and cooperative communications, several research studies on NOMA schemes have been conducted.

5.1. Dataset. It comprises over-the-air observations of authentic radio signals modulated with 11 different modulations derived from real-world radio broadcasts, which were collected from this dataset. The signals were generated via a USRP B210, which was connected to a PC running GNU Radio in order to do so, according to the authors. The numerous transmitters had to be implemented using the same source code and data sources as those used in the production of RadioML2016.10a; therefore, it was essential to utilize the same data sources and source code as before. As an additional point of clarification, it should be noted that the RadioML dataset had an inconsistency with AM modulations that was corrected in later versions of the RadioML dataset.

On the receiver side, we captured the signals using the MIGOU platform, which we designed and built from the

Table 4: Mathematical expression for calculating the different performance metrics.

SL. no.	Performance metrics	Mathematical expression
01	Prediction accuracy (P_a)	$\frac{TP+TN}{TP+TN+FP+FN}$
02	Recall	$\frac{TP}{TP+FN} \times 100$
03	Precision	$\frac{TN}{TP+FP}$
04	Probability of detection (P_d)	Total number of PU/total number of users (PU + noise signals)
05	Probability of missing ratio (P_m)	$1-(P_d)$
06	Probability of false alarm (P_f)	Number of noise signals diagnosed/total number of users (PU + noise signals)

Table 5: Validation and training accuracy for the proposed algorithm.

Sl. no.	No. of epochs	Training accuracy (%)	Validation accuracy (%)
01	20	96.5%	95.0%
02	40	96.5%	95.0%
03	60	96.75%	96.50%
04	80	96.90%	96.95%
05	100	97.25%	97.5%
06	120	97.45%	97.5%
07	140	97.8%	98.0%
08	160	98.5%	98.5%
09	180	98.5%	98.5%
10	200	98.7%	98.5%

Table 6: Performance metrics of the proposed framework using the different composition of data samples.

Composition	Low SNR composition	High SNR composition	Performance metrics		
			Sensing accuracy	Recall	Precision
90 : 10	90	10	0.987	0.982	0.983
80 : 20	80	20	0.986	0.981	0.9825
70 : 30	70	30	0.985	0.979	0.9784
60 : 40	60	40	0.985	0.978	0.9783
50 : 50	50	50	0.9845	0.978	0.9781
40 : 60	40	60	0.9842	0.9772	0.9772
30 : 70	30	70	0.9841	0.9763	0.9734
20 : 80	20	80	0.9840	0.9762	0.9732
10 : 90	10	90	0.9840	0.9761	0.9730

ground up. When combined with software-defined radio (SDR) capabilities, it is designed to overcome the hardware architectural constraints that now impede cognitive radio (CR) research and experimentation with low-power end-devices from being conducted successfully. There was a communication channel detected, and the raw I/Q samples were sent to a computer, which was designed to store the samples in the proper database [31].

We took all of our measurements indoors, in a controlled environment like a lab or an office. Specific measurements were taken at two different distances from the transmitter: one meter and six meters. The average signal-to-noise ratios (SNR) at the two distances from the transmitter were 37 dB and 22 dB, respectively, at the two distances from the transmitter at the two distances from the transmitter. For the final result, all of the collected I/Q signals were divided and processed into 128 bit vectors, which were then each individually normalized to get the final result. Adding 400,000 normalized vectors for each modulation-signal strength ratio (MOD-SNR) combination in the dataset was the last stage, resulting in an overall total of 8.8 million vectors in the final dataset.

Figure 2 shows the proposed architecture for the spectrum sensing. It consists of spectrum data collection and

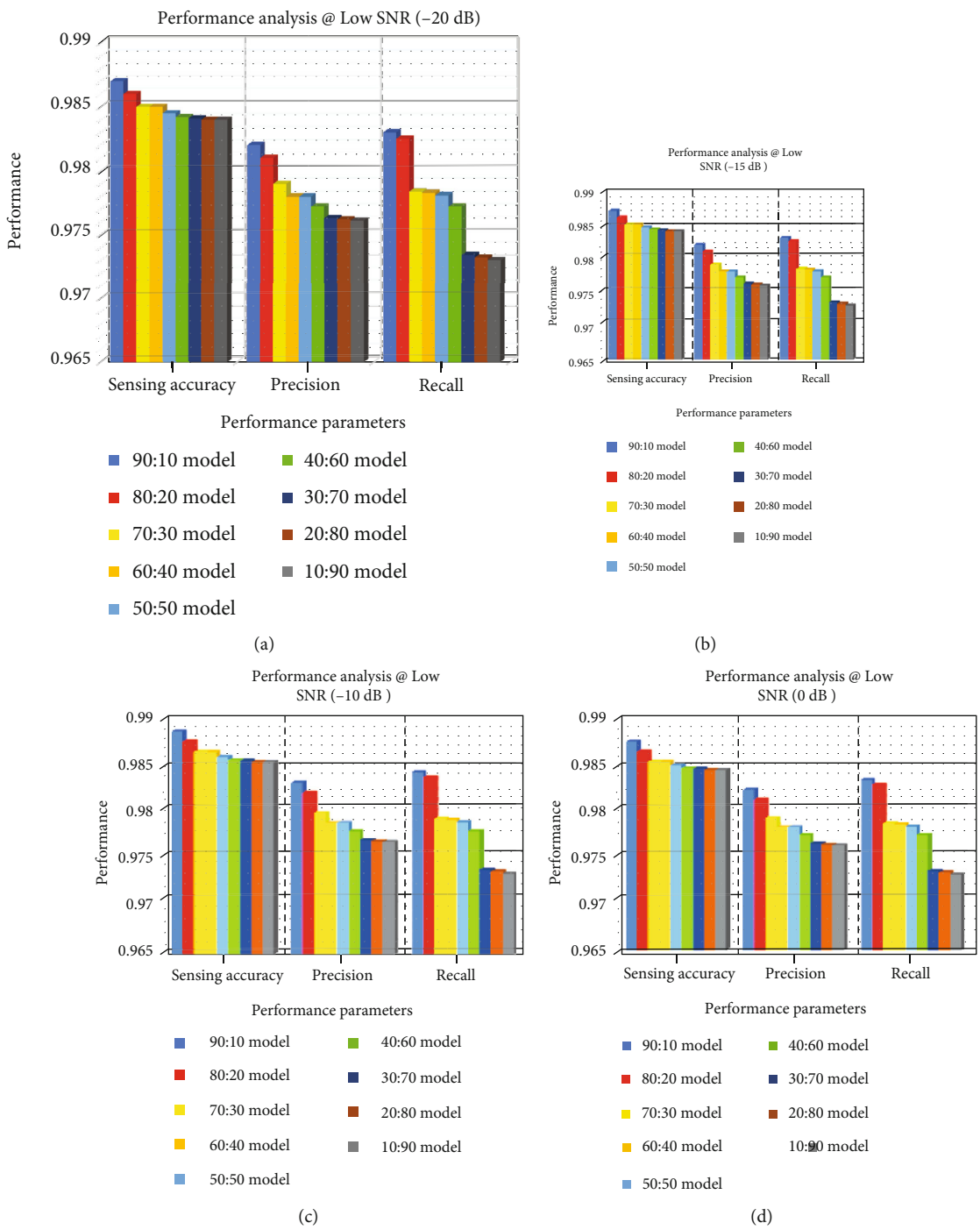

Figure 5: Performance evaluation proposed model for the different composition of data. (a) Low SNR at −20 db, (b) at −15 db, (c) at −10 db, and (d) at −5 db.

proposed hybrid spectrum sensing unit using LSTM-ELM architectures. As mentioned in Section 5, this research work acquired spectrum data by utilizing the empirical testbed. The data are captured using the measurement phase, and then, only the PU signal is obtained and measured in terms of η^{2X}. To validate the model under noisy environments, additive white Gaussian noise is generated [43] and added to the raw PU signal. The signal Y is represented as 2N samples which is represented as follows:

$$X = \left[x^1, x^2, x^3, x^4, \cdots, x^{2N}\right]. \tag{11}$$

Each sample is taken as the inputs to the proposed

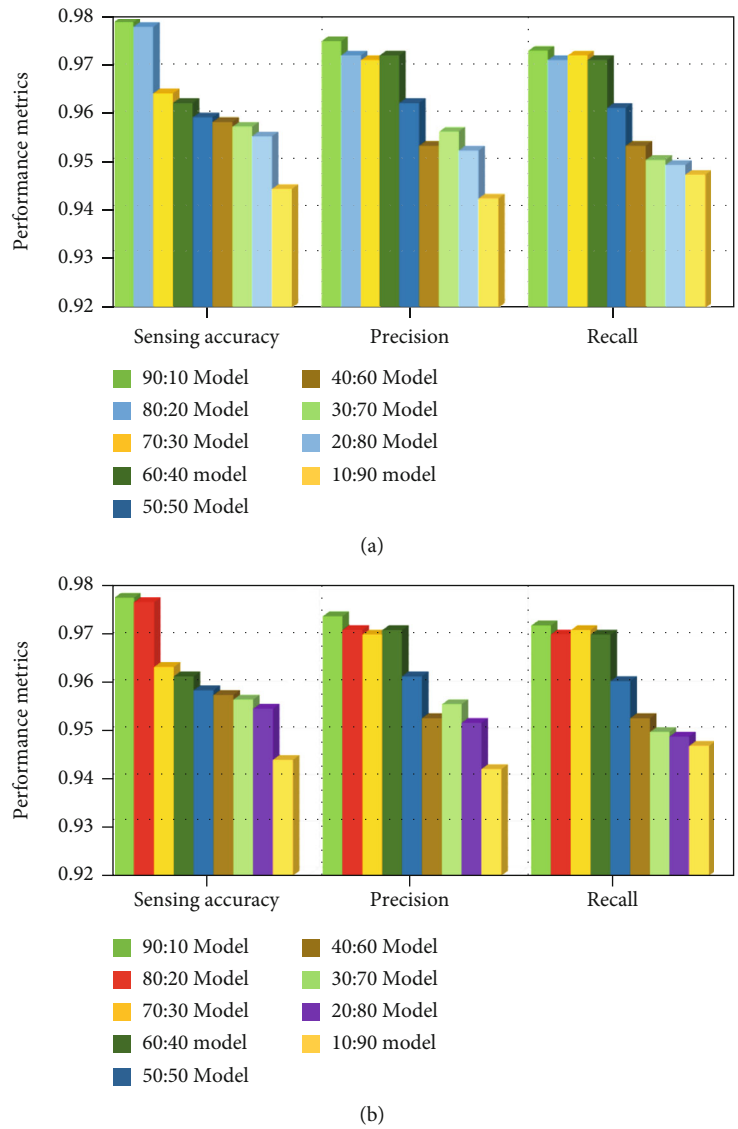

Figure 6: Performance evaluation proposed model for the different composition of data. (a) High SNR from 0 db to 10 db. (b) High SNR from 15 db to 20 db.

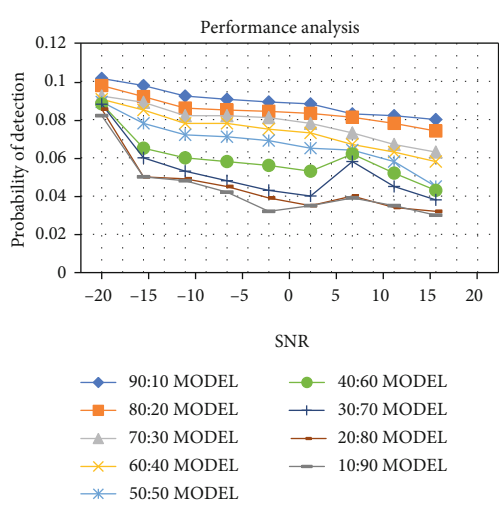

Figure 7: Probability of detection (P_d) vs SNR performance curves.

architecture. In this research work, nearly 350,200 samples are utilized [39] for the normal PU signal (SNR range of −20 dB to +20), and again, 350,200 samples are collected for AWGN signals. The datasets which are required for training the proposed architecture are shown in Algorithm 1.

5.2. Statistical Feature Extraction. Once the data is acquired from the testbed, different features such as duty cycles, on-off time, and distances are calculated. The mathematical expression for calculating the statistical features is shown in Table 1. We compare these measured characteristics to noise thresholds to establish ground truth for future investigation [38]. If the measured levels are greater than the threshold, the data is labelled as one, otherwise zero. These one- and zero-labelled power levels are used to train the LSTM model, and predicted power levels, distance, and duty

Table 7: Performance metrics of the proposed framework using the different composition of data samples.

Composition (%)	Low SNR composition (%)	High SNR composition (%)	Performance metrics		
			P_d	P_f	P_m
90 : 10	90	10	0.1015	0.1012	0.001
80 : 20	80	20	0.0978	0.0889	0.022
70 : 30	70	30	0.0923	0.0878	0.0278
60 : 40	60	40	0.0906	0.0868	0.0320
50 : 50	50	50	0.0892	0.08547	0.0330
40 : 60	40	60	0.0882	0.08423	0.0342
30 : 70	30	70	0.0880	0.0832	0.0352
20 : 80	20	80	0.08546	0.0824	0.0400
10 : 90	10	90	0.08201	0.0810	0.04014

cycles are used to train the ELM for the better classification of PUs.

5.3. Proposed Hybrid Model Training and Hyperparameter Tuning. The hybrid learning model has been formulated for an efficient classification of the PUs under different SNR scenarios. Figure 3 shows the proposed model in which LSTM is normally used for the prediction of the PUs using the power levels where the ELM is used to classify the PU based on the user activity statistical features. The input power level of the raw data is compared to the threshold, and therefore, information is assigned for practical LSTM training. Iterative trials provide the basis of the LSTM model's construction. Table 2 provides the hyperparameters chosen for the network. The training methods for evaluating the LSTM model is presented in Algorithm 2. ELM takes the predicted output along with statistical features for the better classification of PUs. The working of the proposed model is summarized in Algorithm 2.

6. Empirical Experimental Testbed

Figure 4 illustrates the empirical measurement setup. From this setup, the spectrum data are acquired for validation of the proposed E-LSTM0-SS technique. The hardware consists of RTL-SDR dongle interfaced with Raspberry Pi Model 3 and the Windows 10-based computer system for running the software. The software includes GNURADIO and Python 3.8. The different technologies of RTL-SDR configuration on raspberry pi 3 are shown in Table 3. Analyzers built with Python collect high SNR signals that are then analyzed to find PU signals. Analysis results are utilized in offline mode to verify suggested spectrum sensing methods.

6.1. Experimental Results and Discussion. This section presents the proposed algorithm validation. The proposed algorithm is developed using Keras libraries and TensorFlow backend to train and test the models. The datasets were collected and divided into two categories such as high SNR (−5 db to +5 db) and low SNR (−5 db to −20 db) [37]. Nearly 7,00,102 datasets were collected and used for training and testing the datasets. The performance metrics such as the performance metrics considered for evaluation are the prediction accuracy (P_a), precision (P), recall (R), probability of detection (P_d), probability of false alarm (P_f), and probability of miss detection (P_m) [33].

P_d indicates the "probability of declaring the PU presence when it really occupies the spectrum."

P_f indicates the "probability of declaring that PU is present when the spectrum is really vacant."

P_m indicates the "probability of declaring that the spectrum is vacant when actually the PU is present."

The P_d and P_f are measured for different SNR values of the received signals [36].

The mathematical expression used for calculating the above performance metrics is given in Table 4.

6.2. Model Validation. To validate the proposed model, 70% of the total sample is utilized for training which is fed in batches to the proposed hybrid model and output functions are calculated as mentioned in Algorithm 2 [35]. The training and validation accuracies of the proposed model are evaluated and validated as shown in Table 5. In Table 5, it is noticed that the number of epochs increases and training and validation accuracy also increases. It is evident in Table 5 that the LSTM model which is chosen has overcame the overfitting problem and is suitable for obtaining the better classification performance [34].

For the testing purpose, training datasets with different compositions were created by changing the ratio of the no. of samples in low SNR to the no. of samples in high SNR. The performance metrics used in Table 6 is calculated for the different sample compositions.

Figure 5 shows the proposed model performance in low SNR ranges from −20 db to 0 db for the different composition of data. It is evident in Figures 5(a)–5(d) that the performance of the proposed model has shown the highest performances at low SNR using 90 : 10 data composition and least performances at the same range using 10 : 90 and 20 : 80 data composition, respectively.

Figure 6 shows the performance of the proposed model in high SNR ranges from 0 db to 20 db for the different composition of data. It is evident in Figures 5(a)–5(d) that the performance of the proposed model has shown the highest performances at high SNR using 90 : 10 data composition and optimal performance at the same range using 10 : 90 and 20 : 80 data composition, respectively.

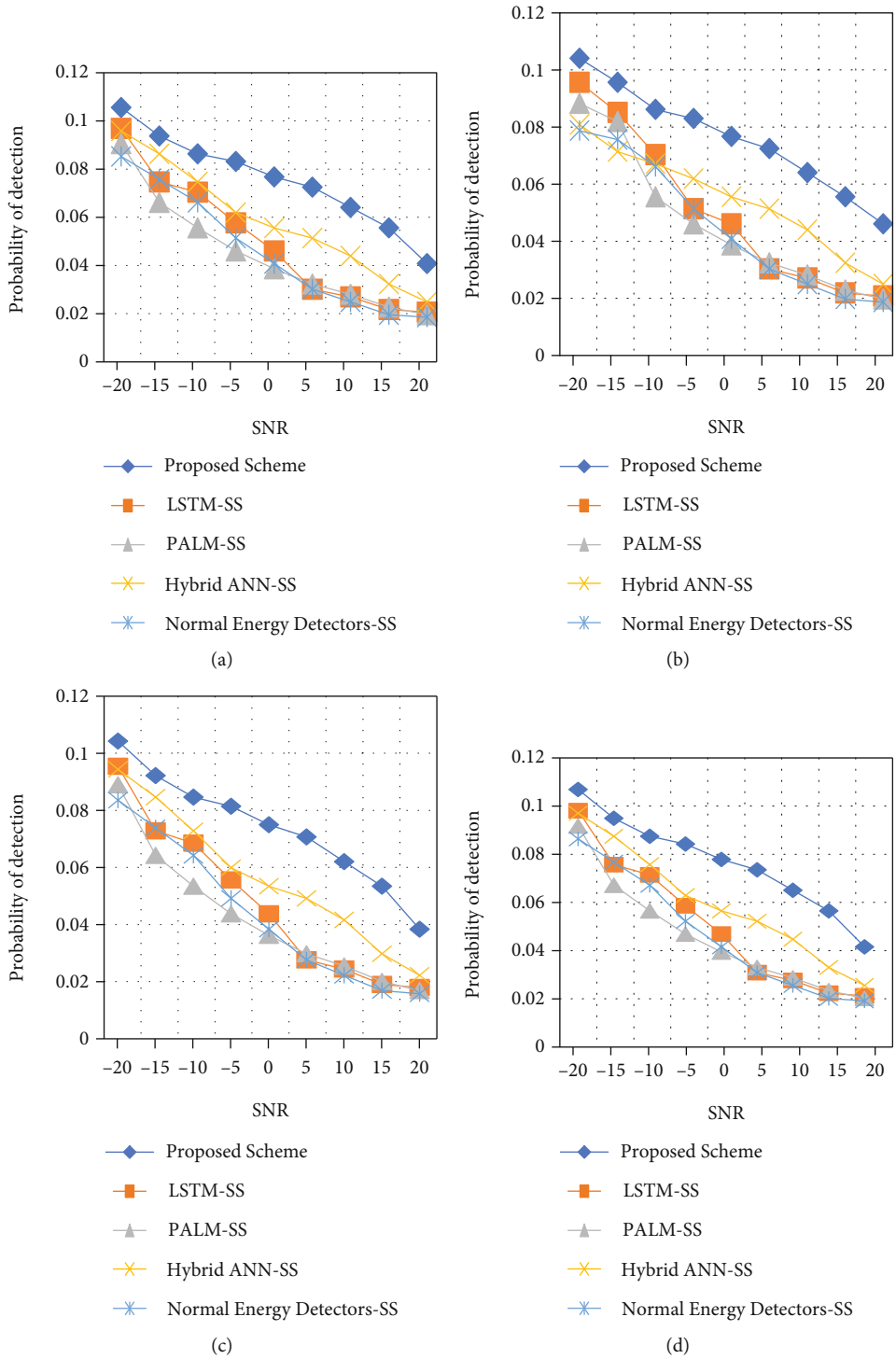

Figure 8: Continued.

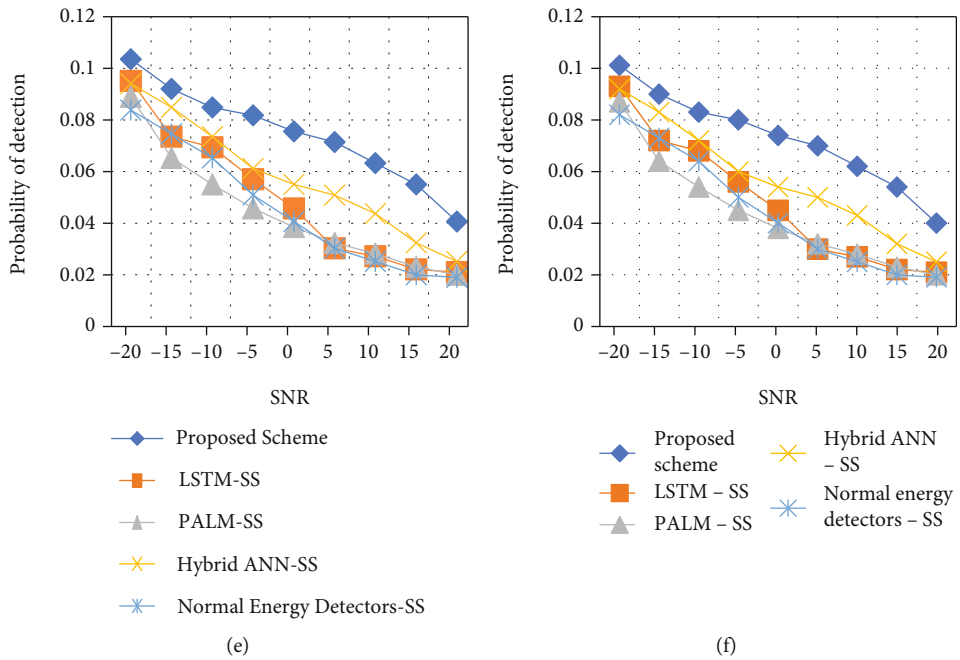

Figure 8: Probability of detection (P_d) metrics (a) @52–2,200 MHz, *(b) @24–1,766 MHz, (c) 22–110 MHz, (d) 22–9,486 MHz, (e) 146–308 MHz, and (f) 438–921 MHz.

Table 8: Performance analysis of the different algorithms at 52–2,200 MHz and low SNR (−20 db to 0 db).

Sl. no.	Algorithm details	Samples (N = testing samples)	Performance metrics				
			Sensing accuracy	Precision	Recall	P_d	P_f
01	LSTM-SS	$N = 200$	0.965	0.955	0.950	0.1012	0.1002
02	PALM-SS		0.942	0.930	0.932	0.093	0.0923
03	Hybrid ANN-SS		0.921	0.910	0.923	0.089	0.087
04	Normal energy detectors-SS		0.782	0.762	0.780	0.086	0.0864
05	RF-SS		0.80	0.82	0.812	0.087	0.085
06	Proposed scheme		0.982	0.973	0.970	0.1012	0.1010

Table 9: Performance analysis of the different algorithms at 24–1766 MHz and low SNR (−20 db to 0 db).

Sl. no.	Algorithm details	Samples (N = testing samples)	Performance metrics				
			Sensing accuracy	Precision	Recall	P_d	P_f
01	LSTM-SS	$N = 200$	0.863	0.833	0.83	0.1012	0.1002
02	PALM-SS						
03	Hybrid ANN-SS		0.842	0.83	0.832	0.083	0.0823
04	Normal energy detectors-SS		0.821	0.81	0.823	0.088	0.087
05	RF-SS		0.782	0.762	0.78	0.086	0.0864
06	Proposed scheme		0.8	0.82	0.812	0.087	0.083

Figure 7 and Table 7 shows the impact of data compositions of training sets on the probability of detection (P_d) at different SNR thresholds. It is evident in Figure 7 that there is a significant impact on P_d at different SNR rates for various compositions of the training set. The low SNR range needs to be raised for the P_d to rise. The magnitudes of the PU signals are pretty comparable to the noise in this situation. So, the LSTM network struggles to differentiate PU signal and noise. But still, integration of ELM in LSTM has produced the optimal performances even at low SNR.

The developed hybrid method was validated on several radio frequencies, as shown in Table 3, and compared to

Table 10: Performance analysis of the different algorithms at 22–1100 MHz and low SNR (−20 db to 0 db).

Sl. no.	Algorithm details	Samples (N = testing samples)	Performance metrics				
			Sensing accuracy	Precision	Recall	P_d	P_f
01	LSTM-SS	$N = 200$	0.761	0.711	0.71	0.1012	0.1002
02	PALM-SS						
03	Hybrid ANN-SS		0.742	0.73	0.732	0.073	0.0723
04	Normal energy detectors-SS		0.721	0.71	0.723	0.087	0.087
05	RF-SS		0.782	0.762	0.78	0.086	0.0864
06	Proposed scheme		0.8	0.82	0.812	0.087	0.081

Table 11: Performance analysis of the different algorithms at 22–9486 MHz and high SNR (0 db to 20 db).

Sl. no.	Algorithm details	Samples (N = testing samples)	Performance metrics				
			Sensing accuracy	Precision	Recall	P_d	P_f
01	LSTM-SS	$N = 200$	0.662	0.622	0.62	0.1012	0.1002
02	PALM-SS						
03	Hybrid ANN-SS		0.622	0.63	0.632	0.063	0.0623
04	Normal energy detectors-SS		0.621	0.61	0.623	0.086	0.087
05	RF-SS		0.782	0.762	0.78	0.086	0.0862
06	Proposed scheme		0.8	0.82	0.812	0.087	0.082

Table 12: Performance analysis of the different algorithms at 146–308 MHz and high SNR (0 db to 20 db).

Sl. no.	Algorithm details	Samples (N = testing samples)	Performance metrics				
			Sensing accuracy	Precision	Recall	P_d	P_f
01	LSTM-SS	$N = 200$	0.881	0.811	0.81	0.1012	0.1002
02	PALM-SS						
03	Hybrid ANN-SS		0.842	0.83	0.832	0.083	0.0823
04	Normal energy detectors-SS		0.821	0.81	0.823	0.088	0.087
05	RF-SS		0.782	0.782	0.78	0.088	0.0884
06	Proposed scheme		0.8	0.82	0.812	0.087	0.081

other sensing approaches, such as LSTM-SS [12], hybrid ANN-SS [14], PALM-SS [16], and regular energy detectors [18], as well as conventional energy detectors.

Figure 8 represents the comparative analysis. In Figures 8(a)–8(f), the proposed algorithm proves that it has better performance when compared with the other learning-based spectrum sensing techniques at different SNR. The ELM learning-based LSTM network is integral to the proposed spectrum sensing technique's improved performance. It has been shown that the suggested method outperforms the other learning models because of its looping structure, information flow regulation, feedforward, and more error-prone ELM training methodology. Since these features are absent in other learning models, these existing spectrum sensing models fail to understand that the hidden features of the spectrum data tend to exhibit the lower performances than the proposed scheme.

The experiments are performed at different SNR with varying time intervals. Using the extreme learning machine approach, which is comprised of a collection of randomly selected hidden units and analytically set output weights, we hope to overcome these restrictions.

Tables 8–11 show the comparative analysis of different algorithms with respective to the different frequencies and SNR.

In Tables 8–12, it is clear that the proposed algorithm has outperformed the other learning-based spectrum sensing techniques. Since the proposed model has learned the statistical features in the better way, performance remains to be optimal even in low SNR whereas the other existing models has shown the degraded performance as SNR decreases in different frequency measurements. Additionally, ELM learns not only the predicted output from LSTM but also other statistical features which makes the proposed model to detect effectively in different SNR.

In proportion to the rise in Eb/No, the average energy consumption per sensor increases. It can be shown that the decrease in energy consumption is enhanced in both conventional and new approaches when we compare them to a noncooperative situation. For example, when Eb/No is

equal to 5 dB, the suggested approach decreases the energy usage by 60%, compared to the conventional way.

The rationale for this improvement is because the CUs will exchange the data regarding the PU's presence, which will raise the overall detection probability overall. Additionally, it can be observed in Figure 8 that the suggested approach provides a considerable increase in detection performance when compared to the previous way of detection. This is due to the employment of two phases in the detection process, which improves the detection performance, particularly in fine sensing, by increasing the detection threshold.

The network animator (NAM) diagram for random topology is shown in the figure below. The total number of packets received is fewer than the total number of packets sent. Because wireless communication is the medium of choice, it is possible that some packets may be lost. The packet delivery ratio, on the other hand, is 87.17 percent, which is an excellent indication of packet delivery even in the case of wireless communication. In order to compensate for a lost packet, only retransmission of that packet may be used; nevertheless, this strategy will incur some latency. Depending on the kind of communication being sent, the delay may be characterized as bearable or nontolerable depending on the length of time it takes. For example, teleprotection, PMU (class A), control messages, smart meters, and other similar packets are admissible since the minimum latency requirement is 8 ms or less. The average delay of the simulation is 7 milliseconds, which is within the theoretical limit of the system.

7. Conclusion

In this research work, hybrid DL-based spectrum sensing was proposed which significantly learns the statistical time series spectrum data. The novel testbed which comprises of Raspberry Pi 3 Model B++ interfaced with RTL-SDR dongle has been constructed to collect the raw spectral data under varying frequency technologies and different SNR conditions. The performance metrics such as sensing accuracy, precision, recall, P_d, and P_f are calculated and compared with the other existing learning model-based spectrum sensing techniques. From the experimentation, it is clear that the proposed framework has outperformed the other algorithm in terms of high sensing accuracy and high detection ratio even under low SNR. Additionally, the proposed scheme has shown the significant performance of detection using the statistical features and hybrid combination of LSTM and ELM techniques. However, the enhanced performance of the proposed algorithm is obtained at the cost of long training time and high computational overhead. The improvisation is required for the proposed algorithm in terms of handling the multiple PU and SU.

The key criteria used by SU to make the PU signal detection are described and explored in detail in this section. For the situation of fullduplex operation, several modes of operation are detailed in detail. The use of learning approaches is also examined at the local and cooperative levels, among other things. Following that, the possibility for using spectrum sensing in WSN/IoT networks is researched, as well as the critical role played by IoT/WSN in the provision of spectrum sensing as a service is explored. In addition, we address the usage of cognitive radio in 5G and B5G networks from the viewpoints of spectrum allocation and frequency efficiency. Based on an in-depth examination of the current state of the art, we identify various problems and astounding issues that need additional investigation.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. Lunden, V. Koivunen, and H. V. Poor, "Spectrum exploration and exploitation for cognitive radio: recent advances," *IEEE Signal Processing Magazine*, vol. 32, no. 3, pp. 123–140, 2015.

[2] M. Wellens and P. Mähönen, "Lessons learned from an extensive spectrum occupancy measurement campaign and a stochastic duty cycle model," *Mobile Networks and Applications*, vol. 15, no. 3, pp. 461–474, 2010.

[3] D. Singh, V. Kumar, M. Kaur, M. Y. Jabarulla, and H.-N. Lee, "Screening of COVID-19 suspected subjects using multi-crossover genetic algorithm based dense convolutional neural network," *IEEE Access*, vol. 9, pp. 142566–142580, 2021.

[4] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[5] P. Pateriya, R. Singhai, and P. Shukla, "Design and implementation of optimum LSD coded signal processing algorithm in the multiple-antenna system for the 5G wireless technology," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 7628814, 12 pages, 2022.

[6] R. Utrilla, *MIGOU-MOD: a dataset of modulated radio signals acquired with MIGOU, a low-power IoT experimental platform*, Mendeley Data, V1, 2020.

[7] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.

[8] Y. Zeng, C. L. Koh, and Y. Liang, "Maximum eigenvalue detection: theory and application," in *IEEE international conference on communications*, pp. 4160–4164, Beijing, China, May 2008.

[9] R. Zhang, T. J. Lim, Y. Liang, and Y. Zeng, "Multi-antenna based spectrum sensing for cognitive radios: a glrt approach," *IEEE Transactions on Communications*, vol. 58, no. 1, pp. 84–88, 2010.

[10] P. Bondada, D. Samanta, M. Kaur, and H.-N. Lee, "Data security-based routing in MANETs using key management mechanism," *Applied Sciences*, vol. 12, no. 3, p. 1041, 2022.

[11] A. Paul, P. Kunarapu, A. Banerjee, and S. P. Maity, "Spectrum sensing in cognitive vehicular networks for uniform mobility model," *IET Communications.*, vol. 13, no. 19, pp. 3127–3134, 2019.

[12] P. Wang, J. Fang, N. Han, and H. Li, "Multiantenna-assisted spectrum sensing for cognitive radio," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1791–1800, 2010.

[13] X. Li, J. Fang, W. Cheng, H. Duan, Z. Chen, and H. Li, "Intelligent power control for spectrum sharing in cognitive radios: a deep reinforcement learning approach," *IEEE Access*, vol. 6, pp. 25463–25473, 2018.

[14] S. Chandhok, H. Joshi, A. V. Subramanyam, and S. J. Darak, *Novel Deep Learning Framework for Wideband Spectrum Characterization at Sub-Nyquist Rate*, arXiv, 2019.

[15] H. Kaushik, D. Singh, M. Kaur, H. Alshazly, A. Zaguia, and H. Hamam, "Diabetic retinopathy diagnosis from fundus images using stacked generalization of deep models," *IEEE Access*, vol. 9, pp. 108276–108292, 2021.

[16] S. Zheng, S. Chen, P. Qi, H. Zhou, and X. Yang, "Spectrum sensing based on deep learning classification for cognitive radios," *China Communications*, vol. 17, pp. 138–148, 2020.

[17] Q. Peng, A. Gilman, N. Vasconcelos, P. C. Cosman, and L. B. Milstein, "Robust deep sensing through transfer learning in cognitive radio," *IEEE Wireless Communications Letters*, vol. 9, pp. 38–41, 2020.

[18] R. R. Althar, D. Samanta, M. Kaur, A. A. Alnuaim, N. Aljaffan, and M. A. Ullah, "Software systems security vulnerabilities management by exploring the capabilities of language models using NLP," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 8522839, 19 pages, 2021.

[19] J. Xie, J. Fang, C. Liu, and X. Li, "Deep learning-based spectrum sensing in cognitive radio: a CNN-LSTM approach," *IEEE Communications Letters.*, vol. 24, no. 10, pp. 2196–2200, 2020.

[20] A. Paul and S. P. Maity, "Kernel fuzzy c-means clustering on energy detection based cooperative spectrum sensing," *Digital Communications and Networks.*, vol. 2, no. 4, pp. 196–205, 2016.

[21] D. Ahirwar, P. K. Shukla, K. R. Bhatele, P. Shukla, and S. Goyal, "Intrusion detection and tolerance in next generation wireless network," in *Next Generation Wireless Network Security and Privacy*, K. I. Lakhtaria, Ed., pp. 313–335, PA: IGI Global, 2015.

[22] J. Wang and L. Bao, "A brief review of machine learning algorithms for cooperative spectrum sensing," *IOP Publishing*, vol. 1852, no. 4, p. 042094, 2021.

[23] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, "An efficient image encryption technique based on two-level security for internet of things," *Multimedia Tools and Applications*, 2022.

[24] S. Khamayseh and A. Halawani, "Cooperative spectrum sensing in cognitive radio networks: a survey on machine learning-based method," *Journal of Telecommunication*, vol. 3, no. 2020, pp. 36–46, 2020.

[25] A. Revathi, R. Kaladevi, K. Ramana, R. H. Jhaveri, M. R. Kumar, and M. S. P. Kumar, "Early detection of cognitive decline using machine learning algorithm and cognitive ability test," *Security and Communication Networks*, vol. 2022, Article ID 4190023, 13 pages, 2022.

[26] J. Gao, X. Yi, C. Zhong, X. Chen, and Z. Zhang, "Deep learning for spectrum sensing," *IEEE Wireless Communications Letters*, vol. 8, pp. 1727–1730, 2019.

[27] Q. Cheng, Z. Shi, D. N. Nguyen, E. Dutkiewicz, and Non-cooperative OFDM Spectrum Sensing Using Deep Learning, *International Conference on Computing*, Machine Learning for Communication and Networking, Networking and Communications (ICNC), 2020.

[28] C. Liu, J. Wang, X. Liu, and Y. C. Liang, "Deep CM-CNN for spectrum sensing in cognitive radio," *IEEE Journal on Selected Areas in Communications.*, vol. 37, no. 10, pp. 2306–2321, 2019.

[29] A. Paul and S. P. Maity, "Machine learning for spectrum information and routing in multi-hop green cognitive radio networks," *IEEE Transactions on Green Communications and Networking.*, 2021.

[30] S. Solanki, V. Dehalwar, and J. Choudhary, "Deep learning for spectrum sensing in cognitive radio," *Symmetry*, vol. 13, p. 147, 2021.

[31] S. Stalin, V. Roy, P. K. Shukla et al., "A machine learning-based big EEG data artifact detection and wavelet-based removal: an empirical approach," *Mathematical Problems in Engineering*, vol. 2021., Article ID 2942808, 11 pages, 2021.

[32] P. Kumar Shukla, P. Kumar Shukla, P. Sharma et al., "Efficient prediction of drug-drug interaction using deep learning models," *IET Systems Biology*, vol. 14, no. 4, pp. 211–216, 2020.

[33] H. A. Shah and I. Koo, "Reliable machine learning based spectrum sensing in cognitive radio networks," *Hindawi Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–17, 2018.

[34] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, 1967.

[35] B. Wang, S. Huang, J. Qiu, Y. Liu, and G. Wang, "Parallel online sequential extreme learning machine based on MapReduce," *Neurocomputing*, vol. 149, pp. 224–232, 2015.

[36] G. B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: theory and applications," *Neurocomputing*, vol. 70, no. 1-3, pp. 489–501, 2006.

[37] J. Xie, J. Fang, C. Liu, and L. Yang, "Unsupervised deep spectrum sensing: a variational auto-encoder based approach," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5307–5319, 2020.

[38] P. K. Shukla, S. Silakari, and S. S. Bhadoriya, "Network security scheme for wireless sensor networks using efficient CSMA MAC layer protocol," in *2009 Sixth International Conference on Information Technology: New Generations*, pp. 1579-1580, Las Vegas, NV, USA, 2009.

[39] 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.

[40] M. Saber, A. El Rharras, R. Saadane, A. Chehri, N. Hakem, and H. A. Kharraz, "Spectrum sensing for smart embedded devices in cognitive networks using machine learning algorithms," *Procedia Computer Science*, vol. 176, pp. 2404–2413, 2020.

[41] V. Roy, P. K. Shukla, A. K. Gupta, V. Goel, P. K. Shukla, and S. Shukla, "Taxonomy on EEG artifacts removal methods, issues, and healthcare applications," *Journal of Organizational and End User Computing*, vol. 33, no. 1, pp. 19–46, 2021.

[42] P. K. Shukla, J. K. Sandhu, A. Ahirwar, D. Ghai, P. Maheshwary, and P. K. Shukla, "Multiobjective genetic algorithm and convolutional neural network based COVID-19 identification in chest X-ray images," *Mathematical Problems in Engineering*, vol. 2021, Article ID 7804540, 9 pages, 2021.

[43] M. P. Debabrata Samanta, M. K. Karthikeyan, D. Parwani, M. Maheshwari, P. K. Shukla, and S. J. Nuagah, "Optimized tree strategy with principal component analysis using feature selection-based classification for newborn infant's jaundice symptoms," *Journal of Healthcare Engineering*, vol. 2021., Article ID 9806011, 9 pages, 2021.

[44] Q. Cheng, Z. Shi, D. N. Nguyen, and E. Dutkiewicz, "Sensing OFDM signal: a deep learning approach," *IEEE Transactions on Communications*, vol. 67, pp. 7785–7798, 2019.

[45] T. J. O'Shea and N. West, *Radio Machine Learning Dataset Generation with GNU Radio*, In Proceedings of the GNU Radio Conference, Boulder, CO, USA, 2016.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8570064, 13 pages
https://doi.org/10.1155/2022/8570064

Research Article

IoT Devices, User Authentication, and Data Management in a Secure, Validated Manner through the Blockchain System

Talha Ahsan,[1] **Farrukh Zeeshan khan**,[1] **Zeshan Iqbal**,[1] **Muneer Ahmed**,[2] **Roobaea Alroobaea**,[3] **Abdullah M. Baqasah**,[4] **Ihsan Ali**,[5] **and Muhammad Ahsan Raza**[6]

[1]*University of Engineering and Technology, Taxila 47080, Pakistan*
[2]*School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Sector H-12, 44000 Islamabad, Pakistan*
[3]*Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*
[4]*Department of Information Technology, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*
[5]*Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur, Malaysia*
[6]*Department of Information Technology, Bahauddin Zakariya University, Multan 60000, Pakistan*

Correspondence should be addressed to Ihsan Ali; ihsanalichd@siswa.um.edu.my

Received 5 October 2021; Revised 28 December 2021; Accepted 7 January 2022; Published 8 February 2022

Academic Editor: Samarendra Nath Sur

Advancement in technology has led to innovation in equipment, and the number of devices is increasing every day. Industries are introducing new devices every day and predicting 50 billion connected devices by 2022. These devices are deployed through the Internet, called the Internet of Things (IoT). Applications of IoT devices are weather prediction, monitoring surgery in hospitals, identification of animals using biochips, providing tracking connectivity in automobiles, smart home appliances, etc. IoT devices have limitations related to security at both the software and hardware ends. Secure user interfaces can overcome software-level limitations like front-end-user interfaces are accessed easily through public and private networks. The front-end interfaces are connected to the localized storage to contain data produced by the IoT devices. Localized storage deployed in a closed environment connected to IoT devices is more efficient than online servers from a security perspective. Blockchain has emerged as a technology or technique with capabilities to achieve secure administrational authentication and accessibility to IoT devices and their computationally produced data in a decentralized way with high reliability, interrogation, and resilience. In this paper, we propose device, end-user, and transactional authentication techniques using blockchain-embedded algorithms. The localized server interacts with the user interface to authenticate IoT devices, end-users, and their access to IoT devices. The localized server provides efficiency by reducing the load on the IoT devices by carrying out end-user heavy computational data, including end-user, IoT device authentication, and communicational transactions. Authentication data are placed on the public ledger in block form, distributed over the system nodes through blockchain algorithms.

1. Introduction

With the rapid growth of smart gadgets and high-speed networks that are used for communication for these smart devices, the Internet of Things (IoT) has gained human attention and popularity in the past few years. These embedded devices or IoT devices connect through public or private networks, are accessed remotely, and perform the desired functionality. Public and private networks use networking protocols for sharing information and communicating among the IoT devices.

IoT devices aid humans by performing various functions such as detecting weather conditions, supporting hospital

equipment for operations, identifying animals using biochips, and providing tracking and connectivity in automobiles. IoT servers gather data from these devices in real time and process the data to enhance the efficiency of the system.

Internet of Things (IoT) is being deployed at a large scale around the world, with Corps Information System Control officers (Cisco) predicting 40 billion devices at the end of the year 2021 [1]. Internet of things (IoT) are resource-consuming appliances and are not capable of fixing and protecting themselves against malicious attacks like Man in the middle attack, masquerading, DOS attacks, etc., and can be easily hacked by hackers. Due to this deficiency, everybody can easily access IoT devices and perform computations accordingly. Therefore, it is the present day need that enhances the security of the IoT devices; for this, it is essential to adopt proper methods for the user as well as device authentication and computational transaction to verify that IoT devices are secure in every respect. There is also the demand for the system to ensure the interaction between end-users and IoT devices. End-users are mapped on IoT devices through networking protocols [1]. Any proper user and IoT device authentication scheme must recognize the reality that these IoT devices are service-constrained appliances and unable to execute heavy transactions and processing. The user and device authentication techniques must be authentic, capable of being scaled, and reliable against multiple threats and attacks.

Numerous authentication techniques [2] are designed and deployed to provide the security to IoT devices, but these are all based on centralized architecture and depend on a centralized authority like database or servers of the system. Centralized authority verifies the end-users, system IoT devices, and communication record between end-users and IoT devices by using different protocols. Mutual authentication, certificate-based authentication, and token-based authentication are all centralized authentication techniques. These techniques have many flaws such as high transactional computational costs, centralized trusted third parties, single point of failure, lack of privacy, and the likelihood of hacking. Because these techniques rely on the trusted third party in this way, double dependency problems occur. Figure 1 describes the double dependency problem.

To reduce the flaws of the centralized (trusted third party) authentication of IoT devices, a decentralized end-user, IoT devices, and transaction authentication scheme are proposed using algorithms that provide blockchain technology. The proposed system provides the facility of end-user and IoT device authentication. The proposed system also facilitates end-users with the secure communication mapping to the IoT devices while ensuring security without any requirement of a centralized identity.

The fundamental purpose of this research is to furnish the security of an end-user, IoT devices, and the interaction between them in a decentralized manner. Particularly, we present a whole system that consists of a design and architecture involving IoT devices, end-users, and blockchain algorithms that apply authentication rules and deploy the blockchain algorithmic logic into the public area network. Furthermore, the main objectives and contributions of this research can be abridged below:

Our main objective in this paper is to provide hardware-level security to IoT devices. For the achievement of this goal, we need to use blockchain technology. Blockchain technology consists of decentralized techniques rather than all other techniques.

(1) We present a reliable, scalable, and authentic decentralized end-user and IoT device authentication technique that utilizes a graphical user interface with connectivity to blockchain algorithms. These algorithms consist of the logic that authenticates end-user access to IoT devices and they also authenticate the devices that are accessible by the end-user. Through these, issues of a centralized third party and the double dependency problem can be removed.

(2) We describe the detailed analysis of the whole system that constitutes the system entities, sequence flow diagram, blockchain algorithm (smart contracts), and interactions between the graphical user interphase and participants in the algorithms.

(3) We present an analysis on the security of our proposed authentication technique and discuss how the proposed technique achieves security goals (of confidential, integrity, and availability), and can overcome eavesdropping, replay, masquerading, denial of service (DoS), and Man in the Middle attacks.

(4) We achieve prevention of the denial-of-service attack through blocking an intruder in the system. If an intruder wants to access the system multiple times with the wrong hash key value, then the system identifies the intruder identity and blocks it.

The research paper is organized as follows. We discuss in Section 2 the IoT Security challenges, and in Section 3 we will present the proposed solutions of these challenges. Both these sections are part of the literature review. An overall description of the system architecture is presented in Section 4, including the interaction between system entities. Section 5 contains the experimental work which consists of a detailed description of the proposed methodology with algorithms. Section 6 presents the evaluation and results that are computed from the proposed work. In Section 7, we discuss the security analysis. The conclusion and future work is given in Section 8.

2. Security Issues in IoT

With the gradual increase in the number of IoT devices and the passage of time and equipment ranging from small embedded processing chips to large high-end servers, it needs to address many security issues at different

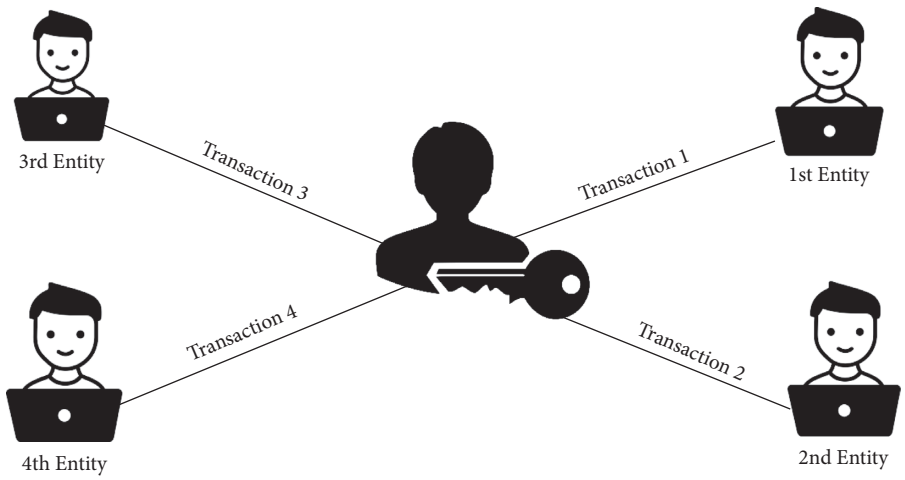

Figure 1: Owners of the system can send the same transaction containing digital currency to the multiple participants of the system.

architectural levels of embedded IoT devices. We categorize the security threats/issues concerning the IoT device deployment architecture as described below:

(1) Low-level security issues

(2) Intermediate-level security issues

(3) High-level security issues

2.1. Low-Level Security Issues. The level of security issues is concerned with Physical (layer one) and DLL (layer two) layers. Low-level security issues are also concerned with the hardware of the security issues.

In jamming attacks, radio frequency signals are emitted without following specific protocols in the wireless IoT devices [3, 4]. These radio frequency signals impact on the operation of the network and they also impact the sending or receiving of data through insecure nontrusted nodes, resulting in an unpredictable behavior of the system.

The Sybil attacks in a wireless network for accessing the IoT devices due to the presence of Sybil nodes in the network which produces fake identification and acts as part of the system to utilize the services of the IoT. At the first layer, a Sybil node utilizes fake addresses of the device's port like MAC values for masquerading [5, 6].

An insecure physical interface means managing poor physical security and not recognizing it from the considerations. The poor physical security tools for debugging/testing software and access through physical interfaces may breach the security through compromise nodes in the network. Though these, nodes can access the service of the IoT devices and perform some maliciousness [7, 8].

2.2. Intermediate-Level Security Issues. The intermediate-level security issues are concerned with network and transport layer communication, routing, and session management.

There is a need for IoT deployment architecture to be identified with every IoT device uniquely in the network. In neighbor discovery, data are transmitted in different steps including router discovery and address resolution [9]. Without proper verification, the utilization of packets got through neighbor discovery may have breached the security. Neighbor discovery packets also cause the occurrence of denial-of-service (DoS).

The Internet Protocol version 6 is routing protocol which generates unsecure networks. Compromised nodes in the network breach the security of the whole network and allow intruders to perform malicious attacks onto the network [10].

IoT devices and end-users are both required to add more security through hash key values or other security techniques. The fourth layer of the OSI model determines transmission pathways. Because of security flaws in the network's routing layer, data is sent in the wrong direction [11–13]. Datagram Transport Level Security and overhead, due to the available resources, need to be minimized [14].

Communicational sessions have been established between two entities of the system at the time of communication. Sessions can hijack on the fourth layer of the networking protocol with the help of fake links. Through this, some maliciousness occurs in the network in terms of denial of services [15, 16]. A session establishes between two nodes, an attacking node, and a victim node. The communicating nodes may even require retransmission of messages by changing the sequence number of the messages.

2.3. High-Level Security Issues. High-level security issues occur on the application layer. Application layer security issues are described below.

The interfaces that are used for accessing IoT services, web, mobile, and cloud can be affected by different attacks which may also affect data privacy [17].

The middleware of Internet of things is developed for the interaction between system entities, so these heterogeneous entities must be secure while service provisioning. Different environments and interfaces using middleware need to provide secure communication [18, 19].

High-level security issues occur when IoT devices are connected to the Internet. IoT devices' front-end interfaces are connected to the Internet; if they compromise, then large loss of data or information occurs. Therefore there is a need

to test XML SQL XSS carefully in which front-ends are designed for access of IoT devices. Constrained application protocols are used for communication between IoT devices and interfaces. CoAP provides end to end communication.

3. Solutions to Security Issues

In the literature, significant efforts have been made to address the security issues discussed in the previous section. Client authentication is the process that substantiates user recognition through a set of accreditations which recognize the data stored in an authentication server or database [3, 20]. In terms of mutual authentication, both the system entity user and the server take part to identify and recognize each other, the server authenticates the user because the user is stored in the server, whereas a user authenticates its presence in the server [21, 22]. Mutual authentication is classified into two types, one is username-/password-based authentication and the second one is certificate-based authentication [22]. Username-/password-based authentication and certificate-based authentication minimize many threats and risks of hacking in various computational processes like shopping websites, ensuring computational transactions with clients and servers for authorized purposes.

Open Authorization (OAuth) is the most eminent and comprehensively used identification and authentication technique for IoT device security. OAuth uses an open standard communicational protocol that provides tokens to end-users and IoT devices. Tokens are stored on the server or database. The system's resources are used by end users. End-users are authenticated in the system using tokens [23, 24]. The open standard protocol consists of four actors: The data and resource owner who generates validated resources and provides the access of the server to the users. The Open Authentication server (OAS) that provides tokens for secure communication with authentic clients/users or any other entity. The resource server or database which provides authenticated resources/data. The user who wants to access services from the server. The open authorization process is described in 6 steps. In the first step, the client generates requests to the resource owner for a successful access to the authenticated resources. In the second step, the username and password are set for the client by the authorization server. In the third step, the authentication of clients with the username and password, the client generates a request to the authorization server for providing access tokens. In the fourth step, the secure server identifies the password as well as the username of the client and assigns a protocol-generated access token to the authenticated clients. The token which is provided to the user consists of the public and private key values. In the fifth step, after getting the access tokens, the client generates access transaction for protected resources and sends it to authorization server or wants to execute any transactions by using the protocol generated token. In the sixth step, the authorization server authenticates the token, if the verification is successful, then protected resources or IoT devices are provided to the clients to perform computations.

A famous third entity technique, Kerberos authentication system, narrated in Ref. [25] utilizes temporal tickets for user authentication. These temporal tickets have many issues to authenticate clients and servers because these are exits for a specific period.

Delegation server is also a well-known technique for the authentication of the user and device [26]. Delegation server incurs high computational costs to authenticate devices through delegation servers every time a user needs to access new values for authentication purposes.

Another authentication technique: Mahalle et al. [27] introduced a process in which a set of user authentication protocols is used for user authentication. Group authentication protocol generates keys that are shared among multiple nodes on the network. Due to key sharing among multiple nodes in the network, many risks occur if one of the nodes breaches the security by sharing the key and creates security holes.

For distributed IoT systems, the technique involves [28] proposing that certificates are used in terms of an authentication protocol. In certification-based authentication protocols, cryptographic techniques are used for identification like hashing key values stored in the server node. Although cryptography certification-based authentication protocol provides much better security than existing techniques, many limitations arise due to the centralized architecture. With a centralized authentication architecture, the system cannot be secure in terms of redundancy, reliability, single point of failure attack, and scalability.

The drawback of user authentication is that they authenticate users with only the username/password. Therefore, usernames and passwords can be easily breached.

The open authentication technique for user authentication is a centralized technique in which all computations are performed across a central identity.

Group authentication technique shares the authentication technique across multiple nodes, but the group authentication technique does not use hash key values, so every entity in the system can perform some maliciousness.

All the abovementioned techniques have many deficiencies, and they only authenticate users rather than authenticating IoT devices and computational transactions for the communication between the user and IoT devices. They also used centralized techniques for authentication. In centralized technique, all computational data are stored on to the server. Entities in the system rely too heavily on the server or central authority to complete desired access transactions. If the centralized authority is nontrusted, then it can breach the security of the whole system. There is a research gap that exists with respect to complete user, device, and computational transaction authentications in decentralized manner.

4. Blockchain-Based Authentication of IoT Devices, End-User, and Transaction between Them

This part of the paper describes the various aspects of the architecture and detailed design of our proposed research blockchain-based IoT devices and end-user registration and

validation system in which blockchain algorithmic logic will be used to identify consumers and available IoT devices in a secure and validated process.

4.1. System Architecture. There are five major entities in the proposed system architecture with access to web-based algorithms through the Internet: Admin, IoT devices, end-users who facilitate direct connection with the system, and MySQL server containing end-users, IoT devices, and communicational data. During registration we assign unique hash addresses (public and private keys) to IoT devices and end-users. Both IoT devices and the end-users are registered on the web. Admin and databases are also part of the system. Detailed architecture of the system is presented in Figure 2.

This summarizes the whole system entities as follows:

4.1.1. Admin. Admin is the most valuable entity of the system and is responsible for user access control, list of users, IoT device services, and permission to end-users for accessing IoT devices. Only the owner of a particular organization or architectural system has the services of management and access control. The primary client within the framework is the proprietor or the maker of the blockchain algorithm. The owner of the blockchain algorithm can add IoT devices per user request as a part of the system. Admin also gives permission through the blockchain algorithm for end-users to access IoT devices. Admin has the ability to block new transactions in the system and add the block into the chain. The very first entity in the system is the admin, so its block does not have a previous hash value.

4.1.2. END_USERS. Within the framework of the system, utilizers are clients who ask for consent from the blockchain algorithm to access particular IoT devices. Once end-users are allowed to get authorization after authentication via the authentication algorithm, they contact the designated server node capable of governing the desired IoT device for authentication and access.

4.1.3. Blockchain Algorithm. The blockchain algorithm allows the authenticated utilizer access to the authenticated smart device. Registration of end-users, smart devices, access control, authentication, and functionalities are deployed to become a centralized architecture through the blockchain algorithm.

4.1.4. Database. In our solution, the database is utilized in overseeing access to IoT devices. Database stores IoT devices, information, end-user data, and computational transactions in the form of public ledgers. The database is distributed among all end-users in the form of a distributed ledger, but they cannot change, delete, or update any records; they can only create their own transaction record.

4.1.5. IoT Devices. The smart appliances in the system are expected to be a resource-consuming device with restricted storage, processing capacity, and memory.

4.2. Interaction between Entities. The interaction between the system entities happens in two major steps, namely, online and off-line interactions. Figure 3 shows a sequence between end-user and IoT devices for successful authentication of the user as well as user access to the IoT devices. A secure session is established for a secure connection between end-users and smart devices. In the online interaction, the admin initially generates the algorithm or smart contract and registers the user into the system and maps it to a MySQL server through select functions. Unique private and public addresses are assigned to the users through algorithms. Admin adds the devices as well into the system and also assigns unique addresses through algorithms and stores them in the MySQL server. That is why authenticated users can access authenticated devices that are part of the system.

When the user successfully authenticates (gains its unique public and private keys) and needs to get a specific IoT device, the user initially transfers the authentication request to the blockchain algorithm by using the registration request. The algorithm will recognize the SQL server of authenticated smart device for that end-user. If the device is unauthentic or the client is not eligible to facilitate the services of that device, then the system rejects the request of the user. Otherwise, if both the IoT device and user are valid and part of the system entities, the blockchain algorithm will allocate access permission to the end-user to access the authorized device and store the access information in the form of an encryption into the SQL server and broadcast it to all users, publicly.

When a user successfully registers into the system through a smart contract, then it stores the user's unique identification (ID), public address (PA), private address (PA), and previous public hash values. A block is generated, and it contains the user public key, transactional data, and previous hash values. Users' public and private addresses are stored in the form of hash key values. SHA-256 hashing key algorithm is used to generate hash key values. 64-bit key values generated by SHA-256 are in encrypted form.

Firstly, users register into the system and get public and private hash key values which are stored in the SQL server, then the user logs into the system by using the public key. The smart contract identifies whether it is a valid user or not. If the user is unauthorized, its request is rejected with an error; otherwise; the user successfully enters into the system with public and private hash key values.

5. Experimental Setup

In the experimental setup, we highlight the key usage viewpoints associated with the algorithm/smart contract of security. The existing blockchain platforms like Ethereum, Ripple, and R3 facilitate the development of apps on Blockchain networks, but these are all paid projects. In the case of Ethereum, we should buy eth currency and spend eth

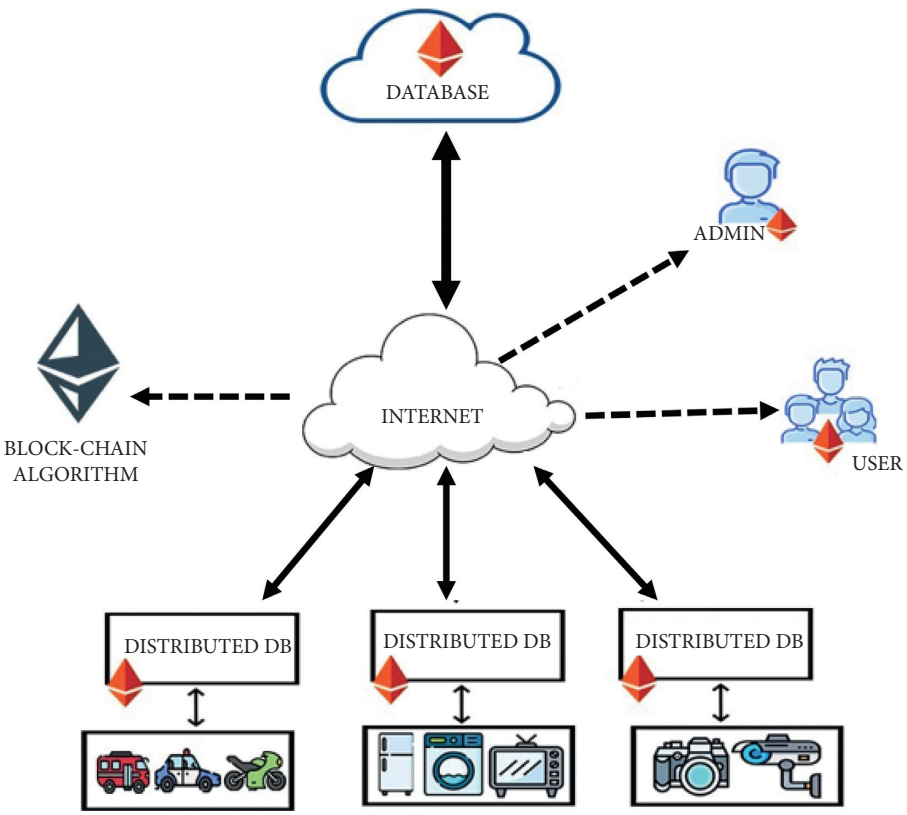

Figure 2: Blockchain-based proposed system architecture.

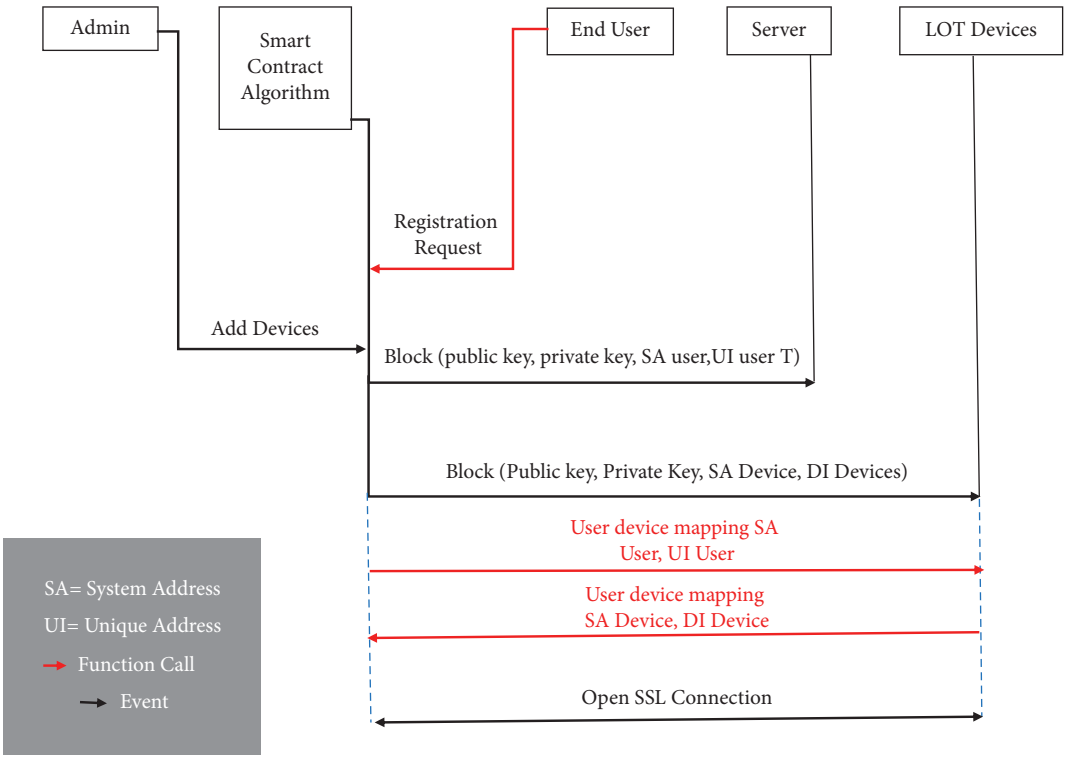

Figure 3: Sequence diagram of successful authentication and communication between end-user and IoT devices.

to perform each computation. Therefore we implement the decentralized logic of blockchain and develop a decentralized application in which end-user and IoT devices registration and authentication is performed in a decentralized manner through a distributed ledger. The implemented smart contract includes three main components: (1) Admin authority and end-user registration and authentication, (2) IoT devices registration, (3) user transactional authentication to IoT devices.

The algorithm was executed and tested using the MySQL server [15], which offers interesting highlights that encourage testing. Our main focus is on the execution of on-chain and off-chain parts of the proposed work which includes authentication components.

5.1. Admin Authorities and End-User Registration and Authentication

5.1.1. Admin Authorities. Smart contract I describes the admin authorities in which other end-users are restricted to add devices into the system. The very first entry of the system contains the address of the public hash value, but it does not contain the address of the previous hash value. Apart from admin, other end-users have previous hash values that can be used to add the next record into the system, but they cannot add IoT devices into the system.

SMART CONTRACT I. Admin authority of only admin can add devices into the system.

```
(i) session_start();
(ii) //connect to the database
(iii) $db = mysqli_connect('localhost', 'root', '', 'registration');
(iv) if (!isset($_SESSION['username'])) {
(v) $_SESSION ['msg'] = "You must log in first";
(vi) header ('location: login.php');}
(vii) if (isset ($_GET ['logout']))
(viii) {
(ix) session_destroy();
(x) unset ($_SESSION['username']);
(xi) header ("location: login.php");
(xii) }
(xiii) $_SESSION ['username'];
(xiv) $favcolor = $_SESSION ['username'];
(xv) switch ($favcolor)
(xvi) {
(xvii) case "admin":
(xviii) echo "Add device";
(xix) break;
(xx) default:
echo "Only Admin Can Enter Device"; header ("location:msg.php");
}
```

5.2. User Registration and Authentication. Smart Contracts II and III present the function through which users register into the system. A list of client hash addresses being displaced in the system might have different users as compared to the initial added users being the owner of the algorithm. A block is created to recognize data related to user authentication in the system. As stated earlier, a block is generated with the verification or authentication of the end-user to get the services of an IoT device. A list of blocks is generated to keep the record of all end-user-generated blocks. These blocks save the address of the user's hash key values (public key, private key) to the server. These hash key values are assigned to the users during the registration of the user.

The block of the very first user does not contain the previous public hash value of the user because the very first user is the owner of the algorithm. The rest of the users who are part of the system contain the previous user public hash value. In this regard, blocks are related and make a chain. Smart Contract IV presents the function to generate the user's previous public hash value.

```
Public key
function generateRandomString ($length = 64) {
$characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
$charactersLength = strlen ($characters);
$randomString = '';
for ($i = 0; $i < $length; $i++) {
$randomString. = $characters [rand (0, $charactersLength - 1)];
}
return $randomString;
}
Private key
function generateRandomString1 ($length = 64)
{
$characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
$charactersLength = strlen ($characters);
$randomString = '';
for ($i = 0; $i < $length; $i++)
{
$randomString. = $characters [rand (0, $charactersLength - 1)];
}
return $randomString;
}
Getting previous hash value
$query = "SELECT * FROM users ORDER BY id DESC LIMIT 1";
$result = mysqli_query ($db, $query);
while ($row = mysqli_fetch_array($result))
```

```
{
$publickey = $row ['publickey'];
}
```

5.3. IoT Devices Registration and Authentication. The communication, networking, and connectivity protocols used on Internet-enabled devices mainly depend on the specific Internet of Things applications deployed. The communication protocols that are used to provide the services of the IoT devices include CoAP, MQTT, and DTLS, among others. Wireless protocols include IPv6, LPWAN, Z-Wave, Bluetooth Low Energy, Zigbee, RFID, and NFC. Wi-Fi, Cellular, satellite, and Ethernet can also be used for communication. IoT devices are deployed on the server site and can be accessed through the abovementioned communication protocols.

```
IoT devices registration into the system
function generateRandomString ($length = 64)
{
$characters = '0123456789abcdefghijklmnopqrstuv
wxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
$charactersLength = strlen ($characters);
$randomString = '';
for ($i = 0; $i < $length; $i++)
{
$randomString. = $characters [rand(0, $character-
sLength - 1)];
}
return $randomString;
}
```

Each option has its tradeoffs like power consumption, bandwidth, and range, all of which must be considered when IoT device services are provided through protocols for particular IoT applications.

Smart Contract V presents the device registration function in the system. Two types of hash addresses are presented during the registration of the IoT device. A block is created to save information related to IoT device authentication in the system. The block contains the server address and hash key values that are assigned to the IoT device for authentication. These blocks save the address of the device hash key values (public key, private key) to the server. IoT devices are added into the system through the AddDevice function call. AddDevice function calls can be accessed only by the admin.

5.4. User Transactional Authentication to IoT Devices. The user's access to a list of devices is mapped through UserDeviceMappingFunction. When an end-user wants to access the services of IoT devices, then UserDeviceMapping function authenticates if it is a valid user. Otherwise, the UserDoesnotValid function is executed, which indicates that the end-user is not valid. Only those IoT devices that can be added into the system by admin to the server can be accessed by the end-user. In addition, only those users that are part of the system and have valid hash key values can access IoT devices.

User authentication and IoT device authentication also provide two-way authentication, also known as 2-Factor authentication. After the authentic transaction of the end-user map to the IoT device, a block is generated in the distributed ledger. A distributed ledger contains a block of data. Each block contains the public address of the user and the IoT device.

```
Nonauthenticated request rejection
session_start();
//connect to the database
$db = mysqli_connect ('localhost', 'root', '',
'registration');
if (!isset ($_SESSION ['username']))
{
$_SESSION ['msg'] = "You must log in first";
header ('location: login.php');
}
if (isset ($_GET['logout']))
{
session_destroy();
unset ($_SESSION ['username']);
header ("location: login.php");
}
```

```
Nonauthenticated request rejection
session_start();//connect to the database
$db = mysqli_connect ('localhost', 'root', '',
'registration');
if (!isset ($_SESSION ['username']))
{
$_SESSION ['msg'] = "You must log in first";
header ('location: login.php');
}
if (isset ($_GET['logout']))
{
session_destroy();
unset ($_SESSION['username']);
header ("location: login.php");
}
```

6. Evaluation and Results

In this section, we essentially pay attention to testing functionality among system entities along the web algorithms deployed in the web server environment. We assign unique Hash Addresses (HA) for multiple system entities. Three main functionalities of the system participants were tested, including end-user authentication, IoT device authentication, and transactional authentication operations.

When attempting to add an end-user through a web server, to access IoT devices, the request produces a hashing address that contains the public and private addresses, and successful addition of IoT devices. Table 1 shows the blocks generated through the user registration algorithm for the authenticated end-users. When an end-user is authenticated and wants to perform a communicational transaction, then end-user record is added into the block. In the same way, the next user's additional requests would facilitate in a similar generated block.

In end-user test scenario, a ledger is generated for end-users. Table 1 consists of ledger for the end-user. A ledger is distributed over the network. A distributed ledger contains blocks that are connected to each other with the previous hash key values. Each block in the distributed ledger contains end-user hash key values and the previous block public hash key values. All information or data in each block of the ledger is in encrypted form, so every end-user can access every block but cannot change, update, delete, or alter data. Through end-user distributed ledger, a secure and validated end-user can access the system IoT devices.

In IoT devices test scenario, IoT devices are also registered in the system. End-users can access only the devices that are registered into the system. IoT device registration data are stored in the distributed ledger. Table 2 shows distributed ledger of registered IoT devices.

IoT devices are authenticated in the same way as an end-user is registered in the system. Only the admin can add devices into the system. When a device adds into the system, a block is generated which assigns the hash key values to the IoT device. The block with IoT device registration is stored in a public distributed ledger. Public distributed ledgers are available for all authenticated users in the system, but they cannot change or update any block. When the end-user accesses IoT devices with its public key address, it can be authenticated with the private hash key value of the IoT device.

When the end-user maps to IoT devices, a transaction with the user request is generated. This transaction creates a block on the server which contains hash values like public key and previous hash value. These hash values are generated with the user data and their ids. The block is distributed over the system through which every end-user can check it, but it cannot be changed as it contains hash values. A distributed ledger shows which user interacts with which device. Table 3 shows authenticated transactions between IoT devices and end-users.

Through algorithm execution, we obtained an output to show that the end-user was successfully mapped onto the IoT devices. The first scenario implies that the user is nonauthorized. Therefore, the services of IoT devices cannot be provided by end-users. In this explanation, if an unauthenticated end-user, which not registered in the system, wants to access IoT devices from the system, then its request is rejected because it has no hash key values.

In the second scenario, the client endeavor is to access an IoT device, but it is not available to the system of IoT devices provided by the admin that is authorized to access. In this scenario, the algorithm allows the user to access only those devices which are mapped to the server. In the explanation of the second scenario, if an authenticated registered end-user in the system wants to access IoT devices which is not the part of the system, then two situations occurs. In the first situation, authenticated end-users ask the admin to add the required IoT devices. In the second situation, end-user request is rejected for IoT device if the device is not available.

The third scenario is for a successful authenticated transaction in which the user maps to the IoT device and its related server node. In this scenario, the algorithm successfully shows a function that contains information as the transaction mines and the execution succeeds. Authentic computational transactional information is stored in Table 4. A distributed ledger is generated for successful transactions. Blocks are created on each transaction. These blocks are linked to the previous block public hash values. Through the distributed ledger, everyone gets to know which IoT devices mapped to the end user and are currently not available. With the help of the distributed ledger, we can implement the blockchain techniques to provide security to IoT devices, end-users, and the communication between them.

7. IoT Security Analysis

IoT security issues arise at both the hardware level and the software level. Our proposed system is used to reduce different security issues at both levels. Table 5 consists of comparison between existing techniques and proposed techniques. The security achievements of integrity, availability, and confidentiality can be accomplished through authentication of each entity in the system, encryption and decryption of data, and access control schemes.

Privacy constrained in the system is attained by performing an authorized user approach to the smart device and its data. The confidentiality is also gained by performing different types of hashing techniques using SHA-256 cryptography for a successful user, IoT device, and transaction (user access to the desired IoT device) authentication. Based on hash key values, a blockchain-based authentication architecture is proposed. Hash key values are distributed over the network via a public distributed ledger. When the end-user becomes a part of the system, it assigns the public and private key addresses. These hash key values also assign to the IoT devices at the time of admin registration of the devices.

These hash key values are unique at every time. Therefore, no collision occurs in the system, and this is a powerful feature of blockchain. Unique hash key values establish a secure session for the purpose of interaction between the authenticated IoT devices and users. The secure block of the transaction is distributed over a public ledger because it consists of hash key values, so it cannot be changed or alternated by any other end-users. After gaining confidentiality in the system, many low-level security issues are overcome.

Redundancy and integrity are major security challenges that are recognized in any IoT device platform to avoid data redundancy to access the account of any other end-users. For achieving these integrity and nonredundancy the system is

Table 1: Distributed ledger of the registered end-users.

Name	Public Key	Private Key
Admin	KPUncAbY0KbyUtdom4TmYhsvQ	
Raza	CDLWGMGv0Ol6uXy0Tc92IRXJST	KPUncAbY0KbyUtdom4TmYhsvQ
Talha	RRKmzUNjtryNB4zFizm3YQ5DMq	CDLWGMGv0Ol6uXy0Tc92IRXJST
Ahsan	xTy2IpZu23Z2da1Msz3jvCxIzatBm	RRKmzUNjtryNB4zFizm3YQ5DMq
Haider	RwfDD9VrROMjosrZzAYFe8Z5JAz	xTy2IpZu23Z2da1Msz3jvCxIzatBm

Table 2: Distributed ledger of registered IoT devices.

Name	Public Key	Private Key
Smart lock	SkOD81SAGJVuKZXarAkrFkh5tDJ	
Mobile robot	nrNYrBZMyTB60C6ExzqIh2TsrXpV	SkOD81SAGJVuKZXarAkrFkh5tDJ
Smart light switch	VuehKkFbUOAP3xyItjhm5z8WIQN	nrNYrBZMyTB60C6ExzqIh2TsrXpV
Air quality meter	gxjJSFFkXNhE3POLkCnxp6Gsq2s	VuehKkFbUOAP3xyItjhm5z8WIQN
Voice controller	h6cvjjF4E9OVUyasddhZctQrZBd9t	gxjJSFFkXNhE3POLkCnxp6Gsq2s

Table 3: Distributed ledger for transactional authentication.

Name	Public Key	Private Key
Raza	CDLWGMGv0Ol6uXy0Tc92IRXJST	KPUncAbY0KbyUtdom4TmYhsvQ
Ahsan	xTy2IpZu23Z2da1Msz3jvCxIzatBm	RRKmzUNjtryNB4zFizm3YQ5DMq

Table 4: The output in the case of an authenticated communicational transaction is performed by the end-user mapped on to the IoT device.

Key Points	Authentic computational transaction description
Status	0 ∗ 1 valid transactional and authentication succeed
From	0 ∗ CDLWGMGv0Ol6uXy0Tc92IRXJSTOlPVlHrvQxJ0VX3iQ23v20YvHP65YR4yBD3Tia
To	0 ∗ SkOD81SAGJVuKZXarAkrFkh5tDJjs9TW5y7XKkzJvhdunX8b5wkrejfjr
Input	User data and device information for the transaction

Decoded input	{ $characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
	$charactersLength = strlen($characters);
	$randomString = “;
	For ($i = 0; $i < $length; $i++) {
	$randomString. = $characters [rand(0, $charactersLength - 1)];
	}

Decoded output	while($row = mysqli_fetch_array($run)){ $id = $row[“id”]; $username = $row[“username”]; $publickey = $row[“publickey”]; $previoushash = $row[“previoushash”];
Transactional cost	Algorithm running cost: O(n)s

Table 5: Comparison between existing techniques and the proposed technique.

Existing techniques	Flaws in the existing techniques	Mitigation of flaws in the proposed technique
Mutual authentication	Centralized architecture	De-centralized architecture
	There is a need to be both client and server for authentication of each other. Both are relaid on each other for authentication	There is no need of both client and server for authentication each other
	Less secure because relies on centralized authority	More secure because does not rely on centralized authority
Open authentication	In open authentication, tokens are generated for end-users for authentication	Directly, hash key values are assigned to the end-users
	Tokens are not in an encrypted form, so everyone can access the token and breach security	Hash key values are in an encrypted form, so other entities do not understand the hash key values and cannot breach security
	Totally based on open authentication server	Not based on server

Table 5: Continued.

Existing techniques	Flaws in the existing techniques	Mitigation of flaws in the proposed technique
Kerberos authentication	Kerberos authentication uses temporal tickets for authentication purposes in a specific period Temporal tickets are not in an encrypted form Dependent on temporal tickets and time, so kerberos authentication follows the centralized architecture	The proposed solution provides hash key values permanently to end-users Hash key values are in an encrypted form Provides decentralized architecture for authentication
Group authentication	Group authentication authenticates entities with the permission of all other entities in the group. Message passing in a group is not in an encrypted form, so every entity in the group can easily perform some maliciousness	Hash key values are distributed across all entities in the system with the help of distributed ledgers. Hash key values are in an encrypted form, so it is hard to understand for any entity in the system.

Table 6: Security issues addressed by the proposed system.

Security Issues	Resolved by the proposed solution
Jamming adversaries	In the proposed solution, unique hash key values are assigned for end-users and IoT devices. In this respect, no redundancy occurs. One to one communication takes place between end-users and IoT devices. Therefore, the proposed solution mitigates the effect of jamming adversaries.
Sybil node attack	Unique hash key values are assigned to end-users. Therefore, only authenticated users that are part of the system can access the system IoT devices. There is no chance for sybil nodes to access IoT devices in the system.
Man-in-the-middle attack	Mitigate the effect of Man-in-the-Middle attack in the same way as the sybil node attack
Insecure physical interface	Virtual private network is created in terms of xamp, MySQL, which hold all records in the distributed ledger. Therefore, each end-user needs hash key values to access the system IoT devices. So any intruder or hacker cannot access the system IoT devices through the interface directly.
Double dependency problem	Proposed solution consists of decentralized architecture. De-centralized architecture is achieved through the blockchain technique. With the help of decentralized architecture, double dependency problem is removed from the system.

more protected against replay attacks and Man-in-the-Middle (MITM). Integrity and nonredundancy can also be achieved through cryptographically as every message exchanges within end-users and IoT devices in an encrypted form. Intermediate-level security issues are removed through cryptography because only an entity can breach the message which has a valid or authentic private key value.

Moreover, using a unique user value (UIDs) and time duration (duration in which users map to IoT devices) in the message authentication makes it secure against replay and Man-in-the-Middle (MITM) attacks. Even in the case of MITM, if the intruder wants to replace the user hash value address with his or her public hash key value, the intruder will not be able to sign in because he or she cannot match the correct user private hash key value.

Lastly, our proposed authentication (end-user, IoT device) scheme is resilient against higher-level attacks like Denial-of-Service (DoS). Denial-of-Service attacks are the most common and popular attacks to breach the security of the system in which an intruder or hacker is continuously attempting to access the services of the system. Concretely, multiple data fields of end-users, IoT devices, admin, and computational transactions are placed on the public ledger distributed over each node in a decentralized manner. Thus, if an intruder wants to access the system multiple times with the wrong key, the system will block the intruder credentials. The public distributed ledger is resistant and robust to DoS attacks as all public nodes are protected through hashing functions that host redundant records with high consistency and integrity. Table 6 indicates security issues addressed by the proposed solution.

8. Conclusion

We proposed an architecture design and implementation of logical blockchain-based algorithms using the hash key values algorithm for end-users, IoT devices, and transaction authentication in a distributed appearance with no interruption of a third entity. We implement the hash key value algorithm using the PHP language and MySQL server for the storage of blocks in the distributed ledger. Authenticating large number of end-users, IoT devices, and transactions produces data deployment with MySQL server, which relieves the end-users and IoT devices from the authentication computational complexity of the blockchain network. We discussed the details of IoT device security issues and presented the system participants, architecture, interactions between system participants, and encrypted message exchanges among participants including the graphical user interface and MySQL server. Furthermore, we highlighted and showed how we executed the logic of the proposed system and examined the overall operations and functionality of the end-user and IoT device authentication mechanism governed by the hash key value algorithm. Different testing scenarios of transaction authentications were presented to verify the end-user and IoT devices of the system

using the PHP platform. Finally, we provided an analysis on the IoT security and presented that the proposed IoT device authentication solution is resilient to IoT device with different security-level attacks such as low-level, intermediate-level, and high-level attacks. In the existing proposed technique, only the users are authenticated in the blockchain, but in this paper, we present the user authentication, IoT device authentication, as well as transaction authentication. If the distributed ledger is not updated after each transaction, loss of data occur, which creates maliciousness between the blocks of a distributed ledger, because every block is connected with the previous block through the previous public hash key value to create a chain. In the future, decentralized architecture can be implemented to provide IoT device server side security.

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 authors are grateful to the Taif University Researchers Supporting Project (number TURSP-2020/36), Taif University, Taif, Saudi Arabia. This research work was partially supported by the Faculty of Computer Science and Information Technology, University of Malaya under Postgraduate Research Grant (PG035-2016A).

References

[1] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes 2018," in *Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1–8, Aqaba, Jordan, October 2018.

[2] M. Adil, M. Amin Almaiah, A. Omar Alsayed, and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 20, no. 8, p. 2311, 2020.

[3] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[4] M. Adil, M. A. Almaiah, A. O. Alsayed, and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 20, pp. 1–19, 2020.

[5] S. Dong, X.-g. Zhang, and W.-g. Zhou, "A security localization algorithm based on DV-hop against Sybil attack in wireless sensor networks," *Journal of Electrical Engineering & Technology*, vol. 15, no. 2, pp. 919–926, 2020.

[6] M. Jamshidi, E. Zangeneh, M. Esnaashari, A. M. Darwesh, and M. R. Meybodi, "A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it," *Wireless Personal Communications*, vol. 105, no. 1, pp. 145–173, 2019.

[7] G. Lally and D. Sgandurra, "Towards a framework for testing the security of IoT devices consistently," in *Proceedings of the First International Workshop on ETAA 2018*, Barcelona, Spain, September 2018.

[8] T. Bhattasali and R. Chaki, "A survey of recent intrusion detection systems for wireless sensor network," in *Proceedings of the Advances in Network Security and Applications*, pp. 268–280, Chennai, India, July 2011.

[9] R. Riaz, K.-H. Kim, and H. F. Ahmed, "Security Analysis Survey and Framework Design for Ip Connected Lowpans," in *Proceedings of the 2009 International Symposium on Autonomous Decentralized Systems (IEEE)*, pp. 1–6, Athens, Greece, March 2009.

[10] A. Dvir, T. Holczer, and L. Buttyan, "VeRA - Version number and rank authentication in RPL," in *Proceedings of the 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems 2011*, pp. 2709–14, Valencia, Spain, October 2011.

[11] J. Granjal, E. Monteiro, and J. S. Silva, "Network-layer security for the internet of things using TinyOS and BLIP," *International Journal of Communication Systems*, vol. 27, no. 10, pp. 1938–1963, 2014.

[12] S. Raza, S. Duquennoy, T. Voigt, and U. Roedig, "Demo abstract: securing communication in 6LoWPAN with compressed IPsec 2011," in *Proceedings of the 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, Barcelona, Spain, June 2011.

[13] W. Osamy, A. M. Khedr, A. Aziz, and A. A. El-Sawy, "Cluster-tree routing based entropy scheme for data gathering in wireless sensor networks," *IEEE Access*, vol. 6, pp. 77372–77387, 2018.

[14] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," *J. Cyber Secur. Mobil.*vol. 1, pp. 309–348, 2013.

[15] N. Park, "Mutual authentication scheme in secure internet of things technology for comfortable lifestyle," *Sensors (Switzerland)*, vol. 16, pp. 1–16, 2015.

[16] M. H. Ibrahim, "Octopus: an edge-fog mutual authentication scheme," *International Journal on Network Security*, vol. 18, pp. 1089–1101, 2016.

[17] S. Mishra and A. Paul, "A critical analysis of attack detection schemes in IoT and open challenges," in *Proceedings of the 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON)*, pp. 57–62, Noida, India, October 2020.

[18] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, and M. A. Spirito, "The Virtus Middleware: An Xmpp Based Architecture for Secure Iot Communications 2012," in *Proceedings of the 21st International Conference on Computer Communications and Networks (ICCCN)*, Munich, Germany, July 2012.

[19] C. H. Liu, B. Yang, and T. Liu, "Efficient Naming, Addressing and Profile Services in Internet-Of-Things Sensory Environments," *Ad Hoc Networks*, vol. 18, pp. 85–101, 2014.

[20] S. Zulkarnain and S. Idrus, "Soft Biometrics for Keystroke Dynamics," in *Proceedings of the International Conference Image Analysis and Recognition*, Niagara Falls, ON, Canada, July 2015.

[21] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the ACM Proceedings - ACM Conference on Computer and Communications Security*, pp. 254–69, October 2016.

[22] Y. Zhang, S. Kasahara, Y. Shen, and X. Jiang, "Smart Contract-Based Access Control for the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1–11, 2018.

[23] A. Álonso, F. Fernández, L. Marco, and J. Salvachúa, "IAA-CaaS: IoT Application-Scoped Access Control as a Service," *Futur Internet*, vol. 9, no. 4, p. 64, 2017.

[24] T. Borgohain, A. Borgohain, U. Kumar, and S. Sanyal, Authentication systems in internet of things, arxiv: 1502.00870, 2015.

[25] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service (V5)," MIT, Cambridge, MA, USA, 2005.

[26] H. Shafagh, S. Raza, T. Voigt, and K. Wehrle, "Delegation-based Authentication and Authorization for the IP-Based Internet of Things," in *Proceedings of the 2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, Singapore, June 2014.

[27] P. N. Mahalle, N. R. Prasad, and R. Prasad, "Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT)," in *Proceedings of the 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, pp. 1–5, Aalborg, Denmark, May 2014.

[28] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications," in *Proceedings of the 2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 2728–33, Istanbul, Turkey, April 2014.

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 2036778, 12 pages
https://doi.org/10.1155/2021/2036778

Research Article

Improving Performance of User Pair Using Reconfigurable Intelligent Surfaces

Kaveti UmaMaheswari,[1] **Arjun Chakravarthi Pogaku**,[1] **Dinh-Thuan Do**,[1] **Anh-Tu Le**,[2] **and Munyaradzi Munochiveyi**[3]

[1]*Department of Computer Science and Information Engineering, College of Information and Electrical Engineering, Asia University, Taichung 41354, Taiwan*
[2]*Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh City 700000, Vietnam*
[3]*Electrical and Electronics Engineering Department, University of Zimbabwe, Mount Pleasant, Harare, Zimbabwe*

Correspondence should be addressed to Munyaradzi Munochiveyi; mmunochiveyi@eng.uz.ac.zw

Received 13 August 2021; Accepted 25 November 2021; Published 23 December 2021

Academic Editor: Vinayakumar Ravi

With the given scope for new use cases and the demanding needs of future 6th generation (6G) wireless networks, the development of wireless communications looks exciting. The propagation medium has been viewed as a randomly behaving entity between the transmitter and the receiver since traditional wireless technology, degrading the quality of the received signal due to the unpredictable interactions of the broadcast radio waves with the surrounding objects. On the other hand, network operators could now manipulate electromagnetic radiation to remove the negative impacts of natural wireless propagation due to the recent arrival of reconfigurable intelligent surfaces (RIS) in wireless communications. According to recent findings, the RIS mechanism benefits nonorthogonal multiple access (NOMA), which can effectively deliver effective transmissions. For simple design, of RIS-NOMA system, fixed power allocation scheme for NOMA is required. The main system performance metric, i.e., outage probability, needs to be considered to look at the efficiency and capability of transmission mode relying on RIS and NOMA schemes, motivated by the potential of these developing technologies. As major performance metrics, we derive analytical representations of outage probability, and throughput and an accurate approximation is obtained for the outage probability. Numerical results are conducted to validate the exactness of the theoretical analysis. It is found that increasing the higher number of reflecting elements in the RIS can significantly boost the outage probability performance, and the scenario with only the RIS link is also beneficial. In addition, it is desirable to deploy the RIS-NOMA since it is indicated that better performance compared with the traditional multiple access technique.

1. Introduction

Due to high demands in terms of system capacity and spectrum efficiency, the traditional orthogonal multiple access (OMA) has been unable to meet the user needs to be associated with the rapid growth of Internet of Things (IoT) and mobile communications [1–7]. To meet the heavy demand for mobile services, nonorthogonal multiple access (NOMA) is researched in recent years with promising applications [8, 9]. In some scenarios, NOMA benefits to device-to-device communications [10, 11] and cognitive radio- (CR-) aided NOMA [12–14], and these are considered as potential key technologies for the fifth-generation mobile communications (5G). The authors in [13] deployed the relaying scheme for the secondary network of the considered CR-NOMA, and the relay can energy harvesting (EH) from the secondary transmitter to serve signal forwarding to distant secondary users. They studied the complex model of EH-assisted CR-NOMA in terms of outage behavior and throughput performance when has imperfect successive interference cancellation (SIC). Reference [14] presented relay-aided CR-NOMA networks to improve the performance of far users by enabling partial relay selection architecture. They explored system performance in terms of full-duplex (FD)

and half-duplex (HD) relays for both uplink and downlink communications.

Recently, due to its high-energy efficiency, reconfigurable intelligent surface (RIS) technique is recognized as the next-generation relay technique, also namely relay 2.0 [15–17]. The RIS elements can independently shift the signal phase and absorbing the signal energy. The reflected signals benefit to wireless transmission due to less energy required [18–25]. In [21], the authors demonstrated an interesting RIS architecture which includes any number of passive reflecting elements, a simple controller for their adjustable configuration, and a single radio frequency (RF) chain for baseband measurements. By assuming sparse wireless channels in the beam space domain, they studied an alternating optimization scheme for explicit estimation of the channel gains at the RIS elements attached to the single RF chain [21]. The authors in [22] explored RIS by combining the functions of phase shift and radiation together on an electromagnetic surface. As such, positive intrinsic-negative (PIN) diodes are employed to realize 2-bit phase shifting for beam forming. Thanks to providing RIS equipped 256 two-bit elements, this radical design is recognized as first wireless communication prototype in the world. The developed prototype includes main components such as modular hardware and flexible software. In this prototype, they used the hosts to set parameter and exchange data. Together with this, they employed the universal software radio peripherals (USRPs) to process baseband and radio frequency (RF) signals, as well as implemented the RIS to transmit and receive signals. Reference [23] studied a mmWave system relying on several RIS arrays which implemented low-precision analog-to-digital converters (ADCs). To assist multiple-input multiple-output (MIMO) transmission, these RIS arrays form a synthetic channel with increased spatial diversity and power gain by enabling the linear spatial processing.

1.1. Related Work. The authors in [26] investigated system performance of NOMA-RIS characterizing the effective channel gains corresponding with the best case and worst case of new channel statistics. They derived the closed-form formulas corresponding to the best case and worst case to examine two main system performance metrics such as the outage probability, the ergodic rate. For providing further insights, they also studied both the diversity orders of the outage probability and the ergodic rate at high signal-to-noise (SNR) region. In [27], a multiple-input multiple-output (MIMO) scheme along with passive beam forming weight are required to implemented NOMA-RIS systems which simultaneously serve groups of two users. The authors concluded that by enabling large number of RIS elements, the intercluster interference can be eliminated. Reference [28] introduced a system model of system with rate splitting multiple access- (RSMA-) aided RIS. Considering the phase shifts of the RIS and beam forming of the base station, the authors presented optimal policy in terms of energy efficiency.

However, a few paper considered advantage of RIS systems relying on NOMA, and most of the derivations are still complicated. Once can recognize different performance between RIS-NOMA and RIS-OMA, users' fairness along with their outage performance are not still studied in detail. Therefore, references [26–28] motivate us to investigate system performance metric for RIS-aided NOMA systems.

The main contributions of this paper are as follows

(i) Different from [29–32], this paper presents a RIS-aided NOMA system in down link to achieve benefits from NOMA to communicate simultaneously with their corresponding destinations via a RIS. It is assumed that the LIS is in the form of a reflect-array comprising N simple and reconfigurable reflector elements and controlled by a communication-oriented software. Unlike other published work dealing with the calculation of symbol error probability (SEP), our work provides outage performance evaluation of the RIS-aided NOMA system in the presence of hardware impairments

(ii) The closed-form expressions of outage probability for the RIS-aided NOMA system are derived. Since they are formulated in terms of various system parameters, the effect of each system parameter on the outage probability can be numerically evaluated. For instance, the effect of the number of metasurfaces in RIS on the outage probability can be evaluated to how the system can improve its performance in practice. It is demonstrated in this work that the outage probability of the system mainly relying on the number of metasurfaces in RIS

(iii) The derivations of asymptotic outage probabilities at high transmit signal-to-noise ratio (SNR) for two users are also provided as an important evaluation to design such the RIS-aided NOMA system in practice. Furthermore, compared with orthogonal multiple access- (OMA-) assisted RIS system, the considered system exhibits more benefits, and it becomes a prominent candidate to implement for forthcoming networks

2. System Model

We consider two-user approach of NOMA downlink relying on RIS to serve dedicated groups of NOMA users, as scheme 1 which is shown in Figure 1. It is reasonable to study two users which are expected acceptable performance. In fact, there are many groups of users which are normally separated by orthogonal access manner. In each group, we assume the representative users including near user (NU) and far user (FU) which are classified based on their locations. In this circumstance, one could not be transmission from the base station (BS) to mobile users directly due to heavy blockage or obstacle. The BS generates two beamforming vectors together with technique of zero forcing beamforming to serve two NOMA users. By grouping of paired users, RIS-NOMA satisfies different QoS requirements which are suitable to develop multiple services for mobile users in future wireless systems. In addition, considering the case of RIS equipped N reflecting elements which cannot serve FU. This

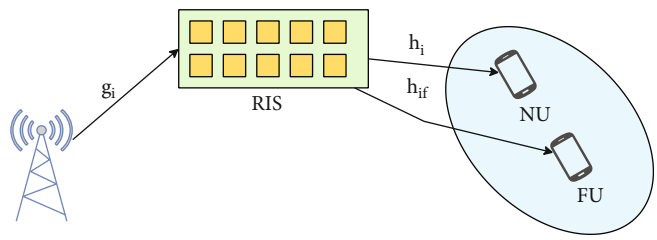

Figure 1: Scheme 1: NOMA-RIS System without direct link.

is reported as scheme 2, in which user U_3 just communicates with the BS, but user U_3 still be paired with user U_1. It is worth noting that U_1 belongs to link BS-RIS-destination. In scheme 2, the RIS has challenged once not only cannot reach to user U_3but also suffers interference from non-NOMA user.

Regarding operation of RIS, it is also equipped with a controller associated with switching procedure including working modes. RIS operate in receiving mode for channel estimation and in reflecting mode for data transmission. Since the RIS is a passive reflecting equipment, we adopt a time-division duplexing (TDD) protocol for uplink and downlink transmissions and assume channel reciprocity for achieving the channel information acquisition in the downlink based on the uplink training sequence. (To enable NOMA scheme in RIS-aided systems, user grouping must be achieved firstly; at the receiving end, we cannot guarantee similar quality of service for users. Therefore, by grouping user's fairness is the main benefit from deployment of NOMA. To guarantee the fairness and system performance, two-user model is adopted which is enough to benefit NOMA to RIS-assisted applications. In case of more users in a group, the worst performance occurs at several users. However, explicit mathematical analysis is also provided in a framework as [29].)

To enable NOMA mode, the superimposed signal $(a_1 s_1 + a_2 s_2)$ transmitted from the BS then is required to serve distant mobile users with the presence of RIS. This study considers NOMA concept to provide user fairness with a_1 and a_2 that are power allocation factors for user NU, and FU, respectively. Due to less amount of power required to supply for user NU, we have $a_1 < a_2$ and $a_1^2 + a_2^2 = 1$. To easy present other steps of signal analysis, we denote main parameters as Table 1.

In particular, the received signals at user NU and user FU are given, respectively, by

$$y_{\mathrm{NU}} = h_N^H \Theta_N G w (a_1 s_1 + a_2 s_2) + n_N, \tag{1}$$

$$y_{\mathrm{FU}} = h_F^H \Theta_F G w (a_1 s_1 + a_2 s_2) + n_F, \tag{2}$$

where G is denoted as the complex Gaussian channel matrix form $N \times 1$ which is transmitted from the BS to the RIS to reflect signal to distant users, n_N and n_F are noise terms, and h_N and h_F represent the complex Gaussian channel vector terms for links RIS-NU and RIS-FU, respectively. It can expand N as where P and Q are integers. The matrix$\Theta_u (u = N, F)$contains its diagonal elements $\beta_u \exp(-j\theta_{u,i})$with$\beta_N$as the amplitude reflection factor while $\theta_{N,i}$stands for the reflection phase shift. We limit our consideration on small scale fading. It is noted that G and h_u follow independent complex Gaussian distribution with zero mean and unit variance. (`The channel state information (CSI) regarding channels G and $h_u$is assumed to be available via the channel estimation approaches in the literature such as work in [33]. It is assumed that the RIS is associated with a reliable control channels, and hence the information about the predetermined beamforming vectors w can be sent to the users the FU and the NU.)

We call $D_u$as a diagonal matrix with its diagonal elements obtained from h_u^H, and V is an N×1 vector which includes the elements on the main diagonal of Θ_u^H. Then, by denoting $A = |v_p^H D_N h_N|$, we can compute some main equations as follows. We can compute the signal to interference plus noise (SINR) for the user NU to decode the FU's signal that is expressed by [29].

$$\mathrm{SINR}(s_2) = \max_{V_P} \frac{A^2 a_2^2}{A^2 a_1^2 + (1/\rho)}, \tag{3}$$

where ρ represents the transmit signal-to-noise ratio (SNR). By performing SIC, the user NU eliminates signal s_2, and then it decodes its signal by computing SNR as

$$\mathrm{SNR}(s_1) = \max_{V_P} A^2 a_1^2 \rho. \tag{4}$$

Before computing SINR to detect the FU's signal, we should denote new variable, i.e., $B = |v_p^H D_F h_F|$. Then, such SINR is given by

$$\mathrm{SINR}_{\mathrm{FU}} = \max_{V_P} \frac{B^2 a_2^2}{B^2 a_1^2 + (1/\rho)}. \tag{5}$$

Remark 1. It is noted that the expressions of SINR or SNR are main factor to evaluate system performance, for example, in (3)–(5), and imply that these factors depend on the SNR at the BS is ρ. Furthermore, we note that the SINR formulas include the products of the complex Gaussian distributed random variables, i.e., A and B, which lead to more complicated computations for RIS-NOMA if we need evaluate other metrics.

Table 1: Main parameters and denotations.

Parameter	Explanation
ρ	Signal-to-noise ratio at the BS
N	The number of RIS elements
a_1	Power allocation coefficient for signal s_1
a_2	Power allocation coefficient for signal s_2
R_1	Target rate of user NU
R_2	Target rate of user FU
$K_n(.)$	Bessel function of second kind
$\Gamma(.)$	Gamma function

3. Performance Analysis Scheme 1

In this section, we analyze the achievable performance of the proposed RIS-NOMA system in some scenarios, and benchmark scheme is also mentioned in Figure 2. It should be pointed out that as there are different decoding conditions for users NU and FU, we should compare performance gap among NU and FU, so that the main parameters are decided to guarantee the fairness. For simplifying the system performance analysis on performance gap among two users, this paper just focuses on main performance metric, i.e., outage probability. Of course, the other system performance metrics of such networks will be further studied but it needs change to other method of computation. However, this study exhibits explicit performance metric and more accuracy formulas if we compare them with the conventional method which is also used to present the outage performance, namely, the central limit theorem (CLT), in which variables A and B are approximated as a Gaussian random variable with fixed mean values and variances. Outage probability is defined as ability of SINR less than the predefined SINR thresholds. Since more complicated computations regarding RIS which is the form of a reflect-array comprising$N$simple and reconfigurable reflector elements, and more matrix variables in computations, unlike other published work dealing with the calculation of symbol error probability (SEP) [34], our work focuses on main metric, i.e., outage performance evaluation of the RIS-aided NOMA system [35] to determine which scenario exhibiting better performance.

By denoting Pr (.) as outage probability, we can formulate such outage probability as

$$P_{\text{out}} = \Pr\left(\psi \le \rho_{\text{th}}\right), \tag{6}$$

where ψ is either SINR or SNR, and ρ_{th} is denoted as SINR/SNR threshold.

3.1. Channel Distribution. We put our attention on the probability density function (PDF) of the product of channels, for example, $\sqrt{Q}v_p^H D_N h_N$ corresponding to the user NU. Since the structure ofv_p,$\sqrt{Q}v_p^H D_N h_N$, is considered as an inner product of two$Q \times 1$ complex Gaussian vector, it is worth noting that v_p,$\sqrt{Q}v_p^H D_N h_N$, is a complex Gaussian random variable with zero mean and variance$|h_N|^2$. More importantly, we have $|h_N|^2$ following gamma distribution. Therefore, the PDF of $\sqrt{Q}v_p^H D_N h_N$ can be obtained as follows [29].

$$f_{A^2}(x) = \frac{2x^{Q-1/2}}{\Gamma(Q)} K_{Q-1}\left(2\sqrt{x}\right). \tag{7}$$

3.2. Outage Probability at User NU. The outage behavior happens at the user NU once it fails to detect the FU's signal s_2 as well as its own signal s_1.

$$P_{\text{NU}} = P_{\text{NU},s_1} \times P_{\text{NU},s_2}, \tag{8}$$

where P_{NU,s_1} and P_{NU,s_2} are probability related to detecting signal s_1 and s_2, respectively. These expressions are determined based on required target rates R_1 and R_2 for users NU and FU, respectively.

In particular, the outage probability to user NU detect signal s_1 is given by

$$P_{\text{NU},s_1} = \Pr\left(\log\left(1 + \text{SINR}(\text{s}_1)\right) < R_1\right). \tag{9}$$

Similarly, the outage probability to user NU detect signal s_2 is given by

$$P_{\text{NU},s_2} = \Pr\left(\log\left(1 + \text{SINR}(\text{s}_2)\right) < R_2\right). \tag{10}$$

Proposition 2. *The outage probability for user NU is given below, where $\psi = Q/\rho a_1^2$,*

$$\psi_1 = \frac{Q\epsilon_1}{\rho\left(a_2^2 - a_1^2\epsilon_1\right)}, \epsilon_1 = 2^{R_1} - 1, C_1 = \frac{1}{\Gamma(Q)^P}\psi^{\frac{P(Q-1)}{2}}, C_2 = \frac{1}{\Gamma(Q)^P}\psi_1^{\frac{P(Q-1)}{2}}, B_1 = K_Q\left(2(\psi)^{\frac{1}{2}}\right) \text{ and } B_2 = K_Q\left(2(\psi_1)^{\frac{1}{2}}\right),$$

$$P_{NU} = C_1 C_2\left[(\psi\psi_1)^{-\frac{Q+1}{2}}(\Gamma(Q))^2 - 2\psi^{-\frac{Q+1}{2}}\Gamma(Q) - 2\psi_1^{-\frac{Q+1}{2}}\Gamma(Q) + 4\psi^{-\frac{1}{2}}\psi_1^{-\frac{1}{2}}B_1 B_2\right]^P. \tag{11}$$

Proof. See in Appendix A. □

3.3. Outage Probability at User FU

Proposition 3. *The outage probability for user FU is given as [12], where $\psi_2 = Q\epsilon_2/\rho(a_2^2 - a_1^2\epsilon_2)$, $\epsilon_2 = 2^{R_2} - 1$, $C_3 = (1/\Gamma(Q)^P)\psi_2^{P(Q-1)/2}$, and $B_3 = K_Q(2(\psi_2)^{1/2})$.*

$$P_{FU} = C_3\left((\psi_2)^{-\frac{Q+1}{2}}\Gamma(Q) - 2(\psi_2)^{-\frac{1}{2}}B_3\right)^P. \tag{12}$$

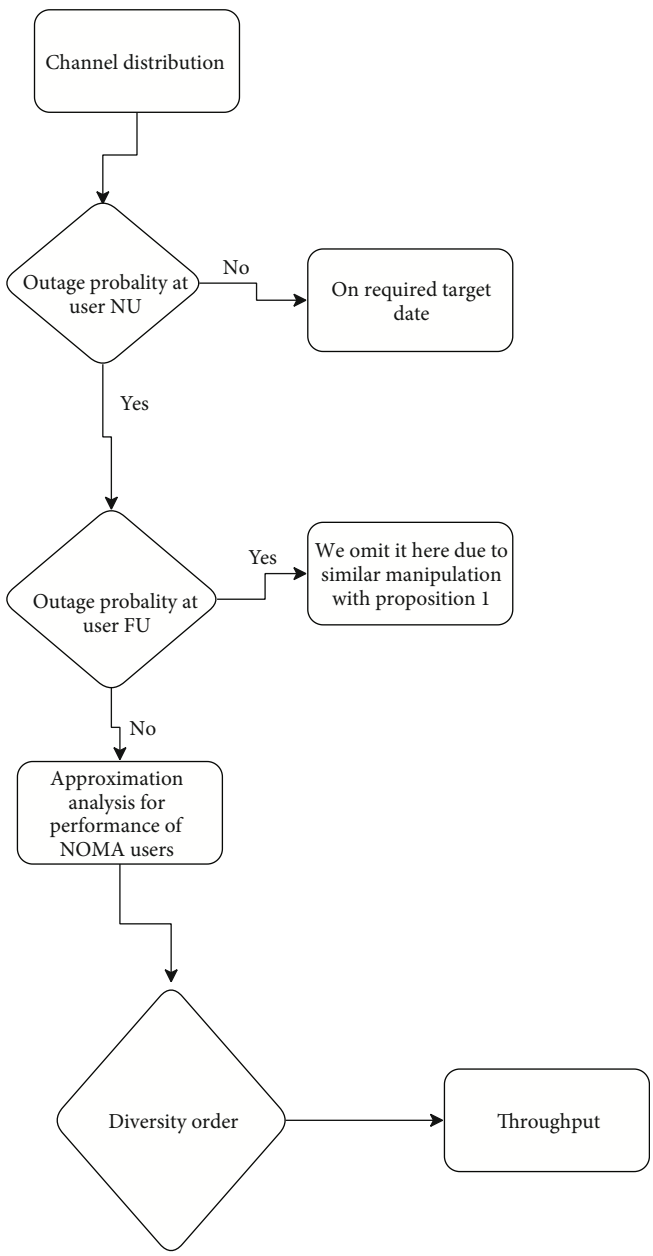

Figure 2: Flowchart for methodology.

Proof. We omit it here due to similar manipulations with Proposition 2. □

3.4. Approximation Analysis for Performance of NOMA Users. To look at insights of the considered system, the approximation computations are necessary to determine outage behavior in simpler manner. In particular, at high SNR regime, we have two cases.

(i) Case 1.

If $Q > 1$ and $n \geq 2$, we can follow $K_Q(z) \approx 1/2((n-1)!/(z/2)^n - (n-2)!/(z/2)^{n-2})$ to achieve valued computation. Precisely, the approximated outage probability of two NOMA users can be obtained as below.

$$P^{\infty}_{NU,s_1} = \frac{\psi^p}{(Q-1)^p}, P^{\infty}_{NU,s_2} = \frac{\psi_1{}^p}{(Q-1)^p}, \tag{13}$$

$$P^{\infty}_{FU,1} = \frac{\left(Q\epsilon_2/\rho\left(a_2^2 - a_1^2\epsilon_2\right)\right)^p}{(Q-1)^p}. \tag{14}$$

(ii) Case 2.

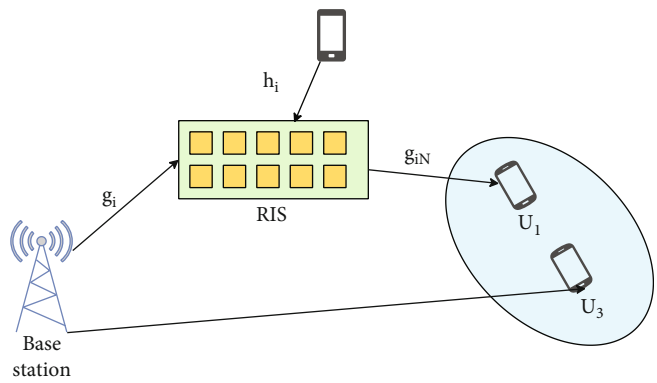

Figure 3: Scheme 2: NOMA-RIS System with direct link.

Table 2: Simulation parameters.

Description	Parameter
Power allocation coefficient	$a_1 = 0.2$ and $a_2 = 0.8$
Relative Channel estimation error	$\eta_k = 1 \times 10^{-4} \sim 9 \times 10^{-4}$
NOMA user corresponding two cases	$Q > 1$ and $Q = 1$
Distance between two nodes	$d_{SU_1} = 0.04$, $d_{SR} = 0.06$ $d_{RU_1} = 0.02$, $d_{SU_2} = 0.04$ $d_{U_1U_2} = 1 - d_{SU_1}$
Transmit SNR	$\rho = 0 \sim 30$dB
Target rates	$R_1 = 1$ BPCU, $R_2 = 1$ 1 BPCU, and $R_{OMA} = 1$ (BPCU)

Especially, at high SNR and $Q = 1$, we have $K_1(z) = 1/2\,(1/(z/2)) + (z/2)In(z/2)$; the approximated result of outage probability for two users are written as

$$P_{NU,s_1}^{\infty,2} = \psi^N\left(-\ln\left(\psi\right)^N\right), P_{NU,s_2}^{\infty,2} = \psi_1{}^N\left(-\ln\left(\psi_1\right)^N\right), \quad (15)$$

$$P_{FU,2}^{\infty,2} = \left(\frac{Q\epsilon_2}{\left(\rho\left(a_2^2 - a_1^2\epsilon_2\right)\right)}\right)^N \left(-\ln\left(\frac{Q\epsilon_2}{\left(\rho\left(a_2^2 - a_1^2\epsilon_2\right)\right)}\right)\right)^N. \quad (16)$$

3.5. Diversity Order. To further evaluate performance of two users in case of high SNR, it needs to consider the diversity order for the case Q = 1. In particular, such diversity order metrics can be formulated by [35].

$$D_{NU} = \underset{\rho\longrightarrow\infty}{-\lim}\left(\frac{\log\left(P_{NU}\right)}{\log\,\rho}\right) = \underset{\psi_1\longrightarrow\infty}{-\lim}\left(\frac{\log\left(P_{NU}\right)}{\log\,\psi_1}\right) = N^2, \quad (17)$$

$$D_{FU} = \underset{\rho\longrightarrow\infty}{-\lim}\left(\frac{\log\left(P_{FU}\right)}{\log\,\rho}\right) = \underset{\psi_2\longrightarrow\infty}{-\lim}\left(\frac{\log\left(P_{FU}\right)}{\log\,\psi_2}\right) = N. \quad (18)$$

Remark 4. Since (17) and (18) show that the number of reflecting elements in RIS decides how the system performance can be improved, once we enhance the main parameter SNR at the BS, in the next section of numerical simulation, it is predicted that the curves of outage probability will be reduced sharply at high value of N.

3.6. Throughput. In delay-limited transmission mode, more system metric, namely, throughput is decided by fixed data rates R_1 and R_2 and achieved outage probability in the previous section. Therefore, the throughput of the whole system is expressed by [35]

$$T = R_1\left(1 - P_{NU}\right) + R_2\left(1 - P_{FU}\right). \quad (19)$$

Further, such throughput is rewritten as

$$T = R_1\left(1 - \left(P_{NU,s_1}\right) \times \left(P_{NU,s_2}\right)\right) + R_2\left(1 - P_{FU}\right). \quad (20)$$

4. Scheme 2: RIS-NOMA System with Direct Link

As Scheme 2 was shown in Figure 3, it is challenging once user U_3 just relies on direct link associated with the BS. Assuming that the corresponding channel h between user$U_3$and the BS follows Rayleigh fading, it is worth noting that RIS still communicates with userU_1while it has interference from external non-NOMA user. In this circumstance, the BS sends signal $(a_1s_1 + a_3s_3)$ with conditions $a_1 + a_3 = 1, a_3 > a_1$ to two users, U_1 and U_3. In the first time slot, user U_1detects U_3's signal and then detects its own signal. In the contrast, user only detects its signal since user U_3 prioritizes to detect signal (more power allocated to user U_3 for such priority $a_3 > a_1$). In particular, the received signals at user U_1 and user U_3 are given, respectively, by

$$y_{U_1} = g_N^H\Theta_N Gw(a_1s_1 + a_2s_2) + n_I + n_{U_1}, \quad (21)$$

$$y_{U_3} = h(a_1s_1 + a_2s_2) + n_{U_3}, \quad (22)$$

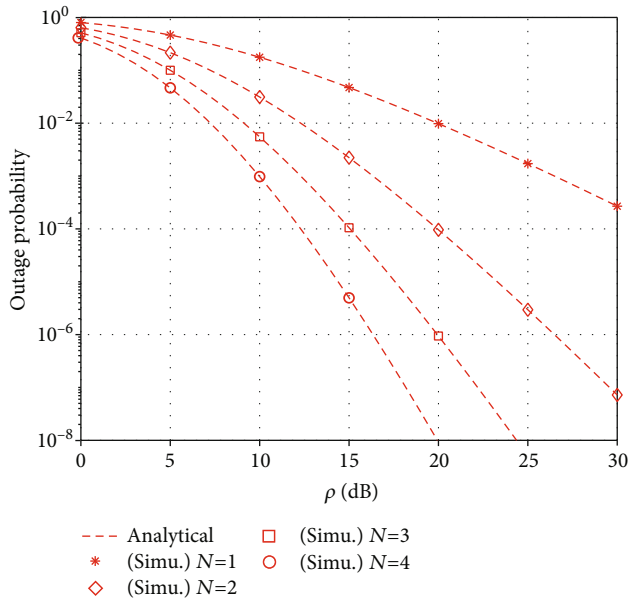

Figure 4: Outage probability of user NU versus the transmit SNR ($Q = 1$).

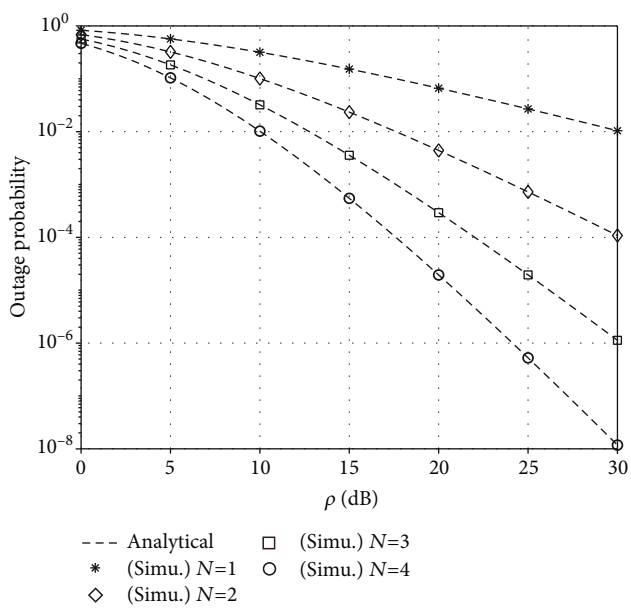

Figure 5: Outage probability for NOMA FU ($Q = 1$).

where n_I is interference term from normal user; n_{U_1}, n_{U_3} are AWGN noise terms. By exploiting the central limit theorem (3.9.2) in [36], all interference signals from external sources can be treated as AWGN noise with $\mathrm{CN}(0, \Omega_I)$.

To proceed signal detection, SINRs can be obtained at user U_1 and U_3, respectively,

$$\mathrm{SINR}_{U_1} = \max_{V_P} \frac{a_1^2 A^2}{h_I + (1/\rho)}, \tag{23}$$

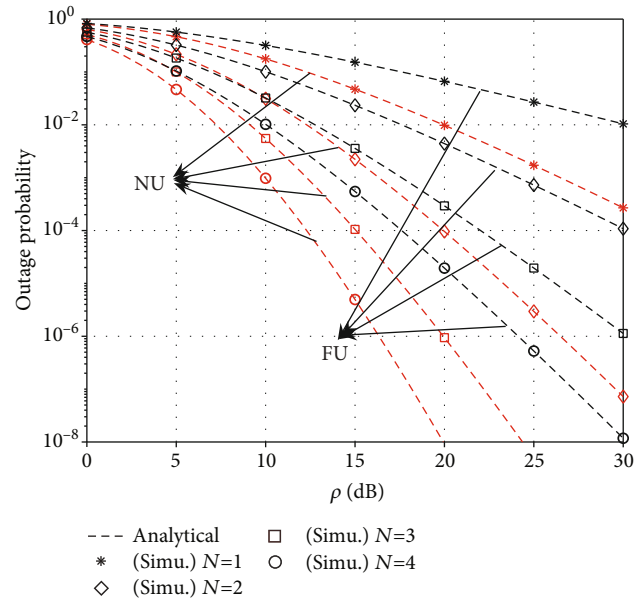

Figure 6: Outage probability comparison for users NU and FU.

$$\mathrm{SINR}_{U_1} = \frac{a_3^2 \rho(h)^2}{a_1^2 \rho(h)^2 + 1}. \tag{24}$$

The outage probability for user U_1 is similar as user NU in scheme 1, and we do not want to replica it in this section. It is noted that the degraded performance is resulted by coefficient Ω_I.

Since channel h follows Rayleigh fading with mean of λ_h, the outage probability of user U_3 is given as

$$P_{U_3} = 1 - e^{\frac{\epsilon_1 \lambda_h}{2\left(a_2^2 - a_1^2 \epsilon_2\right)\rho}}. \tag{25}$$

5. Benchmark Scheme: OMA

In the context of OMA, only single signal is transmitted from the BS to each user. As a result, SNR at the destination associated with the link containing RIS is given by

$$\mathrm{SNR}_{\mathrm{OMA}} = \max_{V_P} \mathrm{A}^2 \rho. \tag{26}$$

Proposition 5. *The outage probability of user in the RIS-aided system relying on OMA scheme is given as*

$$P_{OMA} = \frac{1}{\Gamma(Q)^P} \psi_4^{\frac{P(Q+1)}{2}} \left(\psi_4^{-\frac{P(Q+1)}{2}} \Gamma(Q) - 2\psi_4^{-\frac{1}{2}} K_Q\left(2\psi_4^{-\frac{1}{2}}\right)\right)^P, \tag{27}$$

where $\psi_4 = Q\epsilon_{OMA}/\rho$ *and* $\epsilon_{OMA} = 2^{2R_{OMA}} - 1$.

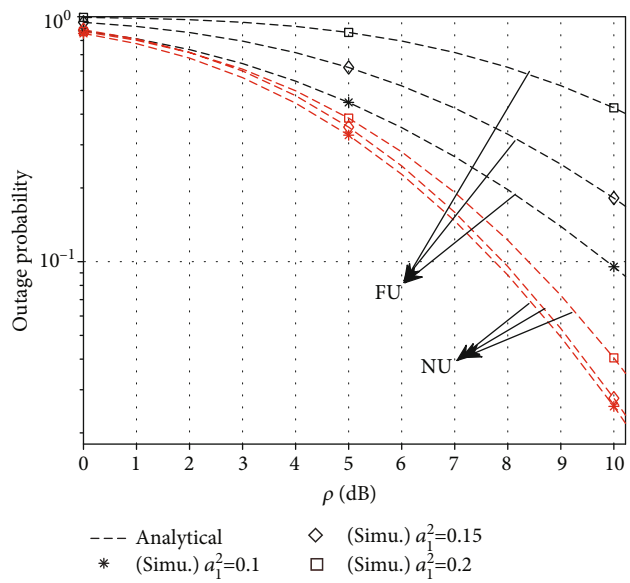

Figure 7: Outage probability comparison for users NU and FU with different power allocation factors ($N = 4$).

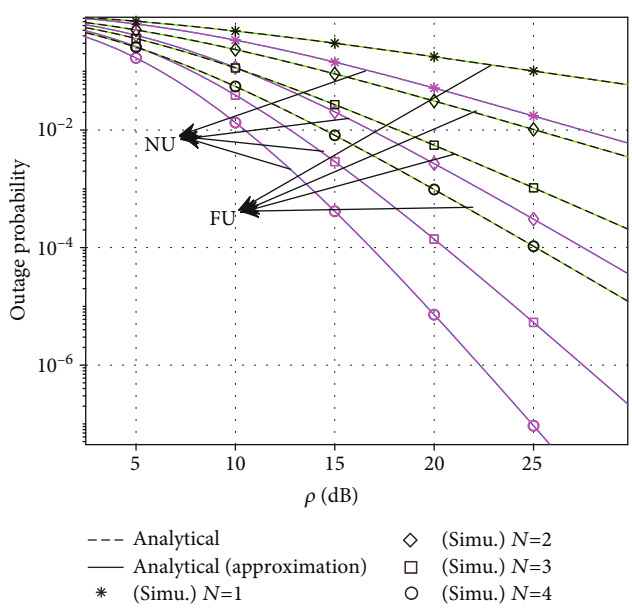

Figure 8: Outage probability comparison between NOMA and NOMA-approximation ($Q = 2$).

Similarly, we also obtain approximated computation for OMA user corresponding to two cases $Q > 1$ and $Q = 1$, respectively, as

$$P_{OMA,1}^{\infty} \approx \frac{\psi_4}{(Q-1)^P}, \tag{28}$$

$$P_{OMA,2}^{\infty} \approx \psi_4^N (-\ln(\psi_4))^N. \tag{29}$$

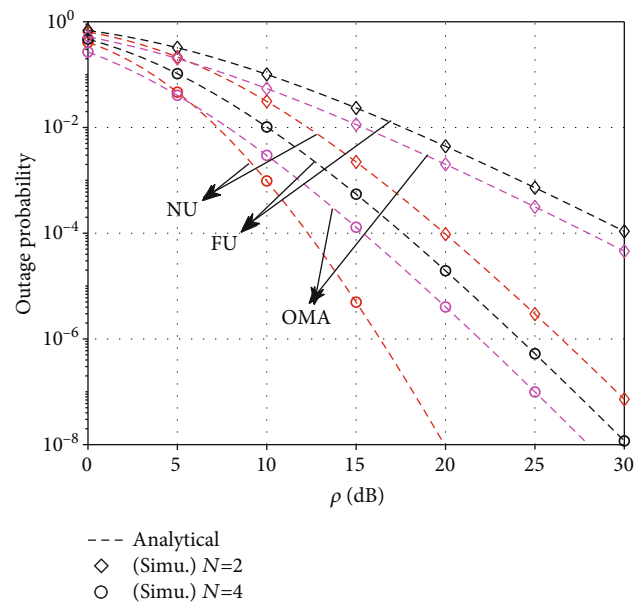

Figure 9: Outage probability comparison between RIS relies on NOMA and OMA ($Q = 1$).

6. Numerical Simulations and Discussions

In this section, we will determine system performance metrics (outage probability and throughput in delay-limited transmission mode). We intend to verify the theoretical results, numerically evaluate, and compare two practical schemes of the RIS-NOMA system. In each figure, we can see the main parameters used for simulation. We call bit per channel use as BPCU for short. We set target rate $R_1 = 1$ (BPCU), $R_2 = 1$ (BPCU), and $R_{\mathrm{OMA}} = 1$ (BPCU) and power allocation factors $a_1^2 = 0.2, a_2^2 = 1 - a_1^2$, except for specific cases indicated later, and simulation parameters used are summarized in Table 2.

Figure 4 shows the outage probability versus transmit SNR at the BS. It can be seen intuitively that the simulation and analytical results are matched very tight. In this graph, it mainly shows how two NOMA groups can make the exchange of the messages between each other. The improvements which are shown over here are mainly regarding the performance of the outage and here the things which are mainly considered are about the SNR. We consider the improvement of outage performance for different numbers of RIS elements for user NU in the range of SNR (from 0 to 30 dB). In particular, the significant improvement can be achieved at ρ equals to 30 dB. It can be observed that when the number of RIS elements increase, the performance of the proposed RIS-NOMA system exhibits its efficiency as expected from our study. Since diversity order depends on the number of metasurfaces N, once can see that significant improvement of outage probability occurs if N increases.

Similarly, since computation of outage probability for user FU is simpler than that of user NU, performance of Figure 4 is similar. Figure 5 shows the trends of outage probability versus transmit SNR. The main purpose of this graph

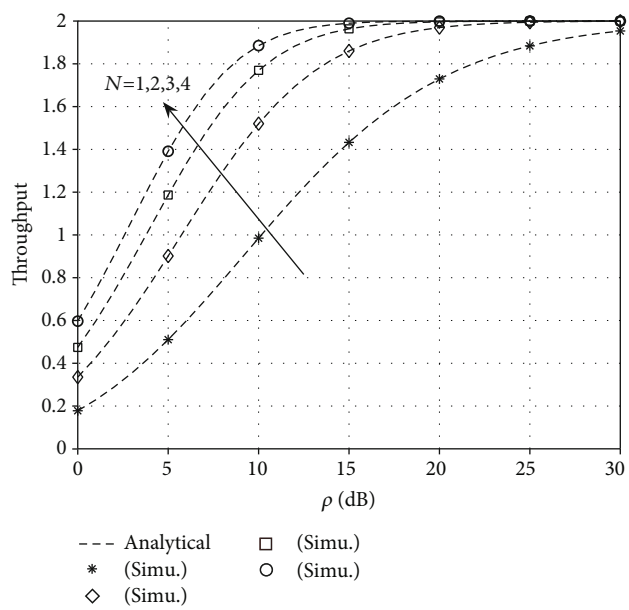

Figure 10: Throughput of the RIS-NOMA system ($Q = 1$).

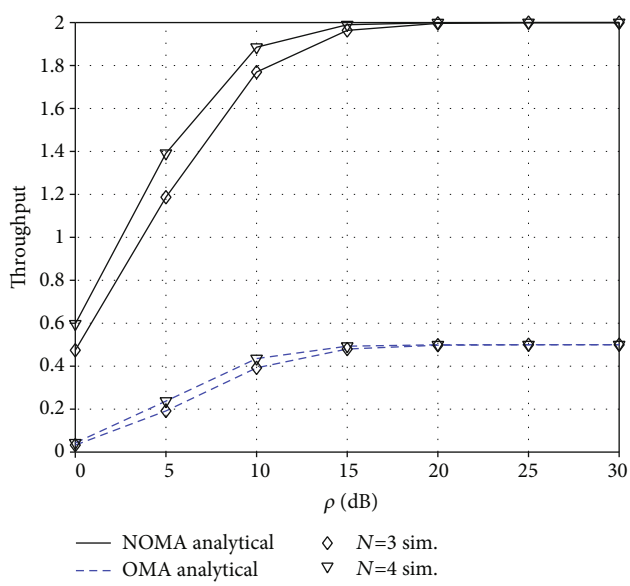

Figure 11: Throughput comparison between RIS-NOMA and RIS-OMA system ($Q = 1$).

is to show the performance of the users which is very important to be understood in order to determine various benefits. Here also, we can observe that the performance of the proposed RIS-NOMA benefits to user at far distance by increasing the number the RIS elements and higher power assigned to user FU.

Figure 6 shows the comparison of the outage probability versus SNR for different numbers of RIS elements for users NU and FU. In this comparison, we can determine that as the RIS elements are increased, the performance of the NU is better that of the FU. It seems that RIS elements which are there used have a great proficiency in case of maintaining

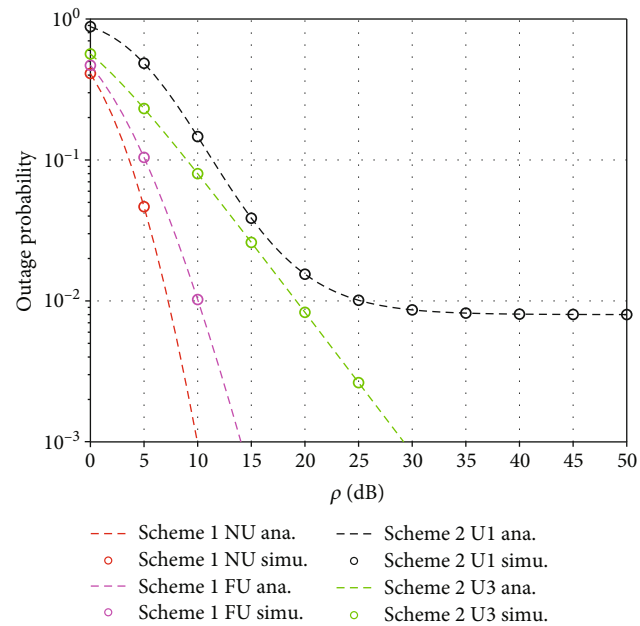

Figure 12: Outage probability comparison for Scheme 1 and Scheme 2, $Q = 1$, $N = 4$, and $\Omega_I = 0.03$.

performance rate. The rate of the determination that is done over here is related to mainly increase rate of the performance. However, it is more complicated processing at user NU compared with that in user FU.

Here, it can be seen from Figure 7 that the comparison is mainly done between NU and FU where the power allocation is shown where $N = 4$. The comparison which is done over here is related to the outage-based probability.

Figure 7 demonstrates the impact of power allocation factors on the outage probability. Since expression of outage probability for user NU depends on ability of detecting user FU's signal, lower factor a_1 results in better performance for user NU. As previous simulations, we can see similar trends of such outage performance in this figure, while Figure 8 indicates that exact and approximated formulas for two users have similar performance. For simple computation, we also benefit similar result. Here, mainly the outage comparison which is done is between the NOMA and NOMA approximation, it is very important to find the difference between the two NOMA in order to fund the trend to be identified.

Figure 9 indicates the comparison of the outage performance for users NU, FU in NOMA scheme, and user in OMA scheme. It can be observed that the outage behavior of user NU is better than OMA user and user FU. The main reason is that different power factors and signal detecting procedure lead to performance gaps. The importance of the RIS lies within the NOMA which is understood with the help of the comparison between NOMA and NOMA with the use of $Q = 1$.

Figure 10 depicts throughput performance versus transmit SNR. It can be concluded that more elements of RIS lead to higher throughput. The main reason is that the

throughput depends on the outage probability while higher number of RIS elements results in better outage performance. The ceiling value of such throughput can be achieved at the point $\rho = 20dB, N = 4$. Two target rates R_1 and R_2 make this ceiling value. The main things which are been depicted here is related to the RIS-NOMA system which shows the rate of activity that is taking place.

The comparison throughput performance for the considered system with OMA is shown in Figure 11, when ρ is raised. We set $R_1 = R_2 = 1$ in this case. This suggests that our system can approach two at a very high ρ value. It is easy to see how such throughput is influenced by the outage probabilities attained in earlier steps. It has been confirmed that our RIS system based on NOMA is superior to that based on OMA.

Figure 12 shows the comparison of the outage probability versus SNR for NOMA-RIS system in two schemes. It can be seen clearly that scheme 1 shows better outage performance compared with that in scheme 2. It is suitable with analytical results once scheme 2 has less benefit from fabrication of RIS. Furthermore, interference from external non-NOMA user limits performance of user U_1 which has similar configuration with user NU in scheme 1. The value regarding the scheme 1 and the scheme 2 has been shown over here which is a value of the external non-NOMA user limits. It is found that all the results which are given are suitable with the limits.

7. Conclusions

In this paper, we study two practical situations for deployment of RIS and NOMA in wireless system. More RIS elements lead to significant improvement in main system metric, i.e., outage probability. In particular, we derived the closed form formulas of outage probability which depend on various parameters such as the number of RIS elements, transmit SNR at the BS, and power allocation factors. By controlling these values, we can achieve reasonable system performance. The numerical results also indicate that the RIS-NOMA in scheme 1 is reported as better case. However, to achieve such ideal performance, it is necessary to release the impact of interference to the RIS. By exploiting NOMA, the RIS-NOMA aided system provides better performance compared with traditional multiple access techniques such as OMA. In addition, by grouping of users, we benefit advantages of NOMA while separating these groups by employing OMA scheme. Therefore, such RIS-NOMA becomes promising system for many applications in wireless systems, especially massive connections is strictly required in future systems.

Appendix

A. Proof of Proposition 2.

The outage probability P_{NU,s_1} can be further computed by

$$P_{\mathrm{NU},s_1} = \int_0^{\psi} f_{A^2}(x)dx. \tag{A.1}$$

From achieved PDF, we then calculate such outage probability as below:

$$P_{\mathrm{NU},s_1} = \int_0^{\psi} \frac{2x^{\mathrm{Q}-1/2}}{\Gamma(Q)} K_{Q-1}\left(2\sqrt{x}\right)dx. \tag{A.2}$$

In the next step, P_{NU,s_1} can be given by

$$P_{\mathrm{NU},s_1} = C_1\left((\psi)^{-\frac{Q+1}{2}}\Gamma(Q) - 2(\psi)^{-\frac{1}{2}}B_1\right)^P. \tag{A.3}$$

Regarding signal processing at the NU, this user needs detect the FU's signal since the NU treats the FU's signal as noise. The outage probability of the NU depends partly on ability of detecting the FU's signal as below:

$$P_{\mathrm{NU},s_2} = \Pr\left(\log\left(1 + \mathrm{SINR}(s_2)\right) < R_2\right). \tag{A.4}$$

Then, P_{NU,s_2} can be rewritten by

$$P_{\mathrm{NU},s_2} = C_2\left((\psi_1)^{-\frac{Q+1}{2}}\Gamma(Q) - 2(\psi_1)^{-\frac{1}{2}}B_2\right)^P. \tag{A.5}$$

It is noted that the outage probability for user NU is decided by two mentioned steps, and then we have such outage probability as

$$P_{\mathrm{NU}} = P_{\mathrm{NU},s_1} \times P_{\mathrm{NU},s_2}. \tag{A.6}$$

Next, we can obtain such outage probability for user NU as [(A.8)]

$$P_{\mathrm{NU}} = C_1\left(\psi^{-\frac{Q+1}{2}}\Gamma(Q) - 2\psi^{-\frac{1}{2}}B_1\right)^P \times C_2\left(\psi_1{}^{-\frac{Q+1}{2}}\Gamma(Q) - 2\psi_1{}^{-\frac{1}{2}}B_2\right)^P, \tag{A.7}$$

$$\begin{aligned} P_{\mathrm{NU}} = C_1C_2\Big[&(\psi\psi_1)^{-\frac{Q+1}{2}}\Gamma(Q)^2 - 2\psi^{-\frac{Q+1}{2}}\psi_1{}^{-\frac{1}{2}}B_2\Gamma(Q) \\ &- 2\psi^{-\frac{Q+1}{2}}\psi_1{}^{-\frac{1}{2}}B_1\Gamma(Q) + 4\psi^{-\frac{1}{2}}\psi_1{}^{-\frac{1}{2}}B_1B_2\Big]. \end{aligned} \tag{A.8}$$

This completes the proof.

B. Proof of Proposition 5.

Similarly, since we have PDF of A is given by

$$\mathrm{f}_{\mathrm{A}^2}(\mathrm{x}) = \frac{2\mathrm{x}^{\mathrm{Q}-1/2}}{\Gamma(\mathrm{Q})}\mathrm{K}_{\mathrm{Q}-1}\left(2\sqrt{\mathrm{x}}\right). \tag{A.9}$$

The outage probability of OMA user can be expressed by

$$P_{\mathrm{OMA}} = \Pr\left(\log\left(1 + \mathrm{SINR}_{\mathrm{OMA}}\right) < R_{\mathrm{OMA}}\right), \tag{A.10}$$

where R_{OMA} is target rate for OMA user.
Next, P_{OMA} is computed by

$$P_{\mathrm{OMA}} = \frac{2}{\Gamma(Q)}\int_0^{\psi_4} x^{\frac{Q-1}{2}}K_{Q-1}\left(2\sqrt{x}\right)dx. \tag{A.11}$$

By apply similar manipulation as the case of NOMA, the final result can be obtained, and hence, the proof is completed.

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] H. Huang, W. Xia, J. Xiong, J. Yang, G. Zheng, and X. Zhu, "Unsupervised learning-based fast beamforming design for downlink MIMO," *IEEE Access*, vol. 7, pp. 7599–7605, 2018.

[2] G. Gui, H. Sari, and E. Biglieri, "A new definition of fairness for non-orthogonal multiple access," *IEEE Communications Letters*, vol. 23, no. 7, pp. 1267–1271, 2019.

[3] B. Wang, F. Gao, S. Jin, H. Lin, and G. Y. Li, "Spatial- and frequency wideband effects in millimeter-wave massive MIMO systems," *IEEE Transactions on Signal Processing*, vol. 66, no. 13, pp. 3393–3406, 2018.

[4] H. Xie, F. Gao, S. Zhang, and S. Jin, "A unified transmission strategy for TDD/FDD massive MIMO systems with spatial basis expansion model," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3170–3184, 2017.

[5] Z. M. Fadlullah, F. Tang, B. Mao et al., "State-of-the-art deep learning: evolving machine intelligence toward tomorrow's intelligent network traffic control systems," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2432–2455, 2017.

[6] N. Kato, Z. M. Fadlullah, B. Mao et al., "The deep learning vision for heterogeneous network traffic control: proposal, challenges, and future perspective," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 146–153, 2016.

[7] F. Tang, B. Mao, Z. M. Fadlullah, and N. Kato, "On a novel deep-learningbased intelligent partially overlapping channel assignment in SDN-IoT," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 80–86, 2018.

[8] D.-T. Do and A.-T. Le, "NOMA based cognitive relaying: transceiver hardware impairments, relay selection policies and outage performance comparison," *Computer Communications*, vol. 146, pp. 144–154, 2019.

[9] T. Do, A.-T. Le, Y. Liu, and A. Jamalipour, "User grouping and energy harvesting in UAV-NOMA system with AF/DF relaying," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11855–11868, 2021.

[10] D.-T. Do, M.-S. Van Nguyen, T.-A. Hoang, and B. M. Lee, "Exploiting joint base station equipped multiple antenna and full-duplex D2D users in power domain division based multiple access networks," *Sensors*, vol. 19, no. 11, p. 2475, 2019.

[11] D.-T. Do, A.-T. Le, C.-B. Le, and B. M. Lee, "On exact outage and throughput performance of cognitive radio based non-orthogonal multiple access networks with and without D2D link," *Sensors*, vol. 19, no. 15, p. 3314, 2019.

[12] D.-T. Do, A.-T. Le, T. N. Nguyen, X. Li, and K. M. Rabie, "Joint Impacts of Imperfect CSI and Imperfect SIC in Cognitive Radio-Assisted NOMA-V2X Communications," *IEEE Access*, vol. 8, no. 7, pp. 128629–128645, 2020.

[13] D.-T. Do, A.-T. Le, and B. M. Lee, "NOMA in cooperative underlay cognitive radio networks under imperfect SIC," *IEEE Access*, vol. 8, pp. 86180–86195, 2020.

[14] D.-T. Do, M. V. Nguyen, F. Jameel, R. Jäntti, and I. S. Ansari, "Performance evaluation of relay-aided CR-NOMA for beyond 5G communications," *IEEE Access*, vol. 8, pp. 134838–134855, 2020.

[15] Y. Liang, R. Long, Q. Zhang, J. Chen, H. V. Cheng, and H. Guo, "Large intelligent surface/antennas (LISA): making reflective radios smart," *Journal of Communications and Information Networks*, vol. 4, no. 2, pp. 40–50, 2019.

[16] E. Basar, "Transmission through large intelligent surfaces: a new frontier in wireless communications," in *2019 European Conference on Networks and Communications (EuCNC)*, Valencia, Spain, 2019IEEE.

[17] Z. Tang, T. Hou, Y. Liu, J. Zhang, and C. Zhong, "A novel design of RIS for enhancing the physical layer security for RIS-aided NOMA networks," *IEEE Wireless Communications Letters*, vol. 10, no. 11, pp. 2398–2401, 2021.

[18] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2020.

[19] M. D. Renzo, M. Debbah, D. T. Phan-Huy et al., "Smart radio environments empowered by reconfigurable AI metasurfaces: an idea whose time has come," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, 2019.

[20] M. di Renzo and J. Song, "Reflection probability in wireless networks with metasurface-coated environmental objects: an approach based on random spatial processes," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, 2019.

[21] G. C. Alexandropoulos and E. Vlachos, "A hardware architecture for reconfigurable intelligent surfaces with minimal active elements for explicit channel estimation," in *ICASSP 2020 - 2020 IEEE international conference on acoustics, speech and signal processing (ICASSP)*, pp. 9175–9179, Barcelona, Spain, 2020.

[22] L. Dai, B. Wang, M. Wang et al., "Reconfigurable intelligent surface-based wireless communications: antenna design, prototyping, and experimental results," *IEEE Access*, vol. 8, pp. 45913–45923, 2020.

[23] X. Yang, C. -K. Wen, and S. Jin, "MIMO detection for reconfigurable intelligent surface-assisted millimeter wave systems," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 8, pp. 1777–1792, 2020.

[24] H. Lu, Y. Zeng, S. Jin, and R. Zhang, "Enabling panoramic full-angle reflection via aerial intelligent reflecting surface," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, Dublin, Ireland, 2020IEEE.

[25] M. Di Renzo, F. H. Danufane, X. Xi, J. de Rosny, and S. Tretyakov, "Analytical modeling of the path-loss for reconfigurable intelligent surfaces–anomalous mirror or scatterer?," in *2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Atlanta, GA, USA, 2020.

[26] T. Hou, Y. Liu, Z. Song, X. Sun, Y. Chen, and L. Hanzo, "Reconfigurable intelligent surface aided NOMA networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2575–2588, 2020.

[27] T. Hou, Y. Liu, Z. Song, X. Sun, and Y. Chen, "MIMO-NOMA networks relying on reconfigurable intelligent surface: a signal cancellation based design," *IEEE Transactions on Communications*, vol. 68, no. 11, pp. 6932–6944, 2020.

[28] Z. Yang, J. Shi, Z. Li, M. Chen, W. Xu, and M. Shikh-Bahaei, "Energy efficient rate splitting multiple access (RSMA) with reconfigurable intelligent surface," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, Dublin, Ireland, 2020.

[29] Z. Ding and H. Vincent Poor, "A simple design of IRS-NOMA transmission," *Communications letters*, vol. 24, no. 5, pp. 1119–1123, 2020.

[30] M. Zeng, W. Hao, O. A. Dobre, Z. Ding, and H. V. Poor, "Power minimization for multi-cell uplink NOMA with imperfect SIC," *IEEE Wireless Communications Letters*, vol. 9, no. 12, pp. 2030–2034, 2020.

[31] M. F. Hanif, Z. Ding, T. Ratnarajah, and G. K. Karagiannidis, "A minorization-maximization method for optimizing sum rate in the downlink of non-orthogonal multiple access systems," *IEEE Transactions on Signal Processing*, vol. 64, no. 1, pp. 76–88, 2016.

[32] Q. Chen, M. Li, X. Yang, R. Alturki, M. D. Alshehri, and F. Khan, "Impact of residual hardware impairment on the IoT secrecy performance of RIS-assisted NOMA networks," *IEEE Access*, vol. 9, pp. 42583–42592, 2021.

[33] Z. Wang, L. Liu, and S. Cui, "Channel estimation for intelligent reflecting surface assisted multiuser communications," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, Seoul, Korea, 2020IEEE.

[34] Y. Liu and W.-K. Ma, "Symbol-level precoding is symbol-perturbed ZF when energy efficiency is sought," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3869–3873, Calgary, AB, Canada, 2018.

[35] A. Hemanth, K. Umamaheswari, A. C. Pogaku, D.-T. Do, and B. M. Lee, "Outage performance analysis of reconfigurable intelligent surfaces-aided NOMA under presence of hardware impairment," *IEEE Access*, vol. 8, pp. 212156–212165, 2020.

[36] T. Q. Quek, G. de la Roche, İ. Güvenç, and M. Kountouris, *Small Cell Networks: Deployment, PHY Techniques, and Resource Management*, Cambridge University Press, Cambridge, U.K., 2013.

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 4655400, 10 pages
https://doi.org/10.1155/2021/4655400

Research Article

VLSI Implementation of Green Computing Control Unit on Zynq FPGA for Green Communication

Anurag Shrivastava,[1] **Ali Rizwan**,[2] **Neelam Sanjeev Kumar**,[3] **R. Saravanakumar**,[4] **Inderjit Singh Dhanoa**,[5] **Pankaj Bhambri**,[6] **and Bhupesh Kumar Singh**[7]

[1]*ECE, Lakshmi Narain College of Technology and Science Indore, India*
[2]*Department of Industrial Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia*
[3]*Department of BME, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, India*
[4]*Department of Wireless Communication Institute of ECE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India*
[5]*Department of Computer Science and Engineering, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India*
[6]*Department of Information Technology, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India*
[7]*Arba Minch Institute of Technology, Arba Minch University, Ethiopia*

Correspondence should be addressed to Bhupesh Kumar Singh; dr.bhupeshkumarsingh@amu.edu.et

Received 21 September 2021; Revised 3 November 2021; Accepted 6 November 2021; Published 30 November 2021

Academic Editor: Samarendra Nath Sur

The issue of the energy shortage is affecting the entire planet. This is occurring because of massive population and industry growth around the world. As a result, the entire world is attempting to implement green networking systems and manufacture the power/energy efficient products. This research work discusses the green networking system technologies. This work introduces a power-efficient control unit (CU) design and implemented on the Zynq SoC (System on Chip) ultrascale field programmable gate array (FPGA). The VIVADO HLx Design Suite is used to simulate and analyze the CU model which is considered as one of the key components of central processing unit (CPU), used for data communication purposes. The CU is made suitable for the green communication by making it power-efficient. Therefore, the power consumption of the CU is analyzed for the various set frequency value ranging between 100 MHz and 5 GHz, and it is discovered that as the clock frequency rises up, the total power consumption also tends to get increased. The total power of the proposed model is reduced by 77.42%, 21.29%, and 17.93% from three models, respectively, being compared in the present paper. Final results shows that the CU is better suited to run at low frequencies to optimize power consumption.

1. Introduction

There have been many issues with the scarcity of natural resources in the Earth because of the rapid population expansion and industrialization in the world [1]. Thus, people are worried about the future generation saving of those resources. This can be done using green technology of connectivity and energy-efficient machines [2]. The work represents a step in the direction of promoting green networking technology and energy-efficient devices. A control unit (CU), to minimize the power consumption, is installed on field programmable gate array (FPGA) in this work. A control unit is a part of a circuitry that regulates activity in the computer [3]. It gives instructions on how to react to instructions that the program sends to these devices in the logic unit, memory, input, and output devices [4]. Figure 1 shows the block scheme for the control unit. It selects and retrieves instructions from the main memory in the proper sequence and interprets them to allow other functional elements to perform the respective operations at the

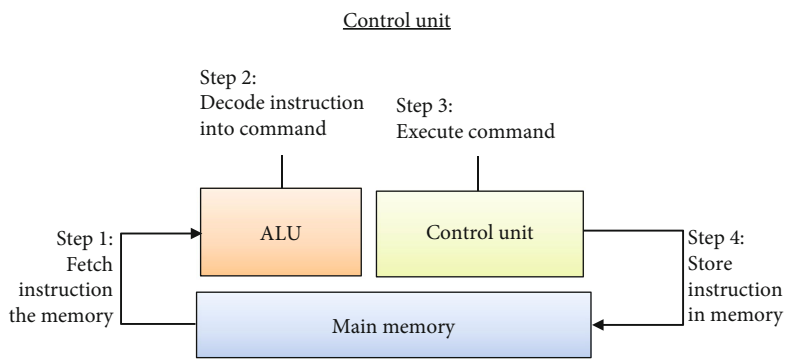

Figure 1: The block scheme for the CU.

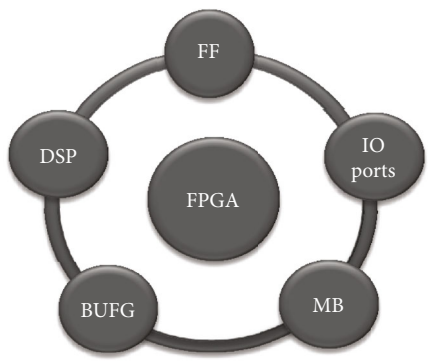

Figure 2: Building components of the FPGA device.

appropriate time [5–7]. Each input data is passed via the main memory to a processing device, comprising the four basic arithmetic functions (i.e., adding, subtracting, multiplying, and dividing) as well as certain logical operations such as data comparison and the selection of the required problem-solving method or a suitable alternative, on the basis of default decision criteria [8, 9].

Of all these features and vast application in the field of computing, CU is regarded as one of the suitable components which can be used for green computing as well as green communication; also, these green computing and green communication makes the environment sustainable. By reducing its power consumption, the CU can be made suitable for green applications. Therefore, the power-efficient CU will be the great choice for communication technologies [10, 11]. The power consumption of CU is optimized by its realization on FPGA devices. FPGAs are those devices which are made-up with semiconductor materials. It is called field programmable because it can be reconfigured/reprogrammed after its manufacturing [12–14]. FPGA devices are made-up with many components, and theses components are regarded as building components such as clock buffers (BUFGs), flip-flops (FF), input/output (IO) ports, memory blocks (MB), and digital signal processors (DSPs) [15, 16]. The building components of the FPGA device are represented in Figure 2.

1.1. Green Computing Communication. Green computing (GC) is a future generation environmentally friendly way of utilizing the computers, mobile device, and their resources. GC is also regarded as green information technology (green IT). In a broad way, GC term can also be coined as the method of designing, manufacturing, implementing, using, and disposing the mobile and computing peripherals and devices with least damage on environment resources. A brief idea of green computing is described in Figures 3 and 4.

Figure 3 shows the things which are associated with green computing. These are such power management of devices, designing of energy-efficient devices, processors, and other computer devices, cloud, and virtualization. In cloud and virtualization, we try to communicate the data with cloud server and access the data from cloud.

Figure 4 represents the utilities of GC. Generally, there 4 major points concerned with GC.

(i) Green use—it implies minimising power consumption of computer and mobile devices

(ii) Green disposal—it implies reusing and recycling of unwanted electronic devices

(iii) Green design—it covers the implementation and designing power and energy efficient devices

(iv) Green manufacturing—green manufacturing discusses about manufacturing computer and mobile devices with minimized waste

The communication of green devices with cloud and virtualization are known to be as green computing communication (GCC). The overview of GCC is shown in Figure 5.

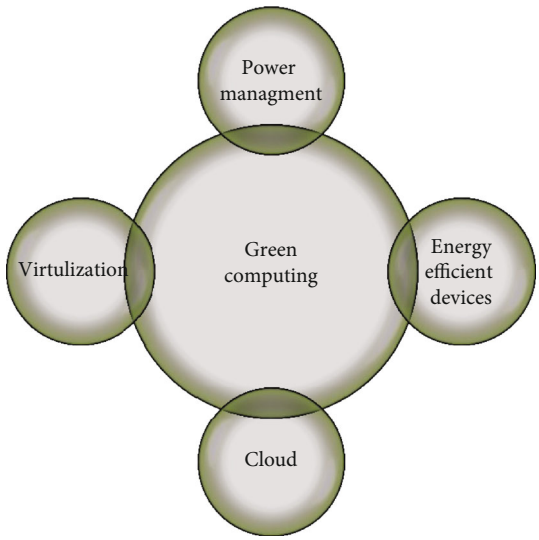

Figure 3: Idea of green computing.

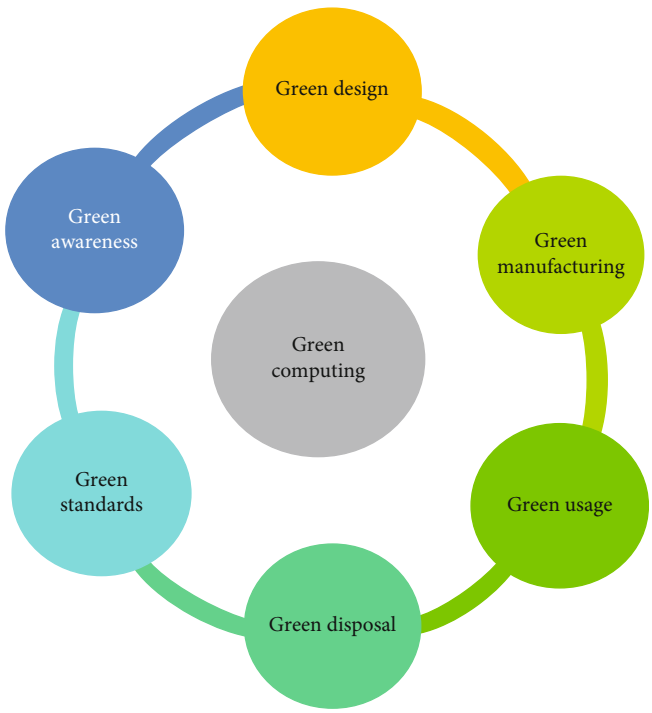

Figure 4: Utilities of green computing.

2. Related Work

With the help of IO standard, researchers have developed a power-efficient CU on Artix-7 FPGA with the support of various Low Voltage CMOS (LVCMOS) technologies. Input and output impedance are used to minimize the electricity consumption. Authors on Artix-7 FPGA design a power-efficient CU by modifying its frequency values. The shift in frequency values would change the CU's power consumption by FPGA [17]. Researchers are using I/O standards of Stub Series Terminated Logic (SSTL) to increase CU power consumption on 40 nm of Virtex-6 FPGA. The standards of the SSTL I/O correspond to the input load impedance w.r.t with the output load to minimize power consumption [18]. An electronic CU has been developed for the control of the vehicle system by FPGA authors. The RISC processor (ARM) is used in combination with FPGA to perform parallel computing tasks [19]. A power-efficient CU on Virtex and the Spartan family FPGA was introduced to support the concepts of Green Communication researchers [20]. Authors have designed the integration of green communication on Virtex 4, Virtex 5, and Virtex 6 FPGA [21] in an energy-efficient instruction register. In [22], FPGA was used by the authors to produce a true random number by

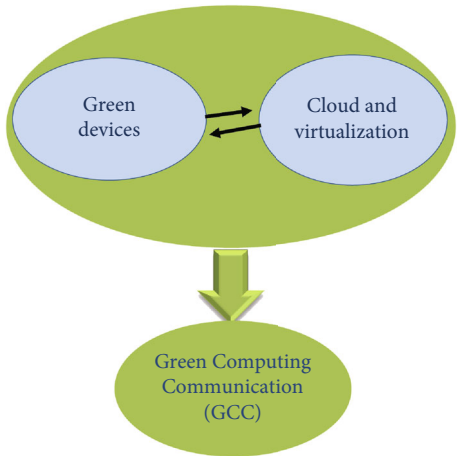

Figure 5: Green communications.

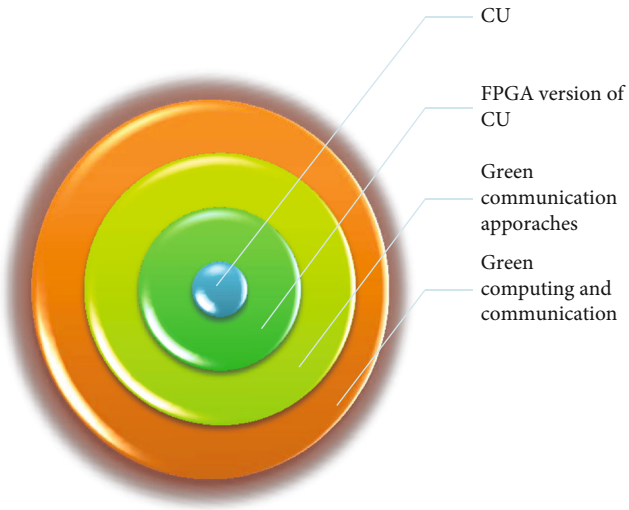

Figure 6: Green computing model of CU.

inducing metastability. In [23], photovoltaic simulation modules with FPGA were built in real time. In [24], researchers carried out a frequency change design of the arithmetic logic unit (ALU) for FPGA. Virtex-6 FPGA was used in [25] researchers to design a four-bit unregistered counter, allowing for clock and cutting. Random access memory (ROM) architecture for Virtex-6 FPGA was interfaced in [26]. In [27], researchers have used FPGA device to design a low power model for wireless data communication. In [28], researchers used energy-efficient techniques such as scaling the capacitance value of the capacitor of output load to design a green communication model of FIR Filter. With the help of Spartan-6 FPGA, authors have designed a green communication model of FIR Filter [29]. In [30], different families of FPGA devices have been used by the authors to develop a green UART for communication purpose. In [31], various FPGAs of the Spartan Group have been used for the implementation of energy-efficient transceiver model. In [32], researchers have developed a green CU with FPGA. For designing such model, authors have used HSTL and HSULIO standards. By using Pseudo Open Drain (POD) IO standards, an efficient FPGA model of ALU has been designed by the researchers [33]. To endorse green communication, researchers have designed an energy-efficient model of instruction register on FPGA [21]. In [34], different FPGAs and SOC has been utilized to enhance the performance of FIR filter for data communication and communication channel. In [35], LVCMOS IO standards are considered to execute a power-efficient UART for green computing and green communication. In order to endorse the green wireless communication, authors have projected the idea of Vedic multiplier design on FPGA devices by

Table 1: Resource utilization of CU on Zynq Soc.

Resource	Used	Available	Utilization %
LUT	14	230400	0.01
FF	4	460800	0.01
IO	23	360	6.39
BUFGs	1	544	0.18

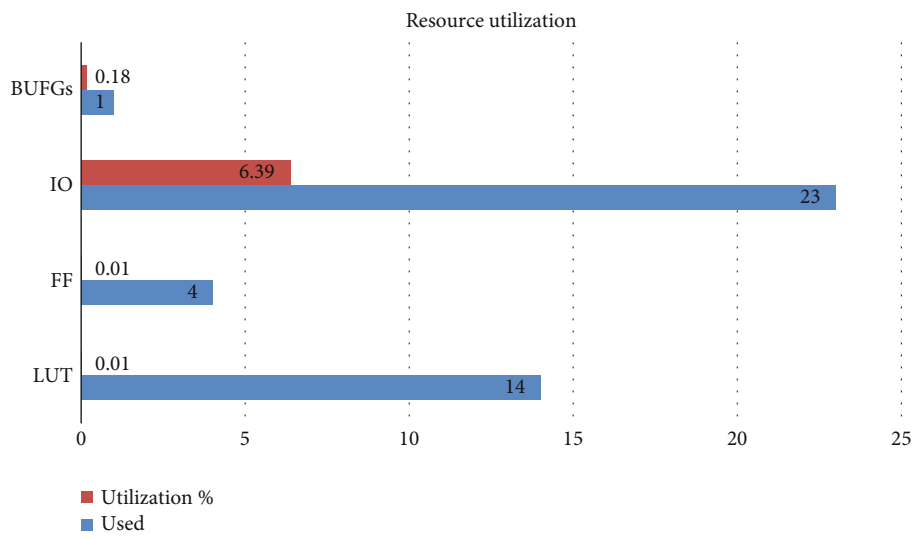

Figure 7: Resource utilization of CU on Zynq Soc.

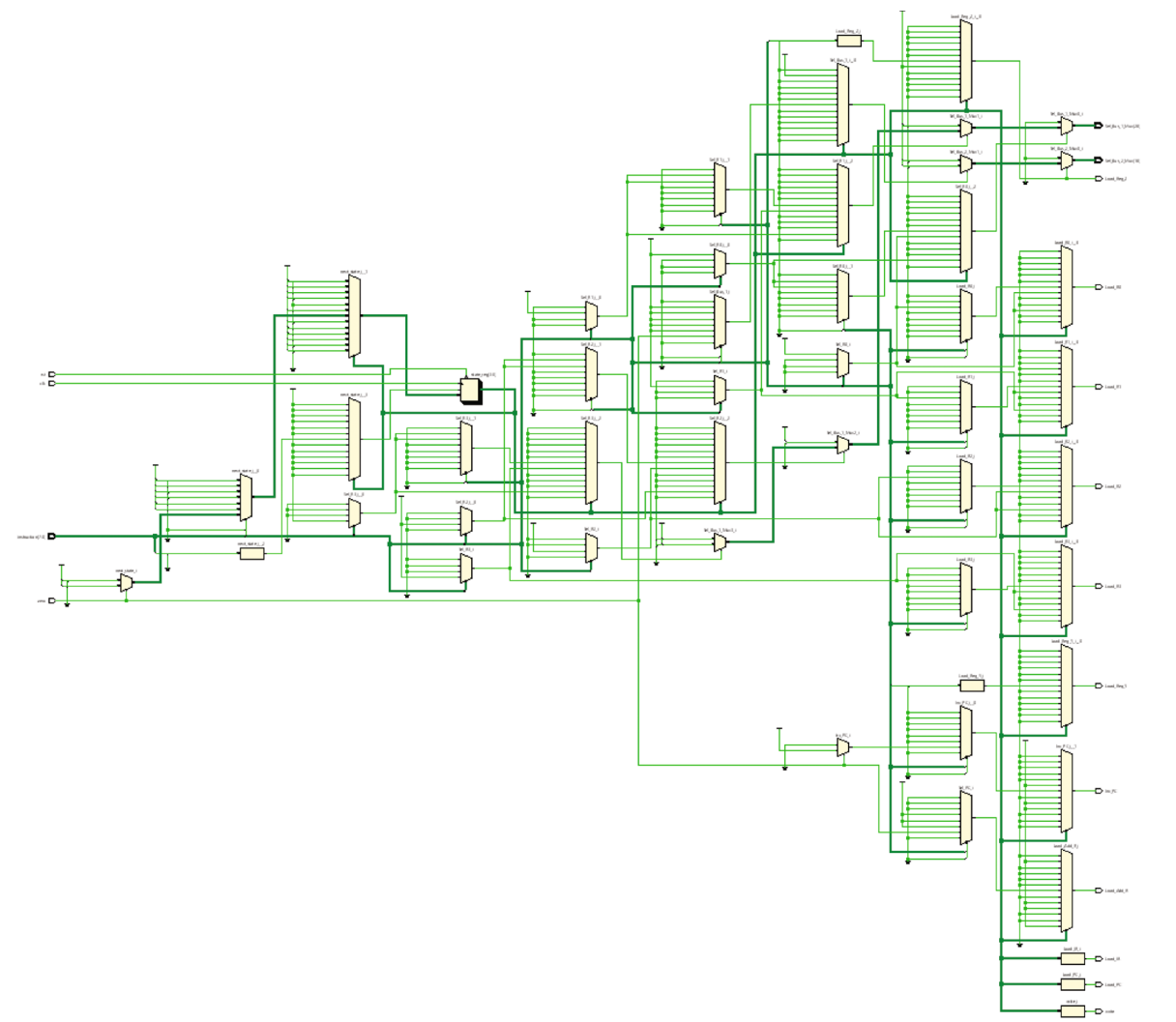

Figure 8: RTL of CU on Zynq SoC.

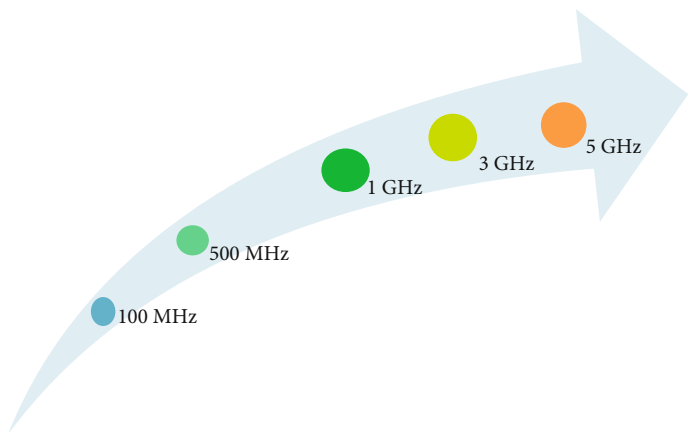

Figure 9: Frequency values for power calculation.

Table 2: Power calculation at 100 MHz.

On chips power	Power (W)
DP	0.006
SP	0.589
TP	0.595

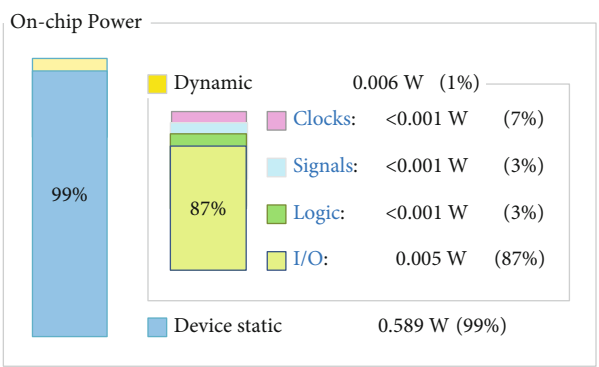

Figure 10: Power calculation at 100 MHz.

Table 3: Power calculation at 500 MHz.

On chips power	Power (W)
DP	0.030
SP	0.589
TP	0.619

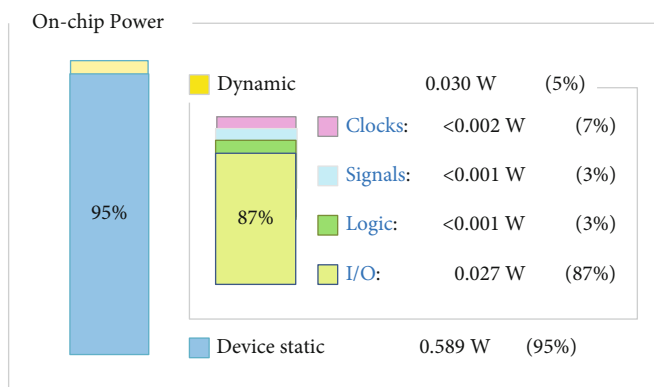

Figure 11: Power calculation at 500 MHz.

Table 4: Power calculation at 1 GHz.

On chips power	Power (W)
DP	0.214
SP	0.590
TP	0.804

reducing its power consumption with the help of several IO standards techniques [36]. In [37], researchers built a power-efficient green communications paradigm employing the data outage and BUFG MB DSP state information (CSI) channel FPGA FF IO ports. In [38], authors have developed a green FF design for green wireless communication using FPGA architectures. In [39], researchers have used 28 nm FPGA device to design a thermal efficient as well as power-efficient CU to incorporate with green communication. Kintex Ultra-scale FPGA has been taken for modeling an energy-efficient CU for promoting the green communication [40, 41]. Therefore, it has been observed that in the recent times, a lot of work has been done for incorporating the concepts of green communication and the energy/power efficient devices for future generations with the help of FPGAs, but a very few works have been done with respect to the implementation of the CU for green communication. Therefore, this work is all about the realization of CU on Zynq Ultra-Scale FPGA for promoting the values and ethics of green computing and green communication. The FPGA version of green computing model of CU is represented in Figure 6.

3. Experimental Setup

The ultrascale Zynq Soc FPGA board is used to set up the CU implementation. The VIVADO HLx architecture suite

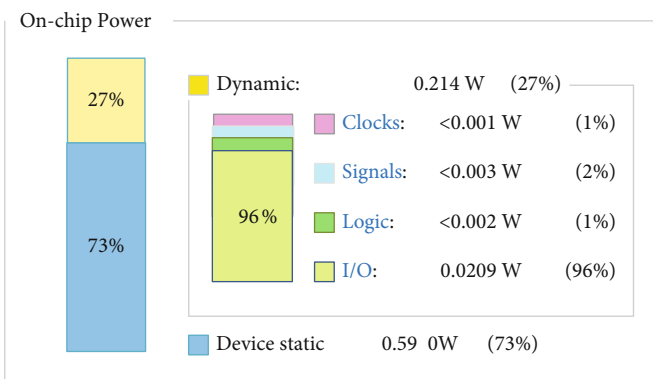

Figure 12: Power calculation at 1 GHz.

is the tool used to simulate CU on the FPGA board. Lookup tables (LUTs), flip-flops (FF), input-output (IO), and global buffers (BUFGs) are among the FPGA tools used to implement CU on the ultrascale Zynq Soc FPGA board, as shown in Table 1 and Figure 7 [42, 43].

The utilization of LUTs is 14, whereas 23-400 LUTs are available on FPGA boards for designing CU. Similarly, the utilization FF, IO, and BUFG are 4, 23, and 1, respectively, for designing CU on the ultrascale Zynq SoC FPGA. The Register Transfer Logic (RTL) of CU on Zynq SoC is shown in Figure 8.

4. Results and Discussion

In addition, FPGA system dynamic power (DP) and static power (SP) are correlated with the power measurement of CUs using the Zynq FPGA [44]. The summation of both DP and SP is the overall total power (TP) consumption. The dynamic power is the device's leakage power release.

The SP is the summation of I/O, logic (L/G), clock (CK), and signal (S/G). The power analysis of CU is done for five set of frequency value such as 100 MHz, 500 MHz, 1 GHz, 3 GHz, and 5 GHz, as shown in Figure 9.

4.1. Power Calculation for 100 MHz. For the frequency of 100 MHz, the SP of the device is 0.589 W, which is 99% of the TP consumption. The SP is the summation of I/O, L/G, CK, and S/G. Here, I/O power is 0.005 W, and the CK, L/G, and S/G power are less than 0.001 W. The DP, also called as leakage power, is 0.006 W, which is only 1% of the TP consumption. The TP for 100 MHz frequency is 0.595 W, as shown in Table 2 and Figure 10.

4.2. Power Calculation for 500 MHz. For the frequency of 500 MHz, the TP consumption is 0.619 W, which is the summation of SP and DP which are 0.589 W and 0.030 W, respectively. The SP consumes 95% of the TP while DP consumes 5% of TP, as shown in Table 3 and Figure 11.

4.3. Power Calculation at 1 GHz. For the frequency of 1 GHz, the SP of the device is 0.590 W, which is 73% of the TP consumption. The SP is the summation of I/O, L/G, CK, and S/G. Here, I/O power is 0.209 W, and the CK power is less than 0.001 W, while L/G and S/G power are 0.002 W and 0.003 W, respectively. The DP, also called as leakage power, is 0.214 W, which is 27% of the TP consumption. The TP for 1 GHz frequency is 0.804 W, as shown in Table 4 and Figure 12.

Table 5: Power calculation at 3 GHz.

On chips power	Power (W)
DP	0.184
SP	0.590
TP	0.773

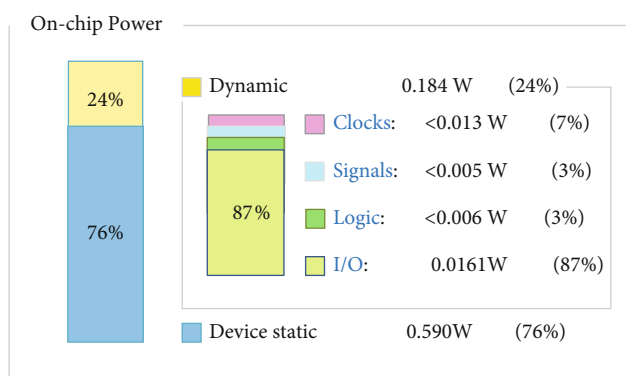

Figure 13: Power calculation at 3 GHz.

Table 6: Power calculation at 5 GHz.

On chips power	Power (W)
DP	0.303
SP	0.590
TP	0.893

4.4. Power Calculation at 3 GHz. For the frequency of 3 GHz, the TP consumption is 0.773 W, which is the summation of SP and DP which are 0.590 W and 0.184 W, respectively.

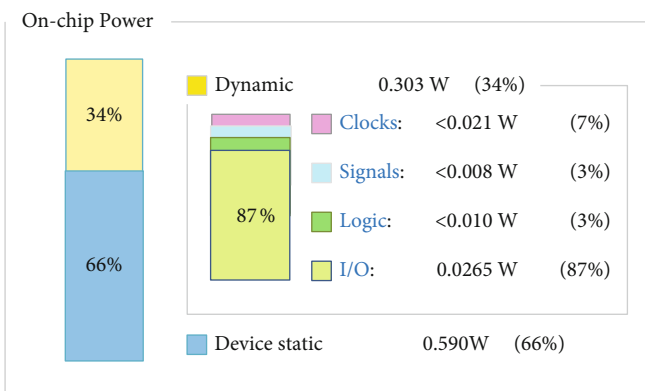

Figure 14: Power calculation at 5 GHz.

Table 7: TP consumption for different frequency.

Frequency	TP (W)
100 MHz	0.595
500 MHz	0.619
1 GHz	0.804
3 GHz	0.773
5 GHz	0.893

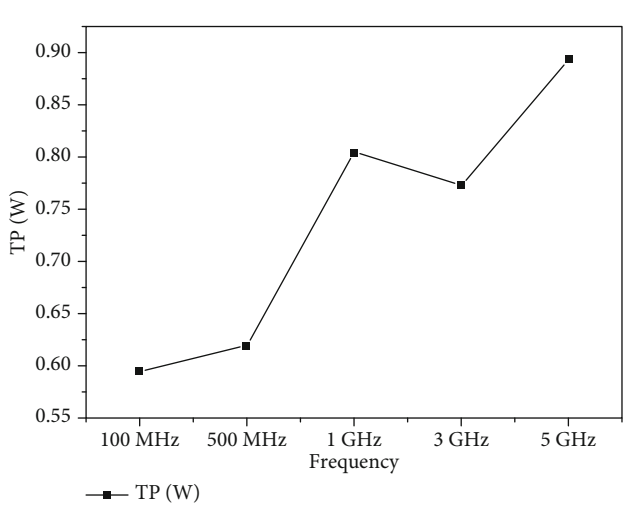

Figure 15: TP consumption for different frequency.

The SP consumes 76% of the TP while DP consumes 24% of TP, as shown in Table 5 and Figure 13.

4.5. Power Calculation at 5 GHz. For the frequency of 5 GHz, the TP consumption is 0.893 W, which is the summation of SP and DP which are 0.590 W and 0.303 W, respectively. The SP consumes 66% of the TP while DP consumes 44% of TP, as shown in Table 6 and Figure 14.

Form the power calculation for different values of frequency, it is found to be that the power consumption is maximum for higher values of frequency, i.e., 5 GHz and minimum for 100 MHz. The TP consumed for all frequency values is depicted in Table 7 and Figure 15. It is also observed that there is an increase of 4.03% in TP as the frequency is raised to 500 MHz from 100 MHz. Also, the increment observed for 1 GHz, 3 GHz, and 5 GHz, which are 35.12%, 29.91%, and 50.08%, respectively.

Table 8: Comparison of TP consumption.

References	TP (W)
[18]	2.636
[20]	0.756
[40]	0.725
Proposed work	0.595

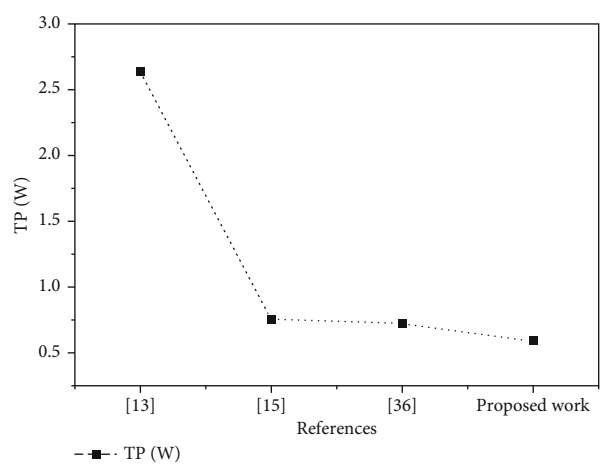

Figure 16: Comparison of TP consumption.

5. Comparative Analysis

In this section, a comparison of TP consumption has been made with the existing works of CU on FPGA and with this work. In [18], with Spartan 6 FPPGA, the TP for CU is found to be 2.636 W, while in [20, 40], the TP consumption for CU was 0.756 W and 0.725 W, respectively. In this work, CU is designed with Zynq SoC FPGA for incorporating with

green communication. The TP consumption with Zynq SoC is found to be optimized for 100 MHz frequency, i.e., 0.595 W. Therefore, it is observed that the TP consumption of CU is optimized in this proposed model. The TP of the proposed model is reduced by 77.42% from [18]. Similarly, the TP of this proposed model is reduced by 21.29% and 17.93% from [20, 40], respectively. The TP consumption of CU with existing models and the proposed model is shown in Table 8 and Figure 16, respectively.

6. Conclusion and Future Scope

The transition to green communication is critical in this period, as energy crises can be seen all over the world. As a result of this study, several steps have been taken to promote the concepts of green communication and power-efficient devices. The implementation of CU is carried out on the Zynq SoC ultrascale FPGA, and the simulation of the CU circuit, resource usage, and power analysis is carried out on the VIVADO Hlx Design Suite. It has been found that as the clock frequency of the circuit is increased, the power consumption decreases. As a result, it can be inferred that the overall power consumption is reduced when the clock frequency is low. Therefore, it is observed that there is an increase of 4.03% in TP as the frequency is raised to 500 MHz from 100 MHz. Also, the increment observed for 1 GHz, 3 GHz, and 5 GHz, which are 35.12%, 29.91%, and 50.08%, respectively. Also, the TP of the proposed model is reduced by 77.42% from [18]. Similarly, the TP of this proposed model is reduced by 21.29% and 17.93% from [20, 40], respectively, as shown in Figure 16. This CU circuit can be studied for other ultrascale and ultrascale plus FPGA devices in the future. Other power-saving methods, such as voltage, current, and capacitance scaling, can be used on the CU circuit as well. Impedance matching methods can also be used to make circuits more energy efficient with the aid of I/O specifications. For better performance, this FPGA design can later be converted to ASIC designs.

Data Availability

Data is available upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] R. Mahapatra, Y. Nijsure, G. Kaddoum, N. Ul Hassan, and C. Yuen, "Energy efficiency tradeoff mechanism towards wireless green communication: a survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 686–705, 2016.

[2] L. Pietrosemoli and C. Rodríguez-Monroy, "The Venezuelan energy crisis: renewable energies in the transition towards sustainability," *Renewable and Sustainable Energy Reviews*, vol. 105, pp. 415–426, 2019.

[3] https://www.computerhope.com/jargon/c/contunit.htm.

[4] https://www.geeksforgeeks.org/computer-organizationcontrol-unit-and-design/.

[5] J. H. Oh, Y. H. Yoon, J. K. Kim et al., "An FPGA-based electronic control unit for automotive systems," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1-2, Las Vegas, NV, USA, 2019.

[6] V. Bhatia, S. Kaur, K. Sharma, P. Rattan, V. Jagota, and M. A. Kemal, "Design and simulation of capacitive MEMS switch for Ka band application," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 2021513, 8 pages, 2021.

[7] J. Bhola and S. Soni, "A study on research issues and challenges in WSAN," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 1667–1671, Chennai, India, 2016.

[8] J. Bhola, M. Shabaz, G. Dhiman, S. Vimal, P. Subbulakshmi, and S. K. Soni, "Performance evaluation of multilayer clustering network using distributed energy efficient clustering with enhanced threshold protocol," *Wireless Personal Communications*, 2021.

[9] K. Jairath, N. Singh, V. Jagota, and M. Shabaz, "Compact ultra-wide band metamaterial-inspired split ring resonator structure loaded band notched antenna," *Mathematical Problems in Engineering*, vol. 2021, Article ID 5174455, 12 pages, 2021.

[10] C. Dou, L. Zheng, W. Wang, and M. Shabaz, "Evaluation of urban environmental and economic coordination based on discrete mathematical model," *Mathematical Problems in Engineering*, vol. 2021, Article ID 1566538, 11 pages, 2021.

[11] A. Rani and N. Grover, "Design and implementation of control unit-ALU of 32 bit asynchronous microprocessor based on FPGA," *International Journal of Engineering and Manufacturing*, vol. 8, no. 3, pp. 12–22, 2018.

[12] S. Hauck and A. DeHon, *Reconfigurable Computing: The Theory and Practice of FPGA-Based Computation*, Elsevier, 2010.

[13] D. Anguita, A. Boni, and S. Ridella, "A digital architecture for support vector machines: theory, algorithm, and FPGA implementation," *IEEE Transactions on Neural Networks*, vol. 14, no. 5, pp. 993–1009, 2003.

[14] I. Kuon, R. Tessier, and J. Rose, *FPGA Architecture: Survey and Challenges*, Now Publishers Inc., 2007.

[15] U. Farooq, Z. Marrakchi, and H. Mehrez, "FPGA architectures: an overview," in *Tree-based Heterogeneous FPGA Architectures*, pp. 7–48, Springer, New York, NY, 2012.

[16] W. Wolf, *FPGA-based system design*, Pearson Education, 2004.

[17] K. Kumar, B. Pandey, D. M. A. Hussain, A. Bhutto, A. K. Pandit, and E.-E. Baker, "Design of energy efficient control unit and implementation on high performance FPGA," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 12S2, pp. 23–26, 2019.

[18] S. P. Chaturvedi, A. Kaushik, and V. Baggan, "Power efficient control unit design using 40nm field programmable gate array," *International Journal of Advanced Science and Technology*, vol. 19, pp. 694–709, 2019.

[19] J. Pérez Fernández, M. Alcázar Vargas, J. M. Velasco García, J. A. Cabrera Carrillo, and J. J. Castillo Aguilar, "Low-cost FPGAbased electronic control unit for vehicle control systems," *Sensors*, vol. 19, no. 8, p. 1834, 2019.

[20] B. Pandey, K. Kumar, S. C. Haryanti, R. R. Mohamed, and D. M. A. Hussain, "Power efficient control unit for green communication," *Test Magazine*, vol. 83, pp. 13422–13427, 2020.

[21] S. M. T. Siddiquee, K. Kumar, B. Pandey, and A. Kumar, "Energy efficient instruction register for green communication," *International Journal of Engineering and Advanced Technology*, vol. 8, pp. 312–314, 2019.

[22] M. Majzoobi, F. Koushanfar, and S. Devadas, "FPGA-based true random number generation using circuit metastability with adaptive feedback control," in *Cryptographic Hardware and Embedded Systems – CHES 2011. CHES 2011*, B. Preneel and T. Takagi, Eds., vol. 6917 of Lecture Notes in Computer Science, pp. 17–32, Springer, Berlin, Heidelberg, 2011.

[23] E. Koutroulis, K. Kalaitzakis, and V. Tzitzilonis, "Development of an FPGA-based system for real-time simulation of photovoltaic modules," *Microelectronics Journal*, vol. 40, no. 7, pp. 1094–1102, 2009.

[24] B. Pandey and M. Pattanaik, "Clock gating aware low power ALU design and implementation on FPGA," *International Journal of Future Computer and Communication2*, vol. 5, pp. 461–465, 2013.

[25] B. Pandey and M. Pattanaik, "Low power VLSI circuit design with efficient HDL coding," in *2013 International Conference on Communication Systems and Network Technologies*, pp. 698–700, Gwalior, India, 2013.

[26] M. Bansal, N. Bansal, R. Saini, B. Pandey, L. Kalra, and D. M. A. Hussain, "SSTL I/O standard based environment friendly energyl efficient ROM design on FPGA," in *3rd International Symposium on Environmental Friendly Energies and Applications (EFEA)*, pp. 1–6, Paris, France, 2014.

[27] G. Verma, T. Singhal, R. Kumar et al., "Heuristic and statistical power estimation model for FPGA based wireless systems," *Wireless Personal Communications*, vol. 106, no. 4, pp. 2087–2098, 2019.

[28] B. Pandey, N. Pandey, A. Kaur, D. M. Akbar Hussain, B. Das, and G. S. Tomar, "Scaling of output load in energy efficient FIR filter for green communication on ultra-scale FPGA," *Wireless Personal Communications*, vol. 106, no. 4, pp. 1813–1826, 2019.

[29] B. Pandey, A. Jain, A. Kumar et al., *Energy Efficient and High–Performance FIR Filter Design on Spartan–6 FPGA*, 3C Tecnología. Glosas de innovación aplicadas a la pyme. Special Issue, 2019.

[30] K. Kumar, A. Kaur, S. N. Panda, and B. Pandey, "Effect of different nano meter technology based FPGA on energy efficient UART design," in *2018 8th International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 1–4, Bhopal, India, 2018.

[31] K. Kumar, B. Pandey, A. K. Pandit, Y. A. Baker El-Ebiary, S. A. Mjlae, and S. Bamansoor, "Design of low power transceiver on Spartan-3 and Spartan-6 FPGA," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 12S2, pp. 27–30, 2019.

[32] K. Kumar and P. Pandey, "HSTL and HSUL I/O standard based energy-efficient control unit circuit design on FPGA," *Gyancity Journal of Electronics and Computer Science*, vol. 4, no. 2, pp. 1–7, 2019.

[33] B. Pandey, P. Sharan, L. L. Dhirani, and D. A. Hussain, "Role of scaling of frequency and toggle rate in POD IO standards based energy efficient ALU design on ultra scale FPGA," in *2018 10th international conference on computational intelligence and communication networks (CICN)*, pp. 50–53, Esbjerg, Denmark, 2018.

[34] B. Pandey, B. Das, A. Kaur et al., "Performance evaluation of FIR filter after implementation on different FPGA and SOC and its utilization in communication and network," *Wireless Personal Communications*, vol. 95, no. 2, pp. 375–389, 2017.

[35] K. H. Abed and R. E. Siferd, "VLSI implementation of a low-power antilogarithmic converter," *IEEE Transactions on Computers*, vol. 52, no. 9, pp. 1221–1228, 2003.

[36] K. Goswami, B. Pandey, T. Kumar, and D. A. Hussain, "Different I/O standard and technology based thermal aware energy efficient Vedic multiplier design for green wireless communication on FPGA," *Wireless Personal Communications*, vol. 96, no. 2, pp. 3139–3158, 2017.

[37] C. C. Zarakovitis, Q. Ni, and J. Spiliotis, "Energy-efficient green wireless communication systems with imperfect CSI and data outage," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 12, pp. 3108–3126, 2016.

[38] G. Gupta, A. Kaur, and B. Pandey, "LVCMOS based green data flip flop design on FPGA," in *2017 ninth international conference on advanced computing (ICoAC)*, pp. 41–45, Chennai, India, 2017.

[39] K. Kumar, S. Ahmad, B. Pandey, A. K. Pandit, D. Singh, and D. M. A. Hussain, "Power efficient frequency scaled and thermal-aware control unit design on FPGA," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9S2, pp. 530–533, 2019.

[40] A. Burg, M. Borgmann, M. Wenk, M. Zellweger, W. Fichtner, and H. Bolcskei, "VLSI implementation of MIMO detection using the sphere decoding algorithm," *IEEE Journal of Solid-State Circuits*, vol. 40, no. 7, pp. 1566–1577, 2005.

[41] V. Degalahal and T. Tuan, "Methodology for high level estimation of FPGA power consumption," in *Proceedings of the 2005 Asia and South Pacific Design Automation Conference*, pp. 657–660, Shanghai, China, 2005.

[42] A. Amara, F. Amiel, and T. Ea, "FPGA vs. ASIC for low power applications," *Microelectronics Journal*, vol. 37, no. 8, pp. 669–677, 2006.

[43] T. Tuan and B. Lai, "Leakage power analysis of a 90nm FPGA," in *Proceedings of the IEEE 2003 Custom Integrated Circuits Conference, 2003*, pp. 57–60, San Jose, CA, USA, 2003.

[44] S. Ishihara, M. Hariyama, and M. Kameyama, "A low-power FPGA based on autonomous fine-grain power gating," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 19, no. 8, pp. 1394–1406, 2011.

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 4342983, 10 pages
https://doi.org/10.1155/2021/4342983

Research Article

Enabling Device-to-Device Transmission for NOMA-Aided Systems

Anh-Tu Le,[1] **Nhan Duc Nguyen**,[2] **Dinh-Thuan Do**,[3] **and Munyaradzi Munochiveyi**[4]

[1]*Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh City 700000, Vietnam*
[2]*Innovation Center, Van Lang University, Ho Chi Minh City, Vietnam*
[3]*Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan*
[4]*Electrical and Electronics Engineering Department, University of Zimbabwe, Mount Pleasant, Harare, Zimbabwe*

Correspondence should be addressed to Nhan Duc Nguyen; nhan.nd@vlu.edu.vn

Received 14 August 2021; Accepted 16 October 2021; Published 16 November 2021

Academic Editor: Vinayakumar Ravi

To utilize the close transmission, we assume that the device-to-device (D2D) link is activated to improve the performance of the far user. We consider two groups of users in the nonorthogonal multiple access- (NOMA)- aided wireless system. These features are necessary for massive connectivity in future wireless systems. The system performance also shows suitable performance at far distance users. To evaluate the performance in detail, we derive novel closed form expressions of outage probability. In practical situations impaired by channel uncertainty, it is necessary to evaluate the impact of channel error levels on outage probability. Our numerical results indicated that the transmit power at the base station and channel error level are the main impacts on system performance. Despite these impacts, our obtained numerical results demonstrated that the proposed scheme can still increase energy efficiency and achieve significant outage performance via many practical challenges.

1. Introduction

1.1. Motivation. Since spectral efficiency and massive connectivity are the main requirements in the fifth generation (5G) networks, and the applications of nonorthogonal multiple access (NOMA) have drawn lots of studies [1–3]. Further, NOMA is considered as a simple way to improve energy efficiency [4, 5]. NOMA allows multiple users to be served at the same frequency and time by superimposing a larger number of users in the power domain at the transmitter. Different from conventional orthogonal multiple access (OMA), the receiver of NOMA acquires successive interference cancellation (SIC) in its detection operation [6, 7]. In the NOMA system, by examining channel conditions (the near user and the far user), the users are divided into different orders of signal detection. The authors in [8] raised the influence of signal processing of the near user to the far user. To ensure user fairness, a power allocation scheme needs to be designed for NOMA users. In particular, more power is assigned to the far user with poor channel condition while less power is assigned to the near user with good channel condition. Recently, to achieve a balance between the performance of two users, NOMA is jointly designed with cooperative techniques. In a cooperative NOMA system, the performance gaps among these NOMA users can be determined by numerous system parameters such as transmit power at the base station [9–15]. To improve energy efficiency for low-power devices, [16] proposed a wireless power transfer paradigm for cooperative NOMA networks. To forward the signal to the far user, the near user can harvest energy from the source node.

Moreover, in [17, 18], the authors proposed the utilization of NOMA in device-to-device (D2D) communication networks. Numerous authors considered using NOMA to enhance D2D in different scenarios. Below, we present some noteworthy examples such as in [19], and the authors considered maximizing the D2D system sum rate by jointly optimizing the subchannel of D2D groups and the power allocation of receivers in each D2D group. In [20], the authors considered a NOMA-aided full-duplex (FD) D2D system. The authors analyzed the outage probability (OP) performance of the system NOMA weak and

strong users. In [21], the authors studied the combination of NOMA and mobile edge computing (MEC) in D2D systems. The authors proposed different algorithms to solve the joint optimization problem of computing resource, power, and channel allocations to minimize the weighted sum of the energy consumption and user delay. In [22], the authors investigated the energy efficiency maximization associated with underlaying NOMA enabled D2D systems. In [23], the authors considered the OP and power control of an unmanned aerial vehicle-(UAV-) enabled D2D underlaying NOMA systems.

Continuing, in [24], the authors maximized the sum rate of D2D user pairs while maintaining the rate requirements of NOMA-based cellular users in D2D underlaying NOMA-based cellular systems. In [25], the authors proposed NOMA to enhance the spectral efficiency of D2D-assisted cooperative relaying system (CRS). The authors demonstrated via simulation results that for D2D-assisted CRS utilizing NOMA with power allocation improved the achievable rate significantly compared to traditional CRSs relying on NOMA and without NOMA. In [26], the authors maximized the sum rate of underlay D2D users aided by NOMA by jointly designing user clustering and power assignment. In [27], the authors considered beamforming in multiuser multiple-input multiple-output (MU MIMO) downlink cellular network with NOMA-aided D2D users. In [28], the authors proposed an interference aware scheme for cooperative hybrid automatic repeat request-(HARQ-) aided NOMA system for massive D2D networks. The authors in [29] considered the secrecy outage probability (SOP) and OP for NOMA-enabled cooperative D2D systems in the presence of an eavesdropper as well as quality-of-service (QoS) provisioning. In [30], the authors studied covert communications in D2D underlay-aided power-domain NOMA. The authors noted that due to D2D devices being power limited, it is easy for them to be comprised easily by adversaries. Hence, it's essential to enable D2D communication links to transmit covert signals to guarantee a low probability of detection.

2. Related Works

So far in this discussion, we have considered several NOMA-aided D2D networks with perfect channel state information (CSI). Differently, in [31], the authors integrated FD relaying and time splitting simultaneous wireless information and power transfer (SWIPT) into D2D networks to address bandwidth and energy losses in conventional D2D networks with half-duplex relays and limited energy storage capability. The authors derived ergodic capacity expressions and closed form OP with imperfect CSI conditions. In another work on D2D networks powered by SWIPT in [32], the authors studied the resource allocation problem in NOMA-enabled D2D systems with SWIPT under imperfect CSI conditions. Here, the authors modeled the problem as a nonconvex optimization problem where the transmit power, power splitting factor, and resource block assignment factor are jointly designed to obtain the maximum OP of each D2D user, the SIC decoding order, and the maximum transmit power of the base station and D2D users. The authors developed a relaxation approach to transforming the obtained mixed-integer fractional programming problem with intractable OP constraints into a nonprobabilistic problem, and then the variable substitution and Dinkelbach's approach are used to transform the nonprobabilistic problem into a nonconvex one. Then, an energy-efficiency-based iterative algorithm is utilized to solve the intractable OP constraints. Recent work in [33] considered power efficient secure FD-aided SWIPT in NOMA-enabled D2D networks with imperfect CSI. The authors studied the system total transmit power minimization and formulated a multiobjective optimization (MOO) problem utilizing the weighted Tchebycheff method. The authors used a set of linear matrix inequalities (LMI) to transform the nonconvex constraints into convex constraints. Also, the authors utilized a bounded transmit beamforming vector design with artificial noise (AN) to satisfy robust power allocation in the presence of an eavesdropper with imperfect CSI.

In [34], the authors considered two-stage power allocation in maximizing the system sum rate of a cooperative NOMA-aided D2D system operating with imperfect CSI at the base station. In [35], the authors also proposed a power allocation algorithm for D2D-assisted cooperative NOMA networks under imperfect CSI. The authors converted the probabilistic nonconvex optimization problem into a nonprobabilistic nonconvex optimization problem solved via successive convex programming (SCP). Then, Lagrangian dual multiplier and Karush-Kuhn-Tucker methods are used to iteratively obtain suboptimal power allocation coefficients. In [36], the authors considered the integration of NOMA-aided D2D communication with fog computing (FC) under imperfect CSI to enhance the spectral efficiency of mission critical applications such as internet-of-medical-things (IoMTs), UAVs, and autonomous vehicles as well as secrecy capacity via coalition game theory. In [37], the authors considered millimeter wave (mmWave) NOMA-aided D2D systems under transceiver hardware and CSI impairments. The authors derived generalized OP expressions and confirmed via simulation results that their proposed system outperforms OMA.

3. Contributions

Motivated by the above, this article considers the closed form OP expressions of groups of users in D2D-enabled NOMA transmissions under imperfect CSI. Differently from the work in [37], we design our NOMA-aided D2D system model to follow a radial approach commonly found in cellular networks with the base station located in the center of the network. Also, unlike [28], which considered large scale NOMA-assisted D2D networks under perfect CSI conditions, in this work, we consider such networks under imperfect CSI conditions. Then, based on the stochastic geometry approach, we investigate the impact of channel estimation error on OP and throughput of the proposed system. Table 1 provides a comparison of this work versus the past studies in [31–37].

Our contributions are listed as follows:

(i) We consider transmission assisted by NOMA where a single antenna base station communicates with two groups of D2D users arranged in a radial manner around the base station. We study the case of imperfect

Table 1: A comparison of existing works on NOMA-aided D2D networks with imperfect CSI.

Scheme	Reference	Major contributions
FD-SWIPT NOMA-D2D	[31]	The authors derived ergodic capacity expressions and closed form OP with imperfect CSI conditions.
SWIPT NOMA-D2D	[32]	The authors studied the resource allocation problem by modeling the problem as a nonconvex optimization problem where the transmit power, power splitting factor, and resource block assignment factor are jointly designed to obtain the maximum OP of each D2D user, the SIC decoding order, and the maximum transmit power of the base station and D2D users.
Secure FD-SWIPT NOMA-D2D	[33]	The authors studied the system total transmit power minimization and formulated a multiobjective optimization (MOO) problem utilizing the weighted Tchebycheff method.
NOMA-D2D	[34]	The authors considered two-stage power allocation in maximizing the system sum rate of a cooperative NOMA-aided D2D system operating with imperfect CSI at the base station.
NOMA-D2D	[35]	The authors proposed a power allocation algorithm for D2D-assisted cooperative NOMA networks under imperfect CSI.
Fog computing NOMA-D2D	[36]	The authors considered the integration of NOMA-aided D2D communication with fog computing (FC) under imperfect CSI and utilized coalition game theory to enhance spectral efficiency and secrecy capacity.
mmWave NOMA-D2D	[37]	The authors considered mmWave NOMA-aided D2D systems under transceiver hardware and CSI impairments. The authors derived generalized OP expressions and confirmed via simulation results that their proposed system outperforms OMA.
NOMA-D2D	Our work	We consider transmission assisted by NOMA where a single antenna base station communicates with two groups of D2D users arranged in a radial manner around the base station. Then, based on the stochastic geometry approach, we investigate the impact of channel estimation error on OP and throughput of the proposed system. Simulations show that our proposed system still enhances spectral efficiency despite imperfect channel estimation and throughput limitations.

channel estimation to determine the downlink OP performance under Rayleigh fading channels

(ii) We determine the signal-to-interference-plus-noise ratios (SINRs) of the D2D grouped devices and then use them to formulate exact OP formulas over Rayleigh fading channels. The derived expressions are validated by Monte Carlo simulations

(iii) We analyze and compare the OP under various conditions. In particular, we find that transmit power at the base station and channel error are the main impacts on system outage performance. Despite these impacts, our obtained numerical results demonstrated that the proposed scheme can still increase energy efficiency and achieve significant outage performance via many practical challenges

(iv) Also, we note the influence of imperfect channel estimation on the throughput performance. We discover that the imperfect channel estimation impacts SIC which then imposes a ceiling on the throughput rate. This is one of the limitations of the present work. Hence, differently from past studies as seen in [31–37], the obtained simulation results of this work further demonstrate the impact of channel estimation on OP and throughput

The rest of this paper is organized as follows. Section 2 describes the downlink NOMA under Rayleigh channels in D2D networks with imperfect CSI. In Section 3, we consider the scenario of NOMA in terms of outage performance. In Section 4, we consider throughput. In Section 5, we provide extensive numerical simulations, and Section 6 concludes the paper.

4. System Model

The NOMA-aided D2D communication is studied, as shown in Figure 1. This system consists of a base station (S), and two groups of randomly deployed users A_n and B_n. Following the distances from users to S, B_n is considered as the near user, and B_n is within disc D_B with radius R_{D_B}. At longer distances, user A_n is the far user and is within disc D_A with radius R_{D_A}, conditioned on $(R_{D_A} > R_{D_B})$.

The source node S wants to send signals x_{A_n} and x_{B_n} to NOMA users An and Bn, respectively. We denote q_{n_1} and q_{n_2} as the corresponding power allocation coefficients with $|q_{n_1}|^2 + |q_{n_2}|^2 = 1$. In addition, d_{A_n}, d_{B_n}, and d_{C_n} are the distance from S to A_n, S to B_n, and Bn to An, respectively. To conduct performance analysis, we treat h_{SA_n}, h_{SB_n}, and h_{BA} as the channels for links S-A_n, S-B_n, and B_n-A_n, which follow Rayleigh fading channels. In this paper, we examine the impact of the channel estimation error [38] on system performance, and the considered channel is given by

$$h = \widehat{h} + \widetilde{h}, \tag{1}$$

where $\widehat{h}$ stands for the estimated fading channel coefficient,

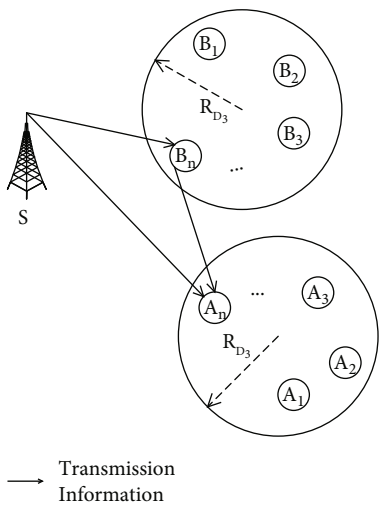

Figure 1: Device-to-device transmission for NOMA-aided systems.

$\tilde{h}$ represents as the error fading channel coefficient with $C N(0, \tilde{\sigma}^2)$, and $\tilde{\sigma}^2$ is constant [39].

In the first time slot, the source node S simultaneously transmits the message $q_{n_1} x_{A_n} + q_{n_2} x_{B_n}$ to users A_n and B_n [16].

Then, the received signal at A_n is given as

$$y_{Sk} = \sqrt{\frac{P_S}{1 + d_k^l}} \left(q_{n_1} x_{A_n} + q_{n_2} x_{B_n} \right) \left(\hat{h}_{Sk} + \tilde{h}_{Sk} \right) + n_k, \tag{2}$$

where $k \in \{A_n, B_n\}$, P_S, is the transmit power at S, l is the path-loss exponent, and n_k is the additive white Gaussian noise (AWGN) with $CN(0, \sigma_k^2)$.

Next, the signal to interference plus noise ratio (SINR) at user A_n to decode the own signal x_{A_n} is given by

$$\begin{aligned} \gamma_{SA_n}^{x_{A_n}} &= \frac{P_S \left| h\wedge_{SA_n} \right|^2 |q_{n1}|^2}{P_S \left| h\wedge_{SA_n} \right|^2 |q_{n2}|^2 + P_S \tilde{\sigma}_{SA_n}^2 + \sigma_{A_n}^2 \left(1 + d_{A_n}^l \right)} \\ &= \frac{\rho_S \left| h\wedge_{SA_n} \right|^2 |q_{n1}|^2}{\rho_S \left| h\wedge_{SA_n} \right|^2 |q_{n2}|^2 + \rho_S \tilde{\sigma}_{SA_n}^2 + 1 + d_{A_n}^l}. \end{aligned} \tag{3}$$

Then, the SINR at user B_n to decode signal x_{A_n} is given by

$$\gamma_{SB_n}^{x_{A_n}} = \frac{\rho_S \left| h\wedge_{SB_n} \right|^2 |q_{n1}|^2}{\rho_S \left| h\wedge_{SB_n} \right|^2 |q_{n2}|^2 + \rho_S \tilde{\sigma}_{SB_n}^2 + 1 + d_{B_n}^l}. \tag{4}$$

Next, the SNR at user B_n to decode the own signal x_{B_n} is given by

$$\gamma_{SB_n}^{x_{B_n}} = \frac{\rho_S \left| h\wedge_{SB_n} \right|^2 |q_{n2}|^2}{\rho_S \tilde{\sigma}_{SB_n}^2 + 1 + d_{B_n}^l}, \tag{5}$$

where $\rho_S = P_S / \sigma_k^2$.

In the second time slot (link D2D), user B_n forwards the signal x_{A_n} to user A_n. Then, the signal at D_q user A_n associated with D2D link is given as

$$y_{Bn}^{x_{A_n}} = \sqrt{\frac{P_{Bn}}{1 + d_{BA}^l}} x_{A_n} \left(\hat{h}_{BA} + \tilde{h}_{BA} \right) + n_{A_n}, \tag{6}$$

where P_{Bn} is the transmit power at the user B_n.

In this step, the SNR to decode signal x_{A_n} at the user A_n is given by

$$\gamma_{B_n, A_n}^{x_{A_n}} = \frac{\rho_S \left| h\wedge_{BA} \right|^2}{\rho_S \tilde{\sigma}_{BA}^2 + 1 + d_{C_i}^{\alpha}}, \tag{7}$$

where $\rho_S = P_S / \sigma_k^2 = P_S / \sigma_{B_n}^2$ is the transmit SNR at source.

By using select combining (SC) scheme, the SINR at the user A_n is given by

$$\gamma_{A_n, SC}^{x_{A_n}} = \max \left(\gamma_{SA_n}^{x_{A_n}}, \gamma_{B_n, A_n}^{x_{A_n}} \right). \tag{8}$$

We achieve the first metric SNR, which is necessary to compute outage probability. We will examine outage performance in the next section.

5. Outage Performance

5.1. Outage Probability. The users in discs D_A and D_B are assumed to follow the homogeneous Poisson point process. The users are modeled as independently and identically distributed (i.i.d.) points. The point W_k has probability density functions (PDFs) given as

$$f_{W_{A_n}} \left(\omega_{A_n} \right) = \frac{1}{\pi \left(R_{D_A}^2 - R_{D_B}^2, \right)}, \tag{9}$$

$$f_{W_{B_n}} \left(\omega_{B_n} \right) = \frac{1}{\pi R_{D_B}^2}. \tag{10}$$

The outage probability is defined as the probability that the expected SNR is less than the threshold SNR. In particular, the outage probability of the user B_n can be formulated by

$$P_{B_n} = 1 - \Pr \left(\gamma_{SB_n}^{x_{B_n}} > \gamma_2 \right). \tag{11}$$

Proposition 1. *The closed form expression of the user B_n is given as*

$$P_{B_n} = 1 - \frac{e^{-\theta_2 \left(\rho \tilde{\sigma}_{B_n}^2 + 1 \right)}}{R_{D_B}^2 \theta_2} \left(1 - e^{-\theta_2 R_{D_B}^2} \right). \tag{12}$$

Proof. With the help of (5), (11) can be rewritten as

$$P_{B_n} = 1 - \Pr\left(\left|h\wedge_{SB_n}\right|^2 > \theta_2\rho\tilde{\sigma}^2_{B_n} + \theta_2\left(1 + d^l_{B_n}\right)\right), \quad (13)$$

where $\theta_2 = \gamma_2/\rho|q_{n2}|^2$.

Then, it can be calculated as

$$P_{B_n} = 1 - \frac{2}{R^2_{D_B}}\int_0^{R_{D_B}}\int_{\theta_2\rho\tilde{\sigma}^2_{B_n}+\theta_2\left(1+d^l_{B_n}\right)}^{\infty} re^{-x}dxdr. \quad (14)$$

By following the result reported in [40], we consider the special case $l = 2$, then, we can express P_{B_n} as

$$P_{B_n} = 1 - \frac{2e^{-\theta_2\rho\tilde{\sigma}^2_{B_n}}}{R_{D_B}}\int_0^{R_{D_B}} re^{-\theta_2\left(1+r^2\right)}dr \quad (15)$$

Based on (3.321.4) in [41], we can obtained (12).

The proof is complete.□ □

Next, the outage probability of the user A_n can be expressed as [42]

$$P_{A_n} = \Pr\left(\gamma^{x_{A_n}}_{A_n,SC} < \gamma_1\right). \quad (16)$$

Proposition 2. *The closed form expression of outage probability for the user A_n is given as*

$$P_{A_n} = \left(1 - \frac{2e^{-\theta_1\left(\rho\tilde{\sigma}^2_{SA_n}+1\right)}\left(e^{-\theta_1 R^2_{D_B}} - e^{-\theta_1 R^2_{D_A}}\right)}{\left(R^2_{D_A} - R^2_{D_B}\right)\theta_1}\right) \left(1 - \frac{\rho e^{-\gamma_1\tilde{\sigma}^2_{BA}}}{\left(R^2_{D_A} - R^2_{D_B}\right)\gamma_1}\left(e^{-\gamma_1 R^2_{D_A}/\rho} - e^{-\gamma_1 R^2_{D_A}/\rho}\right)\right). \quad (17)$$

Proof. In this case, we can rewrite (16) as

$$P_{A_n} = \Pr\left(\gamma^{x_{A_n}}_{A_n,SC} < \gamma_1\right) = \underbrace{\Pr\left(\gamma^{x_{A_n}}_{SA_n} < \gamma_1\right)}_{I_1}\underbrace{\Pr\left(\gamma^{x_{A_n}}_{B_n,A_n} < \gamma_1\right)}_{I_2}. \quad (18)$$

With the help of (10), we can rewrite I_1 as

$$I_1 = 1 - \Pr\left(\left|h\wedge_{SA_n}\right|^2 > \theta_1\rho\tilde{\sigma}^2_{SA_n} + \theta_1\left(1 + d^l_{A_n}\right)\right) = 1 - \frac{2}{R^2_{D_A} - R^2_{D_B}}\int_{R_{D_B}}^{R_{D_A}}\int_{\theta_1\rho\tilde{\sigma}^2_{SA_n}+\theta_1\left(1+r^2\right)}^{\infty} re^{-x}dxdr,$$

where $\theta_1 = \gamma_1/\rho(|q_{n1}|^2 - \gamma_1|q_{n2}|^2)$.

Moreover, I_1 can be rewritten as

$$I_1 = 1 - \frac{2e^{-\theta_1\left(\rho\tilde{\sigma}^2_{SA_n}+1\right)}}{R^2_{D_A} - R^2_{D_B}}\int_{R_{D_B}}^{R_{D_A}} re^{-\theta_1 r^2}dr = 1 - \frac{2e^{-\theta_1\left(\rho\tilde{\sigma}^2_{SA_n}+1\right)}}{R^2_{D_A} - R^2_{D_B}}\left(\int_0^{R_{D_A}} re^{-\theta_1 r^2}dr - \int_0^{R_{D_B}} re^{-\theta_1 r^2}dr\right). \quad (20)$$

Similarly, I_1 can be obtained by

$$I_1 = 1 - \frac{e^{-\theta_1\left(\rho\tilde{\sigma}^2_{SA_n}+1\right)}\left(e^{-\theta_1 R^2_{D_B}} - e^{-\theta_1 R^2_{D_A}}\right)}{\theta_1\left(R^2_{D_A} - R^2_{D_B}\right)}. \quad (21)$$

Next, I_2 can be formulated by

$$I_2 = 1 - \Pr\left(|h\wedge_{BA}|^2 > \gamma_1\tilde{\sigma}^2_{BA} + \frac{\gamma_1\left(1 + d^2_{BA}\right)}{\rho}\right) = 1 - \frac{2e^{-\gamma_1\tilde{\sigma}^2_{BA}-\gamma_1/\rho}}{R^2_{D_A} - R^2_{D_B}}\int_{R_{D_B}}^{R_{D_A}} re^{-\gamma_1/\rho r^2}dr. \quad (22)$$

Similarly, I_2 can be expressed as follows:

$$I_2 = 1 - \frac{\rho e^{-\gamma_1\tilde{\sigma}^2_{BA}}}{\left(R^2_{D_A} - R^2_{D_B}\right)\gamma_1}\left(e^{-\gamma_1 R^2_{D_A}/\rho} - e^{-\gamma_1 R^2_{D_A}/\rho}\right). \quad (23)$$

Substituting (21) and (23) into (18), (17) is obtained.

It completes the proof.□ □

6. Throughput

In this section, we want to consider throughput performance. The throughput in delay-limited transmission mode is further investigated by considering outage probability computed in the previous section. At fixed rates R_1, R_2, the throughput can be examined by [13]

$$\mathcal{T} = (1 - P_{A,n})R_1 + (1 - P_{B,n})R_2. \quad (24)$$

7. Numerical Results

In this section, we present the numerical analysis of our NOMA system along with corroboration of analytical results. We set $|q_{n1}|^2 = 0.8$, $|q_{n2}|^2 = 0.2$, $R_{D_A} = 10$m, $R_{D_B} = 5$ m, $\tilde{\sigma}^2 = \tilde{\sigma}^2_{SA_n} = \tilde{\sigma}^2_{SB_n} = \tilde{\sigma}^2_{BA} = 0.001$, $R_1 = 0.5$, and $R_2 = 1$ bit per channel use.

Figure 2 depicts the outage probability versus transmit SNR at node S. As can be seen from Figure 2, the outage performance can be improved significantly at high SNR region. The outage performance of two groups of users is different. The main reason can be explained in two folds. First, different power allocation factors are assigned to two kinds of users. Secondly, signal detection is different when we examine it at

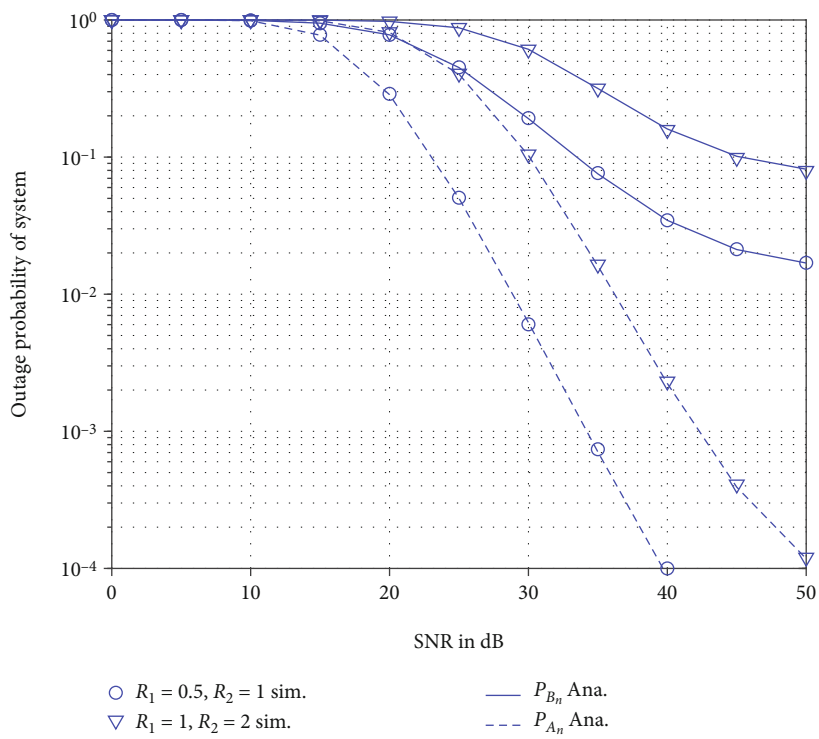

Figure 2: Outage probability of system versus SNR in dB varying $R_1 = R_2$.

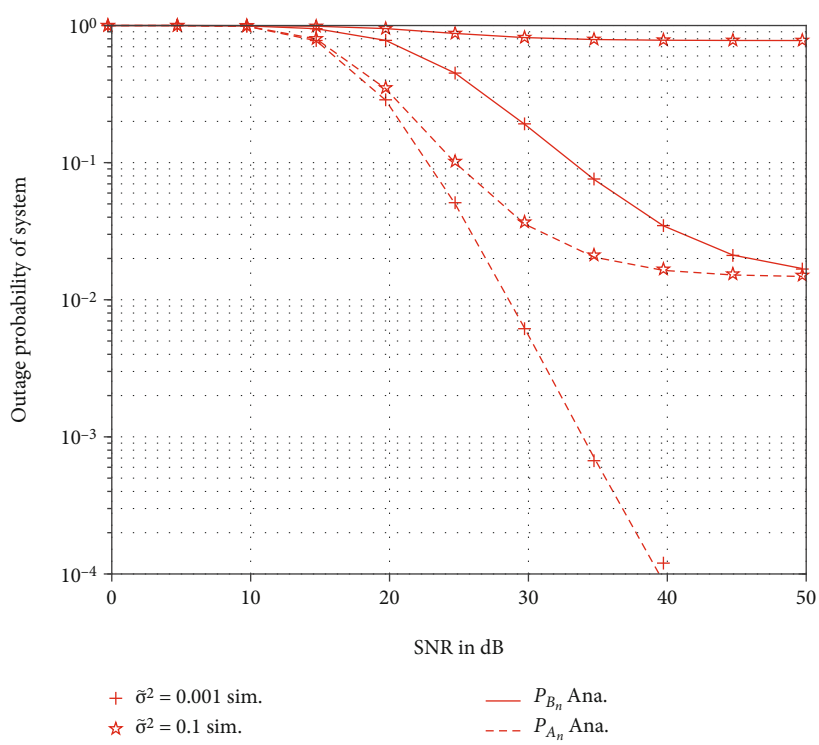

Figure 3: Outage probability of system versus SNR in dB varying $\tilde{\sigma}^2$.

each user B_n, A_n, while A_n is related to D2D link. We can conclude that higher required data rates R_1, R_2, result in worse outage performance.

The impact of channel error level to outage performance can be observed in Figure 3. Especially, the bad performance is seen for the case of $\tilde{\sigma}^2 = 0.1$. That means the exact channel

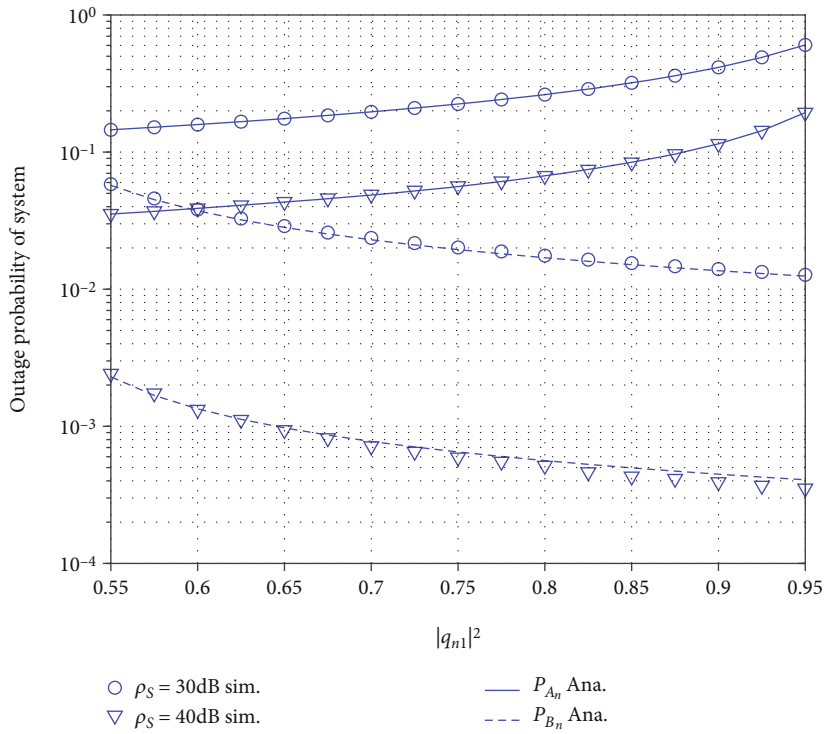

Figure 4: Outage probability of system versus $|q_{n1}|^2$ varying ρ_S.

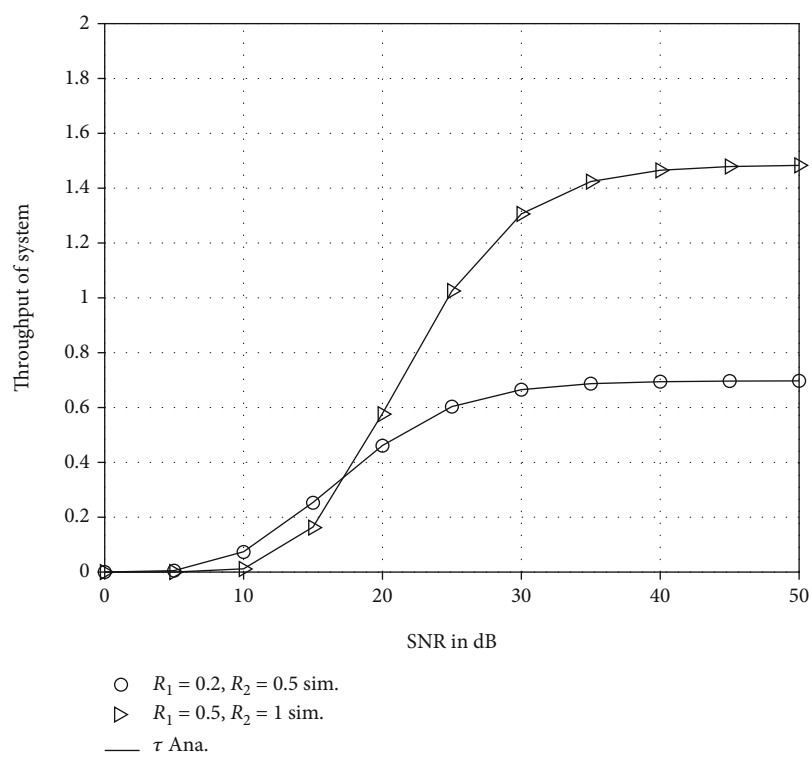

Figure 5: Throughput of system versus SNR in dB varying R_1 and R_2.

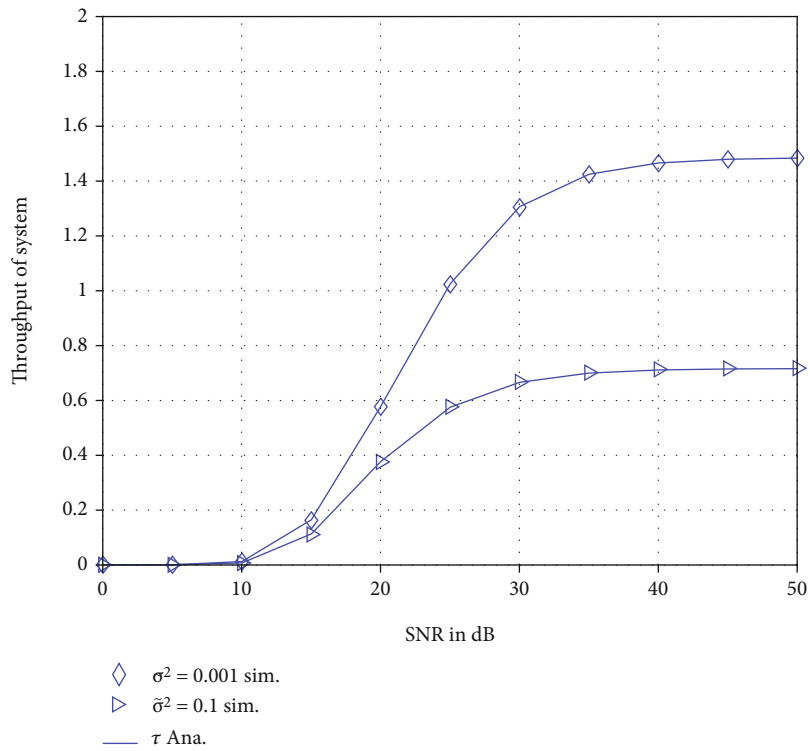

Figure 6: Throughput of system versus SNR in dB varying $\tilde{\sigma}^2$.

estimation plays an important role to keep outage performance at an acceptable level.

In Figure 4, we analyze outage probability versus power allocation $|q_{n1}|^2$ while varying ρ_S. For users in groups A_n and B_n, the best outage probability is achieved by $\rho_S = 40$d B. This shows the impact of base station transmit power and power allocation on the proposed system.

In Figure 5, we observe throughput versus SNR while varying the rates R_1 and R_2. The best throughput performance is achieved by lower R_1 and R_2 rates. Also, the throughput curves approach a ceiling in the high SNR region.

We can see the trend of throughput since it can be improved in the high SNR region, as shown in Figure 6. This figure confirms the role of channel error level to throughput performance. $\tilde{\sigma}^2 = 0.001$ and $\tilde{\sigma}^2 = 0.1$ are two values that result in a big gap of throughput when the value of SNR is greater than 35 dB.

8. Conclusions

We first reviewed previous contributions related to the design of NOMA for two groups of users in this article, and we then show expressions of outage probability for different kinds of users. To provide system performance analysis, we adopted a D2D and stochastic geometry to achieve the closed form expressions. We examine the system parameters to evaluate whether the outage performance can be enhanced. Compared among the cases of channel error levels, the proposed NOMA system can still perform despite the limitation of imperfect channel estimation. It is also worth noting that there may exist ceiling throughput at a high SNR region. In future work, we deploy multiple antennas at the source to further enhance performance at destinations.

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] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-S. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 721–742, 2017.

[2] F. Zhou, Y. Wu, Y.-C. Liang, Z. Li, Y. Wang, and K.-K. Wong, "State of the art, taxonomy, and open issues on cognitive radio networks with NOMA," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 100–108, 2017.

[3] S. M. R. Islam, M. Zeng, and O. A. Dobre, "NOMA in 5G systems: exciting possibilities for enhancing spectral efficiency," *IEEE 5G Tech Focus*, vol. 1, no. 2, pp. 1–6, 2017, http://5g.ieee.org/tech-focus.

[4] W. Hao, M. Zeng, Z. Chu, and S. Yang, "Energy-efficient power allocation in millimeter wave massive MIMO with non-orthogonal multiple access," *IEEE Wireless Communications Letters*, vol. 6, no. 6, pp. 782–785, 2017.

[5] F. Zhou, Y. Wu, R. Q. Hu, Y. Wang, and K.-K. Wong, "Energy-efficient NOMA enabled heterogeneous cloud radio access networks," *IEEE Network*, vol. 32, no. 2, pp. 152–160, 2018.

[6] S. Chen, B. Ren, Q. Gao, S. Kang, S. Sun, and K. Niu, "Pattern division multiple access—a novel nonorthogonal multiple access for fifthgeneration radio networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3185–3196, 2017.

[7] B. Zheng, M. Wen, F. Chen, J. Tang, and F. Ji, "Secure NOMA based full-duplex two-way relay networks with artificial noise against eavesdropping," in *IEEE International Conference on Communications (ICC)*, pp. 1–6, Kansas City, MO, USA, May 2018.

[8] Z. Ding, Y. Liu, J. Choi et al., "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 185–191, 2017.

[9] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Communications Letters*, vol. 19, no. 8, pp. 1462–1465, 2015.

[10] D. T. Do, M. S. Van Nguyen, M. Voznak, A. Kwasinski, and J. N. de Souza, "Performance analysis of clustering car-following V2X system with wireless power transfer and massive connections," *IEEE Internet of Things Journal*, 2021.

[11] D.-T. Do, M.-S. Van Nguyen, T.-A. Hoang, and B. M. Lee, "Exploiting joint base station equipped multiple antenna and full-duplex D2D users in power domain division based multiple access networks," *Sensors*, vol. 19, no. 11, p. 2475, 2019.

[12] A. S. Rajasekaran, O. Maraqa, H. U. Sokun, H. Yanikomeroglu, and S. Al-Ahmadi, "User clustering in mmWave-NOMA systems with user decoding capability constraints for B5G networks," *IEEE Access*, vol. 8, pp. 209949–209963, 2020.

[13] D. T. Do, A. T. Le, and B. M. Lee, "NOMA in cooperative underlay cognitive radio networks under imperfect SIC," *IEEE Access*, vol. 8, pp. 86180–86195, 2020.

[14] D.-T. Do, M.-S. V. Nguyen, F. Jameel, R. Jäntti, and I. S. Ansari, "erformance evaluation of relay-aided CR-NOMA for beyond 5G communications," *IEEE Access*, vol. 8, pp. 134838–134855, 2020.

[15] D.-T. Do, C.-B. Le, and F. Afghah, "Enabling full-duplex and energy harvesting in uplink and downlink of small-cell network relying on power domain based multiple access," *IEEE Access*, vol. 8, pp. 142772–142784, 2020.

[16] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, "Cooperative nonorthogonal multiple access with simultaneous wireless information and power transfer," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 4, pp. 938–953, 2016.

[17] S. Zhang, J. Liu, H. Guo, M. Qi, and N. Kato, "Envisioning device-to-device communications in 6G," *IEEE Network*, vol. 34, no. 3, pp. 86–91, 2020.

[18] J. Zhao, Y. Liu, K. K. Chai, Y. Chen, M. Elkashlan, and J. Alonso-Zarate, "NOMA-based D2D communications: towards 5G," in *2016 IEEE global communications conference (GLOBECOM)*, pp. 1–6, Washington, DC, USA, 2016.

[19] J. Zhao, Y. Liu, K. K. Chai, Y. Chen, and M. Elkashlan, "Joint subchannel and power allocation for NOMA enhanced D2D communications," *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 5081–5094, 2017.

[20] Z. Zhang, Z. Ma, M. Xiao, Z. Ding, and P. Fan, "Full-duplex device-to-device-aided cooperative nonorthogonal multiple access," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4467–4471, 2017.

[21] X. Diao, J. Zheng, Y. Wu, and Y. Cai, "Joint computing resource, power, and channel allocations for D2D-assisted and NOMA-based mobile edge computing," *IEEE Access*, vol. 7, pp. 9243–9257, 2019.

[22] L. Pei, Z. Yang, C. Pan et al., "Energy-efficient D2D communications Underlaying NOMA-based networks with energy harvesting," *IEEE Communications Letters*, vol. 22, no. 5, pp. 914–917, 2018.

[23] Y. Pan, C. Pan, Z. Yang, and M. Chen, "Resource allocation for D2D communications underlaying a NOMA-based cellular network," *IEEE Wireless Communications Letters*, vol. 7, no. 1, pp. 130–133, 2018.

[24] M. M. Selim, M. Rihan, Y. Yang, L. Huang, Z. Quan, and J. Ma, "On the outage probability and power control of D2D underlaying NOMA UAV-assisted networks," *IEEE Access*, vol. 7, pp. 16525–16536, 2019.

[25] J. Kim, I. Lee, and J. Lee, "Capacity scaling for D2D aided cooperative relaying systems using NOMA," *IEEE Wireless Communications Letters*, vol. 7, no. 1, pp. 42–45, 2018.

[26] S. M. A. Kazmi, N. H. Tran, T. M. Ho, A. Manzoor, D. Niyato, and C. S. Hong, "Coordinated device-to-device communication with non-orthogonal multiple access in future wireless cellular networks," *IEEE Access*, vol. 6, pp. 39860–39875, 2018.

[27] H. Sun, Y. Xu, and R. Q. Hu, "A NOMA and MU-MIMO Supported Cellular Network with Underlaid D2D Communications," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, pp. 1–5, Nanjing, China, 2016.

[28] Z. Shi, S. Ma, H. ElSawy, G. Yang, and M. Alouini, "Cooperative HARQ-assisted NOMA scheme in large-scale D2D networks," *IEEE Transactions on Communications*, vol. 66, no. 9, pp. 4286–4302, 2018.

[29] Q. Li, P. Ren, and D. Xu, "Security enhancement and QoS provisioning for NOMA-based cooperative D2D networks," *IEEE Access*, vol. 7, pp. 129387–129401, 2019.

[30] Y. Jiang, L. Wang, H. Zhao, and H. -H. Chen, "Covert communications in D2D Underlaying cellular networks with power domain NOMA," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3717–3728, 2020.

[31] I. Budhiraja, N. Kumar, S. Tyagi, S. Tanwar, and M. Guizani, "SWIPT-enabled D2D communication underlaying NOMA-based cellular networks in imperfect CSI," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 692–699, 2021.

[32] Y. Xu, Z. Liu, Z. Yang, and C. Huang, "Energy-efficient resource allocation with imperfect CSI in NOMA-based D2D networks with SWIPT," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Nanjing, China, April 2021.

[33] J. Wang, X. Song, Y. Ma, and Z. Xie, "Power efficient secure full-duplex SWIPT using NOMA and D2D with imperfect CSI," *Sensors*, vol. 20, no. 18, p. 5395, 2020.

[34] T. Xing, N. Ma, and P. Zhang, "Two-stage power allocation for cooperative NOMA in D2D communications with imperfect CSI," in *2019 11th international conference on wireless communications and signal processing (WCSP)*, pp. 1–6, Xi'an, China, 2019.

[35] J. Wang, X. Song, L. Dong, and X. Han, "Power allocation for D2D aided cooperative NOMA system with imperfect CSI," *Wireless Networks*, 2021.

[36] R. Gupta, S. Tanwar, and N. Kumar, "Secrecy-ensured NOMA-based cooperative D2D-aided fog computing under

imperfect CSI," *Journal of Information Security and Applications*, vol. 59, article 102812, 2021.

[37] L. Tlebaldiyeva, G. Nauryzbayev, S. Arzykulov, Y. Akhmetkaziyev, M. S. Hashmi, and A. M. Eltawil, "A non-ideal NOMA-based mmwave D2D networks with hardware and CSI imperfections," 2020, http://arxiv.org/abs/2004.10506.

[38] D.-T. Do and A.-T. Le, "NOMA based cognitive relaying: transceiver hardware impairments, relay selection policies and outage performance comparison," *Computer Communications*, vol. 146, pp. 144–154, 2019.

[39] Z. Yang, Z. Ding, P. Fan, and G. K. Karagiannidis, "On the performance of non-orthogonal multiple access systems with partial channel information," *IEEE Transactions on Communications*, vol. 64, no. 2, pp. 654–667, 2016.

[40] Y. Ye, Y. Li, D. Wang, and G. Lu, "Power splitting protocol design for the cooperative NOMA with SWIPT," in *2017 IEEE International Conference on Communications (ICC)*, pp. 1–5, Paris, France, May 2017.

[41] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, San Diego, CA, 2000.

[42] H. Dang, M. Van Nguyen, D. Do, H. Pham, B. Selim, and G. Kaddoum, "Joint relay selection, full-duplex and device-to-device transmission in wireless powered NOMA networks," *IEEE Access*, vol. 8, pp. 82442–82460, 2020.