Received 6 November 2023; accepted 26 November 2023. Date of publication 6 December 2023; date of current version 29 December 2023.

Digital Object Identifier 10.1109/OJCOMS.2023.3338775

Sum Capacity-Based Modeling and Secrecy Analysis of MISO-NOMA Cooperative IoT Framework

NAEEM UZ ZAMAN [1], KHALID MUNAWAR [2], MUHAMMAD MOINUDDIN [2], AHMAD KAMAL HASSAN [3], AND UBAID M. AL-SAGGAF [2]

[1]Department of Electrical Engineering, NUST College of Electrical and Mechanical Engineering, Rawalpindi 46000, Pakistan
[2]Center of Excellence in Intelligent Engineering Systems, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[3]Faculty of Electrical Engineering, GIK Institute of Engineering Sciences and Technology, Topi 23460, Pakistan

CORRESPONDING AUTHOR: A. K. HASSAN (e-mail: akhassan@giki.edu.pk)

This research work was funded by Institutional Fund Projects under grant no. (IFPIP: 1990-135-1443). The authors gratefully acknowledge technical and financial support provided by the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

ABSTRACT Non-orthogonal multiple access (NOMA) has emerged as an effective technology, aiding in latency reduction, improving security and reliability, and enhancing the spectral efficiency and capacity in Internet of Things (IoT)-enabled communication systems. In this work, an implementation of cooperative secure multiple-input single-output NOMA IoT framework is proposed and examined in a two-fold manner. First, under the consideration of standalone links, a user selection criteria which relies on the characterization of sum ergodic capacity (SEC) is investigated in the presence of an eavesdropper (ED) and beamforming constraints. Next, using the optimized beamformers, a user selection criteria which relies on the outage probability analysis is performed under cooperative relaying considerations. We demonstrate that our optimization approach achieves reduced capacity and coverage for the ED while maximizing the overall SEC and coverage of the network under multiple network configurations. The proposed optimization solution demonstrates superior performance compared to the benchmarked schemes. Derived closed-form analytical expressions are validated through simulation means.

INDEX TERMS NOMA, IoT, ergodic capacity, eavesdropper, secrecy, SWIPT.

I. INTRODUCTION

DUE TO the rising demand for increased spectral efficiency and huge connectivity for Internet of Things (IoT) applications, non-orthogonal multiple access (NOMA) has proven to be a highly sought-after scheme for future wireless communication systems. However, the unpredictable wireless environment coupled with the existence of eavesdropper (ED) in the network, constitutes a wireless safety risk in NOMA applications. Since nodes in communication networks are energy constrained, security and reliability becomes major concern towards cooperative multi-relay communication systems [1]. To meet the security objectives in the vicinity of multiple EDs in emerging NOMA systems, joint power allocation (PA) and artificial noise (AN) techniques take center stage [2]. Similarly, ensuring security in other NOMA use-cases such as downlink cooperative cognitive radio (CR) networks are essential since these networks enable unlicensed users to access and share spectrum resources in a dynamic and opportunistic manner [3]. Furthermore, NOMA enabled wireless networks employ open broadcasting to serve massive number of nodes while sharing the same resources, any ED in the coverage area can intercept the associated data traffic leading to security risk and users' information leaks [4], [5]. Due to the heightened security concerns within NOMA systems, industry professionals and researchers are collaborating to devise covert NOMA solutions that are both effective and efficient.

A. RELATED WORKS

For secure NOMA transmission, several physical layer security (PLS) techniques have been proposed aiming to reduce

the ED's decoding capabilities while improving the received signal intensity and hence the effective data detection of the target user [6]. The performance of the intended node in a cognitive NOMA enabled IoT relay network under both perfect and imperfect successive interference cancellation (SIC) conditions was evaluated by the authors in [7]. Therein, two iterative approaches were provided for minimization of the outage probability (OP) and maximization of the total ergodic capacity (EC) of NOMA users using a deep neural network technique under real-time environments. The authors of [8] emphasized on the performance analysis of a multi-user (MU) multiple-input single-output (MISO) NOMA IoT framework with simultaneous wireless information and power transfer (SWIPT) protocol. They proposed unique user selection approaches for the energy harvesting (EH) relay, resulting in enhanced system performance in terms of OP. An uplink CR inspired NOMA system was taken into consideration by the authors of [9], in which hybrid SIC and power control schemes integrated with AN scheme were proposed which ensured secure communication for cognitive user without degrading the quality-of-service (QoS) of the intended user. Various physical layer techniques were employed by the authors in [10] for efficient SIC implementation by identifying the channel conditions of an external ED. The authors in [11] evaluated an energy efficient NOMA-assisted secure massive machine-type communication network, in which nodes aspire to convey signals with confidentiality to the target base station (BS) through reliable relays in the locality of a passive ED. Adopting joint relay and PA levels, authors maximized the secrecy energy efficiency (EE).

For analysis of secrecy EC, a novel cooperative NOMA, i.e., C-NOMA system was proposed in [12], where the source was considered to actively provide jamming signals while the relay forwards, hence improving the security of the intended node. The authors of [13] suggested a secure communications architecture for MU-NOMA-IoT downlink system, where each user is considered as a potential ED and by making use of efficient resource allocation, authors presented an efficient method to enhance the sum secrecy rate while maintaining user QoS and power constraints. In [14], the secrecy OP of an AN-aided massive multiple-input multiple-output (MIMO) NOMA network was examined with imperfect channel state information (CSI) consideration. The authors also proposed optimization algorithms for maximization of EE and minimization of secrecy EC. Authors in [15] employed covariance shaping technique to simultaneously optimize the transmit and receive beamformers under statistical CSI considerations only. The authors of [16] aimed on developing a NOMA-enabled secure industrial IoT (IIoT) network for untrusted resource-limited devices by effective optimization of the resources utilizing Karush-Kuhn-Tucker points. For maximizing the minimal secrecy EC among devices, a joint optimization problem was developed. The authors of [17] presented a joint PLS analysis of secrecy OP and EC for cognitive IIoT networks in which nodes rely on the primary spectrum using space-time block coding in conjunction with NOMA in cognitive mode to achieve high spectrum efficiency. The analysis on SWIPT protocol based NOMA framework was considered by the authors in [18], wherein they developed three different techniques for transmit antenna selection (TAS) while keeping the complexity into consideration. Authors in [19] considered a low complexity unified resource orchestration framework for jointly performing the user association and optimal PA in NOMA equipped heterogeneous wireless network where they relied on contract theory and reinforcement learning (RL) to cater for the incompleteness in instantaneous CSI.

Authors in [20] introduced both conventional transmit beamforming and intelligent reflecting surface (IRS) enabled beamforming techniques integrated with NOMA to tackle the security threats from EDs. In [21], authors considered simultaneous transmitting and reflecting reconfigurable intelligent surface (STAR-RIS) with NOMA where an AN aided secure transmission technique was developed for the optimization of AN model and reconfigurable intelligent surface parameters, to achieve better secrecy performance with lower AN power. In [22], authors evaluated a downlink MISO-NOMA network using the STAR-RIS to enhance the secrecy performance. Authors proposed a secure transmission architecture using a joint active and passive beamforming optimization with the optimum PA. A hybrid PA and aerial jamming technique were developed by the authors in [23] considering a unmanned aerial vehicle (UAV) assisted NOMA network with a malicious ED for performance analysis of both LoS and non-LoS channels. The mobile edge computing (MEC) system for an UAV based NOMA system was presented by authors in [24] as a secure communication strategy for a flying ED. The proposed approach ensured a minimal level of security computation for each ground user while maximizing the average security computation capability of the system using sequential convex approximation and block coordinate descent methods. A NOMA equipped airborne vehicular ad-hoc framework was presented in [25] while taking into account high-altitude platforms, UAVs, and vehicles. Authors therein developed a non-convex maximization problem for the downlink transmission rate by effectively optimizing UAV height and sub-carrier allocation.

The authors of [26] addressed the PLS challenges for a 5G NOMA system with a more effective near-end user in the presence of an ED. The authors proposed optimal PA criteria under the restraint of user's data rate and total power consumption. In [27], both code and power domain NOMA systems were investigated with the PLS concerns wherein the secrecy OP was characterized using homogeneous Poisson point processes to differ between the target users and EDs. Power line communication (PLC) networks with NOMA support were studied by the authors of [28] to analyze the secrecy OP for internal and external EDs addressing the PLS challenges. For the considered system, the PLC channel was modeled by correlated log-normal fading while the noise was modeled by employing the Bernoulli-Gaussian random

process. In [29], an optimization framework for enhancing the PLS of the NOMA ambient backscatter IoT system was proposed with the goal of increasing security by efficient optimization of the reflection coefficient and BS's transmit power for the backscatter node. In [30], with the existence of passive EDs, various approaches for improving the downlink PLS performance of a half-duplex C-NOMA network were proposed using AN for analysis of secrecy OP. The authors developed an efficient power allocation coefficients (PACs) method to minimize the secrecy OP for improving the PLS performance even further. Authors in [31] presented a secure transmission method using inter-user interference for an IRS-assisted NOMA system without knowledge of ED's CSI in order to improve PLS. The authors developed a non-convex alternating optimization framework in order to degrade the signal-to-interference-plus-noise ratio (SINR) of the ED. The authors of [32] employed indefinite quadratic form approach to provide exact closed-form formulations for the SINR statistics of MU-MIMO systems over Rayleigh based fading channels, such as EC and leakage rate.

In [33], authors investigated hybrid SIC decoding and PLS in a NOMA assisted MEC framework in the presence of ED. A RL based approach for latency reduction was developed where combined computing resource allocation, task assignment, and PA were taken into consideration in order to address the PA challenges for NOMA and orthogonal multiple access offloading schemes. Several research directions at the cross-roads of NOMA and new generation of communication networks are given in [34] which highlight potentials and challenges of working in this area.

B. MAJOR CONTRIBUTIONS

Most of the works mentioned above are related to NOMA enabled networks focusing on performance and secrecy analysis. To the best of our knowledge, no work has been performed on optimization of beamformers to simultaneously maximize the sum ergodic capacity (SEC) and minimize the EC of ED. Also, the SEC based optimized beamformers are not utilized in performance measures of other KPIs such OP. These are the areas that are addressed in this work. The significant contributions of this work are as follows.

1) Under standalone and non-relaying configuration, closed-form analytical expressions are derived for the EC of all user equipments (UEs), IoT device and ED. Using the closed-form expressions, a new user selection mechanism is developed for the cooperative transmission.
2) Employing the sequential quadratic programming approach, an optimization problem is formulated with beamforming vectors as optimization variables which yield maximized SEC and minimized EC for the ED.
3) Within the framework of a cooperative relaying mechanism and leveraging optimized beamforming vectors, a closed-form expression for OP is presented, accompanied by a user selection criterion based on this metric.

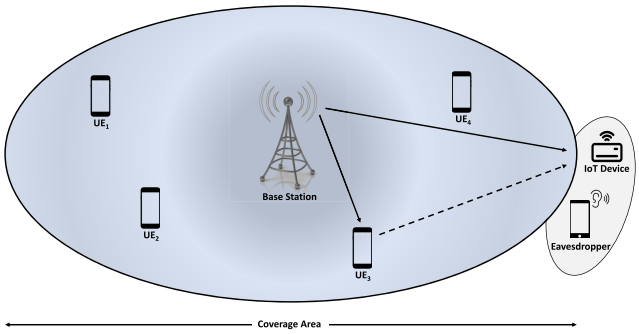


FIGURE 1. Secure downlink MU-MISO-NOMA cooperative IoT framework.

C. ORGANIZATION OF THE PAPER

The remainder of the paper is organized as follows. Section II describes the considered system model and the formulations for signal-to-noise ratio (SNR) and SINR at each UE, IoT device and ED. In Section III, the algorithm for user selection mechanism and the characterization of SEC are presented for non-relaying setup. Section IV discusses the considered optimization problem for improvement of SEC. In Section V, OP characterization for cooperative relaying and relevant user selections schemes are discussed. Validation and analysis of results is given in Section VI. Lastly, the conclusion drawn from the analysis is presented in Section VII.

II. SYSTEM MODEL

For downlink transmissions, MU-MISO-NOMA IoT system is shown in Figure 1, where multiple UEs, an IoT device and an ED capable of wiretapping the information of other nodes is deployed randomly. The BS consists of N transmit antennas while the end nodes are equipped with single antenna element. Both the IoT device and ED are located in close proximity to the cell-edge with non-zero probability that the message of IoT device may be decoded by the ED. The channels from BS to UE, IoT device, and ED are referred to as $\mathbf{h}_u$, $\mathbf{h}_d$, and $\mathbf{h}_e$, respectively. Similarly, the channels involved in relaying from UE to IoT device, and UE to ED are denoted by $\mathbf{h}_{ud}$ and $\mathbf{h}_{ue}$, respectively. For all the wireless channels, Rayleigh based fading is considered having zero mean. Besides, n_u and n_d denote the zero mean additive white Gaussian noise (AWGN) for UE and IoT device, respectively, with noise power as σ_u^2 and σ_d^2. Furthermore, the relaying channel gain is given by the expression $\mathbb{E}[|h_{ud}|^2] = \frac{\beta}{(d_{UE\to D}/d_o)^{\epsilon}}$. Here, β represent the attenuation in signal's power, $d_{UE\to D}$ is the distance from UE to IoT device, d_o is the reference distance and ϵ is the path-loss exponent.

The nodes are designed to utilize hybrid time-switching and power-splitting (TS/PS) mechanism employing SWIPT

TABLE 1. List of notations.

Parameters	Description
α	Time switching factor
α_u, α_d	The power coefficient for the uth UE and the dth IoT device, respectively
$\sigma_u^2, \sigma_d^2, \sigma_e^2$	Variance of the channel noise for the uth UE, dth IoT device, and ED, respectively
$\sigma_{ID_u}^2, \sigma_{ID_d}^2, \sigma_{ID_e}^2$	The variance of noise due to information decoding for the uth UE, dth IoT device, and ED, respectively
η	Coefficient for the conversion of energy during the process of information decoding
ρ	Power splitting factor
$\mathbf{d}_{i\rightarrow j}$	Distance from i to j
$\mathbf{h}_u$, $\mathbf{h}_d$, $\mathbf{h}_e$	Rayleigh fading links of uth UE, dth IoT device, and ED, respectively
$\mathbf{h}_{ud}$, $\mathbf{h}_{ue}$	Exponentially distributed links from relaying UE to IoT device, and relaying UE to ED, respectively
$\|\|\mathbf{h}\|\|^2$	Norm-2 of vector $\mathbf{h}$
n_u, n_d, n_e	Noise power density of antennas
$n_{ID_u}, n_{ID_d}, n_{ID_d}$	The noise power density concerning information decoding
P_S	BS total transmit power
$\mathbf{R}_u$, $\mathbf{R}_d$, $\mathbf{R}_e$	The correlation matrix corresponding to uth UE, dth IoT device and ED, respectively
$\mathbf{w}_u$, $\mathbf{w}_d$	Beamformers of uth UE and dth IoT device, respectively
x_u, x_d	The data signal sent by the uth UE and dth IoT device, respectively

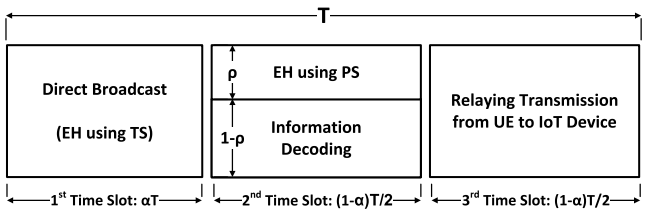


FIGURE 2. SWIPT based hybrid TS/PS mechanism.

protocol in combination with the SIC as shown in Figure 2. The TS factor T is divided into three slots wherein the first time slot αT is used for harvesting energy from the BS. The second time $(1-\alpha)\ T/2$ is utilized in combination with PS factor ρ for the EH purposes, while the rest PS factor, i.e., $(1-\rho)$ is used for information processing during the same time slot. The last time slot $(1-\alpha)\ T/2$ is utilized during the relaying phase where relaying UE exploits the energy that it harvested during the first two time slots. Both TS and PS time parameters range from $0<\alpha<1$ and $0<\rho<1$, respectively. The selection combining (SC) technique comes into play at the IoT device where both the direct and the relayed signals are combined and the one with stronger signal strength is then decoded. Now, for the SWIPT protocol described in Figure 2 and using framework in [35], the signaling overhead of the terminal nodes in our system model is found out as $(1-\alpha T)(U+D+1)/2$. Next, the SNR/SINR expressions are elaborated in the following stages.

A. DIRECT TRANSMISSION DURING FIRST TIME SLOT αT

During αT duration, information is broadcast from BS through N transmit antennas to UEs, IoT device, and ED with different PACs while fulfilling the notion of NOMA, i.e., $\sum_{k=1}^{U}\alpha_k+\sum_{d=1}^{D}\alpha_d=1$, where α_k and α_d denote the allocated PAC of UEs and IoT devices, respectively. During the first time slot αT, the information received at UE and IoT device is divided as follows.

1) FROM BS TO UE

The signal transmitted through N BS antennas and received by the UE is expressed as

$$Y_u=\sqrt{\alpha_u P_S}x_u\mathbf{h}_u^H\mathbf{w}_u+\sum_{k=1;k\neq u}^{U}\sqrt{\alpha_k P_S}x_k\mathbf{h}_u^H\mathbf{w}_k+\sum_{d=1}^{D}\sqrt{\alpha_d P_S}x_d\mathbf{h}_u^H\mathbf{w}_d+n_u, \quad (1)$$

where the first term denotes uth UE's message signal, whereas second and the third terms are due to the interference from other UEs and the IoT devices, respectively. The message of intended UE, other UEs and IoT devices are represented by x_u, x_k, and x_d, respectively. The messages are associated with their respective beamformers, i.e., $\mathbf{w}_u$, $\mathbf{w}_k$, and $\mathbf{w}_d$. The last term n_u represents AWGN having zero-mean and variance σ_u^2.

Utilizing the hybrid TS/PS mechanism, the expression of total harvested energy at the UE linked with wireless channel $\mathbf{h}_u$ is written as

$$E_u=||\mathbf{h}_u^H||^2_{\sum_{k=1}^{U}\mathbf{w}_k\mathbf{w}_k^H(\eta P_S\alpha T+\eta\rho P_S(1-\alpha)T/2)}, \quad (2)$$

where the quadratic formulation [15] is utilized to achieve (2) and η represents the energy conversion coefficient ranging from $0<\eta<1$.

At this stage, the SIC mechanism comes into play at the UE. By adopting the NOMA superposition principle, firstly the message of all other nodes are decoded and then by subtracting the decoded message of all the other nodes, the message of intended UE is decoded. Hence, the SINR at UE for reading the message of intended IoT device is given by

$$\gamma_u^{xD}=\frac{S_{\gamma_u^{xD}}}{I_{\gamma_u^{xD}}+N_{\gamma_u^{xD}}}=\frac{S^1_{\gamma_u^{xD}}}{I^1_{\gamma_u^{xD}}+N_{\gamma_u^{xD}}}, \quad (3)$$

where the desired message to decode is $S_{\gamma_u^{xD}}=\overline{\rho}\alpha_d P_S|\mathbf{h}_u^H\mathbf{w}_d|^2$, and $\overline{\rho}=1-\rho$. The interference and noise terms are given as,

$$I_{\gamma_u^{xD}}=\overline{\rho}P_S\left[\sum_{k=1}^{U}\alpha_k\left|\mathbf{h}_u^H\mathbf{w}_k\right|^2+\sum_{l=1,l\neq d}^{D}\alpha_l\left|\mathbf{h}_u^H\mathbf{w}_l\right|^2\right], \quad (4)$$

$$N_{\gamma_u^{xD}}=\overline{\rho}\sigma_u^2+\sigma_{ID_u}^2 \quad (5)$$

Finally, using the quadratic formulation and whitened transformation, $S^1_{\gamma_u^{xD}}=||\overline{\mathbf{h}}_u^H||^2_{\mathbf{A}\overline{\rho}\alpha_d P_S}$ and $I^1_{\gamma_u^{xD}}=||\overline{\mathbf{h}}_u^H||^2_{\mathbf{B}\overline{\rho}P_S\sum_{k=1}^{U}\alpha_k}+||\overline{\mathbf{h}}_u^H||^2_{\mathbf{C}\overline{\rho}P_S\sum_{l=1,l\neq d}^{D}\alpha_l}$. The relationship for whitened transformation is given by, $\overline{\mathbf{h}}_u=\mathbf{R}_u^{-\frac{H}{2}}\mathbf{h}_u$, where $\mathbf{h}_u\sim\mathcal{CN}(0,\mathrm{R}_u)\Rightarrow\overline{\mathbf{h}}_u\sim\mathcal{CN}(0,\mathrm{I})$.

Moreover, $\mathbf{A}=\mathbf{R}_u^{\frac{1}{2}}\mathbf{w}_d\mathbf{w}_d^H\mathbf{R}_u^{\frac{H}{2}}$, $\mathbf{B}=\mathbf{R}_u^{\frac{1}{2}}\sum_{k=1}^{U}\mathbf{w}_k\mathbf{w}_k^H\mathbf{R}_u^{\frac{H}{2}}$, and $\mathbf{C}=\mathbf{R}_u^{\frac{1}{2}}\sum_{l=1,l\neq d}^{D}\mathbf{w}_l\mathbf{w}_l^H\mathbf{R}_u^{\frac{H}{2}}$. Here, $\mathbf{A}$ represents the weight matrix for the desired message signal, while $\mathbf{B}$ and $\mathbf{C}$ are termed as the interference weight matrices corresponding to the UEs and all other IoT devices except the intended one, respectively.

2) FROM BS TO IOT DEVICE

The SNR expression at IoT device during the direct transmission from the BS is characterized with the premise that IoT device is allocated with higher transmit power, and SIC has already been implemented at all other nodes. Therefore, interference at the IoT device due to all other nodes is considered as noise. Thus, to decode its own message, the SNR at IoT device is written as

$$\gamma_d = \frac{S_{\gamma_d}}{N_{\gamma_d}} = \frac{S^1_{\gamma_d}}{N^1_{\gamma_d}}, \tag{6}$$

where the IoT device's signal is $S_{\gamma_d} = \alpha_d P_S|\mathbf{h}_d^H\mathbf{w}_d|^2$ and the noise term is given by, $N_{\gamma_d} = \sum_{k=1}^{U}\alpha_k P_S|\mathbf{h}_d^H\mathbf{w}_k|^2 + \sum_{l=1,l\neq d}^{D}\alpha_l P_S|\mathbf{h}_d^H\mathbf{w}_l|^2 + \sigma_d^2 + \sigma_{ID_d}^2$. Using the same approach as employed for (3), the expression results in, $S^1_{\gamma_d} = ||\bar{\mathbf{h}}_d^H||^2_{\hat{\mathbf{A}}\alpha_d P_S}$ and $N^1_{\gamma_d} = ||\bar{\mathbf{h}}_d^H||^2_{\hat{\mathbf{B}}P_S\sum_{k=1}^{U}\alpha_k} + ||\bar{\mathbf{h}}_d^H||^2_{\hat{\mathbf{C}}P_S\sum_{l=1,l\neq d}^{D}\alpha_l} + \sigma_d^2 + \sigma_{ID_d}^2$. The whitened transformation in this case becomes, $\bar{\mathbf{h}}_d = \mathbf{R}_d^{-\frac{H}{2}}\mathbf{h}_d$, $\mathbf{h}_d \sim \mathcal{CN}(0,\mathrm{R}_d) \Rightarrow \bar{\mathbf{h}}_d \sim \mathcal{CN}(0,\mathrm{I})$, and the matrices are defined as $\hat{\mathbf{A}}=\mathbf{R}_d^{\frac{1}{2}}\mathbf{w}_d\mathbf{w}_d^H\mathbf{R}_d^{\frac{H}{2}}$, $\hat{\mathbf{B}}=\mathbf{R}_d^{\frac{1}{2}}\sum_{k=1}^{U}\mathbf{w}_k\mathbf{w}_k^H\mathbf{R}_d^{\frac{H}{2}}$ and $\hat{\mathbf{C}}=\mathbf{R}_d^{\frac{1}{2}}\sum_{l=1,l\neq d}^{D}\mathbf{w}_l\mathbf{w}_l^H\mathbf{R}_d^{\frac{H}{2}}$, where $\hat{\mathbf{A}}$ is weight matrix for desired message signal while the rest are noise weight matrices.

3) FROM BS TO ED

The information received at ED is written as

$$Y_e = \sum_{k=1}^{U}\sqrt{\alpha_k P_S}x_k\mathbf{h}_e^H\mathbf{w}_k + \sum_{d=1}^{D}\sqrt{\alpha_d P_S}x_d\mathbf{h}_e^H\mathbf{w}_d + n_e, \tag{7}$$

where the first and second terms are message signals of UEs and IoT devices, respectively which ED taps from the BS.

Now, it is assumed that the ED is capable of differentiating the messages of UEs and IoT device, therefore, the SINR for ED to eavesdrop the information of UE in close proximity is expressed as

$$\gamma_e^{xU} = \frac{S_{\gamma_e^{xU}}}{I_{\gamma_e^{xU}} + N_{\gamma_e^{xU}}} = \frac{S^1_{\gamma_e^{xU}}}{I^1_{\gamma_e^{xU}} + N_{\gamma_e^{xU}}}, \tag{8}$$

where $S_{\gamma_e^{xU}} = \alpha_u P_S|\mathbf{h}_e^H\mathbf{w}_u|^2$ and $I_{\gamma_e^{xU}} = \sum_{k=1,k\neq u}^{U}\alpha_k P_S|\mathbf{h}_e^H\mathbf{w}_k|^2 + \sum_{l=1}^{D}\alpha_l P_S|\mathbf{h}_e^H\mathbf{w}_l|^2$, $N_{\gamma_e^{xU}} = \sigma_e^2 + \sigma_{ID_e}^2$. Furthermore, $S^1_{\gamma_e^{xU}} = ||\bar{\mathbf{h}}_e^H||^2_{\tilde{\mathbf{A}}\alpha_u P_S}$ and $I^1_{\gamma_e^{xU}} = ||\bar{\mathbf{h}}_e^H||^2_{\tilde{\mathbf{B}}P_S\sum_{k=1,k\neq u}^{U}\alpha_k} + ||\bar{\mathbf{h}}_e^H||^2_{\tilde{\mathbf{C}}P_S\sum_{l=1}^{D}\alpha_l}$ and $\bar{\mathbf{h}}_e = \mathbf{R}_e^{-\frac{H}{2}}\mathbf{h}_e$, and $\mathbf{h}_e \sim \mathcal{CN}(0,\mathrm{R}_e) \Rightarrow \bar{\mathbf{h}}_e \sim \mathcal{CN}(0,\mathrm{I})$. Moreover, $\tilde{\mathbf{A}}=\mathbf{R}_e^{\frac{1}{2}}\mathbf{w}_u\mathbf{w}_u^H\mathbf{R}_e^{\frac{H}{2}}$, $\tilde{\mathbf{B}}=\mathbf{R}_e^{\frac{1}{2}}\sum_{k=1,k\neq u}^{U}\mathbf{w}_k\mathbf{w}_k^H\mathbf{R}_e^{\frac{H}{2}}$, and $\tilde{\mathbf{C}}=\mathbf{R}_e^{\frac{1}{2}}\sum_{l=1}^{D}\mathbf{w}_l\mathbf{w}_l^H\mathbf{R}_e^{\frac{H}{2}}$.

Similarly, to wiretap information of IoT device at ED, the SINR becomes

$$\gamma_e^{xD} = \frac{S_{\gamma_e^{xD}}}{I_{\gamma_e^{xD}} + N_{\gamma_e^{xD}}} = \frac{S^1_{\gamma_e^{xD}}}{I^1_{\gamma_e^{xD}} + N_{\gamma_e^{xD}}}, \tag{9}$$

where $S_{\gamma_e^{xD}} = \alpha_d P_S|\mathbf{h}_e^H\mathbf{w}_d|^2$ and $I_{\gamma_e^{xD}} = \sum_{k=1}^{U}\alpha_k P_S|\mathbf{h}_e^H\mathbf{w}_k|^2 + \sum_{l=1,l\neq d}^{D}\alpha_l P_S|\mathbf{h}_e^H\mathbf{w}_l|^2$, $N_{\gamma_e^{xD}} = \sigma_e^2 + \sigma_{ID_e}^2$. Hence, $S^1_{\gamma_e^{xD}} = ||\bar{\mathbf{h}}_e^H||^2_{\tilde{\mathbf{A}}\alpha_d P_S}$ and $I^1_{\gamma_e^{xD}} = ||\bar{\mathbf{h}}_e^H||^2_{\tilde{\mathbf{B}}P_S\sum_{k=1}^{U}\alpha_k} + ||\bar{\mathbf{h}}_e^H||^2_{\tilde{\mathbf{C}}P_S\sum_{l=1,l\neq d}^{D}\alpha_l}$. Moreover, $\tilde{\mathbf{A}}=\mathbf{R}_e^{\frac{1}{2}}\mathbf{w}_d\mathbf{w}_d^H\mathbf{R}_e^{\frac{H}{2}}$, $\tilde{\mathbf{B}}=\mathbf{R}_e^{\frac{1}{2}}\sum_{k=1}^{U}\mathbf{w}_k\mathbf{w}_k^H\mathbf{R}_e^{\frac{H}{2}}$, and $\tilde{\mathbf{C}}=\mathbf{R}_e^{\frac{1}{2}}\sum_{l=1,l\neq d}^{D}\mathbf{w}_l\mathbf{w}_l^H\mathbf{R}_e^{\frac{H}{2}}$.

B. RELAYING TRANSMISSION DURING $(1-\alpha)T/2$

During relaying transmission, the UE forwards information to the IoT device, which can also be wiretapped by the ED. The information received from relaying UE at IoT device and ED is discussed in the following subsections.

1) UE TO IoT DEVICE

In this time slot, using the harvested energy, the relaying UE forwards the information toward IoT device. Therefore, we express the SINR received at IoT device as

$$\gamma_{ud} = |h_{ud}|^2||\mathbf{h}_u||^2_{\frac{\zeta\sum_{k=1}^{U}\mathbf{w}_k\mathbf{w}_k^H}{\sigma_e^2+\sigma_{ID_e}^2}}, \tag{10}$$

where $\zeta = \eta P_S(\frac{2\alpha}{1-\alpha} + \rho)$.

Since, the information at IoT device is received in two stages, hence a tractable SC technique is used. Thus, the expression of SINR becomes

$$\gamma_{d_{SC}}^{xD} = \max(\gamma_d, \gamma_{ud}). \tag{11}$$

2) UE TO ED

Similarly, while relaying transmission, ED may listen to the message signal of an IoT device. As a result, the information obtained from UE at ED is written as follows:

$$Y_{ue} = \sqrt{\alpha_u}\hat{x_d}h_{ue} + n_e + n_{ID_e}, \tag{12}$$

where $\hat{x_d}$ is the re-encoded version of x_d.

Now, the SINR received at ED to listen the message signal of IoT device relayed through UE to the ED's channel is written as

$$\gamma_{ue}^{xD} = |h_{ue}|^2||\mathbf{h}_u||^2_{\frac{\zeta\sum_{k=1}^{U}\mathbf{w}_k\mathbf{w}_k^H}{\sigma_e^2+\sigma_{ID_e}^2}}. \tag{13}$$

At this stage, ED is decoding message of IoT device through BS and UE in two stages, therefore the same SC technique is utilized here resulting in SINR expression as

$$\gamma_{e_{SC}}^{xD} = \max\left(\gamma_e^{xD}, \gamma_{ue}^{xD}\right). \tag{14}$$

III. CHARACTERIZATION OF SEC AND USER SELECTION MECHANISM WITHOUT RELAYING

In this section, we assume perfect SIC and formulate the analytical EC expressions for the UEs, IoT devices and the ED in a standalone configuration. The SEC expressions are obtained using individual EC of each node except the EC of ED. The formulation is later used in the development of a user selection strategy.

A. CHARACTERIZATION OF SEC

Due to perfect SIC mechanism at the UE, the SNR expression to decode its own message is

$$\gamma_u^{xU} = \frac{S_{\gamma_u^{xU}}}{N_{\gamma_u^{xU}}} = c_1 ||\bar{\mathbf{h}}_u^H||_{\mathbf{A}}^2, \tag{15}$$

where $S_{\gamma_u^{xU}} = \overline{\rho}\alpha_u P_S |\mathbf{h}_u^H \mathbf{w}_u|^2$ and $N_{\gamma_u^{xU}} = \overline{\rho}\sigma_u^2 + \sigma_{ID_u}^2$. For characterization of EC, the second equality is obtained by transformation approach where, $c_1 = (\frac{\overline{\rho}\alpha_u P_S}{\overline{\rho}\sigma_u^2 + \sigma_{ID_u}^2})$ and the weight matrix is defined as $\mathbf{A}{=}\mathbf{R}_u^{\frac{1}{2}} \mathbf{w}_u \mathbf{w}_u^H \mathbf{R}_u^{\frac{H}{2}}$.

Hence, EC is characterized as in [32, Prop. 2] and the analytical expression for the EC at the UE becomes

$$\begin{aligned} EC_u &= \mathbb{E}\left[log_2\left(1 + \bar{\mathrm{h}}_u^H \mathbf{A} \bar{\mathrm{h}}_u\right)\right], \\ &= \frac{1}{\ln(2)}\left[\sum_{u=1}^{U} \frac{\lambda_u^{U-1}}{\prod_{\substack{y=1 \\ y\neq u}}^{U} (\lambda_u - \lambda_y)} e^{\frac{1}{\lambda_u}} E_1\left(\frac{1}{\lambda_u}\right) \mathrm{u}(\lambda_u)\right]. \end{aligned} \tag{16}$$

where E_1 is the exponential integral function and λ_u is the uth eigenvalue of the matrix $\mathbf{A}$.

Similarly, the SNR expression under perfect SIC condition for the IoT device becomes

$$\gamma_{d_{SIC}} = \frac{S_{\gamma_d}}{N_{\gamma_d}^2} = c_2 \left\| \bar{\mathbf{h}}_d^H \right\|_{\hat{\mathbf{A}}}^2, \tag{17}$$

where $N_{\gamma_d} = \sigma_d^2 + \sigma_{ID_d}^2$ and $c_2 = (\frac{\alpha_d P_S}{\sigma_d^2 + \sigma_{ID_d}^2})$. Therefore, the analytical expression of the EC for IoT device can be written as

$$\begin{aligned} EC_d &= \mathbb{E}\left[log_2\left(1 + \bar{\mathrm{h}}_d^H \hat{\mathbf{A}} \bar{\mathrm{h}}_d\right)\right], \\ &= \frac{1}{\ln(2)}\left[\sum_{d=1}^{D} \frac{\hat{\lambda}_d^{D-1}}{\prod_{\substack{y=1 \\ y\neq d}}^{D} (\hat{\lambda}_d - \hat{\lambda}_y)} e^{\frac{1}{\hat{\lambda}_d}} E_1\left(\frac{1}{\hat{\lambda}_d}\right) \mathrm{u}\left(\hat{\lambda}_d\right)\right]. \end{aligned} \tag{18}$$

Here, $\hat{\lambda}_d$ is the dth eigenvalue of the matrix $\hat{\mathbf{A}}$.

Now, we assume that ED is trying to wiretap the information of IoT device and SIC is being perfectly employed at the ED, hence the SNR expression becomes

$$\gamma_{e_{SIC}}^{xD} = \frac{S_{\gamma_e^{xD}}}{N_{\gamma_e^{xD}}}, = c_2 \left\| \bar{\mathbf{h}}_e^H \right\|_{\tilde{\mathbf{A}}}^2. \tag{19}$$

Algorithm 1 User Selection Mechanism Based on EC

Input: Coordinates of UEs, IoT device and ED, simulation parameters
Output: Selection of uth UE as a relay
while UEs > 0 **do**
1. Compute $\mathbf{EC}_{\{UE_{1\ldots U}\}} = \{EC_{UE_1}, EC_{UE_2}, \ldots, EC_{UE_U}\}$
2. Index $=$ arg max $\left(\mathbf{EC}_{\{UE_{1\ldots U}\}}\right)$
3. $U_s =$ UE(Index)

end

Hence, using the same approach, the analytical expression of the EC for the ED is written as

$$\begin{aligned} EC_e &= \mathbb{E}\left[log_2\left(1 + \bar{\mathrm{h}}_e^H \tilde{\mathbf{A}} \bar{\mathrm{h}}_e\right)\right], \\ &= \frac{1}{\ln(2)}\left[\sum_{e=1}^{E} \frac{\tilde{\lambda}_e^{E-1}}{\prod_{\substack{y=1 \\ y\neq e}}^{E} \left(\tilde{\lambda}_e - \tilde{\lambda}_y\right)} e^{\frac{1}{\tilde{\lambda}_e}} E_1\left(\frac{1}{\tilde{\lambda}_e}\right) \mathrm{u}\left(\tilde{\lambda}_e\right)\right]. \end{aligned} \tag{20}$$

Here, $\tilde{\lambda}_k$ is the kth eigenvalue of the matrix $\tilde{\mathbf{A}}$.

Hence, utilizing (16) and (18), we achieve the SEC expression which is written as

$$\begin{aligned} SEC &= EC_u + EC_d \\ &= \frac{1}{\ln(2)}\left[\sum_{u=1}^{U} \frac{\lambda_u^{U-1}}{\prod_{\substack{y=1 \\ y\neq u}}^{U} (\lambda_u - \lambda_y)} e^{\frac{1}{\lambda_u}} E_1\left(\frac{1}{\lambda_u}\right) \mathrm{u}(\lambda_u) \right. \\ &\quad \left. + \sum_{d=1}^{D} \frac{\hat{\lambda}_d^{D-1}}{\prod_{\substack{y=1 \\ y\neq d}}^{D} \left(\hat{\lambda}_d - \hat{\lambda}_y\right)} e^{\frac{1}{\hat{\lambda}_d}} E_1\left(\frac{1}{\hat{\lambda}_d}\right) \mathrm{u}\left(\hat{\lambda}_d\right)\right]. \end{aligned} \tag{21}$$

B. ERGODIC CAPACITY BASED USER SELECTION MECHANISM

In the proposed model, there are multiple UEs, an IoT device and an ED, and it is assumed that only UEs are capable to act as a relay forward node. In Algorithm 1, $\mathbf{EC}_{\{UE_{1\ldots U}\}}$ is the vector containing the EC of all the UEs. To ensure the QoS requirements of the IoT device, one of the UE with the maximum EC is chosen to act as an EH relay which has the EC representation as EC_{UE_s}. The computational complexity for the user selection based on the EC is of the order $\mathcal{O}(n)$, where n defines the total number of legitimate devices. Figure 3 refers to the user deployment scenario based on employed user selection mechanism for the considered model. The distances from BS to the IoT device, BS to selected UE, and selected UE to the IoT device are represented by $d_{BS\to D}$, $d_{BS\to UE}$ and $d_{UE\to D}$.

IV. OPTIMIZED BEAMFORMING USING SEC ANALYSIS

In this section, an optimization problem is presented to ensure secure communication for the IoT device. With the assumption that IoT device is located closer to the ED. Hence, there is a risk of getting the information of IoT device wiretapped by the ED. To address this, we propose

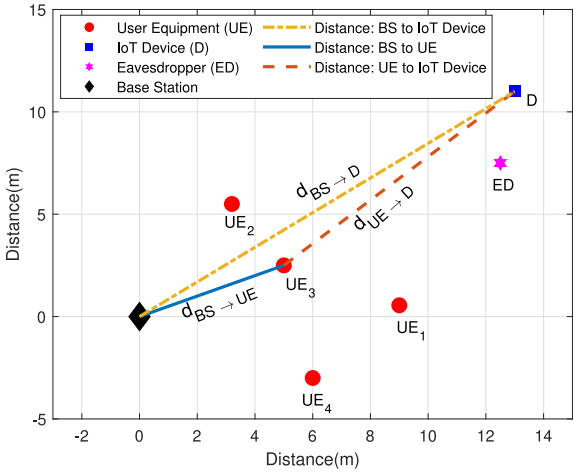


FIGURE 3. Considered UEs, IoT device, and ED deployment in secure MU-MISO-NOMA cooperative IoT framework.

an algorithm which ensures that the ED achieves minimum EC while improving the SEC of the other nodes. The objective function given as a closed-form in (20) is now optimized with respect to the beamforming vector $\mathbf{w}_i$ while taking the constraints into account. Here, $\mathbf{w}_i$ represents the beamforming vector for all the nodes in the proposed model. Thus, we express the objective function as

$$\begin{aligned} \min_{\{\mathbf{w}_i\}_{i=1}^{I}} \quad & EC_e(\mathbf{w}_i) \\ \text{s.t.} \quad & C_1 : ||\mathbf{w}_i||^2 \leq 1, \quad \forall i \\ & C_2 : (SEC)^{j+1} \geq (SEC)^j \end{aligned} \tag{22}$$

where the number of iterations are denoted by j. The constraint C_1 is designed to ensure that $\mathbf{w}_i\mathbf{w}_i^H = 1$, $\forall i$, while C_2 achieves maximized SEC in comparison with the initialized SEC at each incremental iteration. The constraints make the optimization problem NP-hard and for such, an exhaustive search approach is considered. Since this is a single objective constrained optimization problem, hence algorithms such as 'interior-point' and 'sequential programming (sqp)' routines can be used. Since sqp method is more robust and it can recover from infeasible solutions, it is considered in this work. The computational complexity of this method relies on multiple factors. It involves an iterative process with an exhaustive search strategy within the optimization, depending on various constraints. The complexity is affected by the number of iterations required for convergence, the dimensionality of the search space concerning users, IoT devices, and beamforming vectors, and constraints such as power normalization and objective which is EC of the eavesdropper herein. A pseudo-code for optimized beamformers is given in Algorithm 2.

V. OUTAGE PROBABILITY ANALYSIS UNDER COOPERATIVE RELAYING

In this section, the analytical formulation for the OP analysis of IoT device is presented using the SINR formulations. For the beamforming vectors, Algorithm 2 is considered albeit under simplified setup of linearly dependent beamformer considerations. Later, a user selection mechanism based on the OP of IoT device under cooperative relaying is given.

Algorithm 2 Pseudo-Code for Optimized Beamformers

Input: Initialized values of the beamforming vectors.
Output: Optimized beamformer values, EC_e and SEC.
1. Initialize $\{\mathbf{w}_i^{Init.}\}_{i=1}^{I}$ using principle eigenvector method, number of iterations, and time index (j).
2. **repeat**
3. Compute $(EC_e(\mathbf{w}_i))^j$ & $(SEC)^j$
4. $j = j + 1$
5. Compute $(EC_e(\mathbf{w}_i))^j$ & $(SEC)^j$ using 'sqp' method
6. **if** $\{(EC_e(\mathbf{w}_i))^j \leq (EC_e(\mathbf{w}_i))^{j-1}\}$ & $\{(SEC)^j \geq (SEC)^{j-1}\}$.
7. Update local optimal beamformer $\{\mathrm{w}_i^{lo.}\}_{i=1}^{I}$, EC_e and SEC, then perform recursion
8. **else**
9. Return optimized beamformers, EC_e and SEC
10. Stop algorithm = true
11. **else if**
12. **until** {Stop algorithm = true}

A. CHARACTERIZATION OF OUTAGE PROBABILITY

Here, we employ the framework given in [8] under the linearly dependent beamformer constraints produced using Algorithm 2 to characterize the OP of IoT device with cooperative relaying with uth user, $u \in \{1, 2, \ldots, U\}$ as.

$$\begin{aligned} P_{Out_{D,u}} = & \left(1 - \sum_{d=1}^{D} \frac{\lambda_d^{D-1}}{\prod_{\substack{y=1 \\ y\neq d}}^{D}(\lambda_d - \lambda_y)} e^{\frac{-\gamma\sigma_d}{\lambda_d}} \mathrm{u}\left(\frac{\gamma\sigma_d}{\lambda_d}\right)\right) \\ & \times \left[\left(1 - \sum_{u=1}^{U} \frac{\lambda_u^{U-1}}{\prod_{\substack{y=1 \\ y\neq u}}^{U}(\lambda_u - \lambda_y)} e^{\frac{-\gamma\sigma_u}{\lambda_u}} \mathrm{u}\left(\frac{\gamma\sigma_u}{\lambda_u}\right)\right)\right. \\ & \left. + \left(e^{\chi} - \Gamma\left(1, \chi; \frac{\gamma}{c\mu_{ud}||\mathbf{w}||^2}\right)\right)\right]. \end{aligned} \tag{23}$$

where $\chi = \frac{-\gamma}{(a_1 - a_2\gamma_2)||\mathbf{w}||^2}$, $a_1 = \frac{(1-\rho)\alpha_d P_S}{\sigma_u}$ and $a_2 = (1-\rho)P_S[\frac{U\sum_{k=1}^{U}\alpha_k + D\sum_{l=1,l\neq d}^{D}\alpha_d}{\sigma_u}]$. Moreover, $\gamma = \frac{2^{2R_{th,D}}}{1-\alpha} - 1$ is predefined threshold for decoding x_d while $R_{th,D}$ is the target data rate of IoT device.[1] A detailed derivation of the above is available in [8], and it is not included herein to avoid repetition. Also, a similar OP expression can be obtained for ED, i.e., $P_{Out_{E,u}}$ by incorporating the relevant channel characteristics and path-loss exponents.

B. OUTAGE PROBABILITY BASED USER SELECTION MECHANISM

For the considered model, two distinct user selection mechanism are considered. Firstly, Algorithm 3 presents the

1. u(.) represent unit step function and Γ is the generalized incomplete gamma function defined as $\Gamma(a, x; b) = \int_x^{\infty} t^{a-1} exp(-t - bt^{-1})dt$.

Algorithm 3 User Selection Mechanism Based on OP

Input: Coordinates of UEs, IoT device and ED, simulation parameters
Output: Selection of uth UE as a relay
while UEs $>$ 0 **do**
1. Compute $\mathbf{P}_{Out_{D,UEs}} = \{P_{Out_{D,1}}, P_{Out_{D,2}}, \ldots, P_{Out_{D,U}}\}$
2. Index $= \arg\min\ (\mathbf{P}_{Out_{D,UEs}})$
3. $\hat{U}_s$ = UE(Index)

Algorithm 4 User Selection Mechanism With Max Secrecy Rate

Input: Coordinates of UEs, IoT device and ED, simulation parameters
Output: Selection of uth UE as a relay
while UEs $>$ 0 **do**
1. Compute $\mathbf{S}_{Out_{D,E,UEs}} = \left\{\mathbb{E}\left[P_{Out_{E,u}} - P_{Out_{D,u}}\right]\right\}_{u=1}^{U}$
2. Index $= \arg\max\ (\mathbf{S}_{Out_{D,E,UEs}})$
3. $\bar{U}_s$ = UE(Index)

OP based user selection mechanism where the OP of IoT device through cooperative relaying is computed considering each UE as a relay forward node. Herein, $P_{Out_{D,UEs}}$ represent the OP of IoT device through all UEs, whereas $\hat{U}_s$ represent the selected UE which results in the minimum OP of IoT device. Secondly, Algorithm 4 gives a user selection mechanism which ensures the maximum secrecy rate. This is done by calculating the outage probability of IoT device and ED from each user, i.e., $P_{Out_{D,u}}$ and $P_{Out_{E,u}}$, $\forall u$, and then taking the expectation of the differences, refereed as $S_{Out_{D,E,UEs}}$. $\bar{U}_s$ represent the selected UE for relaying based on this mechanism. The computational complexity for the user selection methods based on the outage probability is also of the order $\mathcal{O}(n)$.

VI. RESULTS AND DISCUSSIONS

In this section, we validate the closed-form expressions derived in this work and perform the proposed optimization tasks. In our simulation setup, we consider that all the nodes in the network are deployed randomly, however, in a static setup without mobility. For all the wireless channels, the path loss exponent is set to 3 and the bandwidth is 1 MHz as in [18]. The simulation parameters used are given in Table 2. We consider the network deployment as shown in Figure 3.

The validation of EC based user selection for the proposed secure MU-MISO-NOMA IoT system is presented in Figure 4. From the Figure, it is observed that UE_3 achieves the maximum EC compared to the rest. However, ED is performing much better than UE_1 and IoT device, because of its better channel conditions. In comparison with the EC of UE_4, UE_3 achieved approximately 80% more EC at -13 dB transmit SNR. Similarly, at 16 dB transmit SNR, the EC of UE_1 is observed to be approximately 66% less than the EC of UE_3. Over the whole SNR range, UE_3 outperforms each UE in terms of EC, hence it is selected as the most efficient node for relaying purposes. Furthermore, it also illustrates that analytical results are perfectly matching the simulation results.

The OP based user selection approach in Algorithm 3 is presented in Figure 5. The Figure illustrates that UE_3 achieves the least OP for the IoT device hence, becoming the most efficient UE to be selected for the purpose of cooperative relaying. At 2 dB transmit SNR, it is observed that the OP of IoT device computed from relaying path

TABLE 2. Simulation parameters.

Parameters	Values
Bandwidth	1 MHz
Distance: BS $\rightarrow$ IoT device	17m
Distance: BS $\rightarrow$ selected Sub-UE	5.6m
Distance: Selected Sub-UE $\rightarrow$ IoT device	11.7m
Energy conversion coefficient (η)	0.7
No. of UEs	4
No. of IoT devices	1
No. of ED	1
Noise power density of antennas ($n_u = n_d = n_e$)	-100 dBm/Hz
Noise power density ($n_{ID_u} = n_{ID_d} = n_{ID_e}$)	-90 dBm/Hz
Path-loss exponent (ϵ)	3
Target data rate of IoT device	0.2 bits/sec/Hz

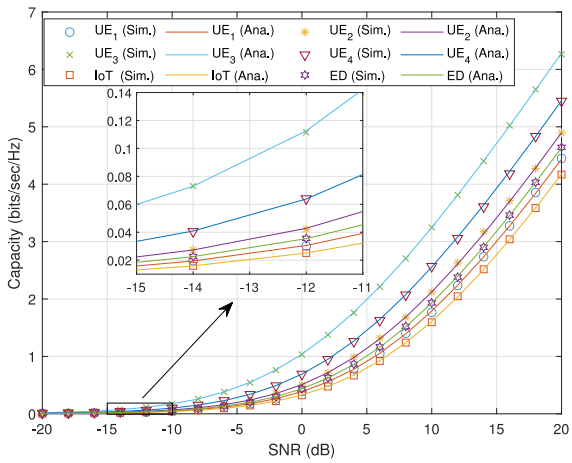


FIGURE 4. Ergodic capacity of each node versus transmit SNR at $N = 3$.

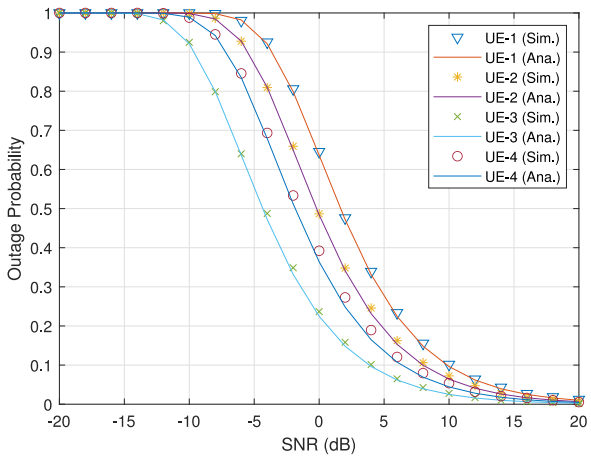
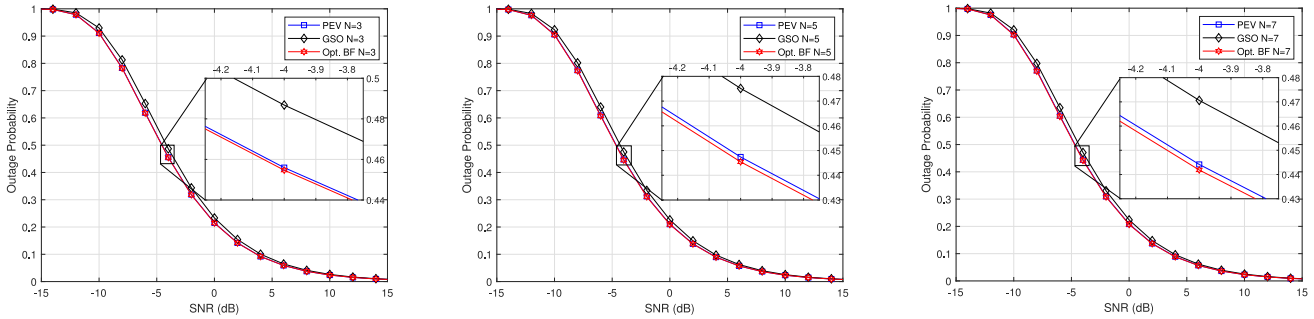


FIGURE 5. Outage probability of IoT device through each node versus transmit SNR at $N = 3$.



(a) N=3 (b) N=5 (c) N=7

FIGURE 6. Outage Probability of IoT device using PEV, GSO and Optimized Beamformers versus transmit SNR at different number of transmit antennas N.

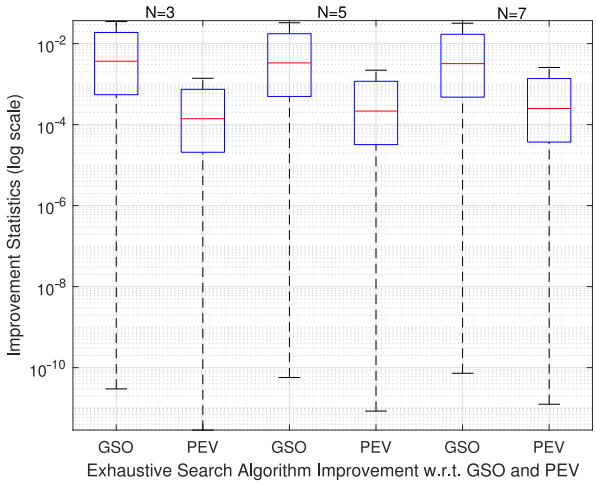


FIGURE 7. Boxplot displaying statistical significance of exhaustive search algorithm's improvement over GSO and PEV based beamforming techniques.

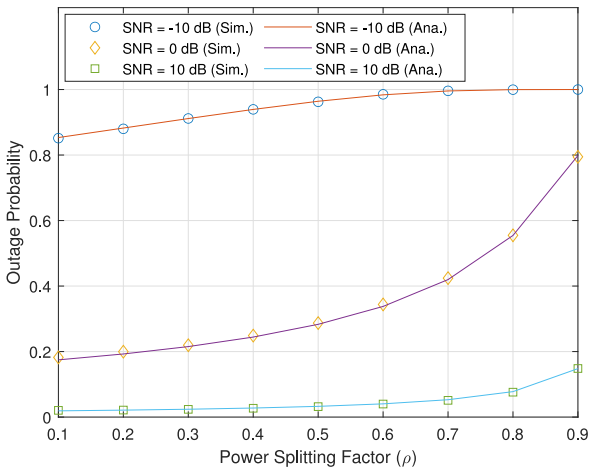


FIGURE 8. Outage probability of IoT device against PS factor (ρ) at various transmit SNR levels. Here, $N = 3$ and TS factor ($\alpha = 0.5$) are considered.

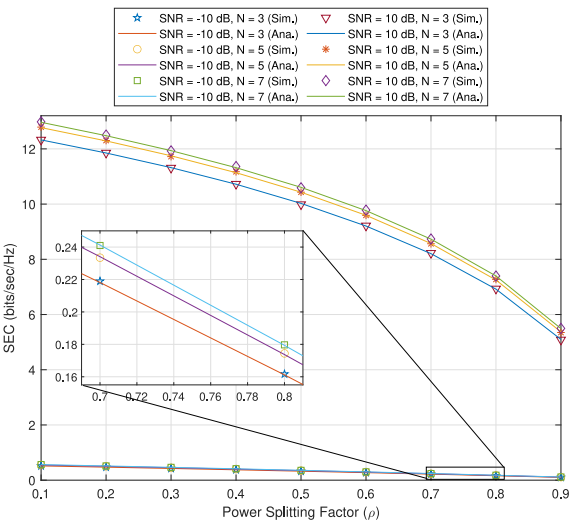
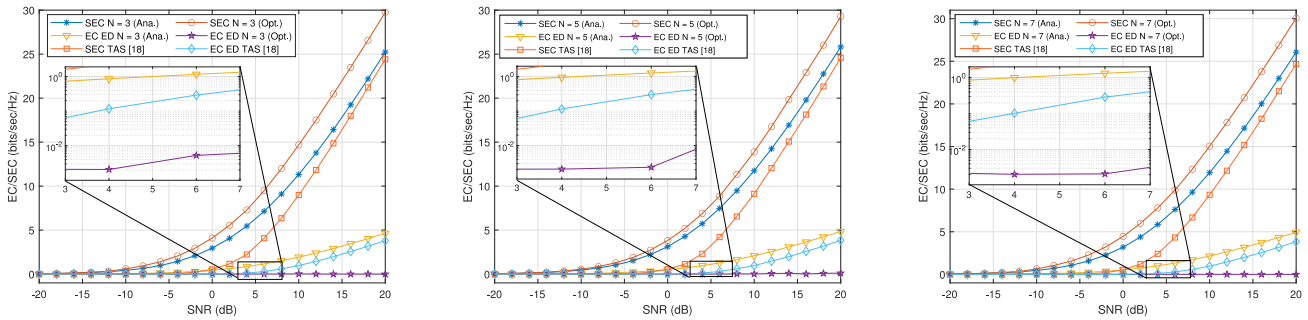


FIGURE 9. Sum ergodic capacity versus PS factor (ρ) at various SNR levels and varying number of antennas N. Here, TS factor $\alpha = 0.5$.

through UE_1, UE_2, and UE_4 is approximately 69%, 56%, and 45% higher than UE_3, respectively. By increasing number of transmit antennas, further reduction in OP can be observed for each UE. Conclusively, both the EC and OP based user selection approaches resulted in selection of the same UE_3 under the considered network configurations. Now, by considering Algorithm 4, it is observed that the best user to be selected as relay is UE_2 as the $\mathbf{S}_{Out_{D,E,2}}$ is marginally higher than UE_3 which is 0.0071. This difference is a little higher for UE_1 and UE_4. However, in all cases the marginal increase may pivot the user selection in favor of Algorithms 1 and 3. In the work that follows, we opt UE_3 as the cooperative relaying node.

Figure 6(a)-(c) gives insights of OP of IoT device against transmit SNR at different number of transmit antennas while considering the beamformers to be generated using Principle Eigenvector (PEV) as in [15], Gram Schmidt Orthogonalization (GSO), e.g., [36], and optimized beamformers achieved using proposed Algorithm 2. From Figure 6(b), it is depicted that at -4 dB transmit SNR, there is approximately 6% reduction in the OP of IoT device when compared with GSO technique. Similarly, at the same transmit SNR, the optimized beamformers resulted in 0.5% and 6.5% reduction in OP of IoT device when compared with PEV and GSO technique, respectively. Furthermore, the



(a) N=3 (b) N=5 (c) N=7

FIGURE 10. Sum ergodic capacity and EC of ED versus transmit SNR at different number of transmit antennas N.

comparative analysis of Figure 6(a)-(c) indicate that due to multiple antenna elements, the OP of IoT device decreases on average by approximately 0.25%, 0.4%, and 0.45% over the predefined transmit SNR range when compared with PEV and optimized beamforming results. From Figure 6, it is concluded that GSO based beamformers performance fall short since the beamformers are random in nature while the optimized beamformers are performing comparatively better than PEV technique in terms of OP of the IoT device.

Figure 7 shows the improvement in exhaustive search algorithm over GSO and PEV based beamforming techniques. The center of each box plot represents the median, while the bottom and top edges of the box signify the 25th and 75th percentiles, respectively. It is observed that for all considered antenna elements, the improvement of both GSO and PEV is observed in the summary statistics shown through the box plots.

Figure 8 highlights the OP against PS factor (ρ), at various transmit SNR levels. The Figure indicates that at low PS factor the OP of IoT device is comparatively less at low transmit SNR level and vice versa for higher transmit SNR levels. This is because lesser PS factor is allocated for the EH process while a bigger chunk of the PS factor is left for the relaying transmissions hence, resulting in better OP of IoT device. Comparative analysis of Figure 6(a) and 8 indicate that there is an exact match between analytical and simulation results.

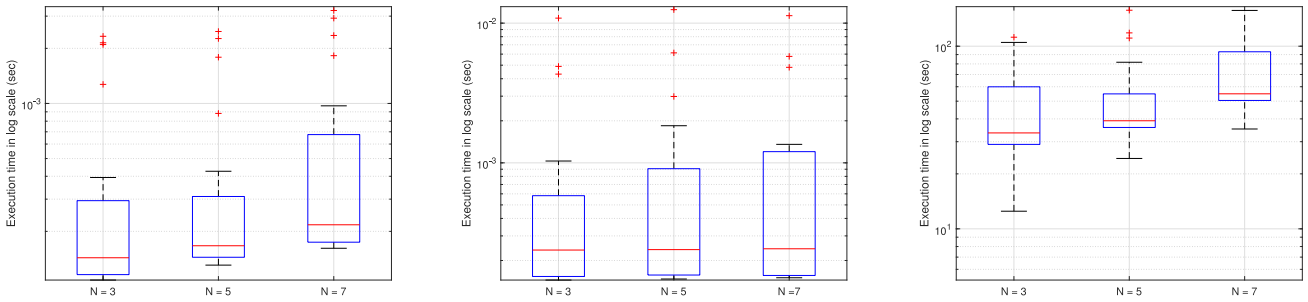
In Figure 9, the SEC is presented against PS factor at various SNR levels and varying number of transmit antennas N. The analysis indicates that at low transmit SNR, the SEC is much affected by the variation of PS factor, however, at high transmit SNR the SEC is better when allocated PS factor is small as smaller PS factor results to have more PS factor for information decoding. Furthermore, for PS factor ρ to be 0.5 and at 10 dB transmit SNR, the introduction of multiple transmit antennas enhanced the SEC by approximately 5%. Similarly, at the same PS factor and -10 dB transmit SNR, the increase in SEC due to multiple transmit antennas is approximately 9%. Hence, compared to higher transmit SNR, the analysis depicts that multiple antenna elements perform better at low transmit SNR. Moreover, it is observed that analytical and simulation results closely match, which again validates our approach.

Figure 10(a)–(c) presents the SEC and EC of ED as a function of SNR at different number of transmit antennas, for validation purposes. Using the 'sqp' algorithm for optimization, it is observed that SEC is improved and EC of the ED is degraded in accordance with the objective function. It can also be observed that at different number of transmit antennas, TAS method always achieved less SEC and EC for the ED when compared with the proposed optimized method. Furthermore, the affect of antenna diversity is observed by comparing Figures 10(a) and 10(c). With increase in number of transmit antennas, the optimized SEC at 10 dB transmit SNR achieved approximately 2.5% increase. In each case, it is observed that EC of ED ranges near 0 bits/sec/Hz. At $N = 3, 5, 7$, the optimized SEC increases on average by approximately 29%, 18%, and 26%, respectively, when compared to the analytical SEC. Similarly, an average reduction in the optimized EC of ED when compared with the analytical EC is approximately 98% which validates our proposed optimization problem. Moreover, it is demonstrated that the proposed technique always outperformed TAS technique given in [18].

The boxplots in Figure 11 demonstrates the comparative execution times of various beamforming techniques, such as PEV, GSO, and the exhaustive search approach, across different numbers of transmit antennas N. Notably, the execution times were computed using an Intel Core i3-7020U CPU @ 2.30 GHz with 8GB RAM. It is observed that the GSO method outperforms the PEV and exhaustive search methods in terms of execution time. However, it is crucial to consider the applications in distinct time contexts. The exhaustive search method is well-suited for non-real-time applications due to its comprehensive exploration of possibilities. Conversely, the GSO and PEV methods offer a balance between search efficiency and speed, making them better options for near real-time scenarios.

VII. CONCLUSION

In this work, we performed the optimization of the beamforming vector on a downlink MU-MISO NOMA IoT system in the presence of ED with the goal to maximize the SEC



(a) PEV approach (b) GSO approach (c) Exhaustive search approach

FIGURE 11. Execution time of different beamforming techniques at varying number of transmit antennas *N*.

and minimize EC of ED. Particularly, we provided the exact closed-form expressions of SEC and EC of ED while considering TS/PS factors, and transmit antenna diversity. A user selection scheme is developed based on EC of each UE for selection of efficient relaying UE. Additionally, an optimization problem has been developed for MU scenario in the presence of IoT device and ED, which is then addressed exploiting the exhaustive search method. A secure MU-MISO NOMA communication is performed by minimizing the EC of ED, resulting in degradation of ED's performance, while improving the SEC of rest of the network. The percentage improvement/decrease in the SEC and EC of ED due to antenna diversity is presented, respectively, where the analytical results are validated by Monte Carlo simulation results. Under cooperative relaying, OP based best user selection is provided which ensures PLS in the considered network. This work can be extended to perform analysis of secrecy performance considering UAVs as relay and multiple IoT devices as end nodes in the presence of EDs and by performing efficient selection on PACs to select a best relaying UE. Also, low complexity solutions for the proposed NP-hard optimization problem needs to be investigated.

REFERENCES

[1] X. Li et al., "Security and reliability performance analysis of cooperative multi-relay systems with nonlinear energy harvesters and hardware impairments," *IEEE Access*, vol. 7, pp. 102644–102661, 2019.

[2] K. Cao et al., "Achieving reliable and secure communications in wireless-powered NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1978–1983, Feb. 2021.

[3] B. Li, X. Qi, K. Huang, Z. Fei, F. Zhou, and R. Q. Hu, "Security-reliability tradeoff analysis for cooperative NOMA in cognitive radio networks," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 83–96, Jan. 2019.

[4] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng, and R. Jia, "Exploiting inter-user interference for secure massive non-orthogonal multiple access," *IEEE Sensors J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 788–801, Apr. 2018.

[5] G. Gomez, F. J. Martin-Vega, F. J. Lopez-Martinez, Y. Liu, and M. Elkashlan, "Physical layer security in uplink NOMA multi-antenna systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 70422–70435, 2019.

[6] L. Lv, Q. Wu, Z. Li, Z. Ding, N. Al-Dhahir, and J. Chen, "Covert communication in intelligent reflecting surface-assisted NOMA systems: Design, analysis, and optimization," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1735–1750, Mar. 2022.

[7] T. H. Vu, T.-V. Nguyen, and S. Kim, "Wireless powered cognitive NOMA-based IoT relay networks: Performance analysis and deep learning evaluation," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3913–3929, Mar. 2022.

[8] N. U. Zaman, A. K. Hassan, Z. H. Abbas, G. Abbas, M. Bilal, and S. Pack, "Performance analysis of NOMA enabled multi-user co-operative IoT network with SWIPT protocol," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 8, 2023, Art. no. 101639.

[9] H. Lei, F. Yang, I. S. Ansari, H. Liu, K. J. Kim, and T. A. Tsiftsis, "Secrecy outage performance analysis for uplink CR-NOMA systems with hybrid SIC," *IEEE Internet Things J.*, vol. 10, no. 15, pp. 13181–13195, Aug. 2023.

[10] Y. Feng, S. Yan, N. Yang, Z. Yang, and J. Yuan, "Safeguarding non-orthogonal multiple access with physical layer techniques," *IEEE Netw.*, vol. 36, no. 3, pp. 145–151, May/Jun. 2022.

[11] S. Lv, X. Xu, S. Han, X. Tao, and P. Zhang, "Energy-efficient secure short-packet transmission in NOMA-assisted mMTC networks with relaying," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1699–1712, Feb. 2022.

[12] C. Yuan, X. Tao, N. Li, W. Ni, R. P. Liu, and P. Zhang, "Analysis on secrecy capacity of cooperative non-orthogonal multiple access with proactive jamming," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2682–2696, Mar. 2019.

[13] C. Yuan, W. Ni, K. Zhang, J. Bai, J. Shen, and A. Jamalipour, "User pairing and power allocation in untrusted multiuser NOMA for Internet-of-Things," *IEEE Internet Things J.*, vol. 10, no. 15, pp. 13155–13167, Aug. 2023.

[14] M. Zeng, N.-P. Nguyen, O. A. Dobre, and H. V. Poor, "Securing downlink massive MIMO-NOMA networks with artificial noise," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 685–699, Jun. 2019.

[15] A. K. Hassan, M. Moinuddin, U. M. Al-Saggaf, O. Aldayel, T. N. Davidson, and T. Y. Al-Naffouri, "Performance analysis and joint statistical beamformer design for multi-user MIMO systems," *IEEE Commun. Lett.*, vol. 24, no. 10, pp. 2152–2156, Oct. 2020.

[16] S. Thapar, D. Mishra, and R. Saini, "Secure transmission in NOMA-enabled Industrial IoT with resource-constrained untrusted devices," *IEEE Trans. Ind. Inform.*, vol. 20, no. 1, pp. 411–420, Jan. 2024, doi: 10.1109/TII.2023.3263276.

[17] M. Li, F. E. Bouanani, S. Muhaidat, and M. Dianati, "Secure STBC-aided NOMA in cognitive IIOT networks," *IEEE Internet Things J.*, early access, Jun. 21, 2023, doi: 10.1109/JIOT.2023.3288452.

[18] T. N. Do, D. B. da Costa, T. Q. Duong, and B. An, "Improving the performance of cell-edge users in MISO-NOMA systems using TAS and SWIPT-based cooperative transmissions," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 49–62, Mar. 2018.

[19] M. Diamanti, G. Fragkos, E. E. Tsiropoulou, and S. Papavassiliou, "Unified user association and contract-theoretic resource orchestration in NOMA heterogeneous wireless Networks," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1485–1502, 2020.

[20] W. Wang et al., "Secure beamforming for IRS-enhanced NOMA networks," *IEEE Wireless Commun.*, vol. 30, no. 1, pp. 134–140, Feb. 2023.

[21] Y. Han, N. Li, Y. Liu, T. Zhang, and X. Tao, "Artificial noise aided secure NOMA communications in STAR-RIS networks," *IEEE Wireless Commun. Lett.*, vol. 11, no. 6, pp. 1191–1195, Jun. 2022.
[22] H. Han et al., "Secure transmission for star-ris aided NOMA against internal eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 72, no. 11, pp. 15068–15073, Nov. 2023.
[23] D. Diao, B. Wang, K. Cao, R. Dong, and T. Cheng, "Enhancing reliability and security of UAV-enabled NOMA communications with power allocation and aerial jamming," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8662–8674, Aug. 2022.
[24] W. Lu et al., "Secure NOMA-based UAV-MEC network towards a flying eavesdropper," *IEEE Trans. Commun.*, vol. 70, no. 5, pp. 3364–3376, May 2022.
[25] Y. He, L. Nie, T. Guo, K. Kaur, M. M. Hassan, and K. Yu, "A NOMA-enabled framework for relay deployment and network optimization in double-layer airborne access VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 11, pp. 22452–22466, Nov. 2022.
[26] C. Zhang, F. Jia, Z. Zhang, J. Ge, and F. Gong, "Physical layer security designs for 5G NOMA systems with a stronger near-end internal eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13005–13017, Nov. 2020.
[27] X. Yue, Y. Liu, Y. Yao, X. Li, R. Liu, and A. Nallanathan, "Secure communications in a unified non-orthogonal multiple access framework," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 2163–2178, Mar. 2020.
[28] R. K. Ahiadormey, P. Anokye, H.-S. Jo, C. Song, and K.-J. Lee, "Secrecy outage analysis in NOMA power line communications," *IEEE Wireless Commun. Lett.*, vol. 25, no. 5, pp. 1448–1452, May 2021.
[29] W. U. Khan, F. Jameel, A. Ihsan, O. Waqar, and M. Ahmed, "Joint optimization for secure ambient backscatter communication in NOMA-enabled IoT networks," *Digit. Commun. Netw.*, vol. 9, no. 1, pp. 264–269, 2023.
[30] T. Nimi and A. V. Babu, "Enhancing the physical layer security of artificial noise-aided half-duplex cooperative NOMA systems," *Phys. Commun.*, vol. 59, Aug. 2023, Art. no. 102090.
[31] W. Tan, C. Zhang, J. Peng, L. Dai, S. Fu, and K. Qiu, "Secure transmission via IUI engineering for IRS-assisted NOMA systems," *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1369–1373, Jul. 2022.
[32] A. K. Hassan and M. Moinuddin, "Beamforming using exact evaluation of leakage and ergodic capacity of MU-MIMO system," *Sensors*, vol. 21, no. 20, p. 6792, 2021.
[33] K. Wang, H. Li, Z. Ding, and P. Xiao, "Reinforcement learning based latency minimization in secure NOMA-MEC systems with hybrid sic," *IEEE Trans. Wireless Commun.*, vol. 22, no. 1, pp. 408–422, Jan. 2023.
[34] M. Vaezi, G. A. A. Baduge, Y. Liu, A. Arafa, F. Fang, and Z. Ding, "Interplay between NOMA and other emerging technologies: A survey," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 4, pp. 900–919, Dec. 2019.
[35] M. Naderpour and H. Khaleghi Bizaki, "Low overhead NOMA receiver with automatic modulation classification techniques," *IET Commun.*, vol. 14, no. 5, pp. 768–774, 2020.
[36] K. Matsumura and T. Ohtsuki, "Orthogonal beamforming using Gram–Schmidt orthogonalization for multi-user MIMO downlink system," *Eurasip J. Wireless Commun. Netw.*, vol. 2011, no. 1, pp. 1–10, 2011. [Online]. Available: https://doi.org/10.1186/1687-1499-2011-41