Wireless Communications and Mobile Computing

Safeguarding 5G Networks through Physical Layer Security Technologies

Lead Guest Editor: Li Sun
Guest Editors: Kamel Tourki, Yafei Hou, and Lu Wei

Safeguarding 5G Networks through Physical Layer Security Technologies

Wireless Communications and Mobile Computing

Safeguarding 5G Networks through Physical Layer Security Technologies

Lead Guest Editor: Li Sun
Guest Editors: Kamel Tourki, Yafei Hou, and Lu Wei

Editorial Board

Contents

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 7503735, 2 pages
https://doi.org/10.1155/2018/7503735

Editorial

Safeguarding 5G Networks through Physical Layer Security Technologies

Li Sun,[1] **Kamel Tourki**,[2] **Yafei Hou**,[3] **and Lu Wei**[4]

[1]*Xi'an Jiaotong University, China*
[2]*Huawei France Research Center, France*
[3]*Okayama University, Japan*
[4]*University of Michigan-Dearborn, USA*

Correspondence should be addressed to Li Sun; lisun@mail.xjtu.edu.cn

Received 10 September 2018; Accepted 10 September 2018; Published 25 September 2018

5G wireless networks are expected to support massive user connections and exponentially increasing wireless services, which makes information security unprecedentedly important. As an emerging network security solution, physical layer security (PLS) takes advantage of the intrinsic characteristics of wireless channels, such as noise, interference, and fading, to degrade the received signal qualities at the malicious users, and achieves keyless secure transmission via signal design and signal processing approaches. In the past few years, the research on PLS has generated a large body of literature, with the topics ranging from information-theoretical studies to practical scheme design. However, it is still challenging to develop PLS solutions that well match the unique features of 5G networks. The aim of this special issue is to provide a venue to publish recent research achievements that address the challenges faced by 5G security.

In this special issue, eight papers were selected based on our rigorous peer review by qualified experts. The topics of the accepted manuscripts mainly include (a) advanced signal design for enhanced security, (b) cooperation based PLS techniques, (c) security provisioning for NOMA, (d) attack detection and countermeasures in 5G networks, and (e) PLS for 5G enabled Internet-of-Things. All accepted papers are briefly introduced as below.

The paper titled "Provoking the Adversary by Detecting Eavesdropping and Jamming Attacks: A Game-Theoretical Framework", by A. Salem *et al.*, developed a mechanism to detect the jamming and eavesdropping attacks launched by an adversary and analyzed the interactions between the legitimate user and the adversary using the stochastic game theory. Numerical results validated the efficiency of the proposed games.

In the paper "Adaptive OFDM-IM for Enhancing Physical Layer Security and Spectral Efficiency of Future Wireless Networks", H. M. Furqan *et al.* proposed three approaches to enhance the physical layer security and improve the spectral efficiency of OFDM systems with Index Modulation. In the proposed schemes, different activation ratios and/or constellation modulation orders are selected adaptively for each subblock based on the legitimate user's channel, such that a high error floor is created at the eavesdropper.

In the paper "Precoding-Aided Spatial Modulation for the Wiretap Channel with Relay Selection and Cooperative Jamming", Z. Bouida *et al.* proposed a PLS scheme for dual-hop cooperative networks with an external eavesdropper. In the proposed scheme, precoding-aided spatial modulation (PSM) and relay selection techniques are combined such that both hops are secured. The authors also analyzed the system performance in terms of the ergodic secrecy rate and secrecy outage probability.

The impact of masquerading attack on the outage and capacity performance of cooperative relaying networks was investigated in "On the Performance of the DNPS-Based Relay Networks under Masquerading Attack", authored by W. Chang. In this paper, multiple masquerade relays with random masquerading behavior were taken into account,

and the geographical effect of the network topology was considered as well. This paper can be recognized as a first step to inspire the investigation of the masquerading attack for relay networks.

The paper entitled "Impact of Antenna Selection on Physical-Layer Security of NOMA Networks", by D. Deng *et al.*, studied the impact of antenna selection algorithms on decode-and-forward (DF) cooperative non-orthogonal multiple access (NOMA) networks, where the signal transmitted from the relay can be overheard by an eavesdropper. It was revealed that the system security performance is highly dependent on the system parameters such as the number of antennas at the relay, SNR, and main-to-eavesdropper ratio (MER).

Z. Xiang *et al.* proposed to exploit NOMA technique to enhance the uplink security performance in 5G-enabled Internet-of-Things (IoT) in their paper "Exploiting Uplink NOMA to Improve Sum Secrecy Throughput in IoT Networks". The authors derived the closed-form expressions for joint connection outage probability, joint secrecy outage probability, and sum secrecy throughput. Based on the theoretical results, the condition that NOMA outperforms OMA was presented.

In the paper titled "On Secrecy Outage Probability and Average Secrecy Rate of Large-Scale Cellular Networks", L. Tao *et al.* investigated the secrecy performance in large-scale cellular networks, where both base stations and eavesdroppers follow independent and different homogeneous Poisson point processes (PPPs). The exact expressions for the secrecy outage probability and average secrecy rate at the typical user were presented by using the tool of stochastic geometry.

The paper entitled "Probabilistic Caching Placement in the Presence of Multiple Eavesdroppers", by F. Shi *et al.*, studied the physical-layer security for the caching aided networks. In this work, the authors designed, analyzed, and optimized the probabilistic caching placement in the presence of multiple eavesdroppers. Simulation results were provided to exhibit the superiority of the proposed probabilistic caching placement compared to the competing solutions.

Conflicts of Interest

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

Acknowledgments

The guest editors would like to thank the authors for their great contributions to this special issue. We also appreciate the experts who participated in the peer review process and provided constructive comments which significantly improved the quality of the manuscripts.

Li Sun
Kamel Tourki
Yafei Hou
Lu Wei

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 1029175, 14 pages
https://doi.org/10.1155/2018/1029175

Research Article

Provoking the Adversary by Detecting Eavesdropping and Jamming Attacks: A Game-Theoretical Framework

Ahmed Salem,[1] **Xuening Liao**,[2,3] **Yulong Shen**,[1] **and Xiaohong Jiang**[2]

[1]*School of Computer Science and Technology, Xidian University, Xi'an, China*
[2]*School of System Information Science, Future University Hakodate, Hokkido, Japan*
[3]*School of Computer Science, Shaanxi Normal University, Xi'an, China*

Correspondence should be addressed to Ahmed Salem; engahmedsalem2@outlook.com

Received 28 April 2018; Accepted 25 July 2018; Published 28 August 2018

Academic Editor: Li Sun

This paper investigates the secrecy and reliability of a communication where the user is assisting an Intrusion Detection System (IDS) in detecting the adversary's attack. The adversary is assumed to be sophisticated such that it can conduct eavesdropping and jamming attacks. The IDS is equipped with the capability of detecting both of those attacks. Two scenarios were considered; the first scenario is that the user is trying to detect the adversary by assisting the IDS, and the second scenario is that the user is equipped with a silent time slot in its communication protocol besides assisting the IDS, in order to provoke the adversary into jamming the channel, thus detecting it with a higher probability. Interestingly, adding the capability of detecting eavesdropping attacks pushed the adversary into conducting jamming attacks much more, thus aiding in detecting the adversary earlier. All of that was modeled by means of stochastic game theory, in order to analyze and study the behavior and the interactions between the user and the adversary. Results show a major improvement in the first scenario by 188% and an improvement by 294% in the second scenario in the game value when the probability of detecting eavesdropping attacks was 0.3, which represents the payoff that the user gains in terms of secrecy and reliability.

1. Introduction

The problem of ensuring a secure and reliable wireless communication is challenging due to several reasons. On one hand, the broadcast nature of wireless channels makes it difficult to shield transmitted signals from unintended recipients. On the other hand, possible interference from other transmitters may degrade the received signals at the receiver. An adversary may exploit this weakness to its benefit and behave either as a passive eavesdropper who tries to intercept signals from ongoing transmissions without being detected [1, 2] or as a malicious user (jammer), which transmits jamming signals to the intended receiver. Thus, studies on security and reliability of wireless communications are of great importance for the design of next generation networks.

Lots of techniques were adopted in securing wireless systems, such as relaying [3–6], caching [7], and game theory, which models the conflict and cooperation between intelligent rational selfish decision-makers, as it has been recognized as a promising method to model the interplay between the legitimate user and the adversary in the network [8]. Assuming a network with one source-destination pair and an adversary, the source node aims to transmit the information securely/reliably to the destination, while the adversary attempts to wiretap/jam the signal. Thus, there is a conflict of benefits between the source node and the adversary. This can be modeled as a two-player game and the source node and the adversary act as two players of the game [9, 10]. Based on the types of the adversary (i.e., an eavesdropper, a jammer, and an active adversary), the game can be divided into three categories.

For networks with a jammer, the source node and the jammer will act as two players. The authors in [11] studied a network where the timing channel was exploited at the nodes to achieve resilience to the jamming attacks. They modeled the interactions between the nodes and the jammer based on game theory and the Nash equilibrium was studied.

Furthermore, the investigation was conducted with perfect and imperfect knowledge of the jammer's utility function. In [12], the authors considered a network where a user is trying to ensure a reliable communication with the existence of a reactive jammer. The authors solved the game by investigating Stackelberg equilibrium. In [13], the authors investigated an antijamming problem by using Stackelberg game model, where they followed it by using Hierarchical Power Control Algorithm (HPCA) to obtain Stackelberg equilibrium. In [1], the authors considered two kinds of jammers, a random jammer and a sophisticated jammer. The random jammer was equipped with the capability of employing a silent mode besides the capability of employing a jamming mode. The sophisticated jammer was equipped with two capabilities: (a) communicating as a law-obedient user, by acting as a relay, and (b) conducting a jamming attack and acting as a malicious user. They constructed optimal antijamming transmission strategies and a stochastic game was used in modeling the game between the user and the adversary. In this work, a silent mode was employed to the user to assist an IDS in detecting the adversary.

For networks with an active eavesdropper, the source node and the active eavesdropper will act as two players [14, 15]. In [14], the authors studied a network, where a user is transmitting to a destination with the existence of an active eavesdropper. That eavesdropper imposes a jamming signal to facilitate its eavesdropping, with the existence of its own residual self-interference. The authors established a game-theoretical framework, where closed-form strategies were obtained. Moreover, they analyzed the secrecy outage probability for the legitimate link in that hostile situation. In [15], the interactions were formulated by using a hierarchical game framework, where the eavesdropper acts as the leader and the user acts as the follower. Thus obtaining the optimal transmission strategy that maximizes the secrecy rate.

For networks with an active adversary who can act as either a passive eavesdropper or an active jammer, the game should consider these differences while being designed. In [16], the authors investigated a Multiple-Input Multiple-Output (MIMO) wiretap channel with an active adversary. They examined the legitimate transmitter and the adversary by modeling their interactions as a two-person zero-sum game and derived equilibrium strategies for the extensive form of the game under scenarios with perfect and imperfect information. In [8], a game theoretic approach was followed in dealing with a network, where a number of users are transmitting their message via several relays in the existence of an active adversary, who is capable of launching eavesdropping and jamming attacks. A fictitious play-based algorithm was proposed to assist in reaching the mixed strategy Nash equilibrium, and results show that an improvement can be achieved in the average expected utility per user up to 49.4%. Moreover, eavesdropping and jamming attacks on mobile Cyber-Physical Systems (CPSs) were studied in [17], where a Stackelberg game was used to maximize the secrecy rate between sensors and controllers. Recently, a new approach that considers a more sophisticated adversary with dual capability of conducting either eavesdropping or jamming attack has been proposed in [9]. In [9], a stochastic game was used in modeling the game between a user and an adversary. Two games were proposed, the two games assumed that the adversary can conduct an eavesdropping or a jamming attack. The user was assisting an IDS by exploiting the usage of a silent mode, which provokes the adversary into jamming the communication to facilitate the detection process. In the first game, the IDS can only detect jamming attacks, and in the second game, a time slot was incorporated in the transmission protocol, where the user will be silent, in order to provoke the adversary into conducting a jamming attack, and, therefore, the adversary can be easily detected. In [1, 9], an OFDM system was applied to model the channels between the user, the adversary, and the destination, where the game-theoretical techniques were applied to study and analyze the behavior of a user and an adversary in a network. In [18], the authors studied the secure communication while satisfying the throughput requirements needed by the higher-layer services. They investigated a fair strategy, which satisfies the two objectives (i.e., ensure secrecy and sufficient throughput), such that security and throughput performances can be finally modeled.

These works demonstrated that game theory is a promising approach that can be used in modeling the interplay between the legitimate user and the adversary. It is notable, however, that all the aforementioned works targeted the security or reliability performances of the network without any help of an IDS which can detect eavesdropping and jamming attacks. In our previous work, we propose a new paradigm where the IDS is equipped with the capability of detecting passive eavesdropping and jamming attacks [19], and the adversary is equipped with the capability of conducting passive eavesdropping and jamming attacks. We have proved that, by adopting the IDS in the system, the security and reliability performances can be greatly improved. As an extended work of our previous study, we aim to explore in this paper the reliability and security of a system with one source-destination pair and an adversary with the capabilities of both eavesdropping and jamming. The IDS is adopted in the system and we consider a silent mode at the source node. The contributions of this paper can be summarized as follows:

(i) Propose two new games: the basic game and the extended game, to model the interactions between the source node and the adversary. This is achieved by using stochastic game modeling techniques. In the basic game, the silent mode is unavailable at the source node, and the silent mode is available at the source node in the extended game

(ii) Derive the optimal probabilities and game values for the user and the adversary for the proposed basic game and extended game

(iii) Conduct extensive numerical analysis to validate the efficiency of the proposed games in terms of game values, and results show that our proposed games can assist in the detecting of the adversary by provoking it into conducting a jamming attack. We also made comparisons between our proposed games and the conventional game to demonstrate the performance improvements achieved by our proposed games in

terms of the security and the ability of provoking the adversary. It is observed that a major improvement was achieved for the basic game by 188% and by 294% for the extended game when we set the probability of detecting eavesdropping attacks as 0.3.

The remainder of this paper is organized as follows. In Section 2, we introduce the system model and present the abilities of the IDS to protect the user (Alice) from the adversary (Eve) while providing the needed mathematical formulations and assumptions. In Section 3, we formulate and solve the stochastic game between Alice and Eve. In Section 4, we investigate and present our model when a silent time slot is added to the communication protocol besides the capability of the IDS in detecting eavesdropping and jamming attacks. In Section 5, we present the results derived and analyze the meaning behind them thoroughly. Finally, we conclude this paper in Section 6.

2. System Model and Problem Formulation

Our proposed network consists of a source (Alice), a destination (Bob), and an eavesdropper (Eve). The communication between Alice and Bob needs to be secured against attacks that exploit the link's own secrecy and reliability. Eve acts as an active adversary that is capable of conducting eavesdropping and jamming attacks. In PHY security, the figure of merit is the secrecy rate, which is defined as the difference between the transmission rate of the source-destination link and that of the source-eavesdropper link [20]. For a Gaussian channel, the achievable secrecy rate equals the difference between the mutual information accumulated at the destination and that accumulated at the eavesdropper, which is not less than zero [21]. This leads us to derive the secrecy capacity under an eavesdropping attack as follows: $\mathcal{U}_{sc}(\mathbf{P}) = \max\{\mathcal{U}(\mathbf{P}, 0) - \mathcal{U}_e(\mathbf{P}), 0\}$, in which $\mathcal{U}_{sc}(\mathbf{P})$ is the secrecy capacity achieved under an eavesdropping attack, $\mathcal{U}(\mathbf{P}, 0)$ is the transmission capacity when no attacks are being conducted, and $\mathcal{U}_e(\mathbf{P})$ is the receiving capacity achieved by Eve while conducting an eavesdropping attack.

Detecting passive eavesdropping attacks relies heavily on detecting the Local Oscillator (LO) leakage power that receivers/eavesdroppers emit from their antennas [22, 23]. The leakage power that is being emitted is an inevitable reverse leakage that couples back through the input port and radiates out of the receiver's/eavesdropper's antenna [24], which is represented as being the signal **E** that aids in detecting passive eavesdropping attacks. Unfortunately, detecting this leakage power directly is impractical for two reasons [25]. Firstly, it would be difficult for the receive circuitry to detect the LO leakage over larger distances. In [25], it was shown that a distance of 20 m would take the order of seconds to detect the LO leakage with a high probability. The detection in practical systems will need to be made in the order of milliseconds at worst. The second reason is that it would be impractical to detect the LO leakage directly because its very variable, and it depends on the receiver/eavesdropper circuitry, model, and year of manufacture. Hence, we assumed that the IDS is capable of performing its operations as a cognitive node. Hence, cognitive radios tend to have a higher probability in detecting the passive receivers/eavesdroppers successfully [23–25].

Alice is always transmitting the signal **P**, and Eve is always transmitting either the signal **E** or the signal **J** when an eavesdropping or a jamming attack is being conducted, respectively. The signal **E** represents the LO leakage that radiates inevitably from the eavesdropper's antenna. Alice's IDS is capable of detecting passive eavesdropping and jamming attacks that are being conducted by Eve. Note that the reliability of the channel is neither affected nor compromised by the signal **E**.

If Eve is eavesdropping, the signal **E** will be inevitably sent while Eve is acting as a receiver for what Alice is sending, which will exploit the secrecy of the communication, and leads Alice to conduct her best response by sending the signal P_e, which will increase the secrecy capacity and satisfy the following inequality:

$$\mathcal{U}(\mathbf{P}, \mathbf{E}) \leq \mathcal{U}(P_e, \mathbf{E}), \tag{1}$$

where $\mathcal{U}(\mathbf{P}, \mathbf{E})$ is the resulting transmission capacity when Alice is transmitting the signal **P** to Bob and Eve is conducting an eavesdropping attack (i.e., emits the signal **E**), and $\mathcal{U}(P_e, \mathbf{E})$ is the transmission capacity when Alice is transmitting her best response signal P_e against an eavesdropping attack, while Eve is eavesdropping. Note that, $\mathcal{U}$ represents the payoff, which is the value of the game when Alice wins if the payoff is positive. Hence, the transmission capacity can be considered as the payoff that Alice wins or losses depending on the payoff's value and whether it is positive, zero, or negative. This yields an equilibrium/saddle point, in which $\mathcal{U}(P_e, \mathbf{E})$ will be the payoff to Alice [26].

On the other hand, if Eve was conducting a jamming attack by sending **J**, then, as a countermeasure, Alice's best response will be conducted by sending the signal P_j. This will lead to the following inequality:

$$\mathcal{U}(\mathbf{P}, \mathbf{J}) \leq \mathcal{U}\left(P_j, \mathbf{J}\right), \tag{2}$$

where $\mathcal{U}(\mathbf{P}, \mathbf{J})$ is the transmission capacity when Alice is transmitting **P** and Eve is conducting a jamming attack, and $\mathcal{U}(P_j, \mathbf{J})$ is the transmission capacity when Alice is transmitting her best response signal P_j while Eve is jamming. In that case, an equilibrium will be reached, which will make $\mathcal{U}(P_j, \mathbf{J})$ be the payoff that Alice will obtain.

An OFDM system is being used in this paper with n separate channels, in which those channels are modeled as Additive White Gaussian Noise (AWGN) channels. The channel coefficients between Alice and Bob, Alice and Eve, and Eve and Bob are denoted as $h_{A,B}$, $h_{A,E}$, and h_J, respectively. Reducing the reliability could be attained through jamming attacks that Eve transmits to Bob through the channel h_J. Guaranteeing the secrecy of the channel was done by following the assumption $h_{A,E} \leq h_{A,B}$ [27]. The signal strategy vector for Alice is **P**, where $\mathbf{P} = (P_1, P_2, \ldots, P_n)$. Eve is associated with a jamming signal strategy vector **J**, where $\mathbf{J} = (J_1, J_2, \ldots, J_n)$. Hence, as a conclusion on what was mentioned before regarding signal **E**, it is not considered as a

		Eve	
		E	J
Alice	E	$\mathcal{U}(P_e, \mathbf{E})$ / $(\beta, 1\text{-}\beta)$	$\mathcal{U}(P_e, \mathbf{J})$ / $(\gamma, 1\text{-}\gamma)$
	J	$\mathcal{U}(P_j, \mathbf{E})$ / $(\beta, 1\text{-}\beta)$	$\mathcal{U}(P_j, \mathbf{J})$ / $(\gamma, 1\text{-}\gamma)$

Figure 1: The first malicious state of the game Γ_{EJ}.

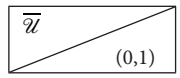


Figure 2: The second safe secure state of the game Γ_{EJ}.

threat on the reliability of the communication. As a result, the signal **E** was not associated with its own channel coefficient. According to [9], the following expressions can be calculated as follows:

$$\mathcal{U}(\mathbf{P}, \mathbf{J}) = \sum_{i=1}^{n} \ln\left(1 + \frac{h_{A,B}P_i}{h_J J_i + \sigma^2}\right), \quad (3)$$

$$\mathcal{U}_e(\mathbf{P}) = \sum_{i=1}^{n} \ln\left(1 + \frac{h_{A,E}P_i}{\sigma_E^2}\right), \text{and} \quad (4)$$

$$\mathcal{U}_{sc}(\mathbf{P}) = \sum_{i=1}^{n} \left(\ln\left(1 + \frac{h_{A,B}P_i}{\sigma^2}\right) - \ln\left(1 + \frac{h_{A,E}P_i}{\sigma_E^2}\right)\right), \quad (5)$$

where P_i is the signal transmitted by Alice through channel i and J_i is the jamming signal transmitted by Eve through channel i. The variances of the noises in the channels of Alice $\longrightarrow$ Bob and Alice $\longrightarrow$ Eve are denoted by σ and σ_E, respectively.

3. The Basic Stochastic Game

3.1. Introduction. In this game, Eve is provided with the capability of performing two kinds of actions (i.e., attacks). The first action is conducting a passive eavesdropping attack and the second action is performing a jamming attack. Eve can choose which attack she prefer to perform. Eve is assumed to choose only one attack at a time. Obviously, Eve will be cautious about choosing which kind of attack to conduct, due to the capability of Alice's IDS in detecting both kinds of attacks. Hence, Alice and Eve are defined to be rational and selfish.

3.2. The Game Modeling. We model the game as a two-state stochastic game as shown in Figures 1 and 2. This model is inspired from the study in [9], where Alice assists an IDS in detecting only jamming attacks. We propose a new scenario, in which Alice's IDS can detect passive eavesdropping attacks, besides detecting jamming attacks.

This game consists of two states. The first state is the malicious state, which the game always begins with, and the second state is the safe secure state, which happens when Eve is detected and removed from the game. Each entry in a state corresponds to a specific action pair that is being performed by Alice and Eve, respectively. Each action pair entry consists of two triangles, the upper left triangle represents the instantaneous payoff (current transmission rate) of Alice in the game, while the lower right triangle gives the probability distribution associated with the future states. As an example, in the first state, in Figure 1, the first block, which is associated with the action pair (E, E), the instantaneous payoff for Alice is shown to be $\mathcal{U}(P_e, E_e)$, and the probability that the next state is state 1 or state 2 is assigned by the probabilities β and (1-β), respectively.

3.3. The Probability Distribution. Eve's detection in both kinds of attacks is represented by a probability distribution. The probability distribution is divided into two probabilities, first, the probability of a missed detection and second, the detection probability. The probability of missed detection is assigned to be β and γ for eavesdropping and jamming attacks, respectively. The missed detection probability also represents the probability of repeating the first state. The detection probability is (1-β) and (1-γ) for eavesdropping and jamming attacks, respectively. The detection probability represents the probability of moving to the second state. We assumed that the probability of a missed detection and the probability of a successful detection are the same in both of the transmission modes of Alice while Eve is performing a specific kind of attack.

3.4. The Epoch Progression. As the epoch progresses, there will be a discount that is being performed on the payoffs, which is modeled by the discount factor δ. The purpose of using a discount factor δ, is to ensure the following: (1) the game will eventually end, (2) the probability of infinite playing will be zero, and (3) all the expected payoffs will be finite [28]. The discount factor δ can be interpreted as a measure of urgency in communications: $\delta = 0$ corresponds to the highest urgency and the transmission must be done in the current time slot. When the urgency is at its peak (i.e., $\delta = 0$), the security will be low as such precautions related to performing the best responses will be missed. If δ was assigned to a high value, this means that a delay can be introduced and the current transmission can be done in other time slots, not necessarily the current one, and this will improve the security.

3.5. Successful and Missed Detection. If Eve was not detected, the game will move to the next time slot and it will be played recursively with a discount factor δ.

If Eve was detected, then Alice will move from the malicious state (i.e., state 1) to the safe secure state (i.e., state 2), and Eve will be removed from the game. In the safe secure state, Alice will send her optimal signal that is designed for the case where there are no threats in the communication (i.e., $P_0 = \text{argmax}_{\mathbf{P}}\mathcal{U}(\mathbf{P}, 0)$).

3.6. Shapley-Bellmann Equation. We denote the game played in state 1 as Γ_{EJ} and the game played in state 2 as Γ_{END}. In state 2, Eve was already detected and Alice can transmit with rate $\overline{\mathcal{U}}$, and the total discounted payoff in state 2 is equal to

$(1+\delta+\delta^2+\cdots)\overline{\mathcal{U}} = \overline{\mathcal{U}}/(1-\delta)$. Studying the malicious state will require modeling the stochastic game Γ_{EJ} as in (6).

$$\Gamma_{EJ} = \begin{matrix} \\ E \\ J \end{matrix} \begin{matrix} \begin{matrix} E \end{matrix} & \begin{matrix} J \end{matrix} \\ \begin{pmatrix} \mathcal{U}(P_e, \mathbf{E}) + \beta\delta\Gamma_{EJ} + \dfrac{\overline{\mathcal{U}}\delta(1-\beta)}{1-\delta} & \mathcal{U}(P_e, \mathbf{J}) + \gamma\delta\Gamma_{EJ} + \dfrac{\overline{\mathcal{U}}\delta(1-\gamma)}{1-\delta} \\ \mathcal{U}(P_j, \mathbf{E}) + \beta\delta\Gamma_{EJ} + \dfrac{\overline{\mathcal{U}}\delta(1-\beta)}{1-\delta} & \mathcal{U}(P_j, \mathbf{J}) + \gamma\delta\Gamma_{EJ} + \dfrac{\overline{\mathcal{U}}\delta(1-\gamma)}{1-\delta} \end{pmatrix} \end{matrix} \tag{6}$$

The notations used in (6) are clarified in [28, 29]. The game is modeled as a two-player zero-sum game, in which what one player wins, the other player loses. A zero-sum game models the payoff of the second player (i.e., Eve) as the negative of the payoff of the first player (i.e., Alice). This leads to assigning the second component (i.e., Eve's payoff) of the payoff vector as the negative of the first component (i.e., Alice's payoff) [29]. In a nutshell, what Alice wins, Eve loses.

Equation (6) is a mathematical representation of the two states in the stochastic game shown in Figures 1 and 2. Equation (6) has four entries that represent the four action pairs that the game consists of. For example, we consider the first entry that represents the action pair (E, E), which is $\mathcal{U}(P_e, \mathbf{E}) + \beta\delta\Gamma_{EJ} + \overline{\mathcal{U}}\delta(1-\beta)/(1-\delta)$. The first term $\mathcal{U}(P_e, \mathbf{E})$ represents the instantaneous payoff gained by Alice from being in that mode (i.e., (E, E)). The second term $\beta\delta\Gamma_{EJ}$ highlights the fact that failing in detecting an eavesdropping attack, which consequently will lead to repeating the first state (i.e., Γ_{EJ}), follows a probability distribution (i.e., β in that case). A discount factor δ was also added to that part to ensure that the game will eventually end. Note that the discount factor δ is understood as a measure of urgency for the wireless communication in this work. Finally, the last part, which is $\overline{\mathcal{U}}\delta(1-\beta)/(1-\delta)$, represents the probability distribution of transferring into the next state (i.e., $(1-\beta)$) with the discount factor δ and the total discounted payoff $\overline{\mathcal{U}}/(1-\delta)$ in state 2.

A stationary strategy maps each single state into an action. Stationary strategies are strategies that are independent of the history of previous plays and the current time of the game, which led us to solve this game by using them. This game has an equilibrium in stationary strategies as it is a discounted game. The solution of this game could be given as a solution to the Shapley-Bellmann equation. Shapley-Bellmann equation defines the value of each state recursively in terms of every other state. The Shapley-Bellmann equation for the game Γ_{EJ} is as follows:

$$\mathcal{V} = val\begin{pmatrix} \mathcal{V}_{ee} + \beta\delta\mathcal{V} + \dfrac{(1-\beta)\delta\overline{\mathcal{U}}}{1-\delta} & \mathcal{V}_{ej} + \gamma\delta\mathcal{V} + \dfrac{(1-\gamma)\delta\overline{\mathcal{U}}}{1-\delta} \\ \mathcal{V}_{je} + \beta\delta\mathcal{V} + \dfrac{(1-\beta)\delta\overline{\mathcal{U}}}{1-\delta} & \mathcal{V}_{jj} + \gamma\delta\mathcal{V} + \dfrac{(1-\gamma)\delta\overline{\mathcal{U}}}{1-\delta} \end{pmatrix}, \tag{7}$$

in which $\mathcal{V}$ is the value of the game. Note that, according to the *minimax theorem*, for every finite two-player zero-sum game, there is a game value $\mathcal{V}$. If $\mathcal{V}$ is zero, then we say the game is fair. If $\mathcal{V}$ is positive, we say the game favors player I (i.e., Alice), and if $\mathcal{V}$ is negative, we say the game favors player II (i.e., Eve) [28].

$$\mathcal{V} = \max_x \min_y \begin{pmatrix} x_e \\ x_j \end{pmatrix}^T \begin{pmatrix} \mathcal{V}_{ee} + \beta\delta\mathcal{V} + \dfrac{(1-\beta)\delta\overline{\mathcal{U}}}{1-\delta} & \mathcal{V}_{ej} + \gamma\delta\mathcal{V} + \dfrac{(1-\gamma)\delta\overline{\mathcal{U}}}{1-\delta} \\ \mathcal{V}_{je} + \beta\delta\mathcal{V} + \dfrac{(1-\beta)\delta\overline{\mathcal{U}}}{1-\delta} & \mathcal{V}_{jj} + \gamma\delta\mathcal{V} + \dfrac{(1-\gamma)\delta\overline{\mathcal{U}}}{1-\delta} \end{pmatrix} \begin{pmatrix} y_e \\ y_j \end{pmatrix} \tag{8}$$

By incorporating the probabilities of the mixed strategies in solving this game, we will have (8), in which x_e and x_j are the probabilities of Alice in using the actions E and J, respectively. The probabilities y_e and y_j are the probabilities that Eve will conduct the actions of E and J, respectively. Hence, $x_e + x_j = 1$ and $y_e + y_j = 1$. The payoffs $\mathcal{V}_{ee}, \mathcal{V}_{ej}, \mathcal{V}_{je}$, and $\mathcal{V}_{jj}$ are defined as follows:

$$\mathcal{V}_{ee} = \mathcal{U}(P_e, \mathbf{E}),$$

$$\mathcal{V}_{ej} = \mathcal{U}(P_e, \mathbf{J}),$$

$$\mathcal{V}_{je} = \mathcal{U}(P_j, \mathbf{E}), \text{ and}$$

$$\mathcal{V}_{jj} = \mathcal{U}(P_j, \mathbf{J}). \tag{9}$$

Referring to II-8 in [28] shows that calculating the average payoff depends on the probability of conducting the actions by the two participating players in a 2x2 game. Calculating the average payoff can use the mixed strategy P (i.e., x_e and x_j for Alice) and Q (i.e., y_e and y_j for Eve) for the first and the second players in conducting their actions, respectively. The average payoff to player 1 will be $P^T AQ = \sum_{i=1}^{m}\sum_{j=1}^{n} p_i a_{ij} q_j$, where A is the game matrix. Note that i and j represents the row's and the column's index, respectively. In a nutshell, (8)

calculates the average payoff (i.e., the game value $\mathscr{V}$) in the case of mixed strategies by incorporating the probabilities of conducting the actions of interest into the equation.

For every two-player zero-sum game, there is a value for the game and a mixed strategy for player I (i.e., Alice) and player II (i.e., Eve). Alice's average gain is at least $\mathscr{V}$ no matter what Eve does, and Eve's average loss is at most $\mathscr{V}$ no matter what Alice does. This is called *minimax theorem*, which investigates $\mathscr{V}$ in three cases, which are as follows. (1) If $\mathscr{V}$ is zero, then the game is fair. (2) If $\mathscr{V}$ is positive, then the game favors Alice. (3) If $\mathscr{V}$ is negative, then the game favors Eve. The main justification for these assumptions came from *utility theory*. Since this game is a two-player zero-sum game, then $\max_x \min_y$ coincides with $\min_y \max_x$ as in (8). Assuming that $P_e \neq P_j$ will lead to the following inequalities:

$$\begin{aligned} &\mathscr{V}_{ee} > \mathscr{V}_{je} \text{ and} \\ &\mathscr{V}_{jj} > \mathscr{V}_{ej}. \end{aligned} \tag{10}$$

3.7. Choosing Pure Equilibrium Strategies. This game has four strategies, which are (E, E), (E, J), (J, E), and (J, J). Choosing which strategy can be a pure equilibrium strategy depending on whether the strategy of interest can be a saddle point or not. The strategy can be considered to be a saddle point when it provides the maximum payoff in its column and the minimum payoff in its row in the game's matrix. In this game, if an equilibrium cannot be reached in pure strategies, then it can be found in mixed strategies. We start by inspecting each single strategy whether it can satisfy the conditions of being a saddle point (pure equilibrium strategy) or not.

3.7.1. Strategy (E, E). In order for strategy (E, E) to be a pure equilibrium, it must satisfy the following two conditions:

(1) $\mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (E, E) satisfies both of those conditions as $\mathscr{V}_{ee} > \mathscr{V}_{je}$, which makes it a pure equilibrium strategy. After this step we proceed to calculate its expected payoff, which can be calculated as follows:

$$\mathscr{V} = \begin{pmatrix} x_e \\ x_j \end{pmatrix}^T \begin{pmatrix} \mathscr{V}_{ee} + \beta\delta\mathscr{V} + \dfrac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_e \\ y_j \end{pmatrix} \tag{11}$$

As this strategy is (E, E), the x_e and y_e will be equal to 1. The expected payoff will be equal to

$$\mathscr{V} = \frac{(1-\delta)\,\mathscr{V}_{ee} + (1-\beta)\,\delta\overline{\mathscr{U}}}{(1-\delta)\,(1-\beta\delta)}. \tag{12}$$

3.7.2. Strategy (E, J). In order for strategy (E, J) to be a pure equilibrium, it must satisfy the following two conditions:

(1) $\mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

The second condition is satisfied in some circumstances, but the first condition will never be satisfied, due to the assumption that $\mathscr{V}_{jj} > \mathscr{V}_{ej}$. This means that strategy (E, J) is not a pure equilibrium strategy.

3.7.3. Strategy (J, E). In order for strategy (J, E) to be a pure equilibrium, it must satisfy the following two conditions:

(1) $\mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

The second condition is satisfied in some circumstances, but the first condition will never be satisfied, due to the assumption that $\mathscr{V}_{ee} > \mathscr{V}_{je}$. This means that strategy (J, E) is not a pure equilibrium strategy.

3.7.4. Strategy (J, J). In order for strategy (J, J) to be a pure equilibrium, it must satisfy the following two conditions:

(1) $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (J, J) satisfies both of those conditions as $\mathscr{V}_{jj} > \mathscr{V}_{ej}$, which makes it a pure equilibrium strategy. After this step we proceed to calculate its expected payoff, which can be calculated as follows:

$$\mathscr{V} = \begin{pmatrix} x_e \\ x_j \end{pmatrix}^T \begin{pmatrix} 0 & 0 \\ 0 & \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta} \end{pmatrix} \begin{pmatrix} y_e \\ y_j \end{pmatrix} \tag{13}$$

As this strategy is (J, J), x_j and y_j will be equal to 1. The expected payoff will be equal to

$$\mathscr{V} = \frac{(1-\delta)\,\mathscr{V}_{jj} + (1-\gamma)\,\delta\overline{\mathscr{U}}}{(1-\delta)\,(1-\gamma\delta)}. \tag{14}$$

3.8. Evaluating Equilibrium in Mixed Strategies. By referring to (7), we can consider the game value to be as follows:

$$\mathscr{V} = val \begin{pmatrix} A & B \\ D & C \end{pmatrix}. \tag{15}$$

Then consequently, A, B, C, and D will be as follows:

$$A = \mathscr{V}_{ee} + \beta\delta\mathscr{V} + \frac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{16}$$

$$B = \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + \frac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{17}$$

$$C = \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \frac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta}, \text{ and} \tag{18}$$

$$D = \mathscr{V}_{je} + \beta\delta\mathscr{V} + \frac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta}. \tag{19}$$

Now all the needed terms are written compactly, which will aid in the next mathematical evaluations. Evaluating the mixed stationary equilibrium for X_e, Y_e, the game value $\mathscr{V}$ will be as follows:

$$X_e = \frac{C-D}{A-B+C-D}, \tag{20}$$

$$Y_e = \frac{C-B}{A-B+C-D}, \tag{21}$$

$$\mathscr{V} = \frac{AC-BD}{A-B+C-D}. \tag{22}$$

We follow the same setting as in a previous study in [9]: $\mathscr{V}_{ee} = 1.3$, $\mathscr{V}_{ej} = 0.1$, $\mathscr{V}_{je} = 0.5$, $\mathscr{V}_{jj} = 0.5$, and $\overline{\mathscr{U}} = 3$. The mixed stationary equilibrium for X_e, Y_e, and the game value $\mathscr{V}$ will be as follows:

$$X_e = -\frac{5\delta(\beta-\gamma)(\delta\mathscr{V}-\mathscr{V}+3)}{6(\delta-1)}, \tag{23}$$

$$Y_e = \frac{1}{3}, \tag{24}$$

$$\mathscr{V} = -\frac{(15\delta - 6\beta\delta - 12\delta\gamma + 3)}{(6\delta + 2\beta\delta + 4\delta\gamma - 2\beta\delta^2 - 4\delta^2\gamma - 6)}. \tag{25}$$

Needless to say, before evaluating X_e and Y_e, the game value $\mathscr{V}$ must be evaluated first. Note that δ is a discount factor and it takes values from 0.1 to 0.9, and β and γ are probabilities and they take values from 0.1 to 0.9.

3.9. The Game's Operation. After substituting the value of $\mathscr{V}$ and evaluating the conditions for stationary equilibrium strategies in a closed form for equilibrium in pure and mixed strategies, the following conditions are investigated, in order to decide whether the equilibrium will be in pure or mixed strategies, and thereby obtaining the optimal probabilities for Alice and Eve (i.e., x_e, x_j, y_e, and y_j), and the game values and these conditions are as follows.

3.9.1. Condition 1. If $(\mathscr{V}_{ee}+\beta\delta\mathscr{V}+(1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)) < (\mathscr{V}_{ej}+\gamma\delta\mathscr{V}+(1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta))$ and $(\mathscr{V}_{ee}+\beta\delta\mathscr{V}+(1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)) > (\mathscr{V}_{je}+\beta\delta\mathscr{V}+(1-\beta)\delta\overline{\mathscr{U}}/(1-\delta))$, then the action (E, E) is a saddle point, which will make x_e and y_e equal to one, and the game value for this case will be equal to (12).

3.9.2. Condition 2. If $(\mathscr{V}_{jj}+\gamma\delta\mathscr{V}+(1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)) < (\mathscr{V}_{je}+\beta\delta\mathscr{V}+(1-\beta)\delta\overline{\mathscr{U}}/(1-\delta))$ and $(\mathscr{V}_{jj}+\gamma\delta\mathscr{V}+(1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)) > (\mathscr{V}_{ej}+\gamma\delta\mathscr{V}+(1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta))$, then the action (J, J) is a saddle point, which will make x_j and y_j equal to one, and the game value for this case will be equal to (14).

		Eve: E	Eve: J
Alice	E	$\mathscr{U}(P_e, \mathbf{E})$ / $(\beta, 1-\beta)$	$\mathscr{U}(P_e, \mathbf{J})$ / $(\gamma, 1-\gamma)$
	J	$\mathscr{U}(P_j, \mathbf{E})$ / $(\beta, 1-\beta)$	$\mathscr{U}(P_j, \mathbf{J})$ / $(\gamma, 1-\gamma)$
	S	0 / $(\beta, 1-\beta)$	0 / $(\gamma_s, 1-\gamma_s)$

Figure 3: The first malicious state of the game Γ_{EJS}.

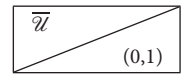


Figure 4: The second safe secure state of the game Γ_{EJS}.

3.9.3. Condition 3. If both conditions 1 and 2 were not satisfied, then a mixed stationary equilibrium arises. Calculating equilibrium in mixed strategies can be done by following (15)-(19), which will lead to (23)-(25).

4. The Extended Stochastic Game

4.1. Introduction. In this game, Alice is aiding an IDS in detecting eavesdropping and jamming attacks. Alice is provided by an additional mode, where she keeps silent, in order to provoke Eve into performing a jamming attack. Strategic allocation of that silent mode is crucial for the successful and effective operation of this mode, where the benefits can be flourished and the secrecy of communication can thrive. A stochastic game has been modeled, in order to tackle this problem and, therefore, the actions of Alice and Eve can be analyzed and investigated even further. It is shown that adding a silent time slot into the transmission protocol can improve the secrecy. Indeed some problems might arise like the delay that such a mode introduces to the communication, but the analysis shows that the benefits and gains can exceed the drawbacks.

4.2. The Game Modeling. As the previous game, we model this game as a two-state stochastic game as shown in Figures 3 and 4. The first state is assumed to be the malicious state, where the communication is being eavesdropped upon or being jammed. It is always assumed that the game is beginning with that state. The second state is the safe secure one. In the stochastic game, remaining in the same state (i.e., state 1) or transferring to the other state (i.e., state 2) depends on a probability distribution. In Figures 3 and 4, the game table for our extended stochastic game is presented. The payoffs for the silent mode are zero; however, Alice will use that mode as it allows her to detect Eve early and remove her from the game and, consequently, she can transmit efficiently without worrying about eavesdropping or jamming attacks.

Figure 3 is the first malicious state, where the probability γ_s is being introduced, as it represents the probability of a missed detection of a jamming attack while Alice is silent. We assumed that γ_s is less than γ, which means that detecting

jamming attacks launched by Eve while Alice is silent is more effective than detecting jamming attacks while Alice is transmitting [9]. Note that the IDS is responsible for detecting Eve whether she is eavesdropping or jamming; however, detecting jamming attacks while being silent is far more efficient and successful. Figure 4 is the second safe secure state that Alice wants to reach. Note that the instantaneous payoffs for the action pairs (S, E) and (S, J) are zero, due to the delay that the silent mode introduces to the communication.

4.3. The Probability Distribution. Detecting Eve is being represented by a probability distribution. If Eve was successfully detected, the game will move to the second state. If Eve was missed, then the cycle will repeat itself until Eve gets detected. The behavior of the game regarding γ and β is the same as the last game. However, some changes are being introduced to this game regarding γ_s. The probability of a successful detection of a jamming attack while Alice is in the silent mode is (1- γ_s), and the probability of a missed detection of a jamming attack while Alice is in the silent mode is γ_s. The probability γ_s was designed to be less than γ, which highlights the effectiveness of detecting Eve's jamming attacks while being silent.

In the case where Alice is silent and Eve is eavesdropping (i.e., the (S, E) action pair), the probability distribution is (β, 1-β), as, in that case, Eve can get provoked to launch a jamming attack especially when the probability of detecting eavesdropping attacks gets higher, and the payoff is zero, due to the delay that the communication will suffer while Alice is being silent.

4.4. The Epoch Progression. The epoch progression in this extended stochastic game is the same as the one that was introduced in the basic stochastic game without any change in its definition or operation.

4.5. Successful and Missed Detection. If Eve was not detected, the game will move to the next time slot and it will be played recursively with a discount factor δ, the same as in the basic game.

If Eve was detected, then Alice will move from the malicious state (i.e., state 1) to the safe secure state (i.e., state 2), the same as in the basic game, adding to that the higher probability in detecting Eve's jamming attacks, especially when Alice is silent as (1 - γ_s) > (1 - γ).

4.6. Shapley-Bellmann Equation. We denote the game in state 1 as Γ_{EJS} and the game played in state 2 as Γ_{END}. In state 2, Eve was already detected and Alice can transmit with rate $\overline{\mathscr{U}}$, which is the most efficient way in communication as no eavesdropping or jamming attacks are being expected.

The extended stochastic proposed game can be presented by (26). The notations have the same meaning and operation as the ones used in the basic stochastic game. The action pairs (S, E) and (S, J) are shown too in (26), where there are no payoffs for both of these actions, but there is a probability distribution assigned to each one of them.

$$\Gamma_{EJS} = \begin{array}{c} \\ E \\ J \\ S \end{array} \begin{array}{c} \begin{array}{cc} E & J \end{array} \\ \begin{pmatrix} \mathscr{U}(P_e, \mathbf{E}) + \beta\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\beta)}{1-\delta} & \mathscr{U}(P_e, \mathbf{J}) + \gamma\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\gamma)}{1-\delta} \\ \mathscr{U}(P_j, \mathbf{E}) + \beta\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\beta)}{1-\delta} & \mathscr{U}(P_j, \mathbf{J}) + \gamma\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\gamma)}{1-\delta} \\ \beta\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\beta)}{1-\delta} & \gamma_s\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\gamma_s)}{1-\delta} \end{pmatrix} \end{array} \quad (26)$$

The action pair (S, E) is represented as $\beta\delta\Gamma_{EJS} + \overline{\mathscr{U}}\delta(1-\beta)/(1-\delta)$. The first part $\beta\delta\Gamma_{EJS}$ represents the probability distribution regarding the case of a missed detection of an eavesdropping attack that can happen with a probability of β and consequently will lead to the repetition of the first state (i.e., Γ_{EJS}), adding to that a discount factor δ to ensure that the game will eventually end. The second part $\overline{\mathscr{U}}\delta(1-\beta)/(1-\delta)$ represents the probability distribution of transferring into the second state, which can happen with a probability of $(1-\beta)$, adding to that the total discounted payoff $\overline{\mathscr{U}}/(1-\delta)$ along with the discount factor δ.

The action pair (S, J) is represented as $\gamma_s\delta\Gamma_{EJS} + \overline{\mathscr{U}}\delta(1-\gamma_s)/(1-\delta)$. The first part $\gamma_s\delta\Gamma_{EJS}$ represents the probability distribution regarding the case of a missed detection of a jamming attack that can happen with a probability of γ_s and consequently will lead to the repetition of the first state (i.e., Γ_{EJS}). The second part $\overline{\mathscr{U}}\delta(1-\gamma_s)/(1-\delta)$ represents the probability distribution of transferring into the second state, which can happen with a probability of $(1-\gamma_s)$, adding to that the total discounted payoff $\overline{\mathscr{U}}/(1-\delta)$.

$$\mathscr{V} = \max_x \min_y \begin{pmatrix} x_e \\ x_j \\ x_s \end{pmatrix}^T \begin{pmatrix} \mathscr{V}_{ee} + \beta\delta\mathscr{V} + \dfrac{(1-\beta)\delta\overline{\mathscr{U}}}{1-\delta} & \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\delta\overline{\mathscr{U}}}{1-\delta} \\ \mathscr{V}_{je} + \beta\delta\mathscr{V} + \dfrac{(1-\beta)\delta\overline{\mathscr{U}}}{1-\delta} & \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\delta\overline{\mathscr{U}}}{1-\delta} \\ \beta\delta\mathscr{V} + \dfrac{(1-\beta)\delta\overline{\mathscr{U}}}{1-\delta} & \gamma_s\delta\mathscr{V} + \dfrac{(1-\gamma_s)\delta\overline{\mathscr{U}}}{1-\delta} \end{pmatrix} \begin{pmatrix} y_e \\ y_j \end{pmatrix} \quad (27)$$

Equation (27) shows the assignment to the optimal probabilities for each action that Alice and Eve can do during the operation of that system. It is shown that there are three actions for Alice in that game, which are being in the eavesdropping mode, jamming mode, or the silent mode. This makes the optimal probabilities be as follows: $x_e + x_j + x_s = 1$. Similarly for Eve, as she is equipped with the action of eavesdropping or jamming, which makes her optimal probabilities for this game be as follows: $y_e + y_j = 1$. Furthermore, by referring to II-8 in [28], it is shown that the average payoff to player 1 is $P^T AQ = \sum_{i=1}^{m} \sum_{j=1}^{n} p_i a_{ij} q_j$ in the case of mixed strategies. Thus by incorporating the probabilities of conducting the actions of interest into the equation, we get (27).

The Shapley-Bellmann equation, where equilibrium strategies can be studied and investigated, is shown in

$$\mathscr{V} = val \begin{pmatrix} \mathscr{V}_{ee} + \beta\delta\mathscr{V} + \dfrac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta} & \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta} \\ \mathscr{V}_{je} + \beta\delta\mathscr{V} + \dfrac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta} & \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta} \\ \beta\delta\mathscr{V} + \dfrac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta} & \gamma_s\delta\mathscr{V} + \dfrac{(1-\gamma_s)\,\delta\overline{\mathscr{U}}}{1-\delta} \end{pmatrix}, \tag{28}$$

in which $\mathscr{V}$ is the value of the game. This game is a two-player zero-sum game. By referring to (26), we follow the same assumptions as in the basic stochastic game such that $P_e \neq P_j$, which leads to the following inequalities:

$$\begin{aligned} &\mathscr{V}_{ee} > \mathscr{V}_{je} \text{ and} \\ &\mathscr{V}_{jj} > \mathscr{V}_{ej}. \end{aligned} \tag{29}$$

4.7. Choosing Pure Equilibrium Strategies. This game has six strategies, which are (E, E), (E, J), (J, E), (J, J), (S, E), and (S, J). Now we start testing which of those strategies can be a saddle point, in which pure equilibrium can be reached. As the equations are quite lengthy, we used the same setting as in [9], in which $\mathscr{V}_{ee} = 1.3, \mathscr{V}_{ej} = 0.3, \mathscr{V}_{je} = 0.8, \mathscr{V}_{jj} = 0.5, \overline{\mathscr{U}} = 5$, and $\gamma = 0.8$. We assume that our proposed parameters β and γ_s are equal to 0.8 and 0.5, respectively. Searching for the pure equilibrium strategies will be based on those parameters.

4.7.1. Strategy (E, E). In order for strategy (E, E) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (E, E) will not be a pure equilibrium strategy as the first condition will never be satisfied, unlike the other two conditions, which are always satisfied.

4.7.2. Strategy (E, J). In order for strategy (E, J) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (E, J) will not be a pure equilibrium strategy as the second condition will never be satisfied, unlike the first condition, which is always satisfied, and the third condition, which is sometimes satisfied based on the parameters.

4.7.3. Strategy (J, E). In order for strategy (J, E) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (J, E) will not be a pure equilibrium strategy as the first and second conditions will never be satisfied, unlike the third condition, which is always satisfied.

4.7.4. Strategy (J, J). In order for strategy (J, J) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (J, J) is a pure equilibrium strategy as all the conditions are satisfied. Specifically, the first two conditions are always satisfied, and the third condition depends on the parameters. The expected payoff can be calculated as follows:

$$\begin{aligned} &\mathscr{V} \\ &= \begin{pmatrix} x_e \\ x_j \\ x_s \end{pmatrix}^T \begin{pmatrix} 0 & 0 \\ 0 & \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_e \\ y_j \end{pmatrix} \end{aligned} \tag{30}$$

Needless to say, as the considered strategy is (J, J), this means that $x_e = 0$, $x_j = 1$, and $x_s = 0$. The same applies for y as $y_e = 0$ and $y_j = 1$. According to that, the game value will be as follows:

$$\frac{\mathscr{V}_{jj} + (1-\gamma)\,\delta\overline{\mathscr{U}}/(1-\delta)}{1-\gamma\delta}. \tag{31}$$

4.7.5. Strategy (S, E). In order for strategy (S, E) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) < \gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (S, E) will not be a pure equilibrium strategy as the second and third conditions will never be satisfied, unlike the first condition, which is always satisfied.

4.7.6. Strategy (S, J). In order for strategy (S, J) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) < \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (S, J) will not be a pure equilibrium strategy as the first condition will never be satisfied, unlike the other two conditions, which can be satisfied based on the parameters.

4.8. Evaluating Equilibrium in Mixed Strategies. By referring to (28), we can consider the game value to be as follows:

$$\mathscr{V} = val\begin{pmatrix} A & B \\ D & C \\ E & F \end{pmatrix}. \tag{32}$$

Consequently, A, B, C, D, E, and F will be as follows:

$$A = \mathscr{V}_{ee} + \beta\delta\mathscr{V} + \frac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{33}$$

$$B = \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + \frac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{34}$$

$$C = \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \frac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{35}$$

$$D = \mathscr{V}_{je} + \beta\delta\mathscr{V} + \frac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{36}$$

$$E = \beta\delta\mathscr{V} + \frac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{37}$$

$$F = \gamma_s\delta\mathscr{V} + \frac{(1-\gamma_s)\,\delta\overline{\mathscr{U}}}{1-\delta}. \tag{38}$$

The extended game has three equilibria in mixed strategies, which are *EJ*, *ES*, and *JS*.

Equilibrium in mixed strategies for *EJ* can be evaluated by using (20), (21), and (22) with (33), (34), (35), and (36).

The mixed stationary equilibrium for *ES* can be obtained by evaluating X_{es}, Y_{es}, and $\mathscr{V}_{es}$ as follows:

$$X_{es} = \frac{F-E}{A-B+F-E}, \tag{39}$$

$$Y_{es} = \frac{F-B}{A-B+F-E}, \tag{40}$$

$$\mathscr{V}_{es} = \frac{AF-BE}{A-B+F-E}. \tag{41}$$

For the sake of brevity, we omitted evaluating those equations as the obtained equations were so lengthy.

The mixed stationary equilibrium for *JS* can be obtained by evaluating X_{js}, Y_{js}, and $\mathscr{V}_{js}$ as follows:

$$X_{js} = \frac{F-E}{D-C+F-E}, \tag{42}$$

$$Y_{js} = \frac{F-C}{D-C+F-E}, \tag{43}$$

$$\mathscr{V}_{js} = \frac{DF-CE}{D-C+F-E}. \tag{44}$$

For the sake of brevity, we omitted evaluating those equations too as the obtained equations were so lengthy.

4.9. The Game's Operation. In the extended game, there will be six conditions that game might be residing in. The conditions are as follows.

4.9.1. Condition 1. If $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta)$, then a pure equilibrium in (J, J) arises. The probabilities x_e, x_s, and y_e will be equal to zero, and the probabilities x_j and y_j will be equal to 1. The game value will be as in equation (31).

4.9.2. Condition 2. If $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$ and $\mathscr{V}_{es} > \mathscr{V}_{js}$, then the game value will be equal to $\mathscr{V}_{es}$, and the optimal probabilities will be as in (39) and (40).

4.9.3. Condition 3. If $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$ and $\mathscr{V}_{js} > \mathscr{V}_{es}$, then the game value will be equal to $\mathscr{V}_{js}$, and the optimal probabilities will be as in (42) and (43).

4.9.4. Condition 4. If $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$ and $\mathscr{V}_{ej} < \mathscr{V}_{es}$, then the game value will be equal to $\mathscr{V}_{es}$, and the optimal probabilities will be as in (39) and (40).

4.9.5. Condition 5. If $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$ and $\mathscr{V}_{ej} > \mathscr{V}_{es}$, then the game value will be equal to $\mathscr{V}_{ej}$, and the optimal probabilities will be as in (20) and (21) while considering the assumptions and parameters for the extended game.

Table 1: Optimal probabilities for each specified game value $\mathscr{V}$.

Game value $\mathscr{V}$	X_e	X_j	X_s	Y_e	Y_j
$\mathscr{V}_{jj}$	0	1	0	0	1
$\mathscr{V}_{ej}$	X_{ej}	1-X_{ej}	0	Y_{ej}	1-Y_{ej}
$\mathscr{V}_{es}$	X_{es}	0	1-X_{es}	Y_{es}	1-Y_{es}
$\mathscr{V}_{js}$	0	X_{js}	1-X_{js}	Y_{js}	1-Y_{js}

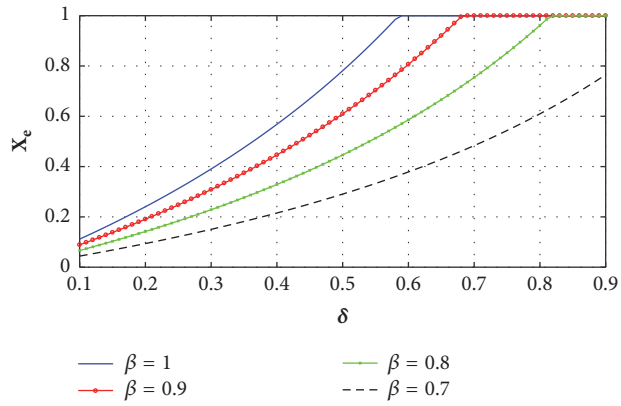


Figure 5: X_e for the basic game.

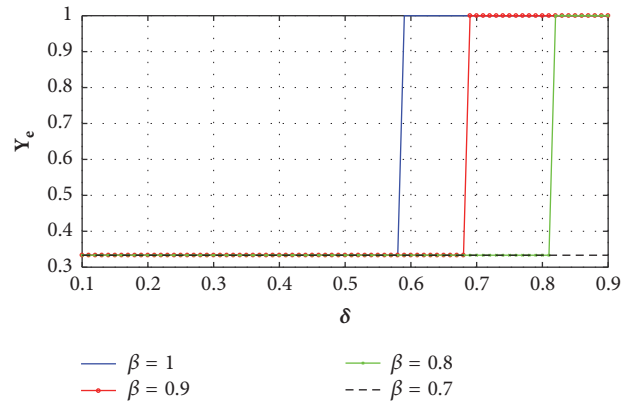


Figure 6: Y_e for the basic game.

4.9.6. Condition 6. If $\gamma_s\delta\mathscr{V}+(1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{ej}+\gamma\delta\mathscr{V}+(1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$, then the game value will be equal to $\mathscr{V}_{ej}$ and the optimal probabilities will be as in (20) and (21).

While considering these conditions, Alice will have three probabilities for the actions that she might consider and the same goes for Eve regarding her two actions. In Table 1, the probabilities are clarified in accordance with each game value that was chosen based on the aforementioned conditions.

5. Results and Analysis

In this section, the optimal probabilities for Alice and Eve and the game value obtained from our proposed games will be presented and investigated. Moreover, we compare our results with the existing work in the literature, in order to validate and verify the effectiveness of our proposed games in providing a better secrecy and reliability to the wireless communication between Alice and Eve.

5.1. Results from the Basic Game. Considering the same setting as the previous study [9], $\mathscr{V}_{ee} = 1.3$, $\mathscr{V}_{ej} = 0.1$, $\mathscr{V}_{je} = 0.5$, $\mathscr{V}_{jj} = 0.5$, and $\overline{\mathscr{U}} = 3$. We fixed γ as 0.5 and we show the optimal probabilities of our basic game for the source Alice to be in the eavesdropping mode and the adversary to be eavesdropping, for $\beta = 1, 0.7, 0.8$, and 0.9, in Figures 5 and 6, respectively. It is worth noting that as $\beta = 1$ our basic scheme will be the same as the conventional game [9].

From Figures 5 and 6, we can see that, as the discount factor δ increases, the optimal probabilities in our basic game and the available game in [9] will increase. This is due to the reason that δ represents the urgency of the communication and the larger the δ is, the lower the urgency of the communication is. Thus, as δ increases, the urgency of the communication decreases and Alice and Eve will go slower toward being in the jamming mode.

Another observation from Figures 5 and 6 indicates that differences between the optimal probabilities in Figures 5 and 6 become more clear when δ takes higher values (higher values of δ means lower communication urgency), thus giving more opportunities for Alice and Eve to take precautions to achieve their goal, i.e., to transmit securely and reliably (Alice's goal) or to eavesdrop or jam the signal (Eve's goal).

Moreover, the results in Figures 5 and 6 indicate that, as the probability of a missed detection of an eavesdropping attack (i.e., β) decreases, the game value of being in the eavesdropping mode increases and Alice and Eve thus start shifting into the jamming mode. This occurs due to the improvement in detecting eavesdropping attacks, which will lead Eve into jamming the signal and consequently; Alice will follow that by being in the jamming mode.

We then illustrate how the overall game values vary with the discount factor δ in Figure 7, from which we can find that the game values increase as δ increases. This is due to the same reason as that for Figures 5 and 6. We can also see from Figure 7 that the game value increases as β decreases. This is because as the probability of detecting eavesdropping attacks increases, the probability of a secure transmission of the information increases and thus the security performance of the system is being improved. Moreover, Figure 7 shows that a noticeable improvement can occur to the game value, especially when δ takes values higher than 0.6. Actually, an improvement of 188% is noticed in the game value after

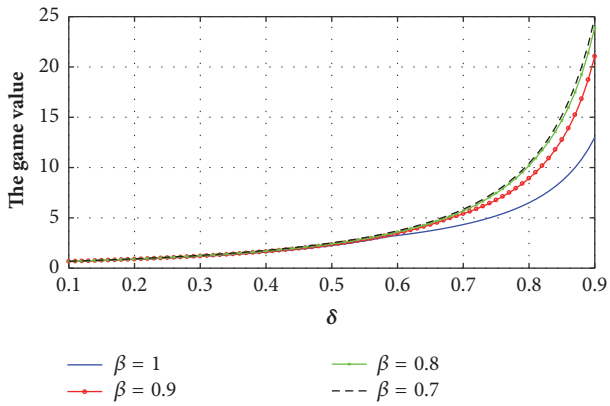


FIGURE 7: The game value for the basic game with $\beta = 0.9$, $\beta = 0.8$, and $\beta = 0.7$, and for the game in [9] with $\beta = 1$.

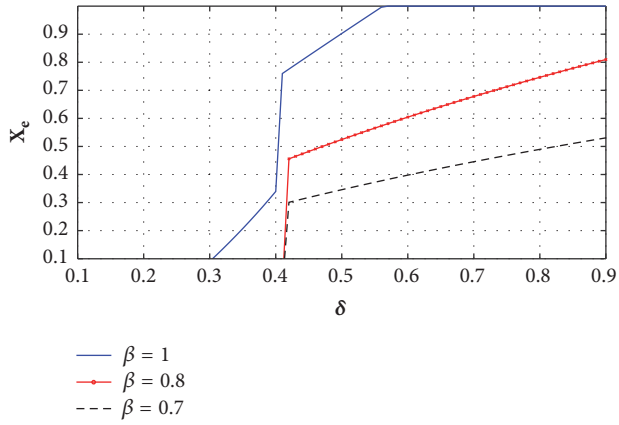


FIGURE 8: X_e for the extended game.

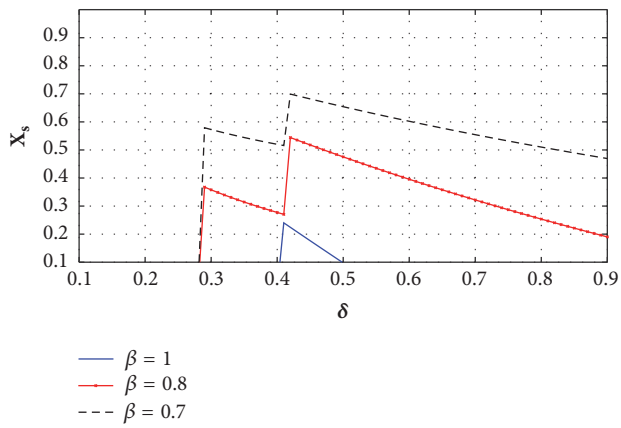


FIGURE 9: X_s for the extended game.

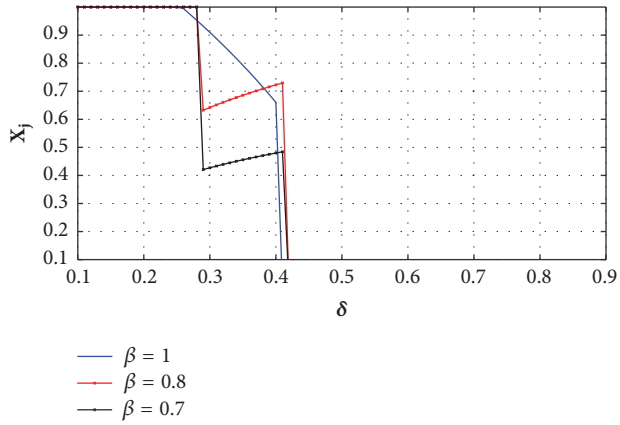


FIGURE 10: X_j for the extended game.

adding the capability of detecting eavesdropping attacks (even though the capability is low) based on the results in Figure 7.

5.2. Results from the Extended Game. In this proposed extended game, we follow the same setting as the previous study [9]: $\mathcal{V}_{ee} = 1.3$, $\mathcal{V}_{ej} = 0.3$, $\mathcal{V}_{je} = 0.8$, $\mathcal{V}_{jj} = 0.5$, and $\overline{\mathcal{U}} = 5$. We fixed γ as 0.8 and we show the optimal probabilities of our extended game when the source Alice is in the eavesdropping, jamming, and silent modes, and when the adversary Eve is eavesdropping and jamming, for $\beta = 1, 0.8$, and 0.7, in Figures 8, 9, 10, 11, and 12, respectively. It is worth noting that, as $\beta = 1$, our basic scheme will be the same as the conventional game [9].

Figures 8 and 11 show that, as the discount factor δ increases, the optimal probability toward being in the eavesdropping mode for Alice or conducting an eavesdropping attack for Eve will increase for both of them. The figures highlight that, as β decrease, the incentives toward being in the eavesdropping mode for Alice or launching an eavesdropping attack for Eve will decrease, as both of them will move toward jamming. Eve will conduct jamming attacks, which will make Alice alter her strategy into being in the jamming or the silent mode.

Figures 9 and 10 integrate with Figure 8. An observation from those two figures must be captured and it is as follows: as β decreases, both of those figures act in an opposite way. In Figure 9, as β decreases, the probability of being in the jamming mode decreases too, but, in Figure 10, as β decreases, the optimal probability of being in the silent mode increases. This means that, as the detection of eavesdropping attacks improves, Eve will start jamming attacks, which in this extended game will result in Alice utilizing her silent mode to increase the probability of detecting Eve while jamming, thus, removing Eve from the game and improving the security of the communication.

Figures 11 and 12 integrate with each other because they represent the actions that Eve can take. As δ increases, Eve becomes more cautious and avoids getting detected so she just launch eavesdropping attacks. The opposite is captured by Figure 12, where Eve conducts jamming attacks with low values of δ. Decreasing the value of β did not have a remarkable effect on Eve's actions; however, as shown before, it affected Alice's actions in a noticeable way and, consequently, it will affect the game value resulting from this game as shown in Figure 13.

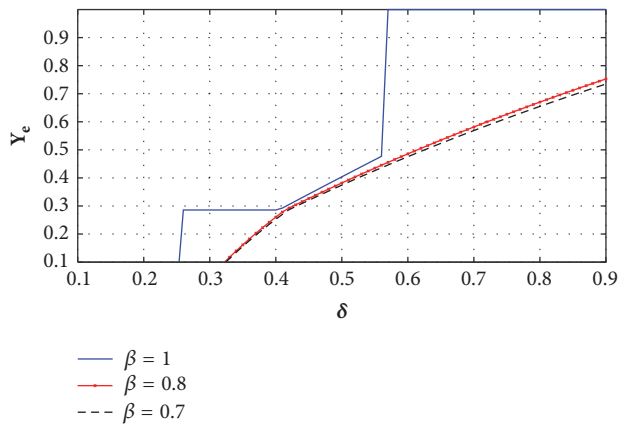


FIGURE 11: Y_e for the extended game.

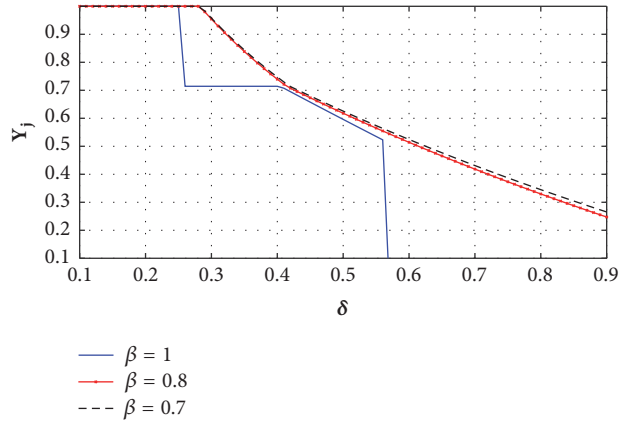


FIGURE 12: Y_j for the extended game.

In Figure 13, the game value is shown, and as δ increases, the game value increases too, for the same reasons mentioned before. Interestingly, when β decreases and becomes 0.8 or 0.7, a huge improvement can be noticed in the game value by 294%. Improvements at high values of β occurs due to embracing the eavesdropping mode by Alice and Eve, as both of them become cautious about choosing the strategy that will generate the highest payoff.

6. Conclusion

This paper studies the secrecy and reliability of a system with one source-destination pair and a sophisticated adversary who conducts eavesdropping and jamming attacks. To analyze and study the behavior and the interactions between the user and the adversary, stochastic game theory is adopted and different games are proposed for different network scenarios. Based on results of the theoretical models, extensive numerical results are then conducted to validate the efficiency of the proposed games. Results show that adding the capability of detecting eavesdropping attacks can push the adversary into jamming the channel much more, which,

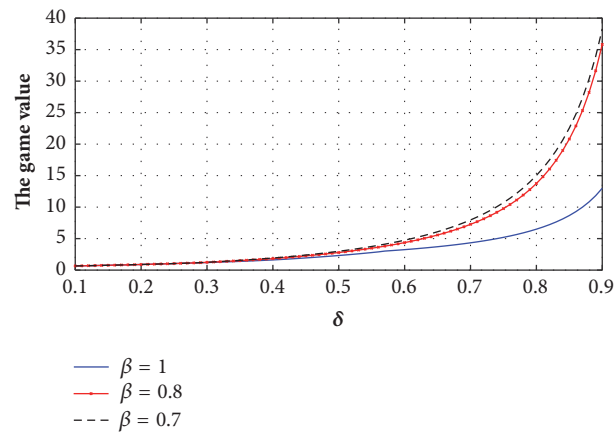


FIGURE 13: The game value for the extended game with $\beta = 0.8$ and $\beta = 0.7$ and for the game in [9] with $\beta = 1$.

on one side, might compromise the reliability of the channel and, on the other side, can aid in detecting the adversary more earlier with an improvement of 188% in the game value. Moreover, when the silent mode is incorporated into the communication protocol of the user, massive payoffs are gained with a huge improvement of 294% in game value. Our work in this paper is of great importance since it can provide theoretical models for the security and reliability study of networks against eavesdropping and jamming attacks, which offers a guideline for the design of future networks.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by The National Key R&D Program of China (Grant no. 2017YFB1400700) and The National Natural Science Foundation of China under Grant nos. U1536202 and 61571352.

References

[1] A. Garnaev and W. Trappe, "Anti-jamming strategies: a stochastic game approach," in *Mobile Networks and Management*, vol. 141 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 230–243, Springer International Publishing, Cham, 2015.

[2] A. Garnaev and W. Trappe, "To eavesdrop or jam, that is the question," in *Ad Hoc Networks*, vol. 129 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 146–161, Springer International Publishing, Cham, 2014.

[3] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel

interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1494–1505, 2016.

[4] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7599–7603, 2017.

[5] J. Xia, F. Zhou, X. Lai et al., "Cache aided decode-and-forward relaying networks: from the spatial view," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 5963584, 9 pages, 2018.

[6] X. Lai, J. Xia, M. Tang, H. Zhang, and J. Zhao, "Cache-aided multiuser cognitive relay networks with outdated channel state information," *IEEE Access*, vol. 6, pp. 897–921, 2018.

[7] F. Shi, L. Fan, X. Liu, Z. Na, and Y. Liu, "Probabilistic caching placement in the presence of multiple eavesdroppers," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 2104162, 10 pages, 2018.

[8] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Basar, "Eavesdropping and jamming in next-generation wireless networks: a game-theoretic approach," in *Proceedings of the Military Communications Conference (MILCOM '11)*, pp. 119–124, November 2011.

[9] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "A game theoretic analysis of secret and reliable communication with active and passive adversarial modes," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2155–2163, 2016.

[10] A. Garnaev and W. Trappe, "The eavesdropping and Jamming Dilemma in multi-channel communications," in *Proceedings of the 2013 IEEE International Conference on Communications, ICC 2013*, pp. 2160–2164, Hungary, June 2013.

[11] S. D'Oro, L. Galluccio, G. Morabito, S. Palazzo, L. Chen, and F. Martignon, "Defeating jamming with the power of silence: a game-theoretic analysis," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2337–2352, 2015.

[12] X. Tang, P. Ren, Y. Wang, Q. Du, and L. Sun, "Securing wireless transmission against reactive jamming: a stackelberg game framework," in *Proceedings of the 58th IEEE Global Communications Conference, GLOBECOM 2015*, USA, December 2015.

[13] L. Jia, F. Yao, Y. Sun, Y. Xu, S. Feng, and A. Anpalagan, "A hierarchical learning solution for anti-jamming Stackelberg game with discrete power strategies," *IEEE Wireless Communications Letters*, vol. 6, no. 6, pp. 818–821, 2017.

[14] X. Tang, P. Ren, and Z. Han, "Combating full-duplex active eavesdropper: a game-theoretic perspective," in *Proceedings of the 2016 IEEE International Conference on Communications, ICC 2016*, Malaysia, May 2016.

[15] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: a hierarchical game perspective," *IEEE Transactions on Communications*, vol. 65, no. 3, pp. 1379–1395, 2017.

[16] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Transactions on Signal Processing*, vol. 61, no. 1, pp. 82–91, 2013.

[17] L. Yuan, K. Wang, T. Miyazaki, S. Guo, and M. Wu, "Optimal transmission strategy for sensors to defend against eavesdropping and jamming attacks," in *Proceedings of the 2017 IEEE International Conference on Communications, ICC 2017*, France, May 2017.

[18] A. Garnaev and W. Trappe, "Bargaining over the fair trade-off between secrecy and throughput in OFDM communications," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 242–251, 2017.

[19] A. Salem, X. Liao, Y. Shen, and X. Lu, "Provoking the adversary by dual detection techniques: a game theoretical framework," in *Proceedings of the 2017 International Conference on Networking and Network Applications (NaNA)*, pp. 326–329, Kathmandu, October 2017.

[20] Q. Wang, P. Xu, K. Ren, and X.-Y. Li, "Towards optimal adaptive UFH-based anti-jamming wireless communication," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 16–30, 2012.

[21] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[22] P. Sanghoon, L. E. Larson, and L. B. Milstein, "Hidden mobile terminal device discovery in a UWB environment," in *Proceedings of the ICUWB2006: 2006 IEEE International Conference on Ultra-Wideband*, pp. 417–421, USA, September 2006.

[23] G. Zhao, W. Shi, L. Li, and S. Li, "Passive primary receiver detection for underlay spectrum sharing in cognitive radio," *IEEE Signal Processing Letters*, vol. 21, no. 5, pp. 564–568, 2014.

[24] S. M. Weiss, R. D. Weller, and S. Driscol, *New measurements and predictions of uhf television receiver local oscillator radiation interference*, Merrill Weiss Group, Metuchen, 2006.

[25] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," in *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05)*, pp. 124–130, November 2005.

[26] M. Felegyhazi and J.-P. Hubaux, "Game theory in wireless networks: a tutorial," Tech. Rep, 2006.

[27] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[28] T. S. Ferguson, *Game Theory*, Mathematics Department, UCLA, 2008.

[29] G. Owen, *Game Theory*, Academic Press, New York, NY, USA, 1982.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 3178303, 16 pages
https://doi.org/10.1155/2018/3178303

Research Article

Adaptive OFDM-IM for Enhancing Physical Layer Security and Spectral Efficiency of Future Wireless Networks

Haji M. Furqan,[1] **Jehad M. Hamamreh**,[1] **and Huseyin Arslan**[1,2]

[1]*Department of Electrical and Electronics Engineering, Istanbul Medipol University, Istanbul 34810, Turkey*
[2]*Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA*

Correspondence should be addressed to Haji M. Furqan; hamadni@st.medipol.edu.tr

Received 27 April 2018; Revised 7 July 2018; Accepted 31 July 2018; Published 15 August 2018

Academic Editor: Lu Wei

In this paper, we propose algorithms for enhancing physical layer security and spectral efficiency of Orthogonal Frequency Division Multiplexing (OFDM) with Index Modulation (IM) systems. Particularly, different activation ratios and/or Constellation Modulation orders are selected adaptively for each subblock based on the channel quality of the legitimate receiver. More specifically, three approaches named as (1) OFDM with Adaptive Index Modulation and Fixed Constellation Modulation (OFDM-AIM-FCM), (2) OFDM with Adaptive Index Modulation and Adaptive Constellation Modulation (OFDM-AIM-ACM), and (3) OFDM with Variable Index Modulation and Variable Constellation Modulation (OFDM-VIM-VCM) are proposed for enhancing physical layer security and spectral efficiency. Simulation results are presented to investigate the effectiveness of the proposed algorithms.

1. Introduction

The inherent broadcast characteristic of wireless communication makes it vulnerable to the passive eavesdropping. Conventionally, security techniques in the upper layers, such as cryptography based techniques, have been employed for secure transmission. However, such security techniques may not be adequate for future decentralized networks due to their high complexity in implementation and computation [1]. Furthermore, the emergence of powerful computing devices makes these techniques vulnerable to sophisticated adversaries. In order to cope up with these problems, Physical Layer Security (PLS) techniques have attracted a lot of attentions [2]. PLS techniques exploit the dynamic features of wireless communications, such as channel randomness, interference, and noise, to prevent the eavesdropper from decoding data while ensuring that the legitimate user can decode it successfully [1]. In the literature, practical signal processing based PLS techniques are proposed in order to secure communication between legitimate parties [3, 4].

On the other hand, Index Modulation (IM) is an emerging technique for future wireless networks because of its higher energy efficiency (EE) and controllable spectral efficiency (SE) [5]. Spatial Modulation (SM) and OFDM-IM are two well-known applications. OFDM-IM especially, has been studied intensively in the literature [5, 6]. Unlike conventional OFDM, which sends data via M-ary signal constellation, in OFDM-IM, data is sent by both M-ary signal constellation and indices of the subcarriers. Due to high EE and adjustable SE, it is considered not only for Machine Type Communication (MTC) but also for high speed wireless communication systems [5, 7]. There are a lot of interesting works for enhancing spectral efficiency of SM and OFDM-IM. In [8], precoding based technique is proposed in which spatial modulation works in both the in-phase and quadrature parts of the received signals, thus conveying additional information bits compared with conventional generalized precoding-aided spatial modulation. In [9], information is conveyed through multiple distinguishable modes and their full permutations. Authors proposed frequency Index Modulation technique and a joint code-frequency Index Modulation techniques for enhancing energy and spectral efficiency in [10, 11], respectively. The proposed techniques are simple and can reduce PAPR without sacrificing data rate. In [12], authors proposed a scheme to enhance the spectral and energy efficiency by using initial conditions to generate different chaotic sequences that can convey extra bits per transmission.

In the following, we will first explain some of the related and popular PLS techniques for OFDM and then for SM and finally for OFDM-IM. In the literature, many promising PLS techniques have been proposed for OFDM. In [13], secret key generation based techniques are proposed for OFDM system. The basic idea is to extract random sequence from the wireless channel. Motivated by the effectiveness of Artificial Noise (AN) for providing PLS, authors in [14] added AN signal on top of OFDM data signal in such a way that when the AN passes through the channel it gets accumulated in Cyclic Prefix (CP) at the legitimate receiver only. Thus, it causes no interference at the legitimate receiver but degrades the performance of Eve. In [15], signal feature suppression based PLS technique was proposed. In this technique certain signal features are suppressed to avoid eavesdropping, such as CP periodicity feature concealing. Furthermore, adaptation based security techniques are also very popular PLS techniques in which transmitter parameters are adjusted in order to fulfill the quality of service (QoS) requirement of the legitimate receiver only, for example, adaptive modulation and coding with Automatic Repeat Request (ARQ) [16], fading based subcarrier activation technique [17], optimal power allocation based techniques [18], channel shortening [19], OFDM-subcarrier index selection for enhancing PLS [20], etc. It may be noted that adaptation based techniques, such as adaptive modulation and coding, can jointly enhance the security and spectral efficiency of wireless systems [18].

Now moving from PLS techniques for OFDM to PLS for IM, there are a few interesting PLS techniques proposed in the literature for SM in MIMO systems [21–25]. In [21], authors proposed transmit precoding based PLS techniques for SM. Moreover, jamming signal based PLS techniques are presented in [22]. In [23], authors proposed PLS techniques based on exploiting the channel reciprocity of Time Division Duplex (TDD) system to redefine the transmit antenna indices. However, the proposed technique cannot secure data symbol modulation. In order to solve this deficiency, the authors in [24] proposed a technique in which the rotation of both the indices of transmit antennas and constellation symbols based on the channel state information of the legitimate receiver are exploited, thus, securing both Index Modulation and data symbol modulation. To the best of the authors' knowledge, the first work related to PLS in OFDM-IM has recently been introduced in [25]. The authors investigate the randomized mapping rules based on channel reciprocity in TDD mode in order to secure both data symbol modulation and Index Modulation but in that work spectral efficiency is not taken into account.

In the literature, the majority of the works related to PLS are focused on the enhancement of security, but only a few works are reported to focus on the joint consideration of both spectral efficiency and security. Moreover, there are some techniques in which security is achieved at the cost of loss in resources.

Inspired by the need for joint consideration of security and SE, in this paper, we propose algorithms for the enhancement of PLS of OFDM-IM and for the quality of service (QoS) based communication in order to enhance SE of OFDM-IM. The proposed algorithms are based on adaptive subcarrier switching and adaptive modulation. More specifically, three approaches are proposed, namely, OFDM with Adaptive Index Modulation and Fixed Constellation Modulation (OFDM-AIM-FCM) for enhancing PLS and SE, OFDM with Adaptive Index Modulation, and Adaptive Constellation Modulation (OFDM-AIM-ACM) for enhancing PLS and SE and OFDM with Variable Index Modulation and Variable Constellation Modulation (OFDM-VIM-VCM) for QoS based communication in order to enhance SE. In particular, the first two approaches are based on channel based adaptation of subcarrier activation ratios and Constellation Modulation orders of subblocks in OFDM-IM by utilizing channel reciprocity concept in TDD mode while the third approach is based on QoS based adaptation. The works in [8, 9] focus on spectral efficiency alone without considering security concerns while first two proposed schemes provide security with some enhancement in spectral efficiency. The scheme in [9] and our third proposed algorithm both target enhanced SE. However, our proposed technique keeps the benefits of OFDM-IM in terms of low ICI and high EE, whereas the scheme presented in [9] does not keep these benefits.

The rest of the paper is organized as follows. The basic system model is presented in Section 2. The details of basic adaptive OFDM-IM are described in Section 3.1. The details of the developed algorithms are revealed in Section 3.2. The throughput of the proposed algorithms is presented in Section 4.1 while the theoretical BER performance analysis of the adaptive OFDM-IM (OFDM-ACM-FIM) is discussed in Section 4.2. Computer simulation results are exhibited and discussed in Section 5. Finally, the paper is concluded in Section 6.

Bold, lowercase, and capital letters are used for column vectors and matrices, respectively. rank ($\mathbf{A}$) and det ($\mathbf{A}$) denote the rank and determinant of $\mathbf{A}$, respectively. $\lambda_i(A)$ is the i_{th} eigenvalue of $\mathbf{A}$. The expectation of an event is denoted by $E\{\cdot\}$ and $P(\cdot)$ stands for probability of an event. $\mathcal{S}$ denotes the complex signal constellation of size M. $\lfloor\cdot\rfloor$ is the floor function and $Q(\cdot)$ denotes the tail probability of the standard Gaussian distribution. $\mathcal{CN}(0, \sigma_X^2)$ represents the distribution of a circularly symmetric complex Gaussian random variable X with variance σ_X^2. $(\cdot)^H$ and $(\cdot)^T$ denote Hermitian transposition and transposition, respectively.

2. System Model and Preliminaries

In this work, we consider a Single Input Single Output (SISO) OFDM-IM system. The basic system model consists of a legitimate transmitter (Tx), Alice, that wants to communicate securely with a legitimate receiver (Rx), Bob, in the presence of an illegitimate node, Eve, as shown in Figure 1, where TDD is considered as an operational mode. The notations $\mathbf{h}_{ab}(\mathbf{h}_b) \in^{[1\times L]}$ and $\mathbf{h}_{ae}(\mathbf{h}_e) \in^{[1\times L]}$ denote the slow varying multipath Rayleigh fading exponentially decaying channel from Alice to Bob and Alice to Eve, respectively, where L is the length of the channel. In this work, Eve is considered to be passive, and hence there is no knowledge of Eve's channel at Alice. Moreover, it is also assumed that Eve is not very

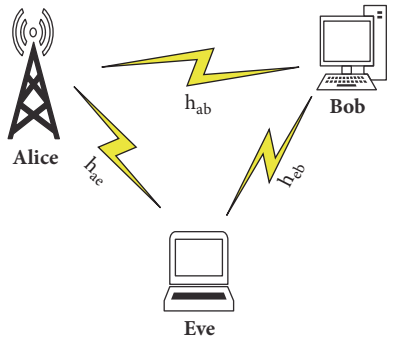


Figure 1: System model.

close to Bob such that Bob and Eve will have independent channel realizations [20]. In addition, the property of channel reciprocity is also adopted in this work, where the channel from Alice to Bob ($\mathbf{h}_{ab}$) can be estimated from the channel of Bob to Alice ($\mathbf{h}_{ba}$) in TDD.

3. Adaptive OFDM-IM Model and Proposed Algorithms

In this Section, basic concepts related to OFDM-IM with respect to adaptivity as well as proposed algorithms for enhancing PLS and SE are presented.

3.1. Adaptive OFDM-IM Model. In this subsection, OFDM-IM model [5, 6] with respect to channel based adaptation (CBA) is explained. In this system, we employ a simplified OFDM-IM model as presented in Figures 2 and 3, where Figure 2 presents the OFDM-IM transmitter (Tx) while Figure 3 presents the OFDM-IM receiver (Rx), respectively. Let us suppose that m_i number of information bits, corresponding to i_{th} block, enters the OFDM-IM for the transmission, where the value of m_i is different for different OFDM-IM blocks due to CBA and will be explained in Section 3.2. These m_i bits are split into G groups, such that each group contains p_j bits, where $j \in \{1, \ldots, G\}$. The p_j may be different for different groups based on CBA. The total number of bits in i_{th} block can be represented as follows:

$$m_i = \sum_{j=1}^{G} p_j \tag{1}$$

In OFDM-IM, the subcarriers are also divided into G subblocks. The number of subcarriers in any subblock, β, is n, where $n = N/G$ and N is the total number of subcarriers in any OFDM-IM block. After that, p_j bits of each group are mapped to corresponding subblock, β. This mapping is done by means of symbols and by the indices of subcarriers based on CBA.

The p_j bits of each group are divided into p_{1j} and p_{2j} bits, where p_{1j} bits are carried by indices and p_{2j} bits are carried by symbols. More specifically, in each OFDM subblock, k_j out of n subcarriers are active and selected by index selector based on p_{1j} bits while the symbols corresponding to inactive subcarriers are set to zero. In the proposed work, each subblock may have different Subcarrier Activation Ratio (SAR), k_j/n, and Constellation Modulation (CM) order based on CBA. In this work, we consider four cases for SAR that are 1/4, 2/4, 3/4, and 4/4 and four cases of CM that are 2, 4, 8, and 16. The index selector of OFDM-IM uses a predefined lookup table for each subblock based on its SAR. Table 1 presents lookup tables for SARs of 1/4, 2/4, and 3/4, while the case of SAR value of 4/4 does not require any lookup table because no information is sent by indices (Classical OFDM). The remaining p_{2j} bits are mapped on to M-ary data symbols, based on subblock CM, that modulates the active subcarriers. In this way, the information is conveyed by both indices of subcarriers and M-ary symbols that modulate the active subcarriers.

Table 1: Lookup table for SAR values of {1/4, 2/4, 3/4}.

(a) SAR: [1/4]

Bits	Subcarrier indices
00	1
01	2
10	3
11	4

(b) SAR: [2/4]

Bits	Subcarrier indices
00	1, 2
01	2, 3
10	3, 4
11	1, 4

(c) SAR: [3/4]

Bits	Subcarrier indices
00	1, 2, 3
01	1, 2, 4
10	1, 3, 4
11	2, 3, 4

The selected indices are given by $I_\beta = \{i_{\beta,1}, \ldots, i_{\beta,k_j}\}$, where $\beta \in \{1, \ldots, G\}$, $i_{\beta,\gamma} \in \{1, \ldots, n\}$, and $\gamma \in \{1, \ldots, k_j\}$. Therefore, the total number of bits carried by the indices of all G groups in the i_{th} block is given by

$$m_{1i} = \sum_{j=1}^{G} p_{1j}, \tag{2}$$

$$p_{1j} = \left\lfloor \log_2 \binom{n}{k_j} \right\rfloor. \tag{3}$$

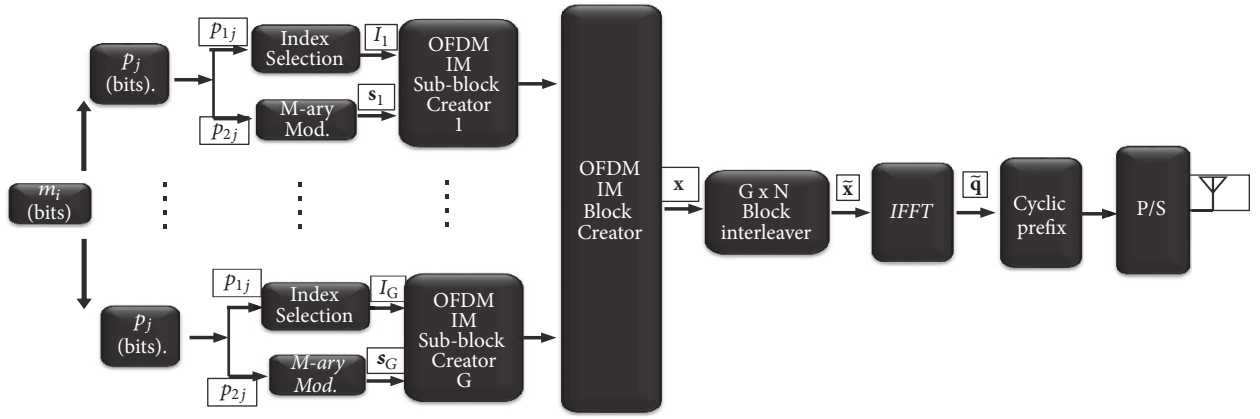


Figure 2: Basic OFDM-IM Tx.

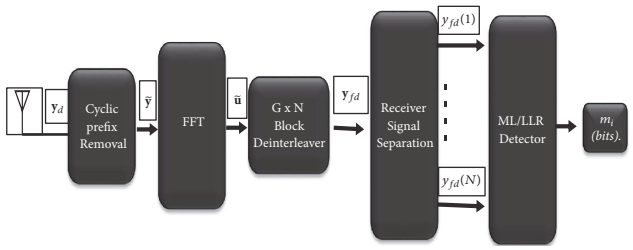


Figure 3: Basic OFDM-IM Rx.

Hence, I_β has $c = 2^{p_{1j}}$ possible realizations. On the other hand, the total number of information bits carried by M-ary signal constellations is given by

$$m_{2i} = \sum_{j=1}^{G} p_{2j}, \tag{4}$$

$$p_{2j} = k_j \log_2 M_j, \tag{5}$$

where M_j is the modulation order and k_j is the number of active subcarriers in each subblock. In this scheme, the total number of active subcarriers in each OFDM block is given as $K = \sum_{j=1}^{G} k_j$. The output of M-ary modulator is given as

$$\mathbf{s}_\beta = \left[s_\beta(1), \ldots, s_\beta\left(k_j\right)\right], \tag{6}$$

where $s_\beta(\gamma) \in \mathcal{S}$. It should also be noted that the signal constellation is normalized to have unit average power. Finally, the OFDM block creator uses I_β and $\mathbf{s}_\beta$ to create all of subblocks and then forms $N \times 1$ main OFDM-IM block by concatenation of G subblocks and is given by

$$\mathbf{x} = \left[x_1, x_2, \ldots, x_N\right]^T. \tag{7}$$

where $x(\alpha) \in \{0, \mathcal{S}\}$, $\alpha \in \{1, \ldots, N\}$. After this point, the block $\mathbf{x}$ is passed through $G \times N$ interleaver to ensure that the subcarriers in each subblocks are affected by uncorrelated wireless fading channels.

The resultant OFDM block after interleaver, $\tilde{\mathbf{x}}$, is then passed through IFFT process, $(N/\sqrt{K})IFFT\{\tilde{\mathbf{x}}\}$, which maps the frequency domain data symbols to time domain points represented as follows:

$$\tilde{\mathbf{q}} = \left[q_1, q_2, \ldots, q_N\right]^T \tag{8}$$

In order to avoid ISI, a CP of length (L_{cp}) is added at the beginning of each block, where L_{cp} is assumed to be equal to or greater than the channel delay spread. Finally, the resultant signal $\tilde{\mathbf{q}} \in C^{[N+L\times 1]}$ is transmitted through the Rayleigh fading channel, which is assumed to be constant during the transmission of each OFDM block and reaches both Bob and Eve. The baseband signal received at Bob can be represented as

$$\mathbf{y}_b = \mathbf{h}_b * \tilde{\mathbf{q}} + \mathbf{z}_b, \tag{9}$$

where $\mathbf{h}_b$ is the channel impulse response seen by Bob and $\mathbf{z}_b$ represents additive white Gaussian noise (AWGN) at Bob with distribution of $\mathcal{CN}(0, N_{0,T})$. Similarly, the baseband signal received at Eve is given by

$$\mathbf{y}_e = \mathbf{h}_e * \tilde{\mathbf{q}} + \mathbf{z}_e, \tag{10}$$

where $\mathbf{h}_e$ is the channel impulse response seen by Eve and $\mathbf{z}_e$ represents AWGN at Eve with distribution of $\mathcal{CN}(0, N_{0,TE})$.

The basic block diagram of the receiver is presented in Figure 3. The receiver (both Bob and Eve) first removes the CP and then applies FFT on the received time domain signal $\mathbf{y}_d$ with normalization factor of $K/\sqrt{N}$ and finally deinterleaves the resultant signal to get the received signal, $\mathbf{y}_{fd} = [y_{fd}(1), y_{fd}(2), \ldots, y_{fd}(N)]^T$, in frequency domain, where d can be Bob or Eve.

The receiver task is to detect the indices of active subcarriers and corresponding symbols by processing, $y_{fd}(\alpha)$, where $\alpha = \{1, \ldots, N\}$. In our algorithm, we use lookup table based modified Log-likelihood-Ratio (LLR) detector for detection of active indices for each subblock [6]. First of all, LLR values of frequency domain symbols corresponding to each subcarrier are calculated as follows:

$$\lambda(\alpha) = \ln\left(\frac{\sum_{\chi=1}^{M} P\left(x(\alpha) = s_\chi \mid y_{fd}(\alpha)\right)}{P\left(x(\alpha) = 0 \mid y_{fd}(\alpha)\right)}\right) \tag{11}$$

The above equation can be further simplified by using Bayes' formula as

$$\lambda(\alpha) = \ln(k) - \ln(n-k) + \frac{\left|y_{fd}(\alpha)\right|^2}{N_{0,f}} + \ln\left(\sum_{\chi=1}^{M} \exp\left(-\frac{1}{N_{0,f}}\left|y_{fd}(\alpha) - h_F(\alpha)\, s_\chi\right|^2\right)\right) \quad (12)$$

where $N_{0,f}$ is the noise variance in frequency domain ($N_{0,f} = (K/N)N_{0,T}$). In (12), numerical overflow can be prevented by using the Jacobian logarithm [27]. For example, for $M = 2$ and $k_j = n/2$, (12) simplifies to

$$\lambda(\alpha) = \max(a,b) + \ln\left(1 + \exp\left(-|b-a|\right)\right) + \frac{\left|y_{fd}(\alpha)\right|^2}{N_{0,f}} \quad (13)$$

where $b = -|y_{fd}(\alpha) + h_f(\alpha)|^2/N_{0,f}$ and $a = -|y_{fd}(\alpha) - h_f(\alpha)|^2/N_{0,f}$. In our work, we also use higher order modulation and use the following identity: $\ln(e^{a_1} + e^{a_1} + \cdots + e^{a_M}) = (f_{max}(f_{max}(\ldots f_{max}(f_{max}(a_1,a_2),a_3),\ldots),a_M))$, where $f_{max}(a,b) = \ln(e^{a_1}+e^{a_1}) = max(a_1,a_2)+\ln(1+e^{-|a_1-a_2|})$.

In order to detect the active indices, LLR value corresponding to each subcarrier is calculated using (12). Afterwards, the receiver calculates the sum of LLRs corresponding to each combination of the subcarriers in the lookup table with respect to subblock based SAR as follows:

$$d_\beta^w = \sum_{\gamma=1}^{k_j} \lambda\left(n(\beta-1) + i_{\beta,\gamma}^w\right) \quad (14)$$

where $w = 1, \ldots, c$ and c is the total number of combinations of subcarriers in the lookup table with respect to any SAR. The receiver makes a decision of set of active indices by selecting the set with maximum value of sum of LLRs as follows:

$$\widehat{w} = \arg\max_w d_\beta^w \quad (15)$$

After selecting the set with maximum LLR, the receiver gets the set of active indices corresponding to SAR. After the detection of active subcarrier, the information is then passed to index demapper based on lookup table to estimate m_{1i} bits. After determination of active indices, the demodulation of the constellation symbols (M-ary symbols) is carried out and finally we get m_{2i} bits.

3.2. Proposed Algorithms for OFDM-IM. In this subsection, proposed algorithms for enhancing PLS and spectral efficiency are presented.

3.2.1. OFDM-AIM-FCM. In OFDM-AIM-FCM, SAR for each subblock is changed adaptively while fixed CM is used for all subblocks. The basic idea of OFDM-AIM-FCM is presented in Figure 4. The basic steps for OFDM-AIM-FCM algorithm are as follows:

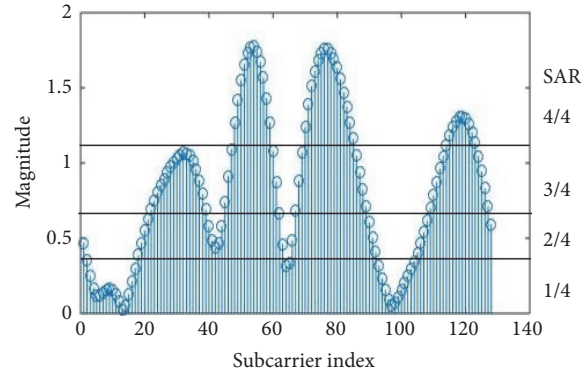


Figure 4: Proposed: OFDM-IM-AIM-FCM.

(i) In the first step, the channel is estimated at all nodes. In order to do that, Alice and Bob send a reference signal to each other (within coherence time). After channel estimation, they take FFT to convert the channel coefficient vector into frequency domain vector, $\mathbf{h}_f$

(ii) Afterwards, the vector $\mathbf{h}_f$ at each node is divided into G subblocks with n elements in each of, β, subblock, where $n = N/G$

(iii) In the next step, the average, $av(\beta)$, of absolute values of subblock's elements is calculated as follows:

$$av(\beta) = \frac{\sum_{r=1}^{n}\left|hs_{\beta,r}\right|}{n}, \quad (16)$$

where $hs_{\beta,r}$ is the r_{th} element of β subblock

(iv) After finding the average value, $av(\beta)$, for each of G subblocks, they are divided into four groups based on their $av(\beta)$. More specifically, find the mean, *me*, of **av**, where **av** is a vector containing average values for all subblocks. Afterwards, divide the subblocks into two groups, $\mathbf{g}_1$ and $\mathbf{g}_2$, by comparing their corresponding $av(\beta)$ values with *me*. The subgroup $\mathbf{g}_1$ contains those subblocks whose $av(\beta)$ values are greater than or equal to *me* while $\mathbf{g}_2$ contains those subblocks whose values of $av(\beta)$ are less than *me*. Afterwards, both $\mathbf{g}_1$ and $\mathbf{g}_2$ are further divided into two subgroups by using mean method as explained above. As a result, G subblocks are divided into four groups such as $\mathbf{g}_{11}$, $\mathbf{g}_{22}$, $\mathbf{g}_{33}$, and $\mathbf{g}_{44}$. The resultant groups are sorted in descending order in terms of average channel magnitude such that $\mathbf{g}_{11}$ contains those subblocks that have the highest values of $av(\beta)$ while $\mathbf{g}_{44}$ contains subblocks with the lowest values of $av(\beta)$

(v) Finally, higher SAR values are selected for those groups that have higher values of $av(\beta)$ while lower values of SAR are selected for those groups that have lower values of $av(\beta)$, such that SAR values of 4/4, 3/4, 2/4, and 1/4 are selected for groups $\mathbf{g}_{11}$, $\mathbf{g}_{22}$, $\mathbf{g}_{33}$, and $\mathbf{g}_{44}$, respectively, as presented in Table 2

Table 2: OFDM-AIM-FCM.

Group	SAR
$\mathbf{g}_{11}$	4/4
$\mathbf{g}_{22}$	3/4
$\mathbf{g}_{33}$	2/4
$\mathbf{g}_{44}$	1/4

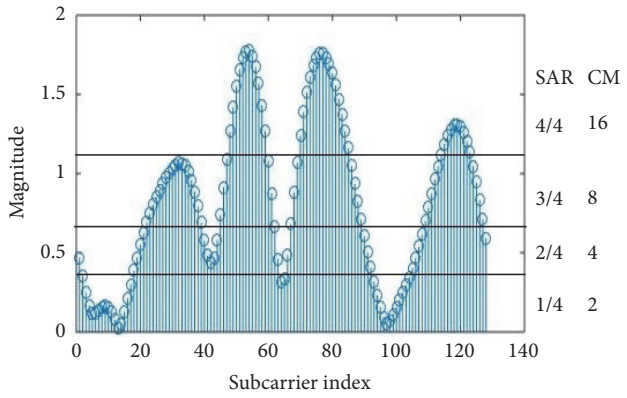


Figure 5: Proposed: OFDM-AIM-ACM.

Based on the above algorithm (OFDM-AIM-FCM), Alice determines SAR for each subblock and the total number of bits, m_i, for i_{th} block. Afterwards, data is loaded to the indices and the symbols based on adaptive SAR and fixed CM and a block is generated using adaptive OFDM-IM model explained in Section 3.1. Finally, the resultant signal $\tilde{\mathbf{q}} \in C^{[N+L\times 1]}$ is transmitted through the Rayleigh fading channel and reaches both Bob and Eve.

Bob and Eve will then detect the active subcarriers based on SAR values of subblocks with respect to OFDM-AIM-FCM. The resultant information is passed to the index demapper that provides the information carried by indices. After determination of active indices, constellation symbols are demodulated.

Thanks to channel decorrelation assumptions, Bob and Eve will have differences in their determined subblock based SAR values. Due to channel reciprocity employment, the SAR values for different subblocks determined by Bob are similar to that of Alice's while they are different at Eve. This dissimilarity in SAR values for different subblocks at Eve leads to wrong detection of bits at Eve. Hence, there is a performance gap at Bob and Eve, which enables the secure communication between Alice and Bob.

3.2.2. OFDM-AIM-ACM. In OFDM-AIM-ACM both the SAR and CM order are adaptively varied based on channel of legitimate node in order to enhance PLS and SE. The basic concept of OFDM-AIM-ACM is presented in Figure 5.

(i) First four steps of OFDM-AIM-ACM are similar to that of OFDM-AIM-FCM. Specifically, $\mathbf{h}_f$ vector is divided into G subblocks. The resultant G subblocks are grouped into four groups such as $\mathbf{g}_{11}$, $\mathbf{g}_{22}$, $\mathbf{g}_{33}$, and $\mathbf{g}_{44}$ using mean method as explained earlier

Table 3: OFDM-AIM-ACM.

Group	SAR	M
$\mathbf{g}_{11}$	4/4	16
$\mathbf{g}_{22}$	3/4	8
$\mathbf{g}_{33}$	2/4	4
$\mathbf{g}_{44}$	1/4	2

(ii) The basic difference in OFDM-AIM-ACM as compared to OFDM-AIM-FCM is that both the SAR and CM order are varied adaptively for each subblock in it. In OFDM-AIM-ACM, higher SAR with higher order CM are selected for those groups that have high values of $av(\beta)$ while lower values of SAR with lower order CM are selected for those groups that have lower values of $av(\beta)$. Based on OFDM-AIM-ACM, SAR value of 4/4 is selected with $M = 16$, 3/4 with 8, 2/4 with 4, and 1/4 with 2 for groups $\mathbf{g}_{11}$, $\mathbf{g}_{22}$, $\mathbf{g}_{33}$, and $\mathbf{g}_{44}$, respectively, as presented in Table 3

Based on the above-mentioned algorithm (OFDM-AIM-ACM), Alice determines SAR and CM order for each subblock and the total number of bits, m_i, for i_{th} block. Afterwards, data is loaded to the indices and symbols based on adaptive SAR and adaptive CM and finally a block is generated using adaptive OFDM-IM model explained in Section 3.1. Finally, the resultant signal $\tilde{\mathbf{q}} \in C^{[N+L\times 1]}$ is transmitted through the Rayleigh fading channel and reaches both Bob and Eve.

Bob and Eve will first detect active subcarriers based on subblock-SAR values with respect to OFDM-AIM-ACM. The resultant information is then passed to the index demapper which provides the information carried by indices. After determination of active indices, constellation symbols are demodulated based on subblock CM order with respect to OFDM-AIM-ACM.

Due to the channel decorrelation, the SAR values and CM orders of different subblocks determined by Bob and Eve based on OFDM-AIM-ACM are different. The SAR values and CM orders of different subblock determined by Bob are similar to that of Alice's due to channel reciprocity, while it is different at Eve as compared to Alice. This difference in subblock based SAR values as well as CM order at Eve compared to Alice will cause errors in the detection of data carried by indices and symbols. Hence, there is a significant performance gap between Bob and Eve. This performance gap will ensure secure communication between Alice and Bob. It should also be noted that OFDM-AIM-ACM is more difficult to be attacked as compared to OFDM-AIM-FCM because in the latter case only subblock based SAR is varied adaptively, while in the former both the SAR and CM are varied adaptively.

3.2.3. OFDM-VIM-VCM for QoS. In OFDM-VIM-VCM, the IM and CM order are varied for QoS based communication in order to maximize the spectral efficiency. The basic motivation behind this approach is that, instead of using complex

optimization based approaches for maximizing spectral efficiency, simple simulation based approach is proposed for this purpose. The basic concept is to vary the SAR and CM with the change in average SNR to maximize the spectral efficiency while fulfilling certain QoS requirement. The basic procedure can be summarized as follows:

(i) First, OFDM-IM is implemented with different modulation order for each SAR. Afterwards, BER and throughput curves are simulated for each of SAR value with higher order modulation; for example, in this work, we are considering SAR values of 1/4, 2/4, 3/4, and 4/4 and CM order of 2, 4, 8, and 16

(ii) Then, all BER curves are merged in one figure and all throughput curves in another figure

(iii) In the next step, certain BER curves are selected based on their performance gap and throughput values. More specifically, among the BER curves that have similar performance, select a curve that has maximum value of throughput. From the selected curves in the former step, select those curves that have a performance gap between them. Afterwards, the throughput curves corresponding to selected BER curves are also selected

(iv) Finally, switching table is constructed based on QoS requirement. The table depicts the values of different SAR and CM of system for different average SNR ranges to maximize the spectral efficiency while fulfilling QoS requirements

(v) After construction of switching table, this table is then used for QoS based communication for maximizing spectral efficiency

4. Performance Analysis of Adaptive OFDM-IM Scheme

4.1. Throughput of Adaptive OFDM-IM. This section presents the details related to the throughput of the adaptive OFDM-IM. The throughput for adaptive OFDM-IM can be given as

$$Throughput = \frac{\sum_{j=1}^{G} p_{1j} + \sum_{j=1}^{G} p_{2j}}{N + N_{CP}} \tag{17}$$

where $p_{1j} = \left\lfloor \log_2 \binom{n}{k_j} \right\rfloor$ and $p_{2j} = k_j \log_2 M_j$. The basic difference between conventional OFDM-IM and adaptive OFDM-IM is in k_j and M_j which are fixed in the former but vary adaptively in the latter. In case of OFDM-ACM-FCM, k_j is different for different subblocks and M_j is the same for all subblocks while in case of OFDM-ACM-AIM and OFDM-VIM-VCM both k_j and M_j are different for different subblocks.

4.2. Performance Analysis of Adaptive OFDM-IM Scheme. This section presents the analytical evaluation for the upper bound of the average bit error probability (ABEP) of the adaptive OFDM-IM scheme (OFDM-AIM-FCM with $M = 2$) based on pairwise error probability (PEP). In this analysis, ML detector with a lookup table is considered whose results are equal to and applicable to the modified LLR detector (near ML) with a lookup table. This is because of the fact that the error performance of ML detector is almost similar to that of modified LLR detector as explained in [6].

In the conventional OFDM-IM, the same SAR values are used in all subblocks while in case of OFDM-AIM-FCM different SARs values are used in different subblocks. As explained earlier, there are N subcarriers that are divided into G subblocks with n subcarriers in each subblock. In OFDM-AIM-FCM, the subblocks are divided into four groups, $\mathbf{g_{44}}$, $\mathbf{g_{33}}$, $\mathbf{g_{22}}$, and $\mathbf{g_{11}}$, with SAR values of 1/4, 2/4, 3/4, and 4/4, respectively, used in them. In order to simplify the analysis, we can assume that the size of each of the above-mentioned groups in OFDM-AIM-FCM is the same. It should be noted that the PEP event is similar in the subblocks corresponding to the same group and is different for subblocks that belong to different groups.

In the first step, the average bit error probability (ABEP) of first subblock of first group is calculated and then the results are extended to include subblocks of other groups. Afterwards, we will find average ABEP for each group and finally find the ABEP of adaptive OFDM-IM subblock.

The input-output relationship in frequency domain for the first subblock of first group is given as follows:

$$\mathbf{y} = \mathbf{X}\mathbf{h} + \mathbf{w}. \tag{18}$$

where $\mathbf{X}$ is an $n \times n$ diagonal matrix containing $[x(1), x(2), \ldots, x(n)]^T$ as diagonal data elements, $\mathbf{y}$ is the received signal subvector containing $[y_{fd}(1), y_{fd}(2), \ldots, y_{fd}(n)]^T$, $\mathbf{h}$ is the channel subvector containing $[h_f(1), h_f(2), \ldots, h_f(n)]^T$, and $\mathbf{w}$ is the noise subvector containing $[w(1), w(2), \ldots, w(n)]^T$. Let us assume that $\mathbf{K_n} = E[\mathbf{h}\mathbf{h}^H]$ is a covariance submatrix of rank r_1 ($r_1 = \text{rank}(\mathbf{K_n})$). This matrix is valid for all subblocks. Moreover, the concatenation of these small covariance submatrices gives $\mathbf{K}$ matrix which is the covariance matrix of $\mathbf{h}_f$.

Let us suppose that $\mathbf{X}$ signal is transmitted through channel and received as erroneous signal $\widehat{\mathbf{X}}$. The receiver can make decision error in both constellation symbols and indices. One of the best ways to analyse these errors is in terms of PEP. In [28], an expression for conditional pairwise error probability (CPEP) is presented for the model of (18) and is given as

$$P\left(\mathbf{X} \longrightarrow \widehat{\mathbf{X}} \mid \mathbf{h}\right) = Q\left(\sqrt{\frac{\delta}{2N_{0,f}}}\right), \tag{19}$$

where $\delta = \mathbf{h^H A h}$ and the $\mathbf{A}$ matrix equals to $(\mathbf{X} - \widehat{\mathbf{X}})^H(\mathbf{X} - \widehat{\mathbf{X}})$. In order to find the unconditional pairwise error probability (UPEP), the expectation of CPEP is taken with respect to the channel and is given as follows: $P(\mathbf{X} \longrightarrow \widehat{\mathbf{X}}) = E_h\{Q(x)\}$. Based on [29], we can define an orthogonal matrix $\mathbf{F}$ where $\mathbf{F^H F} = \mathbf{I}$. The covariance submatrix and channel can be simplified as $\mathbf{K_n} = \mathbf{F D F^H}$ and $\mathbf{h} = \mathbf{F u}$, respectively. Here, $\mathbf{D}$ is a diagonal matrix and is equal to $\mathbf{D} = E[\mathbf{u}\mathbf{u}^\mathbf{H}] = \mathbf{D}$ and $\mathbf{u}$

is eigen vector. Using the probability density function (p.d.f.) of $\mathbf{u}$ [6] and simplification of $Q(x)$ and δ, the unconditional pairwise error probability (UPEP) can be written as

$$P\left(\mathbf{X} \longrightarrow \widehat{\mathbf{X}}\right) = \frac{1/12}{\det\left(\mathbf{I_n} + q_1\mathbf{B}\right)} + \frac{1/4}{\det\left(\mathbf{I_n} + q_2\mathbf{B}\right)}, \quad (20)$$

where $\mathbf{I_n}$ is an identity matrix, $\mathbf{B} = \mathbf{AK_n}$, $q_1 = 1/(4N_{0,f})$, and $q_2 = 1/(3N_{0,f})$. The above equation can be further simplified as follows:

$$P\left(\mathbf{X} \longrightarrow \widehat{\mathbf{X}}\right) = \left(12q_1^r \prod_{\xi=1}^{r} \lambda_\xi (B)\right)^{-1} + \left(4q_2^r \prod_{\xi=1}^{r} \lambda_\xi (B)\right)^{-1} \quad (21)$$

where $r \leq \min\{r_1, r_2\}$ and $r_2 = \text{rank}(A)$. For different SAR, r_2 will be different, so (21) is still applicable to any SAR.

The overall average bit error probability of τ_{th} subblock of any group can be calculated by using UPEP as follows:

$$P_b^\tau (E) \approx \frac{1}{p^\tau n_x^\tau} \sum_{\mathbf{X^\tau}} \sum_{\widehat{\mathbf{X}}^\tau} P\left(\mathbf{X^\tau} \longrightarrow \widehat{\mathbf{X}}^\tau\right) \quad e\left(\mathbf{X^\tau}, \widehat{\mathbf{X}}^\tau\right), \quad (22)$$

where p^τ is the number of information bits in τ_{th} subblock of any group, n_x^τ represents the number of realizations of $\mathbf{X}^\tau$, and $e(\mathbf{X^\tau}, \widehat{\mathbf{X}}^\tau)$ is the number of information bit errors committed by choosing $\widehat{\mathbf{X}}^\tau$ instead of $\mathbf{X^\tau}$. Using (22), the ABEP for Υ_{th} group can be calculated as follows:

$$P_b^\Upsilon (E) \approx \frac{1}{F}\left(\sum_{\tau=1}^{F} P_b^\tau (E)\right) \quad (23)$$

where F is the number of subblocks in any group and $F = 8$ in our case. Equation (23) can be rewritten as follows:

$$P_b^\Upsilon (E) \approx \frac{1}{F}\sum_{\tau=1}^{F}\left(\frac{1}{p^\tau n_x^\tau}\sum_{\mathbf{X^\tau}}\sum_{\widehat{\mathbf{X}}^\tau} P\left(\mathbf{X^\tau} \longrightarrow \widehat{\mathbf{X}}^\tau\right) e\left(\mathbf{X^\tau}, \widehat{\mathbf{X}}^\tau\right)\right) \quad (24)$$

Finally, ABEP for the OFDM-IM block can be calculated as follows:

$$P_b (E) \approx \frac{1}{\Omega}\sum_{\Upsilon=1}^{\Omega} P_b^\Upsilon (E) \approx \frac{1}{\Omega}\left(P_b^1 + P_b^2 + P_b^3 + P_b^4\right) \quad (25)$$

where Ω is the number of groups and in this case $\Omega = 4$. The theoretical BER curve will be presented in Section 5.

5. Simulation Result

This section presents the simulation results to evaluate the effectiveness of the proposed algorithms, named as OFDM-AIM-FCM, OFDM-AIM-ACM, and OFDM-VIM-VCM by using bit error rate (BER) and throughput as performance metrics.

Table 4: System parameters.

Channel	Multipath Rayleigh fading channel
Channel length	10
OFDM frame size (N)	128
Length of subblock	4
Detector	Modified LLR based detector

In this work, we consider an OFDM-IM system with $N = 128$ subcarriers and a CP of length 10. As explained in Section 3.1, OFDM-IM block is divided into $G = N/n = 128/4 = 32$ subblocks, where $n = 4$ is the number of subcarriers in each subblock. The multipath Rayleigh fading channel is considered for both Bob and Eve with equal number of channel taps ($L = 10$). The basic simulation parameters are presented in Table 4. In this work, lookup table based special LLR detector is employed at receiver, as explained in Section 3.1, to determine the active indices and corresponding constellation symbols based on the proposed algorithms. Additionally, we also consider that Eve knows our security algorithms. For simplicity and without loss of generality, CP is not considered in the throughput calculation.

It should be noted that the proposed scheme is a type of scheme which does not cause much difference in the SNR between Bob and Eve, but still Eve cannot decode, while Bob can decode (this case is somehow similar to the case of interleaver or precoder based security techniques [20, 30]). In such cases, BER can be used as a metric to measure secrecy instead of secrecy capacity and secrecy outage probability as reported in [20, 30, 31]. Therefore, in this work, we use BER-based secrecy gap metric [20] to evaluate the secrecy. Furthermore, in this work we are targeting quality of service (QoS) based security [16, 32]. The basic idea behind QoS based security is to secure different services (voice, video, etc.) instead of focusing on providing perfect secrecy. More specifically, it should be noted that perfect secrecy is not always needed to provide a perfectly secure service. In reality, each service has different QoS requirements than the others, and if we ensure that Eve is operating below these requirements, then practical secrecy can be guaranteed. So, in this work we target to provide security for services such as voice and video and make sure that error rate at Eve is greater than minimum required error rate criteria to use that service [16]. For example, voice and video can be made secure at Bob by making sure that PER (corresponding to BER) at Bob is less than minimum required PER (corresponding to BER) in order to use that service while PER at Eve is made greater than minimum required PER. The minimum PER requirement for different services is presented in Table 5 [26]. Hence, although the throughput is nonzero, the proposed scheme can still provide QoS based security (it should be noted that PER can be calculated from BER as follows: $PER = 1 - (1 - BER)^n$), where n is the block size [33]).

In the first phase, OFDM-IM is simulated for different SAR values, such as 1/4, 2/4, 3/4, and 4/4 based on lookup tables presented in Table 1 with FCM (M=2). Afterwards, we simulate OFDM-AIM-FCM for BPSK ($M = 2$) for PLS and

Table 5: QoS lookup table [26].

Service	*PER*
Voice	10^{-2}
Video	10^{-3}

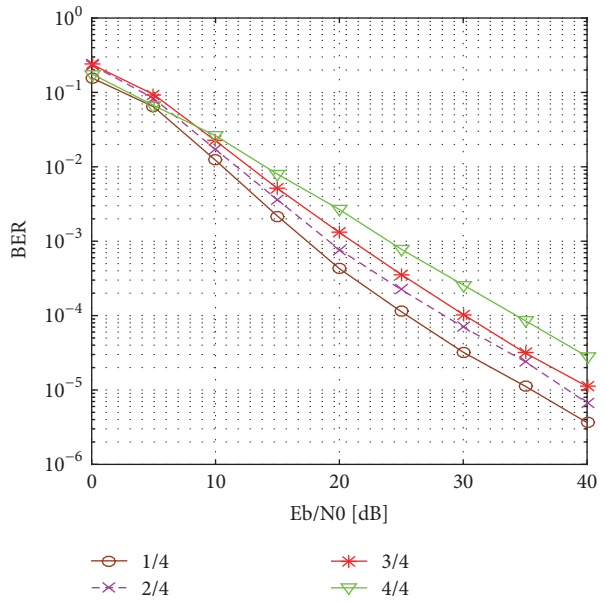


Figure 6: BER performance for OFDM-IM ($n = 4, k = \{1, 2, 3, 4\}$).

also extend it for higher order modulation such as $M = 4$, $M = 8$, and $M = 16$. Then, OFDM-AIM-FCM is extended to OFDM-AIM-ACM for providing another stronger PLS technique. Finally, we implement OFDM-VIM-VCM for QoS based communication in order to maximize the spectral efficiency.

5.1. OFDM-AIM-FCM. Figure 6 presents the BER plots for OFDM-IM with different SAR values, such as 1/4, 2/4, 3/4, and 4/4 for $M = 2$. It should be noted from Figure 6 that the BER performance for lower values of SAR is better than the case of higher values of SAR; for example, the BER performance of 1/4 case is the best while BER performance of 4/4 is the worst. The reason for the better performance of BER at lower SAR is due to the fact that in case of lower SAR there will be less noise in the frequency domain.

Figure 7 presents throughput for OFDM-IM with different SAR values for $M = 2$. It should be noted that the throughput for the system improves as the activation ratio increases except for the case with SAR value of 3/4 which outperforms 4/4 case. The reason is that each subblock carries 4 bits in case of SAR value of 4/4 while each block carries 5 bits in case of 3/4.

Figure 8 presents a comparison of BER performances among the proposed OFDM-AIM-FCM scheme, the scheme presented in [24], and OFDM-IM ($n = 4, k = 2$) (Ref. (Ref. means the reference scheme to which we compare our proposed algorithm)). It is observed from Figure 8 that the BER performances of OFDM-AIM-FCM and OFDM-IM [6]

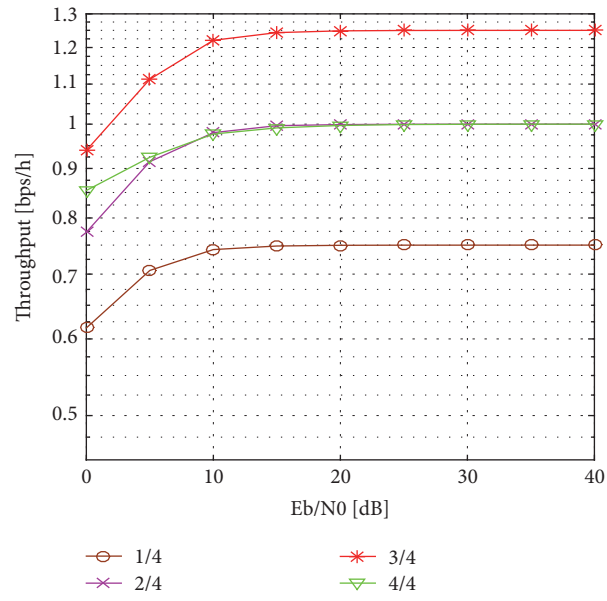


Figure 7: Throughput performance for OFDM-IM ($n = 4, k = \{1, 2, 3, 4\}$).

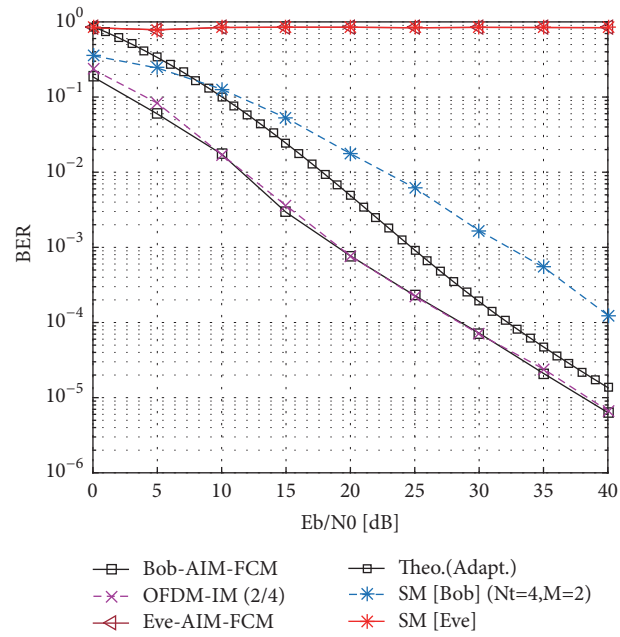


Figure 8: BER performance for OFDM-AIM-FCM, Secure SM [24] and OFDM-IM ($n = 4, k = 2$).

are similar for the case of Bob but the scheme presented in [24] has the worst performance as compared to others. It is also observed that the performance of Eve is the worst for all values of SNR for the proposed OFDM-AIM-FCM technique and the scheme presented in [24] while her performance is similar to that of Bob for the cases of OFDM-IM [6]. Hence, the proposed technique and the technique presented in [24] are secure as compared to OFDM-IM [6]. Figure 8 also presents the theoretical upper bound BER performance of OFDM-AIM-FCM based on (25). It should

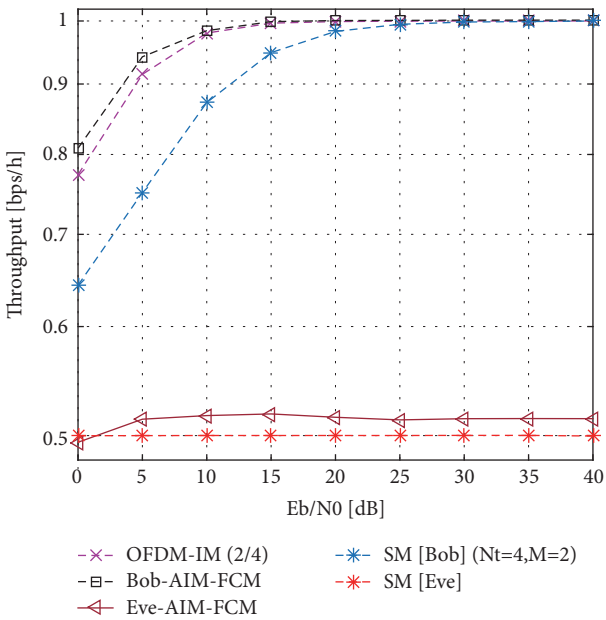


Figure 9: Throughput performance for OFDM-AIM-FCM, Secure SM [24] and OFDM-IM ($n = 4, k = 2$).

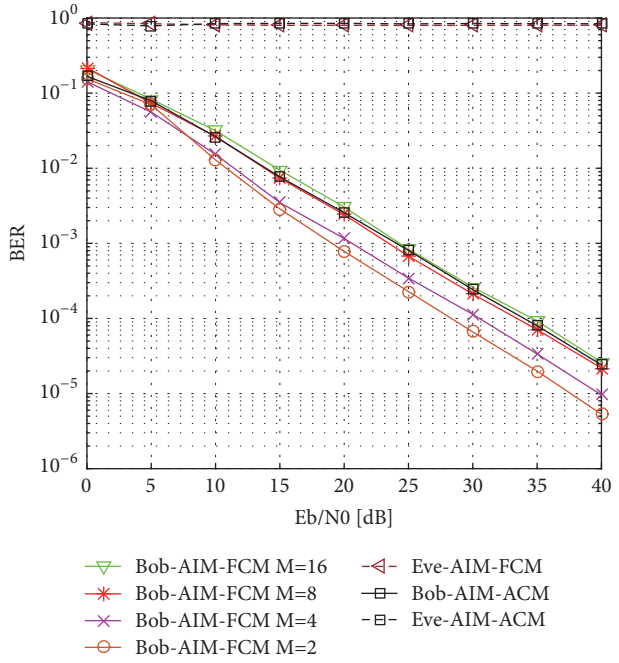


Figure 10: BER performance for OFDM-AIM-FCM and OFDM-AIM-ACM.

be noted that theoretical curve becomes tight at higher SNR with the simulation curve.

Figure 9 shows the comparison of throughput performances among the proposed OFDM-AIM-FCM scheme, the scheme presented in [24], and OFDM-IM ($n = 4$, $k = 2$) [6] with $M = 2$. It is observed that the throughput performances of all of these schemes for Bob are approximately similar at higher values of SNR. At equivalent BER we can notice that the throughput of the proposed OFDM-AIM-FCM scheme outperforms the OFDM-IM (2/4) [6] at lower values of SNR. Moreover, the proposed scheme (OFDM-AIM-FCM) also outperforms in terms of throughput as compared to the scheme presented [24] at lower values of SNR. It is also observed that the throughput performance of Eve is the worst for the proposed OFDM-AIM-FCM technique and the scheme presented in [24] while her performance is similar to that of Bob for the case of OFDM-IM [6] scheme.

5.2. OFDM-AIM-ACM. Figure 10 presents the BER performance of Bob and Eve for OFDM-AIM-FCM for $M = 2$, $M = 4$, $M = 8$, and $M = 16$. It should be noted from the figure that as the modulation order increases the BER performance degrades. The performance of Eve for OFDM-AIM-FCM is the worst for all cases of CM such as $M = 2$, $M = 4$, $M = 8$, and $M = 16$. Figure 10 also presents the BER performance of Bob and Eve for the proposed OFDM-AIM-ACM. It is observed from Figure 10 that the BER performance of OFDM-AIM-AIM is approximately the same as the case of OFDM-AIM-FCM for $M = 8$, while the BER performance of Eve is the worst for all values of SNR. Hence, OFDM-AIM-ACM can provide secure communication between Alice and Bob. Figure 11 presents throughput performance of Bob and Eve for OFDM-AIM-FCM with $M = 2$, $M = 4$, $M = 8$, and $M = 16$. Similarly, Figure 11 also presents the throughput results of our proposed OFDM-AIM-ACM based PLS technique for Bob and Eve. It is clear from Figure 11 that the throughput of OFDM-AIM-ACM is approximately similar to the case of OFDM-AIM-FCM with $M = 8$ while throughput of Eve is the worst for all the values of SNR.

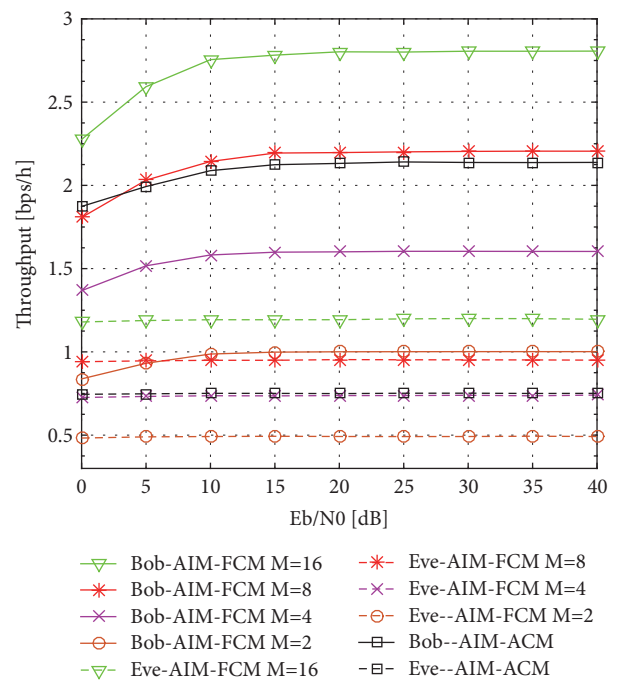


Figure 11: Throughput performance for OFDM-AIM-FCM and OFDM-AIM-ACM.

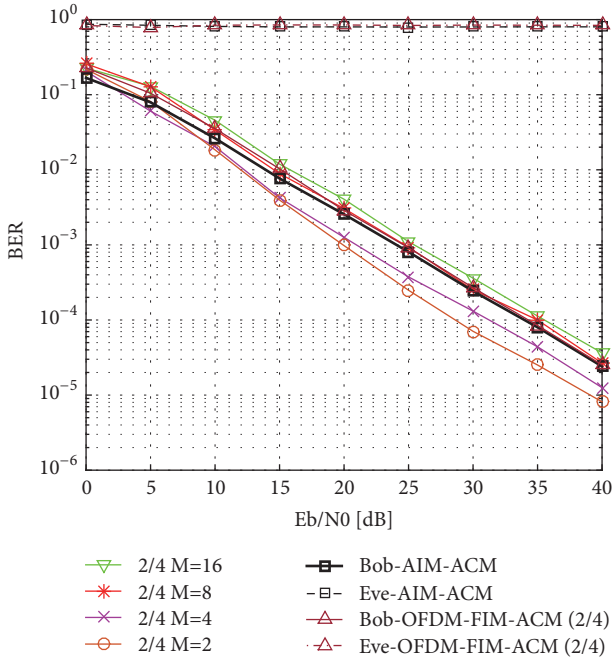


FIGURE 12: BER comparison of OFDM-IM ($n = 4, k = 2$), OFDM-AIM-ACM, and OFDM-FIM-ACM ($n = 4, k = 2$).

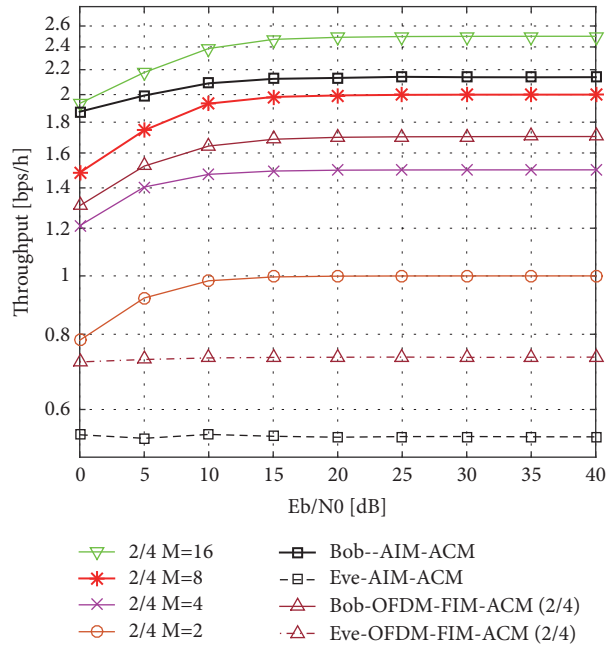


FIGURE 13: Throughput comparison of OFDM-IM ($n = 4, k = 2$), OFDM-AIM-ACM, and OFDM-FIM-ACM ($n = 4, k = 2$).

Figure 12 presents a comparison of BER performances between the proposed OFDM-AIM-ACM scheme and OFDM-IM ($n = 4$, $k = 2$) (Ref.) with CM order of $\{2, 4, 8, 16\}$. It is observed from Figure 12 that the BER performance of OFDM-AIM-ACM is similar to the case of OFDM-IM ($n = 4, k = 2$) (Ref.) with $M = 8$. At equivalent BER, it is also noticed that the throughput of the proposed OFDM-AIM-ACM outperforms the OFDM-IM ($n = 4, k = 2$) (Ref.) with $M = 8$ at all values of SNR as presented in Figure 13. It is also observed from Figures 12 and 13 that the BER and throughput performances of Eve are the worst at all values of SNR for the proposed OFDM-AIM-ACM scheme while her BER and throughput performances are similar to that of Bob for the cases of OFDM-IM ($n = 4$, $k = 2$) (Ref.). Hence, the proposed scheme can enhance security and spectral efficiency jointly.

Moreover, Figures 12 and 13, respectively, also compare the BER and throughput performances of the OFDM-AIM-ACM scheme with the OFDM-FIM-ACM ($n = 4, k = 2$) based on [34]. It is observed from the figures that at approximately equivalent BER the proposed OFDM-AIM-ACM outperforms OFDM-FIM-ACM ($n = 4, k = 2$) in terms of throughput. It is also observed from Figures 12 and 13 that OFDM-FIM-ACM ($n = 4, k = 2$) can also provide security. Note that OFDM-AIM-ACM is more secure as compared to OFDM-AIM-FCM because in the case of OFDM-AIM-ACM both SAR and CM are varied adaptively while in case of OFDM-AIM-FCM only SAR is varied.

The below subsections present the effect of imperfect channel estimation and effect of channel correlation between Bob's channel and Eve's channel on the performances of OFDM-AIM-FCM and OFDM-AIM-ACM.

5.2.1. Security Algorithms under Imperfect Channel Estimation. In order to evaluate the robustness of the proposed security algorithms against imperfect channel estimation, intentional error is added at both the transmitter and receiver ($\Delta\mathbf{h}_{T/R}$) to the true channel ($\mathbf{h}_b$) to obtain new erroneous channels given by $\tilde{\mathbf{h}}_b = \mathbf{h}_b + \Delta\mathbf{h}$ [20, 35]. The intentional error ($\Delta\mathbf{h}$) is modeled as an independent complex Gaussian noise with zero mean and variance ($\sigma^2 = mse \times 10^{-SNR_{dB}/10}$), where *mse* is a variable related to mean square of estimator's quality. Figures 14 and 15, respectively, present the BER performances for OFDM-AIM-FCM and OFDM-AIM-ACM under different estimation qualities with $mse = 0$ (perfect estimation), $mse = 0.02$, $mse = 0.05$, and $mse = 0.1$. It is shown that imperfect channel estimation leads to small degradation in the BER performance. However, this degradation can be overcome by increasing the length or power of the training sequence. Moreover, there are some interesting algorithms proposed in the literature that can minimize the channel estimation error, such as in [1]

5.2.2. Effect of Eve's Channel Correlation with Bob's Channel. This subsection presents the effect of the correlation between the channel of legitimate receiver and Eve and evaluate the performance in terms of BER as a security metric. Firstly, the assumption of channel decorrelation requires that Bob and Eve be located at more than one-half wavelength away from Alice. This is a practical assumption in many realistic scenarios and is assumed in many prominent works in the literature (such as [21, 23, 24]). We have performed additional new simulations to show the effect of the correlation between the channels of legitimate receiver and eavesdropper on the

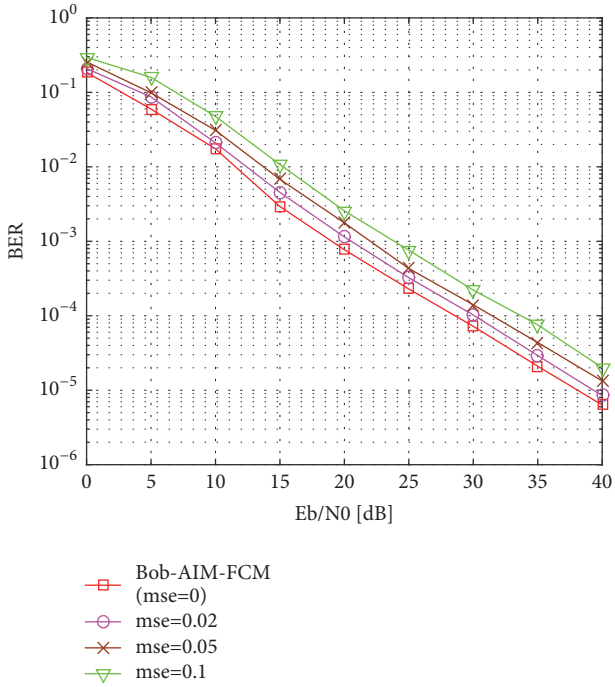


Figure 14: BER comparison of OFDM-AIM-FCM (mse = 0, 0.02, 0.05, 0.1).

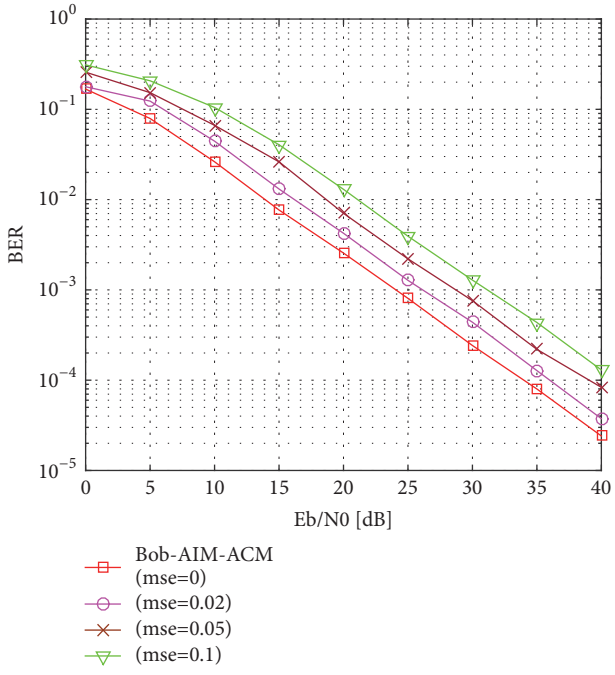


Figure 15: BER comparison of OFDM-AIM-ACM (mse = 0, 0.02, 0.05, 0.1).

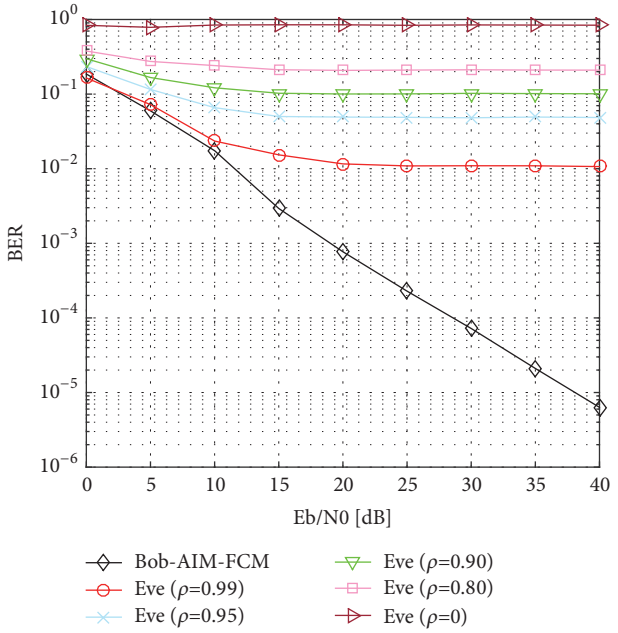


Figure 16: BER comparison of Bob (OFDM-AIM-FCM) and Eve with correlation coefficient (ρ = 0, 0.80, 0.90, 0.95, 0.99).

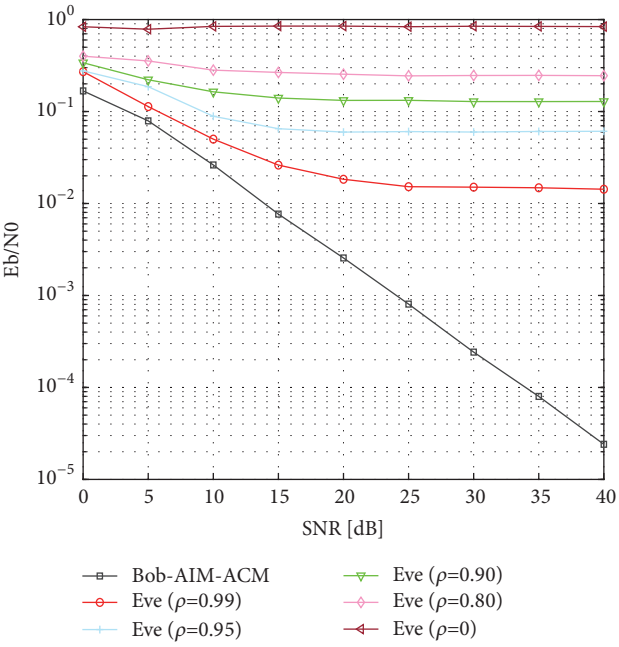


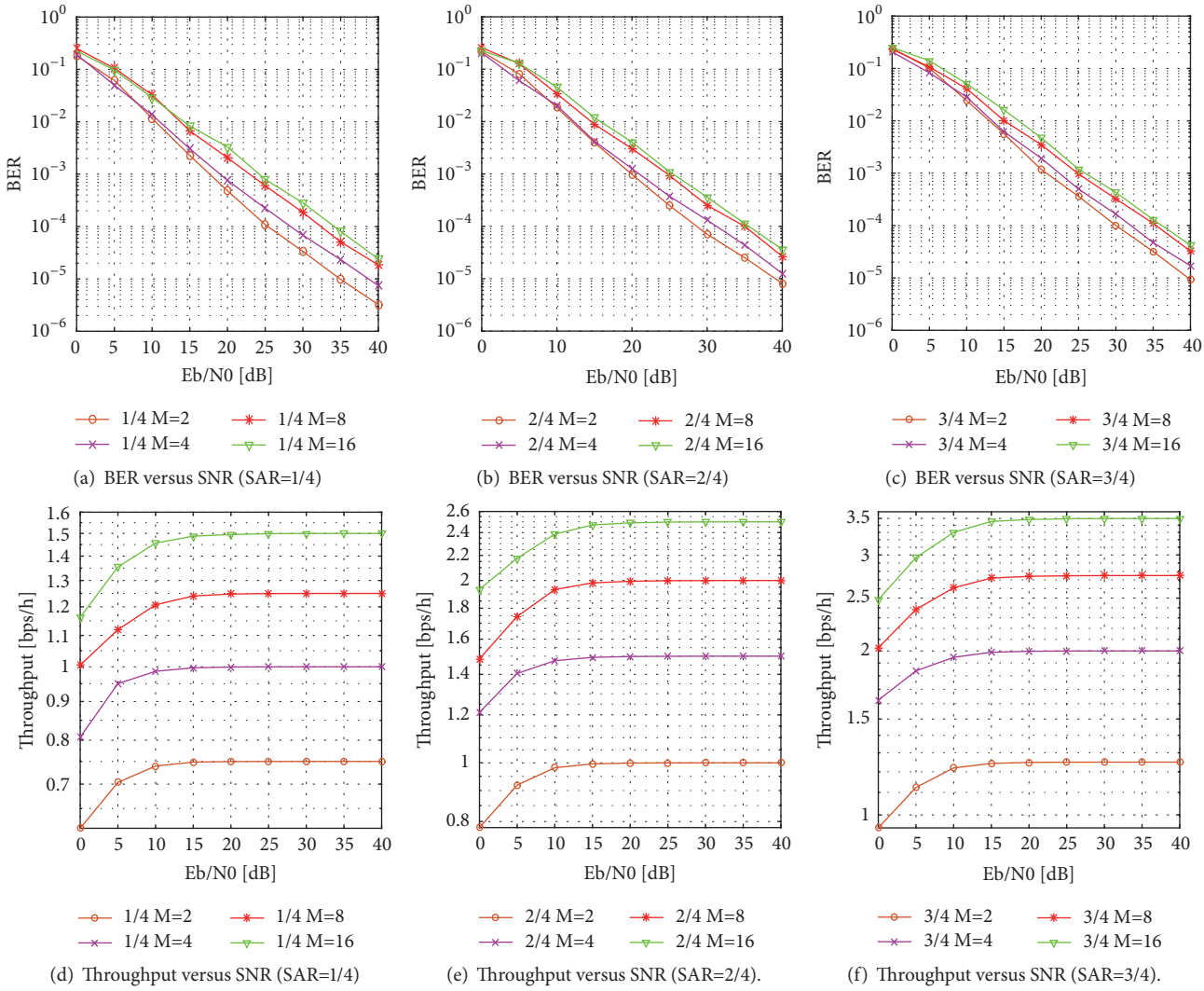
Figure 17: BER comparison of Bob (OFDM-AIM-ACM) and Eve with correlation coefficient (ρ = 0, 0.80, 0.90, 0.95, 0.99).

secrecy performance that is measured in terms of BER as a security metric as explained above.

Figures 16 and 17, respectively, present the BER performances for OFDM-AIM-FCM and OFDM-AIM-ACM when Eve's channel is correlated to Bob's one. The model for channel correlation between the channels of legitimate receiver and eavesdropper assumed in this work is similar to the one presented in [24] and is given as follows:

$$\mathbf{h}_e = \rho \mathbf{h}_b + (1 - \rho)\,\mathbf{E} \tag{26}$$

where E represents an independent channel while ρ is the correlation factor. We present BER performance for the correlation values of (ρ = 0, 0.80, 0.90, 0.95, 0.99). It should be noted that even with correlation between Bob's and Eve's



(a) BER versus SNR (SAR=1/4)
(b) BER versus SNR (SAR=2/4)
(c) BER versus SNR (SAR=3/4)
(d) Throughput versus SNR (SAR=1/4)
(e) Throughput versus SNR (SAR=2/4).
(f) Throughput versus SNR (SAR=3/4).

Figure 18: OFDM-IM with SAR values of (1/4, 2/4, 3/4) and CM orders of (2, 4, 8, and 16).

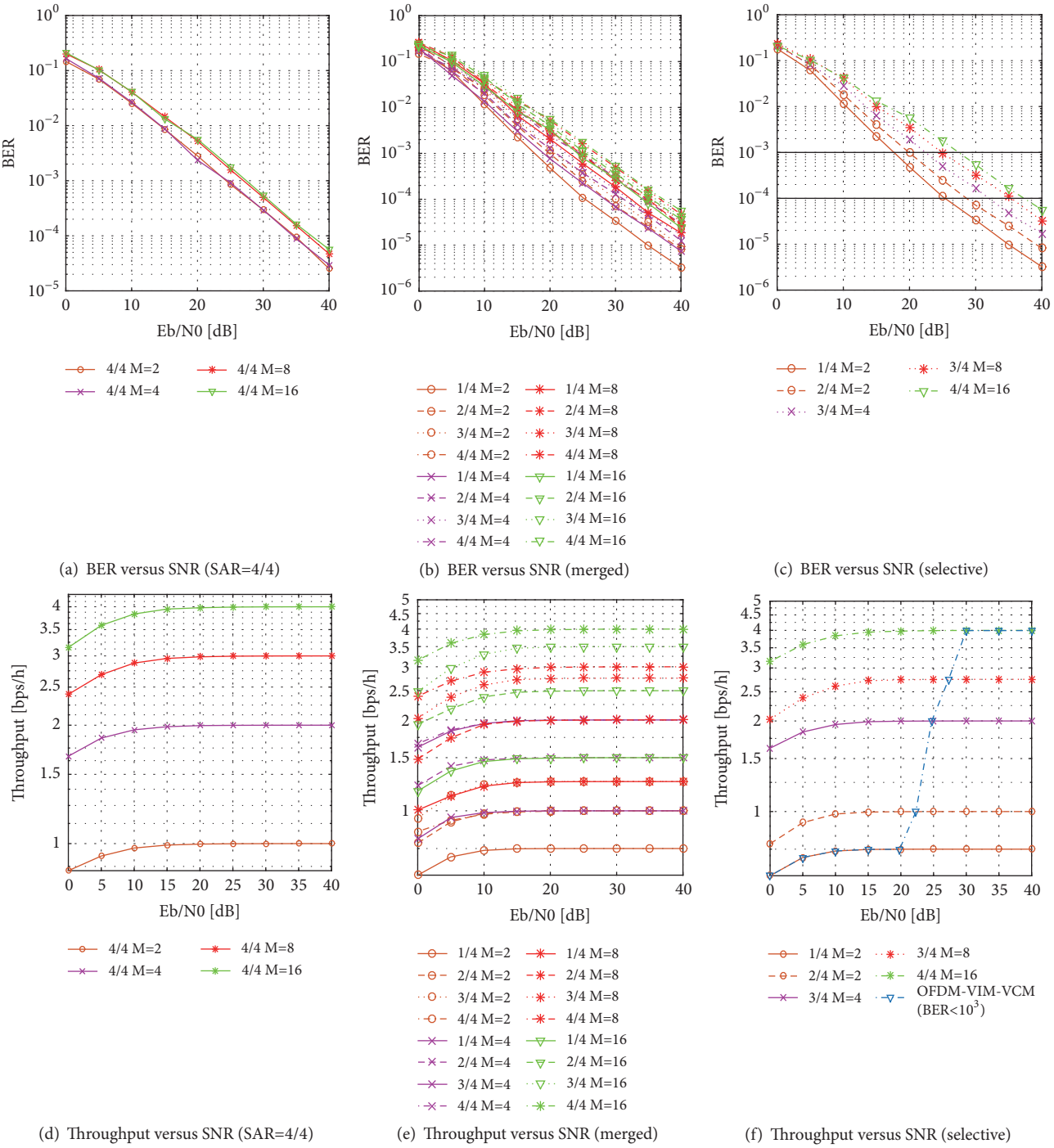
channels, the proposed algorithms can still provide some level of QoS based security.

5.3. OFDM-VIM-VCM. Figures 18 and 19 present the extensive simulations related to OFDM-VIM-VCM scheme for QoS based communication in order to maximize the spectral efficiency. Note that the system model for this technique is the same as explained in Section 2, except the Eve link, which is not considered in this case. The basic concept is to vary the SAR and CM with the increase in SNR to maximize the spectral efficiency while fulfilling certain QoS requirement. In this approach, BER and throughput curves for four types of CM order, such as $M = 2$, $M = 4$, $M = 8$, and $M = 16$, are implemented for each of SAR types, such as 1/4, 2/4, 3/4, and 4/4, and presented in Figures 18, 19(a), and 19(d). Afterwards, certain curves are selected based on OFDM-VIM-VCM for QoS based communication.

In Figure 19(b), we merge the BER curves of SAR values of 1/4, 2/4, 3/4, and 4/4 for CM order of $M = 2$, $M = 4$, $M = 8$, and $M = 16$. Similarly, in Figure 19(e), throughput curves of SAR values of 1/4, 2/4, 3/4, and 4/4 for CM order of $M = 2$, $M = 4$, $M = 8$, and $M = 16$ are also merged.

Afterwards, among the BER curves of Figure 19(b) that have similar performance, we select a curve that has maximum value of throughput. From the selected curves in the former step, we select those curves that have a performance gap among them. Finally, the resultant curves are presented in Figure 19(c). Afterwards, the corresponding throughput curves of Figure 19(e) related to selected BER curves in Figure 19(c) are also selected and presented in Figure 19(f).

Based on Figures 19(c) and 19(f), we develop a switching tables for QoS based communication in order to maximize the throughput. In this work, as an example, switching among different modulation types based on the SNR for the case of $BER < 10^{-3}$ and $BER < 10^{-4}$ is presented in Table 6. The table depicts different SAR and CM values of system for different SNR ranges to maximize the spectral efficiency while fulfilling different QoS requirements. Afterwards, this table can be used for different QoS based communication services for maximizing spectral efficiency in a similar way



(a) BER versus SNR (SAR=4/4)

(b) BER versus SNR (merged)

(c) BER versus SNR (selective)

(d) Throughput versus SNR (SAR=4/4)

(e) Throughput versus SNR (merged)

(f) Throughput versus SNR (selective)

FIGURE 19: OFDM-IM with SAR value of (4/4) and CM orders of (2, $M = 4$, $M = 8$, and $M = 16$), merged curves for different cases of OFDM-IM and selected curves for different cases of OFDM-IM for QoS based communication.

as performed in [16]. The result of OFDM-VIM-VCM for the case of $BER < 10^{-3}$ is presented in Figure 19(f).

6. Conclusion

In this work, effective algorithms that change SAR and/or CM adaptively in each subblock of the OFDM-IM scheme based on the channel characteristics of the legitimate receiver are proposed for enhancing PLS and SE. Particularly, the first two algorithms named as OFDM-AIM-FCM and OFDM-AIM-ACM are designed for enhancing PLS and SE, while the third algorithm named as OFDM-VIM-VCM is designed for QoS based communication for enhancing SE. Simulation results show that the first two algorithms can provide significant security enhancement whereas the third algorithm ensures

Table 6: Switching table for OFDM-VIM-VCM.

(a) $BER < 10^{-3}$

	BER < 10^{-3}	
Eb/NO (E)	M	SAR
17.6<E<19.9	2	1/4
19.9<E<22.4	2	2/4
22.4<E<24.8	4	3/4
24.8<E<27.4	8	3/4
27.4<E	16	4/4

(b) $BER < 10^{-4}$

	BER < 10^{-4}	
Eb/NO (E)	M	SAR
25.3<E<28.6	2	1/4
28.6<E<32	2	2/4
32<E<35.3	4	3/4
35.3<E<37.3	8	3/4
37.3<E	16	4/4

QoS based communication aiming to maximize spectral efficiency.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

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

References

[1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure pre-coding and post-coding for OFDM systems along with hardware implementation," in *Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1338–1343, Valencia, Spain, June 2017.

[2] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in *Proceedings of the 13th International Symposium on Wireless Communication Systems, ISWCS 2016*, pp. 597–602, Poland, September 2016.

[3] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *in IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[4] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. H. Chen, "A Survey on multiple-antenna techniques for physical layer security," ΓΓ *in IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.

[5] E. Basar, M. Wen, R. Mesleh, M. Di Renzo, Y. Xiao, and H. Haas, "Index Modulation Techniques for Next-Generation Wireless Networks," *IEEE Access*, vol. 5, pp. 16693–16746, 2017.

[6] E. g. Basar, U. Aygolu, E. Panayirci, and H. V. Poor, "Orthogonal frequency division multiplexing with index modulation," *IEEE Transactions on Signal Processing*, vol. 61, no. 22, pp. 5536–5549, 2013.

[7] J. Choi, "Coded OFDM-IM with Transmit Diversity," *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 3164–3171, 2017.

[8] J. Li, M. Wen, X. Cheng, Y. Yan, S. Song, and M. H. Lee, "Generalized Precoding-Aided Quadrature Spatial Modulation," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1881–1886, 2017.

[9] M. Wen, E. Basar, Q. Li, B. Zheng, and M. Zhang, "Multiple-Mode Orthogonal Frequency Division Multiplexing with Index Modulation," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3892–3906, 2017.

[10] E. Soujeri, G. Kaddoum, M. Au, and M. Herceg, "Frequency Index Modulation for Low Complexity Low Energy Communication Networks," *IEEE Access*, vol. 5, pp. 23276–23287, 2017.

[11] M. Au, G. Kaddoum, S. Francois, and S. Ebrahim, "A Joint Code-Frequency Index Modulation for Low-complexity, High Spectral and Energy Efficiency Communications," https://arxiv.org/abs/1712.07951.

[12] E. Soujeri, G. Kaddoum, and M. Herceg, "Design of an initial condition-index chaos shift keying modulation," *IEEE Electronics Letters*, vol. 54, no. 7, pp. 447–449, 2018.

[13] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proceedings of the IEEE INFOCOM*, pp. 1422–1430, Shanghai, China, April 2011.

[14] H. Qin, Y. Sun, T.-H. Chang et al., "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2717–2729, 2013.

[15] Z. E. Ankaral, M. Karabacak, and H. Arslan, "Cyclic Feature Concealing CP Selection for Physical Layer Security," in *Proceedings of the 2014 IEEE Military Communications Conference (MILCOM)*, pp. 485–489, Baltimore, MD, USA, October 2014.

[16] J. M. Hamamreh, M. Yusuf, T. Baykas, and H. Arslan, "Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation," in *Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, WCNC 2016*, Qatar, April 2016.

[17] E. Guvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in *Proceedings of the 2014 IEEE International Conference on Communications Workshops, ICC 2014*, pp. 813–818, Australia, June 2014.

[18] D. W. Ng, E. S. Lo, and R. Schober, "Energy-Efficient Resource Allocation for Secure OFDMA Systems," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2572–2585, 2012.

[19] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM systems using channel shortening," in *Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–5, Montreal, QC, October 2017.

[20] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-Subcarrier Index Selection for Enhancing Security and Reliability of 5G URLLC Services," *IEEE Access*, 2017.

[21] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 467–471, 2016.

[22] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy Enhancement Analysis Against Unknown Eavesdropping in Spatial Modulation," *IEEE Communications Letters*, vol. 19, no. 8, pp. 1351–1354, 2015.

[23] X. Wang, X. Wang, and L. Sun, "Spatial modulation aided physical layer security enhancement for fading wiretap channels," in *Proceedings of the 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP)*, pp. 1–5, Yangzhou, China, October 2016.

[24] X. Jiang, M. Wen, H. Hai, J. Li, and S. Kim, "Secrecy-Enhancing Scheme for Spatial Modulation," *IEEE Communications Letters*, vol. 22, no. 3, pp. 550–553, 2018.

[25] Y. Lee, H. Jo, Y. Ko, and J. Choi, "Secure Index and Data Symbol Modulation for OFDM-IM," *IEEE Access*, vol. 5, pp. 24959–24974, 2017.

[26] "3GPP, Policy and charging control architecture, 3GPP Std. TS 23.203 V11.6.0," 2012, http://www.qtc.jp/3GPP/Specs/23203-b60.pdf.

[27] P. Robertson, E. Villebrun, and P. Hoeher, "A comparison of optimal and sub-optimal MAP decoding algorithms operating in the log domain," in *Proceedings of the IEEE International Conference on Communications (ICC '95)*, vol. 2, pp. 1009–1013, IEEE, Seattle, Wash, USA, June 1995.

[28] H. Jafarkhani, *Space-Time Coding*, Cambridge University Press, Cambridge, 2005.

[29] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, UK, 1985.

[30] H. Li, X. Wang, and J.-Y. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1155–1165, 2015.

[31] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Physical Communication*, vol. 25, pp. 14–25, 2017.

[32] J. M. Hamamreh and H. Arslan, "Joint PHY/MAC Layer Security Design Using ARQ with MRC and Null-Space Independent, PAPR-Aware Artificial Noise in SISO Systems," *IEEE Transactions on Wireless Communications*, pp. 1-1.

[33] ICAO, "Uniting Aviation," in *Proceedings of the AN-Conf/13 - ICAO Thirteenth - Air Navigation Conference*, Montereal, Canada, Oct. 2018, https://www.icao.int.

[34] J. Faezah and K. Sabira, "Adaptive modulation for OFDM systems," *International Journal of Communication Networks and Information Security*, vol. 1, no. 2, pp. 1–8, 2009.

[35] J. M. Hamamreh and H. Arslan, "Secure Orthogonal Transform Division Multiplexing (OTDM) Waveform for 5G and beyond," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1191–1194, 2017.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 8407297, 11 pages
https://doi.org/10.1155/2018/8407297

Research Article

Precoding-Aided Spatial Modulation for the Wiretap Channel with Relay Selection and Cooperative Jamming

Zied Bouida,[1] **Athanasios Stavridis**,[2] **Ali Ghrayeb**,[3,4] **Harald Haas**,[2] **Mazen Hasna**,[5] **and Mohamed Ibnkahla**[6]

[1] *Systems and Computer Engineering (SCE) Department, Carleton University, Ottawa, Canada*
[2] *The Institute for Digital Communications and the Joint Research Institute for Signal and Image Processing, School of Engineering, The University of Edinburgh, Edinburgh EH9 3JL, UK*
[3] *The Electrical and Computer Engineering Department, Texas A&M University at Qatar, Doha, Qatar*
[4] *Qatar Computing Research Institute (QCRI), Doha, Qatar*
[5] *The College of Engineering, Qatar University, Doha, Qatar*
[6] *Cisco Research Chair in Sensor Technology for the Internet of Things with the SCE Department, Carleton University, Ottawa, Canada*

Correspondence should be addressed to Zied Bouida; bouidazied@gmail.com

Received 17 February 2018; Revised 7 June 2018; Accepted 8 July 2018; Published 5 August 2018

Academic Editor: Yafei Hou

We propose in this paper a physical-layer security (PLS) scheme for dual-hop cooperative networks in an effort to enhance the communications secrecy. The underlying model comprises a transmitting node (Alice), a legitimate node (Bob), and an eavesdropper (Eve). It is assumed that there is no direct link between Alice and Bob, and the communication between them is done through trusted relays over two phases. In the first phase, precoding-aided spatial modulation (PSM) is employed, owing to its low interception probability, while simultaneously transmitting a jamming signal from Bob. In the second phase, the selected relay detects and transmits the intended signal, whereas the remaining relays transmit the jamming signal received from Bob. We analyze the performance of the proposed scheme in terms of the ergodic secrecy capacity (ESC), the secrecy outage probability (SOP), and the bit error rate (BER) at Bob and Eve. We obtain closed-form expressions for the ESC and SOP and we derive very tight upper-bounds for the BER. We also optimize the performance with respect to the power allocation among the participating relays in the second phase. We provide examples with numerical and simulation results through which we demonstrate the effectiveness of the proposed scheme.

1. Introduction

Due to the broadcast nature of the wireless propagation environment, information transmission security has been considered as prominent frontier in wireless communications [1]. In this context, physical-layer security (PLS) has been introduced in order to ensure confidential communication by applying communication techniques in the physical layer by exploiting the spatiotemporal characteristics of wireless channels [2]. The key idea behind PLS is to exploit different characteristics of both the main and the eavesdropper's channels [3]. The pioneering work on wiretap channel [4] has shown that perfect secrecy can be achieved if the eavesdropper's channel is a degraded version of the main channel. Later in [5], it has been shown that perfect secrecy can be achieved even if the eavesdropper's channel is on average better than the main channel, by exploiting the channel fading.

Due to the importance of physical-layer security, research work on this topic is gaining more and more interest in the context of next generation networks. In particular, information security is becoming very important in 5G systems where massive user connections and exponentially increasing wireless services are supported as investigated in [6, 7] and references therein. In this context, several techniques have been used in order to safeguard 5G systems. Focusing on precoding-aided spatial modulation and cooperative jamming, we provide in what follows the motivation behind each

of these techniques and how it contributes to 5G systems safeguarding.

In light of the above, a plethora of works has appeared in the literature, addressing different aspects of physical-layer security. Based on the concept of spatial modulation (SM) [8, 9] and owing to its spatial focusing property and its nondeterministic precoding algorithm, precoding-aided spatial modulation (PSM) has been presented as a suitable precoding technique to realize PLS [10–13]. In PSM, two types of modulations, namely, a variation of space shift keying (SSK) [14, 15] and conventional amplitude-phase modulation (APM), are jointly used to convey information. Specifically, Pre-SSK is implemented using the indices of receiver antennas rather than transmit antennas, with the aid of zero forcing precoding (ZFP) [16]. In this context, PSM employs two distinctive advantages: (i) additional information transmission in space domain and (ii) low-complexity detection [17]. Due to the several advantages of SM in terms of error performance, energy efficiency, and complexity (and PSM for all these advantages with additional security), it becomes a promising candidate for 5G systems [18, 19]. Therefore, using PSM for the security of 5G results from the combination of SM with additional security features.

While PSM has gained attention in the literature as a solution to enhance the secrecy performance of wiretap channels, this technique has not been studied in the context of cooperative communications where the secrecy performance can be further improved and fit more in 5G systems. Indeed, relays can be used to enhance the secrecy of the system by increasing the capacity of the main channel while reducing the capacity of the eavesdropper channel [20]. In this context, an appropriate relay selection is used in [21] to enhance the secrecy performance by taking eavesdroppers' links into consideration. In [22], relay selection with destination-based jamming under a total power constraint is proposed. While this technique enhances the secrecy performance, it assumes that Eve has no direct link with Alice and thus puts a limitation on the location of Eve. Moreover, it requires the channel state information (CSI) at the relays in order to select the best relay to the destination.

Considering a dual-hop cooperative scenario, we propose a PSM-based scheme aimed at enhancing the communication secrecy between Alice and Bob in the presence of a passive Eve. Assuming that Alice and Bob can only communicate through the help of a number of trusted relays, we use different techniques to enhance the secrecy communication between these nodes without putting any constraint on the location of Eve with respect to Alice and Bob. In this context, using PSM at Alice while simultaneously transmitting a jamming signal from Bob guarantees the secrecy during the first phase. In the second phase, the secrecy performance is enhanced through the use of jamming from multiple relays. Specifically, the relay selected by PSM detects and forwards the useful signal while other relays contribute to the jamming of the eavesdropper. In this paper, we analyze the performance of the proposed scheme in terms of the ergodic secrecy capacity (ESC) and secrecy outage probability (SOP) where we obtain closed-form expressions for those metrics. We also optimize the performance with respect to the power allocation among the participating relays in the second phase. We provide examples with numerical and simulations results through which we demonstrate the effectiveness of the proposed scheme.

In light of the above, the main contributions behind the work proposed in this paper can be summarized as follows:

(i) Taking advantage of its low probability of interception, PSM is extended in this paper to the cooperative communication scenario where Alice and Bob communicate through the help of N_R trusted relays.

(ii) While the secrecy performance for the first phase is enhanced using PSM, a cooperative jamming from multiple relays is considered to improve the secrecy performance during the second phase.

(iii) The ESC and SOP are derived in closed-form expressions and the results are confirmed for accuracy using Monte-Carlo simulations. Power allocation optimization is also given by simulation to further enhance the secrecy performance of the proposed scheme.

(iv) The ABEP upper-bound expressions at Bob and Eve are derived and the results are confirmed for accuracy using Monte-Carlo simulations. These results show the advantages of PSM and multirelay jamming during the first and the second phase, respectively. Indeed, the proposed techniques enhance the ABEP performance at Bob while degrading that of Eve.

The remainder of this paper is organized as follows. Section 2 defines the system and channel models and the mode of operation of the proposed PSM-based technique. Section 3 analyzes the secrecy performance in terms of the ESC and the OSC. Section 4 confirms this performance via selected numerical results. Section 5 concludes the paper.

Notation. In this paper, we use boldface uppercase and lowercase letters to, respectively, denote matrices and vectors. The Hermitian transpose, inverse, and trace of a matrix $\mathbf{A}$ are, respectively, represented by $\mathbf{A}^H$, $\mathbf{A}^{-1}$, and $tr(\mathbf{A})$. The N-dimensional identity matrix is denoted by $\mathbf{I}_N$. The Euclidean norm, Frobenius norm, absolute value, and real part are, respectively, represented by $\|\cdot\|$, $\|\cdot\|_F$, $|\cdot|$, and $\Re\{\cdot\}$. $\mathbb{C}^{i\times j}$ stands for a set of complex matrices of $i \times j$ dimensions.

2. System and Channel Models

2.1. System Model. In Figure 1, we consider a secure dual-hop communication system between Alice and Bob through the help of N_r single-antenna trusted relays in the presence of an eavesdropper, Eve, where Alice has no direct link to Bob. The number of antennas of Alice, Bob, and Eve are denoted as N_a, N_b, and N_e, respectively. The practical number of antennas at these nodes depends on the used wireless and antenna technologies. Indeed, while current LTE devices can accommodate a maximum of four antennas, future 5G user equipment will accommodate a larger number of antennas thanks to the use of millimeter-wave and massive MIMO [23].

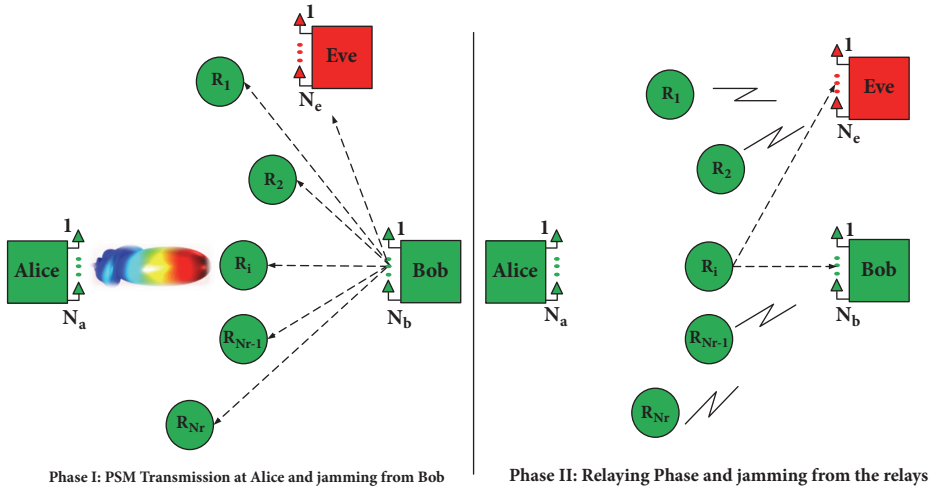


Figure 1: System model.

Table 1: Precoded SSK mapper rule example for $N_r = 4$; i.e., $k_1 = 2$.

k_1 bits	Relay activated	$\mathbf{e}_i$
$[0\ 0]$	1	$[1\ 0\ 0\ 0]^T$
$[0\ 1]$	2	$[0\ 1\ 0\ 0]^T$
$[1\ 0]$	3	$[0\ 0\ 1\ 0]^T$
$[1\ 1]$	4	$[0\ 0\ 0\ 1]^T$

In this work, we use a PSM-based relay-selection scheme in order to take advantage of the low probability of interception (LPI) of PSM. Following the principles of PSM [16, 17], we assume that $N_a > N_r$ and that $N_r = 2^{k_1}$, where k_1 is a positive integer to be able to use PSM. Hence, in PSM, relays' indices can be used by Alice to convey k_1 bits per symbol information following SSK principles. Therefore, the relay intended by reception is selected based on the k_1 incoming bits. In addition to SSK, we assume that Alice also exploits a conventional $M(= 2^{k_2})$-ary APM. Thus, each PSM symbol to be transmitted consists of $k = k_1 + k_2$ bits, which is first divided into two subsymbols, a k_1-bit SSK symbol and a k_2-bit APM symbol. The k_1-bit SSK symbol is mapped to a vector $\mathbf{e}_i$, which is the ith column of an identity matrix $\mathbf{I}_{N_r}$, and the subscript i is determined by the decimal value of the k_1-bit SSK symbol. The k_2-bit APM symbol is mapped to a unit-power symbol b_j chosen from the constellation according to the decimal value of the k_2-bit APM symbol. Then, the PSM symbol is formed as $\mathbf{s}_i^j = \mathbf{e}_i b_j$. After precoding, this signal is transmitted via the N_a transmit antennas of Alice. An example of relay selected based on the k_1 incoming bits is given in Table 1.

2.2. Channel Models. In this work, we consider Rayleigh block fading channels and we denote by h_{ij} the channel coefficient between nodes i and j. These coefficients have a complex Gaussian distribution with zero-mean and variance $d_{ij}^{-\alpha}$, i.e., $\mathcal{CN}(0, d_{ij}^{-\alpha})$, where d_{ij} is the distance between nodes i and j, and α is the path-loss exponent of wireless channels. Let $\mathbf{H}_{AR} = [\mathbf{h}_{AR_1}, \mathbf{h}_{AR_2}, \ldots, \mathbf{h}_{AR_{N_r}}]^T$ be the channel matrix between Alice and different relays, where $\mathbf{h}_{AR_i} \in \mathbb{C}^{1\times N_r}$ is the channel vector between Alice and the ith relay having $\mathcal{CN}(0, d_{AR_i}^{-\alpha})$ distributed components, where d_{AR_i} is the distance between Alice and the ith relay.

3. Performance Analysis

3.1. Received Signals. During the first phase, Alice transmits symbol $\mathbf{s}_i^j$ via its N_a antennas. Assuming that the channel state information to all relays is known to Alice, let $\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{Nr}]$ be a $N_a \times N_r$ precoding matrix used by Alice in order to send information to one of the relays. Then, the received signal from Alice at the relays is expressed as

$$\mathbf{y}_R = \mathbf{H}_{AR}\mathbf{P}\mathbf{s}_i^j + \boldsymbol{\eta}_R, \tag{1}$$

where $\boldsymbol{\eta}_R \in \mathbb{C}^{N_r\times 1}$ is the additive white Gaussian noise (AWGN) experienced by different relays, having complex Gaussian distributions of $\mathcal{CN}(0, \sigma_r^2)$. All channels are assumed to experience a block Rayleigh fading. While Alice knows the CSI of Alice-Relays channels, it is unable to acquire the CSI of Eve because this latter is assumed to be a passive eavesdropper.

Using the zero forcing precoder, the precoding matrix used by Alice can be expressed similar to [16] as

$$\mathbf{P} = \beta\mathbf{H}_{AR}^H\left(\mathbf{H}_{AR}\mathbf{H}_{AR}^H\right)^{-1}, \tag{2}$$

where

$$\beta = \sqrt{\frac{\left(\left(1-\delta_1\right)P/2\right)}{tr\left[\left(\mathbf{H}_{AR}\mathbf{H}_{AR}^H\right)^{-1}\right]}} \tag{3}$$

is a power normalization factor to achieve the power constraint of $tr(\mathbf{P}\mathbf{P}^H) = (1-\delta_1)P/2$, P denotes the total

transmitted power during the two phases, and δ_1 is a power allocation factor, $\delta_1 \in (0, 1]$. In the proposed scheme, the total power P is divided equally between the two transmission phases. Thus, $P/2$ is used in the first phase while being divided between the useful signal from Alice and the jamming signal from Bob. This division happens through the use of the power allocation factor δ_1; i.e., $(1-\delta_1)P/2$ is used by Alice and $\delta_1 P/2$ is used by Bob. During the second phase, the remaining $P/2$ is shared among all relays using the power allocation factor $\delta_2 \in (0, 1]$ as follows: (i) $P_s = \delta_2 P/2$ is used by the selected relay to transmit the useful signal and (ii) $P_J = (1-\delta_2)P/(2(N_r-1))$ is used by each of the remaining $N_r - 1$ relays to send the jamming signal received from Bob.

Thanks to the use of ZFP, the signal is only received by the ith relay and this can be seen by substituting (2) in (1). Thus, the received signal from Alice at different relays is given by

$$\begin{aligned} y_{Ri} &= \beta b_j + \eta_{Ri}, \\ y_{Rk} &= \eta_{Rk}, \quad \forall k \neq i. \end{aligned} \tag{4}$$

In this first phase, Bob also cooperates by broadcasting a jamming signal J_B. Thus, the received signals from Alice and Bob during this phase at all relays is given by

$$\begin{aligned} y_{Ri} &= \beta b_j + \sqrt{\frac{\delta_1 P}{2}}\mathbf{h}_{BR_i} J_B + \eta_{Ri}, \\ y_{Rk} &= \sqrt{\frac{\delta_1 P}{2}}\mathbf{h}_{BR_k} J_B + \eta_{Rk}, \quad \forall k \neq i, \end{aligned} \tag{5}$$

where $\mathbf{h}_{BR_k} \in \mathbb{C}^{N_b \times 1}$ is the channel vector between Bob and the kth relay R_k. To simplify the detection of Alice's signal at the relays, the jamming signal is assumed to have a complex Gaussian distribution with zero-mean and variance σ_J^2; i.e., $J_B \sim \mathcal{CN}(0, \sigma_J^2)$. Thus, the received signal at different relays can be reformulated as

$$\begin{aligned} y_{R_i} &= \beta b_j + \widetilde{\eta}_{Ri}, \\ y_{Rk} &= \widetilde{\eta}_{Rk}, \quad \forall k \neq i, \end{aligned} \tag{6}$$

where $\widetilde{\eta}_{Rk}$ has a complex Gaussian distribution with zero-mean and variance $\widetilde{\sigma}^2 = \delta_1 P/2 \|\mathbf{h}_{BR_k}\|_{\mathrm{F}}^2 \sigma_J^2 + {\sigma_r}^2$.

Similar to [24], we assume that the relays communicate via a backhaul-link (this link can be established through control channels and does not necessary imply that the used channels are dedicated). Thus, taking into consideration the received CSI at the relays from Bob, we can employ the following centralized low-complexity Maximum Likelihood (ML) detector:

$$\begin{aligned} \left[\widehat{i}, \widehat{j}\right] &= \arg\min_{i,j} \left\| \mathbf{y}_R - \beta \mathbf{s}_i^j \right\| \\ &= \arg\min_{i,j} \beta \left| b_j \right|^2 - 2\Re\left\{ y_{R_i}^* b_j \right\}. \end{aligned} \tag{7}$$

The use of the ML detector in (7) ensures that a single relay is activated during the second transmission phase. In this context, the relay intended by the PSM selection is used at the second phase to transmit the decoded APM signal b_j using power P_s and the remaining $N_r - 1$ relays send the perfectly estimated jamming signal received from Bob during the first phase each using a power $P_J = (P/2 - P_s)/(N_r - 1)$. When the relayed signals are received by Bob, this latter can employ self-interference subtraction as it knows the jamming signal J_B and it has received channel estimations with all relays. Thus, the received signal at Bob is given by

$$\mathbf{y}_B = \sqrt{P_s} b_j \mathbf{h}_{R_i B} + \boldsymbol{\eta}_B, \tag{8}$$

where η_B is the $\mathcal{CN}(0, \sigma_b^2)$ AWGN at Bob and $\mathbf{h}_{R_i B}$ is the channel coefficient between the ith relay R_i and Bob.

During the first phase, the received signal from Alice and Bob at Eve is expressed as

$$\mathbf{y}_{E,1} = \mathbf{H}_{AE}\mathbf{P}\mathbf{s}_i^j + \sqrt{\frac{\delta_1 P}{2}}\mathbf{H}_{BE} J_B + \boldsymbol{\eta}_{E,1}, \tag{9}$$

where $\boldsymbol{\eta}_{E,1} \in \mathbb{C}^{N_e \times 1}$ is the AWGN experienced by Eve during the first phase, having complex Gaussian distribution of $\mathcal{CN}(0, \sigma_e^2 \mathbf{I}_{N_e})$. $\mathbf{H}_{AE} \in \mathbb{C}^{N_e \times N_a}$ is the channel matrix between Alice and Eve having $\mathcal{CN}(0, d_{AE}^{-\alpha})$ distributed components. $\mathbf{H}_{BE} \in \mathbb{C}^{N_e \times N_b}$ is the channel matrix between Bob and Eve having $\mathcal{CN}(0, d_{BE}^{-\alpha})$ distributed components.

The received signal at Eve for the second phase is given by

$$\mathbf{y}_{E,2} = \sqrt{P_s} b_j \mathbf{h}_{R_i E} + \sqrt{P_J}\sum_{k \neq i} \mathbf{h}_{R_k E} J_B + \boldsymbol{\eta}_{E,2}, \tag{10}$$

where $\boldsymbol{\eta}_{E,2} \in \mathbb{C}^{N_e \times 1}$ is the $\mathcal{CN}(0, \sigma_e^2)$ AWGN experienced by Eve during the second phase.

3.2. Ergodic Secrecy Capacity. Using the received signal expression in (8), the signal-to-noise ratio (SNR) at Bob can be expressed as

$$\Gamma_B = \frac{P_s}{\sigma_b^2} \left\| \mathbf{h}_{R_i B} \right\|_{\mathrm{F}}^2. \tag{11}$$

The SNRs at Eve for both the first and second phases are derived using (9) and (10), respectively, as follows:

$$\gamma_{E,1} = \frac{\left\| \mathbf{H}_{AE}\mathbf{P} \right\|_{\mathrm{F}}^2}{\delta_1 (P/2) \left\| \mathbf{H}_{BE} \right\|_{\mathrm{F}}^2 \sigma_g^2 + \sigma_e^2} \tag{12}$$

and

$$\gamma_{E,2} = \frac{P_s \left\| \mathbf{h}_{R_i E} \right\|_{\mathrm{F}}^2}{P_J \sum_{k \neq i} \left\| \mathbf{h}_{R_k E} \right\|_{\mathrm{F}}^2 \sigma_g^2 + \sigma_e^2}. \tag{13}$$

Similar to [22], the ergodic secrecy capacity for the considered dual-hop scheme can be given as

$$C_s = \mathbb{E}\left\{ \left[\frac{1}{2}\log_2\left(\frac{1+\Gamma_B}{1+\Gamma_E} \right) \right]^+ \right\}, \tag{14}$$

where $\Gamma_E = \max(\gamma_{E,1}, \gamma_{E,2})$ in order to account for the worst-case scenario.

In this paper, we take advantage of the low probability of interception of PSM to guarantee the secrecy of the transmission during the first phase and thus assume that $\Gamma_E = \gamma_{E,2}$. Indeed, as discussed in [11], if the Alice-Relays channels vary fast enough, the transmission from Alice to each relay is more or less a "one-time pad" cryptographic scheme, which is rendered absolutely secure. In this scenario, Eve cannot detect any information sent from Alice to Bob due to the one-time pad effect. When the Alice-Bob channels vary sufficiently slow, Eve is still incapable of detecting the SSK symbol i, as Eve is unable to estimate the precoding matrix $\mathbf{P}$ separately. Consequently, Eve needs to have both its CSI of $\mathbf{H}_{A,E}$ and the perfect knowledge of $\mathbf{P}$ to successfully eavesdrop $\mathbf{s}_i^j$. Thus, we assume that Eve is not able to get any useful information during the first phase. In order to confirm this assumption, we show in Figure 2 that $\gamma_{E,2}$ exceeds $\gamma_{E,1}$ almost surely for different simulation scenarios and parameters.

Due to intractability of (14), we can derive a lower bound on the ESC as follows:

$$\begin{aligned} C_s \geq C_{s_{lb}} &= \left[\mathbb{E}\left\{\frac{1}{2}\log_2\left(\frac{1+\Gamma_B}{1+\Gamma_E}\right)\right\}\right]^+ \\ &= \frac{1}{2\ln 2}\left[\mathbb{E}\left\{\ln\left(1+\Gamma_B\right)\right\} - \mathbb{E}\left\{\ln\left(1+\Gamma_E\right)\right\}\right]^+. \end{aligned} \tag{15}$$

Assuming that all noise variances are equal to σ^2, we define the average SNRs $\rho = P/(2\sigma^2)$ and $\rho_s = P_s/\sigma^2$. Thus, the received SNR at Bob can be written as

$$\Gamma_B = \rho_s \sum_{k=1}^{N_b} \left|h_{R_i B_k}\right|^2, \tag{16}$$

and the cumulative distribution function (CDF) of Γ_B is given by

$$F_{\Gamma_B}(\gamma_b) = 1 - \sum_{k=0}^{N_b-1} \frac{1}{k!}\left(\frac{\gamma_b}{\overline{\gamma}_b \rho_s}\right)^k e^{-\gamma_b/\rho_s\overline{\gamma}_b}, \tag{17}$$

where $\overline{\gamma}_b = d_{R_i B}^{-\alpha}$.

Using the CDF approach, the first part of the ergodic secrecy capacity lower bound is given in closed-form by

$$\begin{aligned} \mathbb{E}\left\{\ln\left(1+\Gamma_B\right)\right\} &= \int_0^\infty \frac{1-F_{\Gamma_B}(\gamma_b)}{1+\gamma_b} d\gamma_b \\ &= \sum_{k=0}^{N_b-1} \frac{1}{k!\overline{\gamma}_b{}^k \rho_s{}^k} \int_0^\infty \frac{\gamma_b^k}{1+\gamma_b} e^{-\gamma_b/\rho_s\overline{\gamma}_b} d\gamma_b \\ &= \sum_{k=0}^{N_b-1} \frac{1}{\overline{\gamma}_b{}^k \rho_s{}^k} \Psi\left(k+1, k+1; \frac{1}{\rho_s\overline{\gamma}_b}\right), \end{aligned} \tag{18}$$

where $\Psi(\cdot,\cdot;\cdot)$ is the Confluent Hypergeometric function of the second kind [25, equation (9.211.4)]. Similarly, using (13), the CDF of Eve's SNR is given by

$$F_{\gamma_{E,2}}(\gamma_e) = \int_0^\infty F_X\left(\frac{1}{\rho_s}\left(P_J y + 1\right)\gamma_e\right) f_Y(y)\, dy, \tag{19}$$

where $F_X(\cdot)$ is the CDF of the random variable $X = \|\mathbf{h}_{R_i E}\|_{\mathrm{F}}^2$ and $f_Y(\cdot)$ is the probability density function (PDF) of the RV $Y = \sum_{k\neq i} \|\mathbf{h}_{R_k E}\|_{\mathrm{F}}^2$ representing in this case the summation of $N = N_e(N_r - 1)$ exponential random variables.

Using the CDF approach, similar to (18), the second part of the ergodic secrecy capacity lower bound can be obtained:

$$\begin{aligned} \mathbb{E}\left\{\ln\left(1+\Gamma_E\right)\right\} &= \int_0^\infty \frac{1-F_{\Gamma_E}(\gamma_e)}{1+\gamma_e} d\gamma_e \\ &= \sum_{k=0}^{N_e-1} \sum_{j=0}^{k} \frac{(N+j-1)! P_J^j \rho_s{}^{N+j-k}}{j!\,(k-j)!\,(N-1)!\overline{\gamma}_e^{k-j}} \\ &\quad \times \int_0^\infty \frac{\gamma_e^k}{\left(\gamma_e+1\right)\left(P_J\gamma_e+\rho_s\right)^{N+j}} e^{-\gamma_e/\overline{\gamma}_e\rho_s} d\gamma_e, \end{aligned} \tag{20}$$

where $\overline{\gamma}_e = d_{R_i,E}^{-\alpha}$.

3.3. Secrecy Outage Probability. The secrecy outage probability is defined as the probability of the secrecy capacity C_s being less than a predetermined secrecy rate $\mathscr{R}_s$ [5] and it is given by

$$\begin{aligned} P_{\text{out}}(\mathscr{R}_s) &= \Pr\left[C_s \leq \mathscr{R}_s\right] \\ &= \Pr\left[\Gamma_B \leq 2^{\mathscr{R}_s}\left(1+\Gamma_E\right) - 1\right] \\ &= \int_0^\infty F_{\Gamma_B}\left(2^{\mathscr{R}_s}\left(1+\gamma_e\right) - 1\right) f_{\Gamma_E}(\gamma_e)\, d\gamma_e \\ &= 1 - \sum_{l=0}^{N_b-1} \frac{P_J^N}{l!\overline{\gamma}_b{}^l \rho_s{}^l} \sum_{k=0}^{N_e-1} \sum_{j=0}^{k} \frac{(N+j-1)!\rho_s{}^{N+j-k}}{j!\,(k-j)!\,(N-1)!\overline{\gamma}_e^{k-j}} \\ &\quad \times \sum_{m=0}^{l} \sum_{n=0}^{m} \binom{l}{m}\binom{m}{n} (-1)^{l-m} 2^{m\mathscr{R}_s} e^{-2^{\mathscr{R}_s}-1/\rho_s\overline{\gamma}_e} \\ &\quad \times \int_0^\infty \left(\frac{1}{\rho_s\overline{\gamma}_e}\gamma_e^2 + \left(N+j-k+\frac{1}{P_J\overline{\gamma}_e}\right)\gamma_e - k\frac{\rho_s}{P_J}\right) \\ &\quad \times \frac{\gamma_e^{n+k-1}}{\left(\gamma_e+\rho_s/P_J\right)^{N+j+1}} e^{-(2^{\mathscr{R}_s}+1)\gamma_e/\rho_s\overline{\gamma}_e} d\gamma_e. \end{aligned} \tag{21}$$

Using change of variables and Binomial expansion, the outage probability can be obtained in closed-form in (22)

where $a = (2^{\mathscr{R}_s} + 1)/P_J\overline{\gamma}_e$, $b = \rho_s/P_J$, and $\Gamma(\cdot,\cdot)$ is the upper incomplete Gamma function:

$$\begin{aligned} P_{\text{out}}(\mathscr{R}_s) &= 1 - \sum_{l=0}^{N_b-1} \frac{P_J^N}{l!\overline{\gamma}_b{}^l \rho_s{}^l} \\ &\cdot \sum_{k=0}^{N_e-1}\sum_{j=0}^{k} \frac{(N+j-1)!\rho_s{}^{N+j-k}}{j!\,(k-j)!\,(N-1)!\overline{\gamma}_e^{k-j}} \\ &\cdot \sum_{m=0}^{l}\sum_{n=0}^{m} \binom{l}{m}\binom{m}{n}(-1)^{l-m} 2^{m\mathscr{R}_s} e^{-2^{\mathscr{R}_s}-1/\rho_s\overline{\gamma}_e} \\ &\times \left\{ \frac{1}{\rho_s\overline{\gamma}_e} \sum_{p=0}^{n+k+1} \binom{n+k+1}{p} (-b)^{n+k+1-p} \left(\frac{b}{a}\right)^{p+1} \right. \\ &\cdot \Gamma(p-N-j,a) + \left(N+j-k+\frac{1}{P_J\overline{\gamma}_e}\right) \\ &\cdot \sum_{q=0}^{n+k} \binom{n+k}{q} \times (-b)^{n+k-q} \left(\frac{b}{a}\right)^{q+1} \Gamma(q-N-j,a) \\ &- kb \sum_{r=0}^{n+k-1} \binom{n+k-1}{r} (-b)^{n+k-1-r} \Gamma(r-N-j,a) \\ &\left. \cdot \left(\frac{b}{a}\right)^{r+1} \right\} e^{-a/b}. \end{aligned} \tag{22}$$

3.4. Average Bit Error Probability

3.4.1. ABEP of Bob. In this part, the theoretical ABEP of Bob is derived. Based on the analysis of [26, 27], the end-to-end ABEP is expressed as

$$P_{\text{Bob}}(\gamma_1,\gamma_2) = P_1(\gamma_1) + P_2(\gamma_2) - P_1(\gamma_1)P_2(\gamma_2). \tag{23}$$

Here, $P_1(\gamma_1)$ is the ABEP between Alice and the RN, during the first time slot, for a given transmit SJNR γ_1 and $P_2(\gamma_2)$ is the ABEP between the RN and Bob, during the second slot, for a given transmit SNR γ_2. Hence the evaluation of the ABEP of Bob requires the evaluation of $P_1(\gamma_1)$ and $P_2(\gamma_2)$.

During the first slot, assuming ZF precoding at Alice with

$$\mathbf{P} = \mathbf{H}_{\mathbf{AR}}^H \left(\mathbf{H}_{\mathbf{AR}}\mathbf{H}_{\mathbf{AR}}^H\right)^{-1}, \tag{24}$$

the received signal at the RN is given as

$$\mathbf{y}_{\text{R}} = \sqrt{P_A d_{\text{AR}}^{-\alpha}}\mathbf{D}\mathbf{x} + \widetilde{\mathbf{w}}. \tag{25}$$

Here, it holds that $\mathbf{H}_{\mathbf{AR}} = \sqrt{d_{\text{AR}}^{-\alpha}}\widetilde{\mathbf{H}}_{\text{AR}}$, with $\widetilde{\mathbf{H}}_{\text{AR}} \sim \mathscr{CN}(\mathbf{0},\mathbf{I})$. In (25), P_A denotes Alice's transmit power and $\widetilde{\mathbf{w}}$ is a vector denoting the composite effect of noise plus jamming from Bob. Also, $\mathbf{D}$ is the $N_r \times N_r$ diagonal normalization matrix defined as $\mathbf{D} = \sqrt{d_{\text{AR}}^{-a}}\mathbf{diag}(d_1,\ldots,d_{N_r})$, where

$$d_i = \sqrt{\frac{1}{\left[\left(\widetilde{\mathbf{H}}_{\text{AR}}\widetilde{\mathbf{H}}_{\text{AR}}^H\right)^{-1}\right]_{i,i}}}. \tag{26}$$

Here, we note that the ZF precoder defined in (24) is equivalent to the one defined in (2). We use the new definition only for analytical tractability and for the sake of the simplicity of the derived ABEP results. This also enriches the paper by giving two different ways of defining the ZF precoder used at Alice under the same assumptions.

Since jamming is treated as noise at the RN, the detector at the RN is given as

$$(\overline{\mathbf{x}}) = \arg\min_{\mathbf{x}} \left\|\mathbf{y}_{\text{R}} - \mathbf{D}\mathbf{x}\right\|_2^2. \tag{27}$$

In particular, (27) is the ML detector of PSM. Therefore, $P_1(\gamma_1)$ is the ABEP of PSM with the jamming effect. Hence, the ABEP during the first hop at the RN is given as

$$P_1(\gamma_1) \le \frac{1}{Mk_t}\sum_{\mathbf{x}}\sum_{\mathbf{x}\neq\widehat{\mathbf{x}}} d(\mathbf{x}\longrightarrow\widehat{\mathbf{x}})\,P_{\text{R-SM}}(\mathbf{x}\longrightarrow\widehat{\mathbf{x}}), \tag{28}$$

where $d(\mathbf{x}\longrightarrow\widehat{\mathbf{x}})$ is the Hamming distance between the bit sequences represented by $\mathbf{x}$ and $\widehat{\mathbf{x}}$. $k_t = (k_1+k_2)/2$ is equal to the total number of bits transmitted per symbol period. We note that $k_1 + k_2$ is divided by two because the transmitted bitstream requires two symbol periods to reach Bob. Also, $P_{\text{R-SM}}(\mathbf{x}\longrightarrow\widehat{\mathbf{x}})$ is the PEP of transmitting $\mathbf{x}$ at Alice and erroneously detecting $\widehat{\mathbf{x}}$ at the relay nodes.

Based on the analysis presented in [28, Section IV], the instantaneous PEP is given as

$$P_{\text{R-SM}}\left(\mathbf{x}\longrightarrow\widehat{\mathbf{x}},\gamma_1 \mid \mathbf{D}^2\right) = Q\left(\sqrt{\frac{\mathbf{c}^H\mathbf{D}^2\mathbf{c}}{2}P_A d_{\text{AR}}^{-a}\gamma_1}\right), \tag{29}$$

where $\mathbf{c} = \mathbf{x} - \widehat{\mathbf{x}}$. Considering the following upper bound of the Q-function [29]:

$$Q(x) \le \sum_{i=1}^{3}\beta_i e^{-\mu_i x^2}, \tag{30}$$

in (29) and averaging over all possible realizations of the Alice-RN channel, the average PEP of PSM is expressed as [28, Section IV]

$$\begin{aligned} P_{\text{R-SM}}(\mathbf{x}\longrightarrow\widehat{\mathbf{x}}) \le \sum_{i=1}^{3} &\frac{\beta_i\left[\prod_{l=1}^{N}(\alpha_1/\alpha_l)^L\right]}{2\left(\mu_i\alpha_1 P_A d_{\text{AR}}^{-a}\gamma+1\right)^L} \\ &\times \sum_{k=0}^{+\infty}\delta_k\left(\mu_i\alpha_1 P_A d_{\text{AR}}^{-a}\gamma+1\right)^{-k}. \end{aligned} \tag{31}$$

Here, it holds that $\beta_1 = 1/2$, $\beta_2 = 1/12$, $\beta_3 = 1/4$, $\mu_1 = 2$, $\mu_2 = 1$, and $\mu_3 = 1/2$. Furthermore, for a given pair of $\mathbf{x}_i$ and $\widehat{\mathbf{x}}_i$, N is the number of nonzero elements of $\mathbf{c}$. Also, α_l, $l = 1,\ldots,N$, stand for the eigenvalues of $\mathbf{A} = \mathbf{BR}$ in ascending order. Here, $\mathbf{B}$ is a diagonal matrix, defined as $\mathbf{B} = \mathbf{diag}(b_1,\ldots,b_N)$, where b_l, $l = 1,\ldots,N$, is the absolute

value of the lth nonzero element of $\mathbf{c}_i$. In addition, $\mathbf{R}$ is a $N \times N$ matrix given as shown in (33).

$$\delta_{k+1} = \begin{cases} 1, & k = -1, \\ \dfrac{k}{k+1} \displaystyle\sum_{i=1}^{k+1} \left[\sum_{j=1}^{N} \left(1 - \frac{\alpha_1}{\alpha_j} \right)^i \right] \delta_{k+1-i}, & k = 0, 1, 2, \ldots. \end{cases} \tag{32}$$

$$\mathbf{R} = \begin{bmatrix} 1 & \sqrt{\rho_c} & \cdots & \sqrt{\rho_c} \\ \sqrt{\rho_c} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \sqrt{\rho_c} \\ \sqrt{\rho_c} & \cdots & \sqrt{\rho_c} & 1 \end{bmatrix}. \tag{33}$$

In (33), ρ_c denotes the Pearson product-moment correlation coefficient between any pair of two different random variables (RVs) $d_1^2, \ldots, d_R^2$. Moreover, δ_k, $k = 0, 1, 2, \ldots$, are given in (32). Finally, it holds that $L = N_t - N_r + 1$.

During the second hop, the received signal at Bob is expressed as

$$\mathbf{y}_{\mathrm{B}} = \sqrt{P_R} \mathbf{H}_{\mathbf{RB}} \overline{\mathbf{x}} + \mathbf{w}_{\mathrm{B}}, \tag{34}$$

after the ideal removal of the jamming signal. In (34), it holds that $\mathbf{H}_{\mathbf{RB}} = \sqrt{d_{\mathrm{RB}}^{-a}} \widetilde{\mathbf{H}}_{\mathrm{RB}}$, with $\widetilde{\mathbf{H}}_{\mathrm{RB}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$. Also, P_R is the transmission power at the RN. Note that the value of P_R is selected such that the transmitted signal at the RN is normalized. As the RN retransmits binary information by using SM, Bob can deploy the following ML detector [8]:

$$(\check{\mathbf{x}}) = \arg \min_{\mathbf{x}} \left\| \mathbf{y}_{\mathrm{B}} - \sqrt{P_B d_{\mathrm{RB}}^{-a}} \widetilde{\mathbf{H}}_{\mathrm{RB}} \mathbf{x} \right\|_2^2. \tag{35}$$

Therefore, the ABEP of the second hop is given as

$$P_2(\gamma_2) \leq \frac{1}{M k_t} \sum_{\mathbf{x}} \sum_{\mathbf{x} \neq \widehat{\mathbf{x}}} d(\mathbf{x} \longrightarrow \widehat{\mathbf{x}}), \quad P_{\mathrm{SM}}(\mathbf{x} \longrightarrow \widehat{\mathbf{x}}), \tag{36}$$

where $P_{\mathrm{SM}}(\mathbf{x} \longrightarrow \widehat{\mathbf{x}})$ is the average PEP of transmitting $\mathbf{x}$ at the RN, while the detector of Bob decides in favor of $\widehat{\mathbf{x}}$. Considering the statistical characteristics of the noise at Bob, it can be shown that the instantaneous PEP is given as

$$P_{\mathrm{SM}}\left(\mathbf{x} \longrightarrow \widehat{\mathbf{x}}, \gamma_2 \mid \widetilde{\mathbf{H}}_{\mathrm{RB}}\right) = Q\left(\sqrt{\frac{\left\| \widetilde{\mathbf{H}}_{\mathrm{RB}} \mathbf{c} \right\|_2^2}{2} P_R d_{\mathrm{RB}}^{-a} \gamma_2} \right). \tag{37}$$

In (37), it is shown that the RV $X = \|\widetilde{\mathbf{H}}_{\mathrm{RB}} \mathbf{c}\|_2^2$ follows an Erlang distribution with the following PDF [30]:

$$f_X(x) = \frac{1}{\|\mathbf{c}\|_2^{2N_r} \Gamma(N_r)} x^{N_r} e^{x/\|\mathbf{c}\|_2^2} H_0(x), \tag{38}$$

where $H_0(x)$ is the Heaviside step function defined as $H_0(x) = 0$ for $x < 0$ and $H_0(x) = 1$ for $x \geq 0$. Considering (30) and (38) in (37), the average PEP of the second hop is given as

$$P_{\mathrm{SM}}(\mathbf{x} \longrightarrow \widehat{\mathbf{x}}) \leq \sum_{i=1}^{3} \frac{\beta_i}{\|\mathbf{c}\|_2^{2N_r} \Gamma(\mathrm{N}_r)} \times \int_0^{+\infty} x^{N_r - 1} e^{-(P_R d_{\mathrm{RB}}^{-a} \mu_i \gamma_2 + 1/\|\mathbf{c}\|_2^2) x} \mathrm{d}x, \tag{39}$$

by averaging over possible realizations of the RV X. From [25, p.346, 3.381, 4], it holds that

$$\int_0^{+\infty} x^{\nu - 1} e^{-\mu x} dx = \mu^{-\nu} \Gamma(\nu). \tag{40}$$

The use of (30) and (40) into (39), after a straightforward elaboration, results in

$$P_{\mathrm{SM}}(\mathbf{x} \longrightarrow \widehat{\mathbf{x}}) \leq \sum_{i=1}^{3} \beta_i \left(\|\mathbf{c}\|_2^2 \mu_i P_R d_{\mathrm{RB}}^{-a} \gamma_2 + 1 \right)^{-N_r}. \tag{41}$$

In this way, the ABEP of Bob is computed via (23) by using (28), (31), (36), and (41).

3.4.2. ABEP of Eve. In this part, the theoretical ABEP of Eve is derived. As previously shown in Figure 2, the Signal-to-Jamming-Plus-Noise Ratio at Eve during the second phase is much higher than the SJNR during the first phase for different simulation scenarios and parameters. Thus, the ABEP of Eve during the first phase is much worse than the ABEP during the second phase. Accounting for the worst-case scenario (i.e., taking the highest SNR at Eve and assuming perfect detection at the relays during the first phase), the SJNR at Eve when the ith relay is used during the second phase is given by

$$\gamma_E = \frac{P_s \left\| \mathbf{h}_{R_i E} \right\|_{\mathrm{F}}^2}{P_J \sum_{k \neq i} \left\| \mathbf{h}_{R_k E} \right\|_{\mathrm{F}}^2 \sigma_g^2 + \sigma_e^2}. \tag{42}$$

In light of the above, the asymptotic performance bound of the ABEP at Eve with optimal detection is derived using the union bound as

$$P_E \leq \sum_{q=1}^{M} \sum_{\widehat{q}=1}^{M} \frac{N_r N(q, \widehat{q})}{M} P\left(x_{jq} \longrightarrow x_{\widehat{jq}} \right), \tag{43}$$

where $N(q, \widehat{q})$ is the number of bits in error between the symbol x_q and $x_{\widehat{q}}$, and $P(x_{jq} \longrightarrow x_{\widehat{jq}})$ denotes the PEP of deciding on the constellation vector $x_{\widehat{jq}}$ given that x_{jq} is transmitted and can be formulated as

$$P\left(x_{jq} \longrightarrow x_{\widehat{jq}} \right) = \int_{v=0}^{\infty} Q\left(\sqrt{v} \right) f_\kappa(v) \, dv, \tag{44}$$

where $f_\kappa(\cdot)$ is the PDF and is a chi-squared random variable with $2N_e$ degrees of freedom given by [31, p. 41] as

$$f_\kappa(v) = \frac{v^{N_e - 1} \exp\left(-v / \left(2\alpha^2 \right) \right)}{\left(2\alpha^2 \right)^{N_e} (N_e - 1)!}, \tag{45}$$

where

$$\alpha^2 = \frac{\delta_2 \rho}{(1-\delta_2)\rho + 1}\left(\frac{\left|x_q\right|^2 + \left|x_{\widehat{q}}\right|^2}{4}\right). \quad (46)$$

Thus, the PEP in (44) is obtained in closed-form as

$$P\left(x_{jq} \longrightarrow x_{\widehat{jq}}\right) = \gamma^{N_e} \sum_{w=0}^{N_e-1} \binom{N_e + w - 1}{w} (1-\gamma)^w, \quad (47)$$

where

$$\gamma = \frac{1}{2}\left(1 - \sqrt{\frac{\alpha^2}{1+\alpha^2}}\right). \quad (48)$$

Finally, plugging in (47) in (43), the ABEP at Eve is obtained as

$$P_E \leq \sum_{q=1}^{M} \sum_{\widehat{q}=1}^{M} \frac{N_r N(q,\widehat{q})\, \gamma^{N_e} \sum_{w=0}^{N_e-1} \binom{N_e+w-1}{w} (1-\gamma)^w}{M}. \quad (49)$$

4. Numerical Results

In this section, we present selected numerical examples to confirm the ergodic secrecy capacity and the secrecy outage probability results derived in the previous section. We also present the bit error rate (BER) comparison for Bob and Eve by simulations. In these results, we assume that the secrecy during the first phase is guaranteed thanks to the use of PSM [10]. Indeed, the received SNR at Eve during the second phase exceeds that of the first phase with very high probability as discussed in Section 3.2 and shown in Figure 2.

As discussed earlier, the total power is allocated during the first and second phases using the power allocation factors δ_1 and δ_2, respectively. While both power allocation factors have effect on the performance of the proposed scheme, δ_2 has more weight and affects the BER performance more than δ_1. Indeed, the beamforming used at Alice during the first phase maximizes the received SNR at the intended relay which reduces the effect of the power allocation factor δ_1. In what follows, we study the effect of δ_2 and show that it has more weight and affects the performance more than δ_1. In this context, Figure 3 presents the effect of the power allocation coefficient δ_2 during the second phase on the secrecy outage probability. We can see from this figure that the value of the optimal power allocation coefficient δ_2^* depends on different parameters including the number of antennas at different nodes. For instance, while δ_2^* is equal to 0.3 for $N_b = 4$ and $N_e = 2$, it is equal to 0.45 for $N_b = 4$ and $N_e = 16$. The exact values for the optimal power allocation coefficient can be mathematically derived by optimizing the SOP expression in (22). It can also be obtained through the asymptotic outage secrecy performance and we look at addressing this as a future extension to this work in order to further enhance the performance of the proposed scheme. In the following results, we use the optimal power allocation coefficient values obtained by simulations when generating the SOP curves.

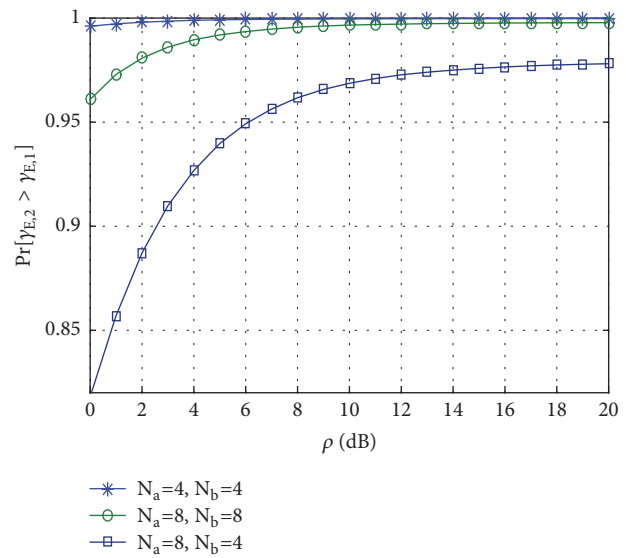


Figure 2: Probability that $\gamma_{E,2}$ exceeds $\gamma_{E,1}$ as a function of the average SNR with different N_a and N_b for $N_r = N_e = 4$ and $\delta_1 = \delta_2 = 0.5$.

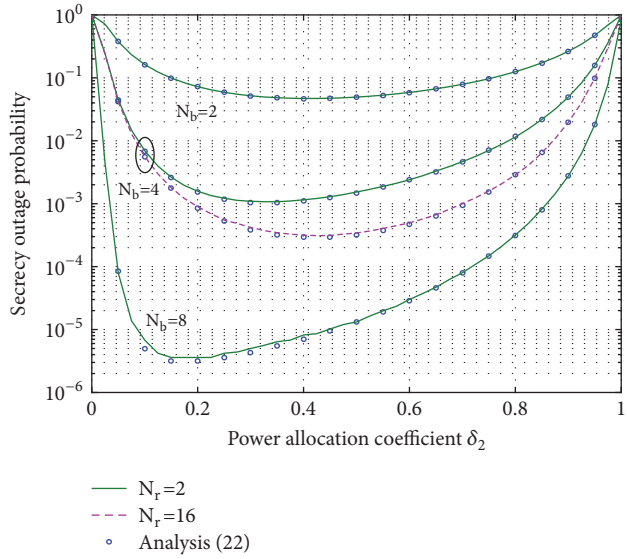


Figure 3: Effect of the power allocation at the second phase on the SOP with different N_b and N_r, for $N_e = 4$, $\rho = 20$ dB, $\mathscr{R}_s = 1$, and $\delta_1 = 0.5$.

In Figure 4, we present the secrecy outage probability as a function of the average received SNR with both simulation and analysis. This figure is given for a secrecy rate threshold $\mathscr{R}_s = 1$ bits/s/Hz, $N_r = 4$, $N_e = 4$, and for different number of antennas at Bob. The power allocation coefficient δ_2 is selected as discussed above and is equal to δ_2^* corresponding to each number of antennas at Bob. Figure 4 also compares the performance of the proposed scheme to the case where a single relay participates in transmitting the jamming signal at the second phase. We can clearly see the advantage of using

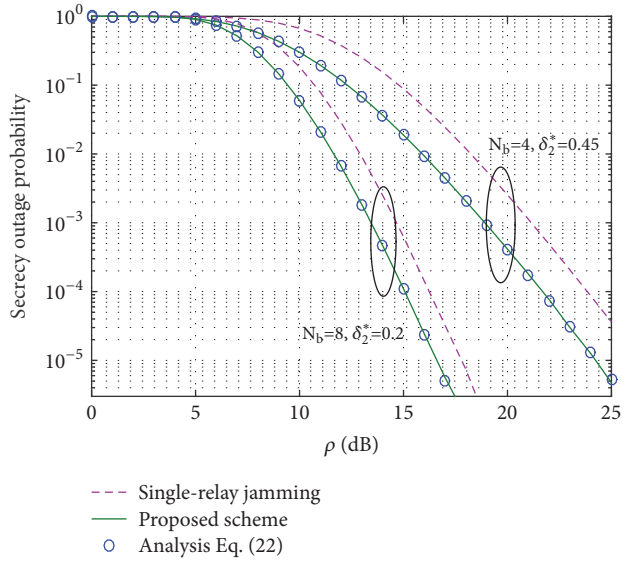


FIGURE 4: SOP comparison with the case where a single relay is used for jamming, for $\mathscr{R}_s = 1$ bits/s/Hz, $N_a = 4$, $N_r = 4$, $N_e = 4$, and $\delta_1 = 0.5$.

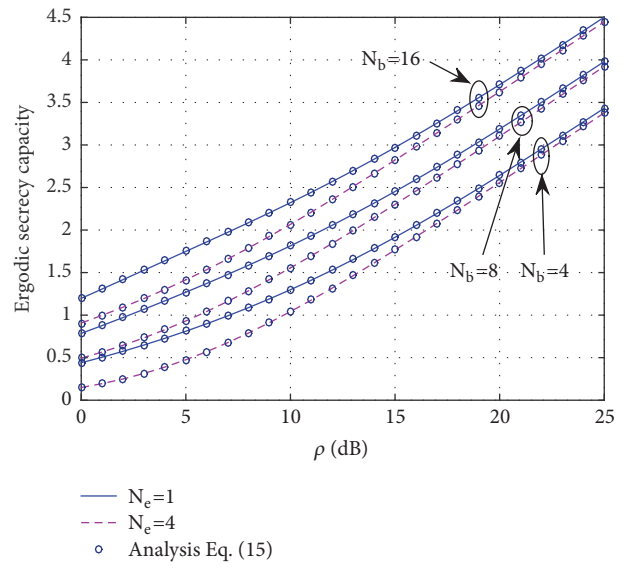


FIGURE 5: ESC with different number of antennas at Bob and Eve, for $N_a = 4$, $N_r = 4$, $\delta_1 = 0.5$, and $\delta_2 = 0.75$.

multiple relays for jamming as it enhances the secrecy outage probability by further degrading the received SNR at Eve.

Figure 5 presents the ESC in bits/s/Hz as a function of the average SNR $\rho = P/(2\sigma^2)$ with different number of antennas at Bob and Eve, for $N_a = 4$, $N_r = 4$, $\delta_1 = 0.5$, and $\delta_2 = 0.75$. These results show the accuracy of the analytical derivations presented in the previous section. We can also see from this figure the effect of different parameters on the ESC. In this context, we can confirm the improvement of the secrecy rate through increasing the number of antennas at Bob and its degradation by increasing the number of antennas at Eve. We can also see that, for high average SNRs, the number of

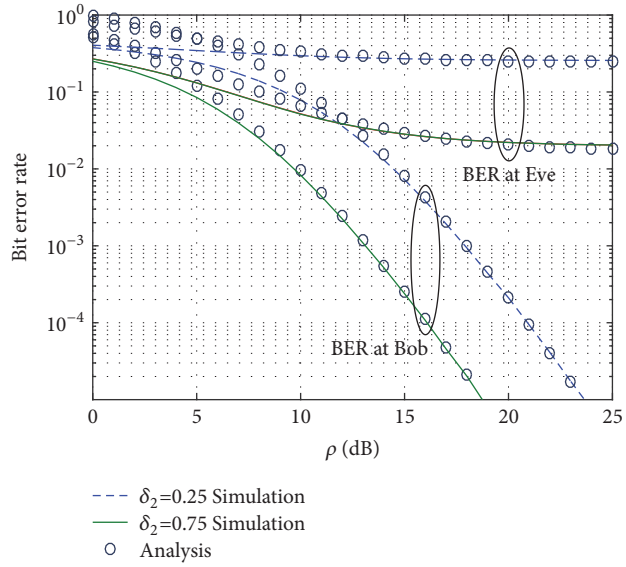


FIGURE 6: BER comparison at Bob and Eve for different power allocations during the second phase, for $N_a = 4$, $N_r = 4$, $N_b = 4$, $N_e = 4$, and $\delta_1 = 0.5$.

antennas at Eve has less effect of the ESC performance and the curves for $N_e = 1$ and $N_e = 4$ converge.

Figure 6 depicts the BER at Bob and Eve as a function of ρ for different power allocation coefficients δ_2. This figure confirms the tightness of the ABEP bounds derived in the previous section. The main goal of the proposed scheme is to make sure that Eve is not able to detect the information exchanged between Alice and Bob. To this end, we use precoding-aided spatial modulation and cooperative jamming. Thanks to these techniques, the SNR at Eve becomes very low and, thus, the error performance degrades. The simulation results shown in Figure 6 confirm the improvement of the BER at Bob compared to the BER at Eve thanks to the use of the multirelay jamming. From this figure, we can also see that the BER at both Bob and Eve improves when more power is allocated for the relay selected by PSM (i.e., the relay transmitting the message). On the other hand, the BER at both receivers degrades when more power is allocated to the jamming relays.

In Figure 7, we study the effect of the number of receive antennas on the BER at Bob and Eve as a function of ρ for $N_a = 4$, $N_r = 4$, $\delta_1 = 0.5$, and $\delta_2 = 0.7$. These simulation results show the improvement of the BER at Bob and Eve for higher number of receive antennas at each of these nodes. From this figure, we can also confirm that the use of multirelay jamming comes with improved BER at Bob compared to the BER at Eve. Indeed, Eve experiences much worse detection performance thanks to the use of PSM and jamming from Bob in the first phase and the use of jamming from $N_r - 1$ relays in the second phase.

In the above results, we note that we used a fixed number of relays, equal to four, only to simplify the simulations. However, we need to highlight that the performance of the proposed scheme depends on the number of available relays.

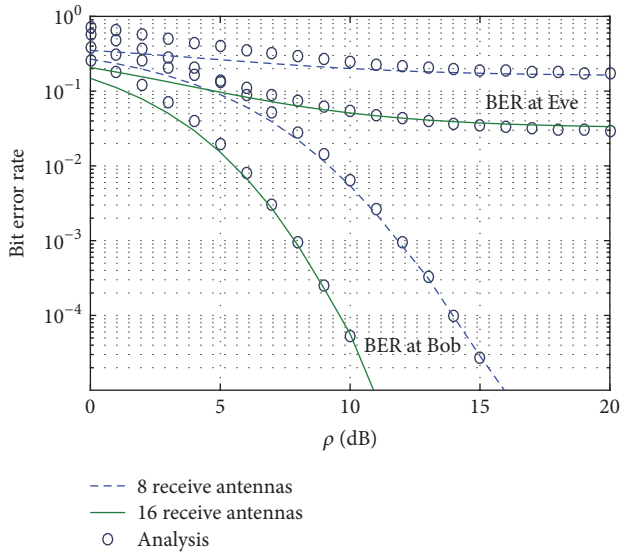


FIGURE 7: BER comparison at Bob and Eve for different number of receive antennas, for $N_a = 4$, $N_r = 4$, $\delta_1 = 0.5$, and $\delta_2 = 0.7$.

Indeed, in the proposed work, while increasing the number of relays enhances the spectral efficiency as a property of precoding-aided spatial modulation, it causes a degradation in the BER performance [32]. Indeed, the increase in N_r is equivalent to increasing the constellation size of the index modulation used during the second phase while keeping the same transmit power. This case will generate more errors at the ML detector as the distance between different constellation points shrinks with a higher N_r and a constant transmit power, divided between all relays using the power allocation factor δ_2.

5. Conclusion

In this paper, we have studied the physical-layer security of a wiretap channel using a PSM-based relay-selection scheme with multiple relays' jamming. The performance of the proposed system is evaluated in terms of the ergodic secrecy capacity, secrecy outage probability, and bit error rate performances. Numerical results, confirmed by analysis, show an enhanced secrecy performance when compared to selected schemes. Using simulations, we use power allocation optimization in order to divide the power between the relay transmitting the useful information and the jamming relays, and thus we further improve the secrecy performance of the proposed scheme. In this paper, we have also provided closed-form expressions for the ESC and SOP and we derive very tight upper-bounds for the BER. These results confirm the ESC, SOP, and BER performance improvements at Bob and its degradation at Eve, which confirms the high secrecy performance of the proposed scheme.

Data Availability

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

Disclosure

The statements made herein are solely the responsibility of the authors. This work was presented in part at the 2017 IEEE WCNC Conference, San Francisco, CA, USA [33].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by Qatar National Research Fund (a member of Qatar Foundation) under National Priorities Research Program (NPRP) Grant NPRP 8-052-2-029.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 29, no. 4, pp. 656–715, 1949.

[2] R. Liu and W. Trappe, *Securing Communications at the Physical Layer*, Springer-Verlag, New York, NY, USA, 2010.

[3] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Communications Magazine*, vol. 19, no. 1, pp. 40–47, 2012.

[4] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[6] 5GPPP, *5G Vision*, 2015. [Online]. Available: http://5g-ppp.eu/wpcontent/uploads/2015/02/5G-Vision-Brochure-v1.pdf.

[7] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[8] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Spatial modulation: Optimal detection and performance analysis," *IEEE Communications Letters*, vol. 12, no. 8, pp. 545–547, 2008.

[9] M. D. Renzo, H. Haas, A. Ghrayeb, S. Sugiura, and L. Hanzo, "Spatial modulation for generalized MIMO: challenges, opportunities, and implementation," *Proceedings of the IEEE*, vol. 102, no. 1, pp. 56–103, 2014.

[10] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 467–471, 2016.

[11] F. Wu, C. Dong, L. Yang, and W. Wang, "Secure Wireless Transmission Based on Precoding-Aided Spatial Modulation," in *Proceedings of the GLOBECOM 2015 - 2015 IEEE Global Communications Conference*, pp. 1–6, San Diego, CA, USA, December 2015.

[12] F. Wu, L.-L. Yang, W. Wang, and Z. Kong, "Secret Precoding-Aided Spatial Modulation," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1544–1547, 2015.

[13] Y. Chen, L. Wang, Z. Zhao, M. Ma, and B. Jiao, "Secure Multiuser MIMO Downlink Transmission Via Precoding-Aided Spatial Modulation," *IEEE Communications Letters*, vol. 20, no. 6, pp. 1116–1119, 2016.

[14] J. Jeganathan, A. Ghrayeb, L. Szczecinski, and A. Ceron, "Space shift keying modulation for MIMO channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 3692–3703, 2009.

[15] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Generalized space shift keying modulation for MIMO channels," in *Proceedings of the IEEE PIMRC*, pp. 1–5, Cannes, France, 2008.

[16] L. Yang, "Transmitter Preprocessing Aided Spatial Modulation for Multiple-Input Multiple-Output Systems," in *Proceedings of the 2011 IEEE Vehicular Technology Conference (VTC 2011-Spring)*, pp. 1–5, Budapest, Hungary, May 2011.

[17] R. Zhang, L.-L. Yang, and L. Hanzo, "Generalised pre-coding aided spatial modulation," *IEEE Transactions on Wireless Communications*, vol. 12, no. 11, pp. 5434–5443, 2013.

[18] C.-X. Wang, F. Haider, X. Gao et al., "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 122–130, 2014.

[19] D. A. Basnayaka, M. Di Renzo, and H. Haas, "Massive but few active MIMO," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 6861–6877, 2016.

[20] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1756–1770, 2015.

[21] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[22] A. Mabrouk, K. Tourki, and N. Hamdi, "Relay selection for optimized cooperative jamming scheme," in *Proceedings of the 23rd European Signal Processing Conference, EUSIPCO 2015*, pp. 86–90, Nice, France, September 2015.

[23] Y. Huo, X. Dong, and W. Xu, "5G cellular user equipment: From theory to practical hardware design," *IEEE Access*, vol. 5, pp. 13992–14010, 2017.

[24] A. Stavridis, D. Basnayaka, S. Sinanovic, M. Di Renzo, and H. Haas, "A virtual MIMO dual-hop architecture based on hybrid spatial modulation," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3161–3179, 2014.

[25] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, New York, NY, USA, 7th edition, 2007.

[26] M. O. Hasna and M.-S. Alouini, "End-to-end performance of transmission systems with relays over Rayleigh-fading channels," *IEEE Transactions on Wireless Communications*, vol. 2, no. 6, pp. 1126–1131, 2003.

[27] N. Serafimovski, S. Sinanovic, M. Di Renzo, and H. Haas, "Dual-Hop Spatial Modulation (Dh-SM)," in *Proceedings of the 2011 IEEE Vehicular Technology Conference (VTC 2011-Spring)*, pp. 1–5, Budapest, Hungary, May 2011.

[28] A. Stavridis, M. Di Renzo, and H. Haas, "Performance Analysis of Multistream Receive Spatial Modulation in the MIMO Broadcast Channel," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 1808–1820, 2016.

[29] M. Chiani, D. Dardari, and M. K. Simon, "New exponential bounds and approximations for the computation of error probability in fading channels," *IEEE Transactions on Wireless Communications*, vol. 2, no. 4, pp. 840–845, 2003.

[30] E. Bjornson, D. Hammarwall, and B. Ottersten, "Exploiting quantized channel norm feedback through conditional statistics in arbitrarily correlated MIMO systems," *IEEE Transactions on Signal Processing*, vol. 57, no. 10, pp. 4027–4041, 2009.

[31] J. Proakis, *Digital Communications*, McGraw-Hill, 4th edition, 2001.

[32] Z. Bouida, A. Ghrayeb, and K. A. Qaraqe, "Adaptive spatial modulation for spectrally-efficient MIMO spectrum sharing systems," in *Proceedings of the 2014 25th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communication, IEEE PIMRC 2014*, pp. 354–358, Washington, DC, USA, September 2014.

[33] Z. Bouida, A. Stavridis, A. Ghrayeb, H. Haas, and M. Hasna, "Precoded spatial modulation for the wiretap channel with relay selection and cooperative jamming," in *Proceedings of the 2017 IEEE Wireless Communications and Networking Conference, WCNC 2017*, pp. 1–6, San Francisco, CA, USA, March 2017.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 4602146, 13 pages
https://doi.org/10.1155/2018/4602146

Research Article

On the Performance of the DNPS-Based Relay Networks under Masquerading Attack

Wenson Chang

Department of Electrical Engineering, National Cheng Kung University, Tainan 701, Taiwan

Correspondence should be addressed to Wenson Chang; wenson@ee.ncku.edu.tw

Received 8 March 2018; Revised 15 June 2018; Accepted 2 July 2018; Published 17 July 2018

Academic Editor: Yafei Hou

In the relay networks, two typical issues of physical layer security are selfishness and garbling. As a matter of fact, a certain nontypical but severely harmful misbehavior can also remove the cooperative diversity gain. Here, we coin the masquerading attack to indicate this kind of misbehavior. A masquerade relay can always pretend to be the best one to forward signals and, in consequence, deprive the others of the opportunities to cooperate. To the best of our knowledge, the impact of the masquerading attack has not yet been fully investigated. In this paper, multiple masquerade relays with random masquerading behavior are taken into account. Also, the complete channel effects, including the effects of the flat Rayleigh fading, log-normal shadowing, and path loss, are considered such that the geographical effects of the network topology can be completely captured. At last, the impact of the masquerade relays are evaluated in terms of the outage probability and end-to-end capacity.

1. Introduction

Nowadays, the hyperdense heterogeneous network (HetNet) has been widely recognized as a necessity to boost data rate for future generation of wireless communication systems [1–3]. With hyperdense deployment, the cooperative communication technologies can effectively extend system coverage and enhance quality of service (QoS). One important paradigm to accomplish these tasks is the cooperative relay networks [4–7]. In the literature, many aspects of the relay networks have been investigated, including the relay selection scheme, network code design, and power allocation. However, one important issue about the physical layer security in the relay networks is still not being completely inspected, i.e., the masquerading attack.

In the relay networks, two typical issues of physical layer security are the selfishness and garbling [8, 9]. In the selfishness scenarios, the hypocritical relays may forward signals using minimum transmission power or, even worse, refuse to transmit any in-transit messages [10–12]. On the other hand, the in-transit messages may also be garbled [10, 13]. To unmask the hypocritical relays, some specific tracing symbols can be added to the informative messages [10, 13]; otherwise, the malicious detection can also be conducted blindly, based on the characteristics of hybrid automatic repeat request [11], the credit-based incentive transmission scheme [12], or the received signal's correlation [14].

In addition to the selfishness and garbling, we find that a certain nontypical but severely harmful misbehavior can also deprive the relay networks of cooperative diversity gain. It is well-known that a cooperative relay can be opportunistically selected to forward signals based on the distributed network path selection (DNPS) protocol [15]. In DNPS, each candidate relay can set a timer according to channel gain; and the best cooperative relay can then be distributedly decided once its timer expires earlier than the others. However, in this scenario, it is highly possible that a hypocritical relay can maliciously set a timer which can always expire earliest, even though it owns the worst channel gain. Although the signals are forwarded, the degree of freedom (DoF) as well as the cooperative diversity gain can be seriously weakened [16]. As a result, the advantage of deploying the hyperdense relay networks can be seriously diluted. To clearly indicate this problem, we pioneeringly coin masquerading attack to describe this kind of misbehavior.

To the best of our knowledge, the masquerading attack has not yet been fully investigated. Although its impact has been analyzed in [16], only single masquerade relay

was considered. Likewise, it neglected the complete channel effects; i.e., only the Rayleigh fading with different variances was included. In consequence, the geographical effects of the network topologies can not be completely characterized by the analytical results. Here, to capture the complete effects of fading environment, including the effects of flat Rayleigh fading, log-normal shadowing, and path loss, the composite exponential log-normal (CELN) distributed channel gain is considered [17]. Furthermore, multiple masquerade relays with random masquerading behavior are taken into account, i.e., the probability of a relay to become a masquerade relay and probability of a masquerade relay to become active. Then, the impact of the masquerading attack is evaluated in terms of the outage probability and end-to-end capacity. Note that part of this work has been presented in IEEE Wireless Communications and Networking Conference 2017 [18]. However, herein, some important related works are surveyed, and all the details of the mathematical derivations are provided. Furthermore, additional topologies of relay networks (as shown in Figures 2(b) and 5) are considered to investigate the influence of the masquerading attack on the device-to-device (D2D) and cellular networks.

The rest of this paper is organized as follows. In Section 2, the system model of the DNPS-based relay network is introduced. Also, the problem description is expounded therein. Section 3 mathematically describes the masquerading behaviors. Then, the outage probability and end-to-end capacity are derived in Section 4. Simulation results and conclusion remarks, including some suggestions for future works, are given in Sections 5 and 6, respectively.

2. System Model

Assume that N relays are deployed to assist the data transmissions between the source S and destination D. The decode-and-forward protocol is applied for relay-assisted transmissions. That is, during Phase I's transmission period, the i-th node R_i can be included into the decodable set $\mathscr{D}(S)$ when its normalized capacity C_i^I is larger than the predefined threshold C_{th} as

$$C_i^I = \log_2\left(1 + \left|h_{SR_i}\right|^2 \gamma_S\right) \geq C_{th}, \tag{1}$$

where $\gamma_S = P_S/N_0$ is the transmitting signal-to-noise ratio (SNR) at the source; P_S is the source's transmission power; N_0 is the power spectrum density of the additive white Gaussian noise; $|h_{SR_i}|$ is the channel gain of the link between S and R_i. To capture the complete effects of fading environment, including the effects of flat Rayleigh fading, log-normal shadowing and path loss, the CELN distributed channel gain are considered [17]. Thus, the probability density function (pdf) of $|h_{SR_i}|^2$ can be modeled by

$$f_i^I(\zeta) = \frac{\xi}{\sqrt{2\pi}\widehat{\sigma}\zeta}\exp\left[-\frac{\left(\xi\ln\zeta - \widehat{\mu}_i^I\right)^2}{2\widehat{\sigma}^2}\right], \quad \zeta > 0, \tag{2}$$

where $\widehat{\mu}_i^I = \mu_i^I - \xi\kappa$; $\widehat{\sigma} = \sqrt{\sigma + 5.57^2}$; and $\kappa \approx 0.577$ is Euler's constant; μ_i^I and σ are the mean and standard deviation (std.) of the log-normal shadowing in the dB domain during Phase I's transmission period; $\xi = 10/\ln 10$. Note that the mean of $|h_{SR_i}|^2$ is distance-dependent. Thus, a superscription is needed to distinguish μ_i^I and $\widehat{\mu}_i^I$ during Phase I from those during Phase II, i.e., μ_i^{II} and $\widehat{\mu}_i^{II}$. Specifically, the μ_i^{II} and $\widehat{\mu}_i^{II}$ are associated with $|h_{R_iD}|^2$, where h_{R_iD} stands for the channel gain of the link between R_i and D. Since only one hop is required for the transmissions via the direct link, no superscription is needed for μ_d and $\widehat{\mu}_d$ (which are associated with $|h_{SD}|^2$). Similarly, there is no superscription to distinguish $\widehat{\sigma}$ and σ during Phase I from those during Phase II because the same environment is assumed for both Phases I and II. Moreover, the cumulative distribution function (cdf) of the CELN distribution can be obtained by integrating (2) as follows:

$$F_i^I(\zeta) = \int_0^\zeta f_i^I(\eta)\, d\eta = Q\left(\frac{\widehat{\mu}_i^I - \xi\ln\zeta}{\widehat{\sigma}}\right). \tag{3}$$

During Phase II's transmission period, one of the candidate nodes in $\mathscr{D}(S)$ is selected to forward data packets to the destination D using the DNPS protocol [15] (will be briefly introduced in the latter). Finally, at the destination, the signal directly from S and that from the selected relay are combined according to the maximal ratio combining (MRC) rule, which gives the effective end-to-end capacity as

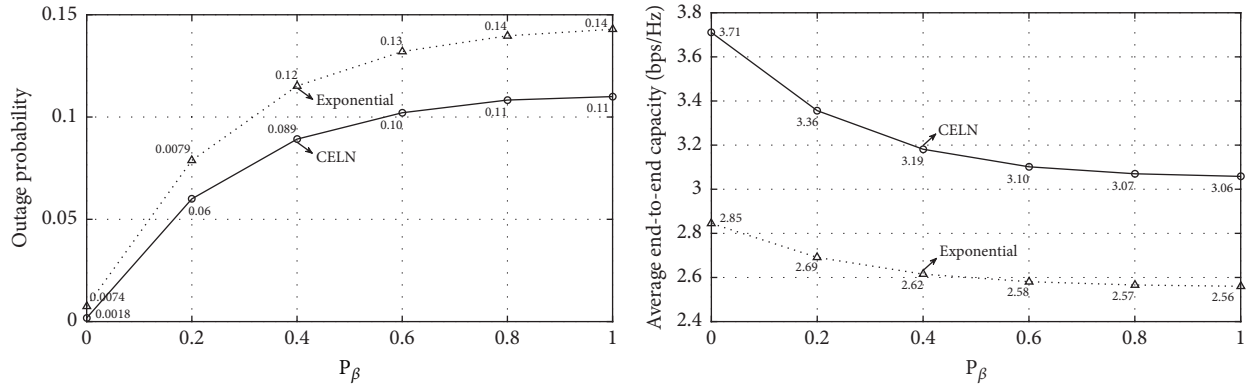
$$C_i^{II} = \frac{1}{2}\log_2\left(1 + \left|h_{SD}\right|^2\gamma_S + \left|h_{R_iD}\right|^2\gamma_R\right), \tag{4}$$

where $\gamma_R = P_R/N_0$ is the transmitting SNR at the relay; P_R is relay's transmission power; h_{SD} represents the channel gain of the direct link. Note that when $\mathscr{D}(S)$ is empty, only the signal received via the direct link, i.e., from S to D, is used for the demodulation process. In this case, the end-to-end capacity C_S can be expressed as

$$C_S = \log_2\left(1 + \left|h_{SD}\right|^2\gamma_S\right). \tag{5}$$

2.1. DNPS Relay Selection. Generally speaking, the DNPS protocol is an efficient distributed algorithm for relay selection. In the DNPS protocol, each candidate relay R_i belonging to $\mathscr{D}(S)$ sets a timer T_i whose expiry period is set inversely proportional to its channel gain of the link towards the destination D, i.e., $|h_{R_iD}|\ \forall i = 1, \ldots, N$. In other words, a relay with the largest channel gain in Phase II can expire earliest. Once a timer expires, the associated relay broadcasts a flag signal to inform the neighboring relays so that it can solely occupy the channel for delivering packets in Phase II. More details about the DNPS protocol can be found in [15].

2.2. Problem Description. To begin with, the "masquerader" and "nonmasquerader" are defined as the "masquerade" and "ordinary" relays, respectively. Now, it is assumed that the masqueraders attack the relay-assisted networks by mimicking virus' behavior so that it can be violent and untraceable. Specifically, it can be contagious; and the infected relays can be asymptomatic carrier or explicitly symptomatic. To well describe this kind of masquerading attack, P_α is



(a) Outage probability

(b) Average end-to-end capacity

FIGURE 1: (a) Outage probability and (b) average end-to-end capacity with respect to P_β for the infected relay-assisted cellular network under the exponential and CELN channel environments, where $P_\alpha = 0.5$. Also, $N = 9$ relays are fixed at middles of the sector as illustrated in Figure 5(a). Therein, the radius of the cell is $R_{cell} = 1000$ m, and the location of the mobile station (MS) is uniformly distributed over the sector's coverage area, while the minimum distance between the MS and base-station (BS) is 50 m. The transmission power of the source (i.e., the MS) P_S is set so that the thermal noise outage (O_N) at the destination (i.e., the BS) can be 0.2 as the MS is at the cell edge [19]. Similarly, the transmission power of each relay P_R is set so that $O_N = 0.2$ can be achieved at the BS. The required SNR corresponding to $O_N = 0.2$ is defined as 0 dB, whereas, for the purpose of evaluating the outage probability, the SNR threshold is set at 8 dB. The results are obtained by averaging over 200,000 simulation rounds.

defined as the probability for an ordinary relay to become a masquerader. Moreover, a masquerader can be active (i.e., explicitly symptomatic in other words) and attack with probability P_β. Note that this kind of masquerading attack was ignored in the conventional counterpart [16]. Moreover, solely the Rayleigh fading with different variances (i.e., the exponential channel model) was considered therein. Figure 1 demonstrates the performance degradation for the infected relay-assisted cellular network under the exponential and CELN channel environments. Apparently, the masquerading attack can cause serious performance degradation. Moreover, the performance differences between the cases under the exponential and CELN channel environments are significant. Thus, one can tell that it is necessary and important to investigate the impact of the random masquerading attack by taking the CELN environment into account. Note that the larger dynamic range of the channel gain incurred by log-normal shadowing results in the higher diversity gain, which explains the better performance for the CELN environment.

3. Analytical Characteristics of Masquerader

The impact of masquerading attack will be evaluated in terms of the outage probability and end-to-end capacity in Section 4. To this end, two scenarios of the decodable set $\mathscr{D}(S)$ are firstly analyzed in this section, i.e., at least one masquerader in $\mathscr{D}(S)$ and no masqueraders in the nonempty $\mathscr{D}(S)$.

3.1. At Least One Masquerader in $\mathscr{D}(S)$. In this scenario, the impact of the ordinary relays belonging to $\mathscr{D}(S)$ can be ignored. This is because once an active masquerader exists in the decodable set $\mathscr{D}(S)$, the ordinary relays can never be selected to forward packets during Phase II. To facilitate the presentation, some terminologies are defined as follows.

(1) $\mathbf{M}(n)$: the relay set which includes all possible combinations (subsets in other words) of n masqueraders, where $1 \le n \le N$. Specifically, that means n out of the N relays belonging to $\mathbf{N}$ become masqueraders. Therefore, in this case, there are $\binom{N}{n}$ subsets in $\mathbf{M}(n)$, which are denoted by $\mathbf{M}(n,i)$ $\forall i = 1, \ldots, \binom{N}{n}$.

(2) $\mathbf{M}_d(m)$: under the condition of n masqueraders, this relay set includes all possible combinations of m decodable masqueraders, where $1 \le m \le n \le N$. In other words, m out of the n masqueraders belonging to $\mathbf{M}(n,i)$ are decodable. Therefore, given $\mathbf{M}(n,i)$, there are $\binom{n}{m}$ subsets in $\mathbf{M}_d(m)$, which are denoted by $\mathbf{M}_d(m,j) \subseteq \mathbf{M}(n,i)$, $\forall j = 1, \ldots, \binom{n}{m}$.

(3) $\mathbf{M}_a(\ell)$: under the conditions of n masqueraders and m decodable masqueraders, this relay set includes all possible combinations of ℓ active-and-decodable masqueraders, where $1 \le \ell \le m \le n \le N$. That means ℓ out of the m masqueraders belonging to $\mathbf{M}_d(m,j)$ are decodable. In this case, there are $\binom{m}{\ell}$ subsets in $\mathbf{M}_a(\ell)$, which are denoted by $\mathbf{M}_a(\ell,k) \subseteq \mathbf{M}_d(m,j) \subseteq \mathbf{M}(n,i), \forall k = 1, \ldots, \binom{m}{\ell}$.

Consider a masquerader being selected from a particular subset $\mathbf{M}_a(\ell,k)$. Since $\mathbf{M}_a(\ell,k) \subseteq \mathbf{M}_d(m,j) \subseteq \mathbf{M}(n,i)$, the joint probability for this case can be expressed as (6).

$$\begin{aligned} &P\left[\mathbf{M}_a(\ell,k), \mathbf{M}_d(m,j), \mathbf{M}(n,i)\right] \\ &\quad = P\left[\mathbf{M}_a(\ell,k) \mid \mathbf{M}_d(m,j), \mathbf{M}(n,i)\right] \\ &\quad \cdot P\left[\mathbf{M}_d(m,j) \mid \mathbf{M}(n,i)\right] P\left[\mathbf{M}(n,i)\right] \end{aligned} \tag{6}$$

Apparently, we can have

$$P\left[\mathbf{M}\left(n,i\right)\right]=\left(P_{\alpha}\right)^{n}\left(1-P_{\alpha}\right)^{N-n}. \tag{7}$$

Also, the conditional probability $P[\mathbf{M}_d(m,j) \mid \mathbf{M}(n,i)]$ can be expressed as

$$\begin{aligned}&P\left[\mathbf{M}_{d}\left(m,j\right)\mid\mathbf{M}\left(n,i\right)\right]\\&=\prod_{k\in\mathbf{M}_{d}(m,j)}^{m}P\left[C_{k}^{I}>C_{th}\right]\\&\times\prod_{k\in(\mathbf{M}(n,i)/\mathbf{M}_{d}(m,j))}^{n-m}P\left[C_{k}^{I}\leq C_{th}\right],\end{aligned} \tag{8}$$

where $\mathbf{A}/\mathbf{B}$ is the set-operator to remove set $\mathbf{B}$ from set $\mathbf{A}$;

$$\begin{aligned}P\left[C_{k}^{I}\leq C_{th}\right]&=P\left[\left|h_{SR_{k}}\right|^{2}<\frac{2^{C_{th}}-1}{\gamma_{S}}\right]\\&=Q\left(\frac{\widehat{\mu}_{k}^{I}-\xi\ln\lambda_{th}}{\widehat{\sigma}}\right),\end{aligned} \tag{9}$$

where $\lambda_{th}=(2^{C_{th}}-1)/\gamma_S$. Since

$$Q\left(\frac{\xi\ \ln\lambda_{th}-\widehat{\mu}_{k}^{I}}{\widehat{\sigma}}\right)+Q\left(\frac{\widehat{\mu}_{k}^{I}-\xi\ln\lambda_{th}}{\widehat{\sigma}}\right)=1, \tag{10}$$

we can have

$$P\left[C_{k}^{I}>C_{th}\right]=Q\left(\frac{\xi\ln\lambda_{th}-\widehat{\mu}_{k}^{I}}{\widehat{\sigma}}\right). \tag{11}$$

Moreover, it is intuitional to obtain

$$\begin{aligned}&P\left[\mathbf{M}_{a}\left(\ell,k\right)\mid\mathbf{M}_{d}\left(m,j\right),\mathbf{M}\left(n,i\right)\right]\\&=\left(P_{\beta}\right)^{\ell}\left(1-P_{\beta}\right)^{(m-\ell)}.\end{aligned} \tag{12}$$

At last, multiplying (7), (8), and (12) gives (6). It should be noticed that, with $\ell \geq 2$, the following performance metric (i.e., the outage probability and capacity in Section 4) should be averaged over the ℓ cases. This is because each of the ℓ masquerade relays individually sets a timer such that it can expire earliest. Then, the relay selection in Phase II becomes a random selection approach, which means each of them can be selected with probability $1/\ell$.

3.2. No Active Masqueraders in the Nonempty $\mathscr{D}(S)$. As implied by the name, this scenario means that all the relays belonging to $\mathscr{D}(S)$ are ordinary ones. Thus, it includes three cases, i.e., (1) Case $\mathscr{A}$: no relays become the masqueraders; (2) Case $\mathscr{B}$: no masqueraders are decodable; and (3) Case $\mathscr{C}$: no decodable masqueraders are active. Some terminologies are defined as follows:

(1) $\mathbf{O}(n)$: the relay set includes all possible combinations of n nonmasqueraders, where $1 \leq n \leq N$. Thus, there are $\binom{N}{n}$ subsets in $\mathbf{O}(n)$, which are denoted by $\mathbf{O}(n,i)\ \forall i=1,\ldots,\binom{N}{n}$.

(2) $\mathbf{O}_d(m)$: under the condition of n nonmasqueraders, this relay set includes all possible combinations of m decodable nonmasqueraders, where $1 \leq m \leq n \leq N$. That means given $\mathbf{O}(n)$, there are $\binom{n}{m}$ subsets in $\mathbf{O}_d(m)$, which are denoted by $\mathbf{O}_d(m,i)\ \forall i=1,\ldots,\binom{n}{m}$.

(3) $\overline{\mathbf{M}}_d(n,i)$: the relay set consists of the same masqueraders as $\mathbf{M}(n,i)$. However, all of the n masqueraders are nondecodable. By definition, we can have $\overline{\mathbf{M}}_d(n)=\overline{\mathbf{M}}_d(n,1)\cup\overline{\mathbf{M}}_d(n,2)\cdots\cup\overline{\mathbf{M}}_d(n,\binom{N}{n})$.

(4) $\overline{\mathbf{M}}_a(m,j)$: the relay set consists of the same masqueraders as $\mathbf{M}_d(m,j)$. However, all the m decodable masqueraders are inactive. Given $\mathbf{M}_d(n,i)$, we can have $\overline{\mathbf{M}}_a(m)=\overline{\mathbf{M}}_a(m,1)\cup\overline{\mathbf{M}}_a(m,2)\cdots\cup\overline{\mathbf{M}}_a(m,\binom{n}{m})$.

(1) Case $\mathscr{A}$: No Relays Become the Masqueraders. Firstly, all the relays are well-behaved with probability

$$P\left[\mathbf{O}\left(N\right)\right]=\left(1-P_{\alpha}\right)^{N}; \tag{13}$$

and the conditional probability $P[\mathbf{O}_d(n,i) \mid \mathbf{O}(N)]$ can be obtained by replacing $\mathbf{M}_d(m,j)$, $\mathbf{M}(n,i)$, n, and m in (8) with $\mathbf{O}_d(n,i)$, $\mathbf{O}(N)$, N, and n, respectively.

(2) Case $\mathscr{B}$: No Masqueraders Are Decodable. Consider that $\overline{\mathbf{M}}_d(n,i)$ occurs on a given condition of $\mathbf{M}(n,i)$. The conditional probability $P[\overline{\mathbf{M}}_d(n,i) \mid \mathbf{M}(n,i)]$ can be written as

$$\begin{aligned}P\left[\overline{\mathbf{M}}_{d}\left(n,i\right)\mid\mathbf{M}\left(n,i\right)\right]&=\prod_{k\in\overline{\mathbf{M}}_{d}(n,i)}^{n}Q\left(\frac{\widehat{\mu}_{k}^{I}-\xi\ln\lambda_{th}}{\widehat{\sigma}}\right)\\&=\prod_{k\in\mathbf{M}(n,i)}^{n}Q\left(\frac{\widehat{\mu}_{k}^{I}-\xi\ln\lambda_{th}}{\widehat{\sigma}}\right).\end{aligned} \tag{14}$$

Assume that m out of the rest $N-n$ nonmasqueraders belonging to $\mathbf{N}/\overline{\mathbf{M}}_d(n,i)$ are decodable. Let $\mathbf{O}_d(m,j)$ represent these m decodable nonmasqueraders. Then, replacing $\mathbf{M}_d(m,j)$, $\mathbf{M}(n,i)$, and n in (8) with $\mathbf{O}_d(m,j)$, $\mathbf{N}/\overline{\mathbf{M}}_d(n,i)$, and $N-n$ gives $P[\mathbf{O}_d(m,j) \mid \overline{\mathbf{M}}_d(n,i),\mathbf{M}(n,i)]$.

(3) Case $\mathscr{C}$: No Decodable Masqueraders Are Active. Consider that $\overline{\mathbf{M}}_a(m,j)$ occurs on the given conditions of $\mathbf{M}_d(m,j)$ and $\mathbf{M}(n,i)$. Then, it leads to the conditional probability as

$$P\left[\overline{\mathbf{M}}_{a}\left(m,j\right)\mid\mathbf{M}_{d}\left(m,j\right),\mathbf{M}\left(n,i\right)\right]=\left(1-P_{\beta}\right)^{m}. \tag{15}$$

Assume that ℓ out of the remaining $N-n$ nonmasqueraders belonging to $\mathbf{N}/\mathbf{M}(n,i)$ are decodable. Let $\mathbf{O}_d(\ell,k)$ represent these ℓ decodable nonmasqueraders; and then we can have the conditional probability $P[\mathbf{O}_d(\ell,k) \mid \overline{\mathbf{M}}_a(m,j),\mathbf{M}_d(m,j),\mathbf{M}(n,i)]$ by replacing $\mathbf{M}_d(m,j)$, $\mathbf{M}(n,i)$, n, and m in (8) with $\mathbf{O}_d(\ell,k)$, $\mathbf{N}/\mathbf{M}(n,i)$, $N-n$, and ℓ, respectively.

4. Performance Analysis

Let the z-th relay be selected to forward packets during Phase II. Therefore, z must belong to a particular subset of $\mathbf{M}_a(\ell)$ or

$\mathbf{O}_d(n)$, e.g., the aforementioned $\mathbf{M}_a(\ell,k)$, $\mathbf{O}_d(n,i)$, $\mathbf{O}_d(m,j)$, or $\mathbf{O}_d(\ell,k)$ in Section 3. To ease the presentation, let $x = |h_{R_zD}|^2$; and then μ_x stands for the mean of x in the dB domain, which leads to $\widehat{\mu}_x = \mu_x - \xi\kappa$. Moreover, $F_X(x)$ and $f_X(x)$ represent the *cdf* and *pdf* of x, respectively. Similarly, let $y = |h_{SD}|^2$; and, in consequence, we can have μ_y to represent the mean of y in the dB domain, which leads to $\widehat{\mu}_y = \mu_y - \xi\kappa$. Likewise, $F_Y(y)$ and $f_Y(y)$ stand for the *cdf* and *pdf* of y.

Denote $P_{out}(M)$ and $P_{out}(O)$ as the outage probability for the cases of z belonging to a subset of $\mathbf{M}_a(\ell)$ or $\mathbf{O}_d(n)$, respectively, while $P_{out}(\emptyset)$ denotes that with an empty decodable set $\mathscr{D}(S)$. Also, let $C_{end}(M)$, $C_{end}(O)$, and $C_{end}(\emptyset)$ represent the corresponding average end-to-end capacity. Since $P_{out}(M)$, $P_{out}(O)$, and $P_{out}(\emptyset)$ are mutually exclusive, the overall outage probability can be expressed as

$$P_{out} = P_{out}(M) + P_{out}(O) + P_{out}(\emptyset). \tag{16}$$

Similarly, we can have

$$C_{end} = C_{end}(M) + C_{end}(O) + C_{end}(\emptyset). \tag{17}$$

In the following, we derive the mathematical expressions of $P_{out}(M)$, $P_{out}(O)$, and $P_{out}(\emptyset)$. The closed form expressions of $C_{end}(M)$, $C_{end}(O)$, and $C_{end}(\emptyset)$ will be derived as well.

4.1. At Least One Masquerader in $\mathscr{D}(S)$. To facilitate the presentation, denote $P_M(z \mid \ell,m,n,k,j,i)$ as the probability of the selected z-th relay belonging to the subset $\mathbf{M}_a(\ell,k)$. Then, it gives

$$\begin{aligned} &P_M(z \mid \ell,m,n,k,j,i) \\ &\quad = P\left[\mathbf{M}_a(\ell,k), \mathbf{M}_d(m,j), \mathbf{M}(n,i)\right]. \end{aligned} \tag{18}$$

Let $P_{\text{out}}(M \mid z)$ and $C_{end}(M \mid z)$ represent the conditional outage probability and end-to-end capacity. Given ℓ, m, and n, it follows that

$$\begin{aligned} &P_{out}(M \mid \ell,m,n) \\ &\quad = \sum_{i=1}^{\binom{N}{n}} \sum_{j=1}^{\binom{n}{m}} \sum_{k=1}^{\binom{m}{\ell}} P_{out}(M \mid z) P_M(z \mid \ell,m,n,k,j,i) \end{aligned} \tag{19}$$

and

$$\begin{aligned} &C_{end}(M \mid \ell,m,n) \\ &\quad = \sum_{i=1}^{\binom{N}{n}} \sum_{j=1}^{\binom{n}{m}} \sum_{k=1}^{\binom{m}{\ell}} C_{end}(M \mid z) P_M(z \mid \ell,m,n,k,j,i), \end{aligned} \tag{20}$$

respectively. Finally, the overall outage probability and end-to-end capacity for the case with at least one masquerader in $\mathscr{D}(S)$ can be expressed as

$$P_{out}(M) = \sum_{n=1}^{N} \sum_{m=1}^{n} \sum_{\ell=1}^{m} P_{out}(M \mid \ell,m,n) \tag{21}$$

and

$$C_{end}(M) = \sum_{n=1}^{N} \sum_{m=1}^{n} \sum_{\ell=1}^{m} C_{end}(M \mid \ell,m,n). \tag{22}$$

$P_{out}(M \mid z)$ and $C_{end}(M \mid z)$ are derived as follows.

(1) . Recall that there are ℓ active-and-decodable masqueraders in the subset $\mathbf{M}_a(\ell,k), \forall k = 1,\ldots,\binom{m}{\ell}$. When $\ell > 1$, one of the ℓ active-and-decodable masqueraders is randomly selected to forward packets during Phase II's transmission period. Thus, the conditional outage probability should be averaged over these ℓ cases. Then, $P_{out}(M \mid z)$ can be expressed as

$$\begin{aligned} P_{out}(M \mid z) &= \frac{1}{\ell} \sum_{z \in \mathbf{M}_a(\ell,k)} P\left[C_z^{II} < C_{th}\right] \\ &= \frac{1}{\ell} \sum_{z \in \mathbf{M}_a(\ell,k)} P\left[\frac{1}{2}\log_2(1 + y\gamma_S + x\gamma_R) < C_{th}\right] \\ &= \frac{1}{\ell} \sum_{z \in \mathbf{M}_a(\ell,k)} P\left[(x\gamma_R + y\gamma_S) < \lambda'_{th}\right] \\ &= \frac{1}{\ell} \sum_{z \in \mathbf{M}_a(\ell,k)} P\left[x < \frac{\lambda'_{th} - y\gamma_S}{\gamma_R}\right], \end{aligned} \tag{23}$$

where $\lambda'_{th} = 2^{2C_{th}} - 1$. Substituting (2) and (3) into (23) gives

$$P_{out}(M \mid z) = \frac{1}{\ell} \sum_{z \in \mathbf{M}_a(\ell,k)} \int_0^{\lambda'_{th}/\gamma_S} F_X\left(\frac{\lambda'_{th} - y\gamma_S}{\gamma_R}\right) f_Y(y)\, dy \tag{24}$$

$$\begin{aligned} P_{out}(M \mid z) = \frac{1}{\ell} &\cdot \sum_{z \in \mathbf{M}_a(\ell,k)} \int_0^{\lambda'_{th}/\gamma_S} \int_0^{(\lambda'_{th} - y\gamma_S)/\gamma_R} \frac{\xi}{\sqrt{2\pi}\widehat{\sigma}x} \exp\left(-\frac{(\xi \ln x - \widehat{\mu}_x)^2}{2\widehat{\sigma}^2}\right) \\ &\cdot \frac{\xi}{\sqrt{2\pi}\widehat{\sigma}y} \exp\left(-\frac{(\xi \ln y - \widehat{\mu}_y)^2}{2\widehat{\sigma}^2}\right) dx\, dy \end{aligned} \tag{25}$$

Let $u = (\xi \ln x - \widehat{\mu}_x)/\widehat{\sigma}$ and $v = (\xi \ln y - \widehat{\mu}_y)/\widehat{\sigma}$. Then, (25) can be rewritten as

$$\begin{aligned} P_{out}(M \mid z) = \frac{1}{\ell} &\cdot \sum_{z \in \mathbf{M}_a(\ell,k)} \int_{-\infty}^{(\xi \ln(\lambda'_{th}/\gamma_S) - \widehat{\mu}_y)/\widehat{\sigma}} \int_{-\infty}^{(\xi \ln y' - \widehat{\mu}_x)/\widehat{\sigma}} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{u^2}{2}\right) \frac{1}{\sqrt{2\pi}} \\ &\cdot \exp\left(-\frac{v^2}{2}\right) du\, dv \end{aligned} \tag{26}$$

where

$$y' = \left(\frac{\lambda'_{th} - \gamma_S \exp\left(\left(v\widehat{\sigma} + \widehat{\mu}_y\right)/\xi\right)}{\gamma_R}\right). \tag{27}$$

Since there is no closed form expression for (26), it can only be reduced to

$$P_{out}(M \mid z) = \frac{1}{\ell} \cdot \sum_{z \in \mathbf{M}_a(\ell,k)} \int_{-\infty}^{(\xi \ln(\lambda'_{th}/\gamma_S) - \widehat{\mu}_y)/\widehat{\sigma}} Q\left(\frac{\widehat{\mu}_x - \xi \ln y'}{\widehat{\sigma}}\right) \frac{1}{\sqrt{2\pi}} \cdot \exp\left(-\frac{v^2}{2}\right) dv. \quad (28)$$

(2) . Similar to (23), $C_{end}(M \mid z)$ can be expressed as

$$C_{end}(M \mid z) = \frac{1}{\ell} \sum_{z \in \mathbf{M}_a(\ell,k)} E\left[\frac{1}{2}\log_2\left(1 + x\gamma_R + y\gamma_S\right)\right], \quad (29)$$

where $E[\cdot]$ is the operator to take expectation. Substituting (2) into (29) renders (30).

$$C_{end}(M \mid z) = \frac{1}{\ell} \cdot \sum_{z \in \mathbf{M}_a(\ell,k)} \int_0^{\infty} \int_0^{\infty} \frac{1}{2}\log_2\left(1 + x\gamma_R + y\gamma_S\right) \cdot \frac{\xi}{\sqrt{2\pi}\widehat{\sigma}x} \exp\left(-\frac{(\xi \ln x - \widehat{\mu}_x)^2}{2\widehat{\sigma}^2}\right) \times \frac{\xi}{\sqrt{2\pi}\widehat{\sigma}y} \exp\left(-\frac{(\xi \ln y - \widehat{\mu}_y)^2}{2\widehat{\sigma}^2}\right) dx\, dy \quad (30)$$

Let $u = (\xi \ln x - \widehat{\mu}_x)/(\sqrt{2}\widehat{\sigma})$ and $v = (\xi \ln y - \widehat{\mu}_y)/(\sqrt{2}\widehat{\sigma})$ which leads to

$$C_{end}(M \mid z) = \frac{1}{\ell} \sum_{z \in \mathbf{M}_a(\ell,k)} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \frac{1}{2}\log_2\left[1 + \gamma_R \exp\left(\frac{\sqrt{2}\widehat{\sigma}u + \widehat{\mu}_x}{\xi}\right) + \gamma_S \exp\left(\frac{\sqrt{2}\widehat{\sigma}v + \widehat{\mu}_y}{\xi}\right)\right] \times \frac{1}{\pi} e^{-v^2} e^{-u^2} du\, dv. \quad (31)$$

It is known that the Hermite polynomial approach can be applied to calculate the following integration:

$$\int_{-\infty}^{\infty} f(x)\, e^{-x^2} dx = \sum_{\eta=1}^{N_H} \omega_\eta f\left(t_\eta\right), \quad (32)$$

where t_η and ω_η are the abscissas and the weight factor of the Hermite polynomials with order N_H, respectively [20]. Applying (32) into (31) renders

$$C_{end}(M \mid z) \cong \frac{1}{\ell} \sum_{z \in \mathbf{M}_a(\ell,k)} \sum_{\eta=1}^{N_H} \sum_{\kappa=1}^{N_H} \frac{\omega_\eta \omega_\kappa}{2} \log_2\left[1 + \gamma_R \exp\left(\frac{\sqrt{2}\widehat{\sigma}t_\eta + \widehat{\mu}_x}{\xi}\right) + \gamma_S \exp\left(\frac{\sqrt{2}\widehat{\sigma}t_\kappa + \widehat{\mu}_y}{\xi}\right)\right]. \quad (33)$$

4.2. No Active Masqueraders in the Nonempty $\mathscr{D}(S)$. According to Section 3.2, three cases should be considered in this scenario; i.e., the z-th relay is selected from $\mathbf{O}_d(n,i)$, $\mathbf{O}_d(m,j)$, or $\mathbf{O}_d(\ell,k)$. Similar to Section 4.1, let $P_{out}^{\mathscr{A}}(O)$, $P_{out}^{\mathscr{B}}(O)$, and $P_{out}^{\mathscr{C}}(O)$ denote the outage probability for these cases. Also, $C_{end}^{\mathscr{A}}$, $C_{end}^{\mathscr{B}}$, and $C_{end}^{\mathscr{C}}$ are the corresponding end-to-end capacity, respectively. Then, we can have

$$P_{out}(O) = P_{out}^{\mathscr{A}}(O) + P_{out}^{\mathscr{B}}(O) + P_{out}^{\mathscr{C}}(O) \quad (34)$$

and

$$C_{end}(O) = C_{end}^{\mathscr{A}}(O) + C_{end}^{\mathscr{B}}(O) + C_{end}^{\mathscr{C}}(O). \quad (35)$$

(1) Case $\mathscr{A}$: No Relays Become the Masqueraders. Denote $P_{out}^{\mathscr{A}}(O \mid z)$ and $C_{end}^{\mathscr{A}}(O \mid z)$ the outage probability and end-to-end capacity when the z-th relay is selected from $\mathbf{O}_d(n,i)$ under the condition of $\mathbf{O}(N)$. Similar to the procedures of deriving (21) and (22), the average outage probability and end-to-end capacity can be expressed as

$$P_{out}^{\mathscr{A}}(O) = \sum_{n=1}^{N} \sum_{i=1}^{\binom{N}{n}} P_{out}^{\mathscr{A}}(O \mid z)\, P\left[\mathbf{O}_d(n,i) \mid \mathbf{O}(N)\right] P\left[\mathbf{O}(N)\right] \quad (36)$$

and

$$C_{end}^{\mathscr{A}}(O) = \sum_{n=1}^{N} \sum_{i=1}^{\binom{N}{n}} C_{end}^{\mathscr{A}}(O \mid z)\, P\left[\mathbf{O}_d(n,i) \mid \mathbf{O}(N)\right] \cdot P\left[\mathbf{O}(N)\right], \quad (37)$$

respectively.

(a) . Regardless of which relay is selected from $\mathbf{O}_d(n,i)$ in Phase II, an outage event can occur when the end-to-end capacity of all the relays belonging to $\mathbf{O}_d(n,i)$ is below the target value, i.e., $C_z^{II} < C_{th}\ \forall z \in \mathbf{O}_d(n,i)$. Let $\widehat{F}_X(\zeta)$ denote the cdf of this case. Referring to (3), the outage probability with a given y can be written as

$$\widehat{F}_X\left(\frac{\lambda'_{th} - y\gamma_S}{\gamma_R}\right) = \prod_{z \in \mathbf{O}_d(n,i)} Q\left(\frac{\widehat{\mu}_x - \xi \ln\left(\left(\lambda'_{th} - y\gamma_S\right)/\gamma_R\right)}{\widehat{\sigma}}\right). \quad (38)$$

Then, similar to (24), the outage probability in this case can be expressed as

$$P_{out}^{\mathscr{A}}(O \mid z) = \int_0^{\lambda'_{th}/\gamma_S} \widehat{F}_X\left(\frac{\lambda'_{th} - y\gamma_S}{\gamma_R}\right) f_Y(y)\, dy$$
$$= \int_0^{\lambda'_{th}/\gamma_S} \prod_{z \in \mathbf{O}_d(n,i)} Q\left(\frac{\widehat{\mu}_x - \xi \ln\left(\left(\lambda'_{th} - y\gamma_S\right)/\gamma_R\right)}{\widehat{\sigma}}\right) \cdot f_Y(y)\, dy \quad (39)$$

Applying the same procedures of deriving (28) gives

$$P_{out}^{\mathscr{A}}(O \mid z) = \int_{-\infty}^{(\xi \ln(\lambda'_{th}/\gamma_S) - \widehat{\mu}_y)/\widehat{\sigma}} \prod_{z \in \mathbf{O}_d(n,i)} Q\left(\frac{\widehat{\mu}_x - \xi \ln y'}{\widehat{\sigma}}\right) \cdot \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{v^2}{2}\right) dv, \quad (40)$$

where y' is the same as that in (27).

(b) . In this case, the end-to-end capacity can be written as

$$C_{end}^{\mathscr{A}}(O \mid z) = \int_0^{\infty} \int_0^{\infty} \frac{1}{2}\log_2\left(1 + x\gamma_R + y\gamma_S\right) \times f_Y(y)\, \widehat{f}_X(x)\, dx\, dy, \quad (41)$$

where $\widehat{f}_X(\zeta)$ represents the corresponding *pdf* of (38). Taking derivation of (38) gives

$$\widehat{f}_X(\zeta) = \sum_{z \in \mathbf{O}_d(n,i)} \frac{\xi}{\sqrt{2\pi}\widehat{\sigma}\zeta} \exp\left(-\frac{\left(\xi \ln \zeta - \widehat{\mu}_x\right)^2}{2\widehat{\sigma}^2}\right) \times \prod_{z' \in \mathbf{O}_d(n,i), z' \neq z} Q\left(\frac{\widehat{\mu}_{x'} - \xi \ln \zeta}{\widehat{\sigma}}\right), \quad (42)$$

where $\mu_{x'}$ associated with the z'-th relay in $\mathbf{O}_d(n,i)$ is similar to μ_x associated with the z-th relay in $\mathbf{O}_d(n,i)$. Then, the average end-to-end capacity can be expressed as

$$C_{end}^{\mathscr{A}}(O \mid z) = \sum_{z \in \mathbf{O}_d(n,i)} \int_0^{\infty} \int_0^{\infty} \frac{1}{2}\log_2\left(1 + x\gamma_R + y\gamma_S\right) \cdot \frac{\xi}{\sqrt{2\pi}\widehat{\sigma}x} \exp\left(-\frac{\left(\xi \ln x - \widehat{\mu}_x\right)^2}{2\widehat{\sigma}^2}\right) \cdot \prod_{z' \in \mathbf{O}_d(n,i), z' \neq z} Q\left(\frac{\widehat{\mu}_{x'} - \xi \ln x}{\widehat{\sigma}}\right) \times \frac{\xi}{\sqrt{2\pi}\widehat{\sigma}y} \exp\left(-\frac{\left(\xi \ln y - \widehat{\mu}_y\right)^2}{2\widehat{\sigma}^2}\right) dx\, dy \quad (43)$$

Letting $u = (\xi \ln x - \widehat{\mu}_x)/(\sqrt{2}\widehat{\sigma})$ and $v = (\xi \ln y - \widehat{\mu}_y)/(\sqrt{2}\widehat{\sigma})$ gives

$$C_{end}^{\mathscr{A}}(O \mid z) = \sum_{z \in \mathbf{O}_d(n,i)} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \frac{1}{2}\log_2\left[1 + \gamma_R \exp\left(\frac{\sqrt{2}\widehat{\sigma}u + \widehat{\mu}_x}{\xi}\right) + \gamma_S \exp\left(\frac{\sqrt{2}\widehat{\sigma}v + \widehat{\mu}_y}{\xi}\right)\right] \times \prod_{z' \in \mathbf{O}_d(n,i), z' \neq z} Q\left(\frac{\widehat{\mu}_{x'} - \widehat{\mu}_x - u\sqrt{2}\widehat{\sigma}}{\widehat{\sigma}}\right) \frac{1}{\pi} e^{-v^2} e^{-u^2}\, du\, dv \quad (44)$$

Applying the Hermite polynomial approach into (44) renders

$$C_{end}^{\mathscr{A}}(O \mid z) \cong \sum_{\eta=1}^{N_H} \sum_{\kappa=1}^{N_H} \sum_{z \in \mathbf{O}_d(n,i)} \frac{\omega_\eta \omega_\kappa}{2} \log_2\left[1 + \gamma_R \exp\left(\frac{\sqrt{2}\widehat{\sigma}t_\eta + \widehat{\mu}_x}{\xi}\right) + \gamma_S \exp\left(\frac{\sqrt{2}\widehat{\sigma}t_\kappa + \widehat{\mu}_y}{\xi}\right)\right] \times \prod_{z' \in \mathbf{O}_d(n,i), z' \neq z} Q\left(\frac{\widehat{\mu}_{x'} - \widehat{\mu}_x - t_\eta\sqrt{2}\widehat{\sigma}}{\widehat{\sigma}}\right). \quad (45)$$

(2) Case $\mathscr{B}$: No Masqueraders Are Decodable. Denote by $P_{out}^{\mathscr{B}}(O \mid z)$ and $C_{end}^{\mathscr{B}}(O \mid z)$ the conditional outage probability and end-to-end capacity when the z-th relay is selected from $\mathbf{O}_d(m, j)$ under the conditions of $\overline{\mathbf{M}}_d(n,i)$ and $\mathbf{M}(n,i)$. Then, the outage probability and end-to-end capacity can be expressed as (46) and (47), respectively.

$$P_{out}^{\mathscr{B}}(O) = \sum_{n=1}^{N} \binom{N}{n} \sum_{i=1}^{N-n} \sum_{m=1}^{\binom{N-n}{m}} \sum_{j=1} P_{out}^{\mathscr{B}}(O \mid z)\, P\left[\mathbf{O}_d(m,j) \mid \overline{\mathbf{M}}_d(n,i), \mathbf{M}(n,i)\right] P\left[\overline{\mathbf{M}}_d(n,i) \mid \mathbf{M}(n,i)\right] P\left[\mathbf{M}(n,i)\right]. \tag{46}$$

$$C_{end}^{\mathscr{B}}(O) = \sum_{n=1}^{N} \binom{N}{n} \sum_{i=1}^{N-n} \sum_{m=1}^{\binom{N-n}{m}} \sum_{j=1} C_{end}^{\mathscr{B}}(O \mid z)\, P\left[\mathbf{O}_d(m,j) \mid \overline{\mathbf{M}}_d(n,i), \mathbf{M}(n,i)\right] P\left[\overline{\mathbf{M}}_d(n,i) \mid \mathbf{M}(n,i)\right] P\left[\mathbf{M}(n,i)\right]. \tag{47}$$

Applying the same procedures as mentioned in Case $\mathscr{A}$ by replacing $\mathbf{O}_d(n,i)$ in (40) and (45) with $\mathbf{O}_d(m,j)$ gives the conditional outage probability $P_{out}^{\mathscr{B}}(O \mid z)$ and end-to-end capacity $C_{end}^{\mathscr{B}}(O \mid z)$ for this case.

(3) Case $\mathscr{C}$: No Decodable Masqueraders Are Active. Similar to Cases $\mathscr{A}$ and $\mathscr{B}$, let $P_{out}^{\mathscr{C}}(O \mid z)$ and $C_{end}^{\mathscr{C}}(O \mid z)$ represent the conditional outage probability and end-to-end capacity when the z-th relay is selected from $\mathbf{O}_d(\ell,k)$ under the conditions of $\overline{\mathbf{M}}_a(m,j)$, $\mathbf{M}_d(m,j)$, and $\mathbf{M}(n,i)$. Moreover, the outage probability and end-to-end capacity can be expressed as (48) and (49), respectively.

$$\begin{aligned} P_{out}^{\mathscr{C}}(O) = \sum_{n=1}^{N} \sum_{m=1}^{n} \sum_{\ell=1}^{N-n} \binom{N}{n} \binom{n}{m} \binom{N-n}{\ell} \sum_{k=1} P_{out}^{\mathscr{C}}(O \mid z)\, P\left[\mathbf{O}_d(\ell,k) \mid \overline{\mathbf{M}}_a(m,j), \mathbf{M}_d(m,j), \mathbf{M}(n,i)\right] \\ \times P\left[\overline{\mathbf{M}}_a(m,j) \mid \mathbf{M}_d(m,j), \mathbf{M}(n,i)\right] P\left[\mathbf{M}_d(m,j) \mid \mathbf{M}(n,i)\right] P\left[\mathbf{M}(n,i)\right]. \end{aligned} \tag{48}$$

$$\begin{aligned} C_{end}^{\mathscr{C}}(O) = \sum_{n=1}^{N} \sum_{m=1}^{n} \sum_{\ell=1}^{N-n} \binom{N}{n} \binom{n}{m} \binom{N-n}{\ell} \sum_{k=1} C_{end}^{\mathscr{C}}(O \mid z)\, P\left[\mathbf{O}_d(\ell,k) \mid \overline{\mathbf{M}}_a(m,j), \mathbf{M}_d(m,j), \mathbf{M}(n,i)\right] \\ \times P\left[\overline{\mathbf{M}}_a(m,j) \mid \mathbf{M}_d(m,j), \mathbf{M}(n,i)\right] P\left[\mathbf{M}_d(m,j) \mid \mathbf{M}(n,i)\right] P\left[\mathbf{M}(n,i)\right]. \end{aligned} \tag{49}$$

At last, replacing $\mathbf{O}_d(n,i)$ in (40) and (45) with $\mathbf{O}_d(\ell,k)$ gives $P_{out}^{\mathscr{C}}(O \mid z)$ and $C_{end}^{\mathscr{C}}(O \mid z)$.

4.3. Empty Decodable Set $\mathscr{D}(S)$. Denote by $\mathscr{D}(S) = \emptyset$ the empty decodable set. Then, we can have the occurring probability for this case as

$$P\left[\mathscr{D}(S) = \emptyset\right] = \prod_{\eta \in \mathbf{N}} Q\left(\frac{\widehat{\mu}_{\eta}^{II} - \xi \ln \lambda_{th}}{\widehat{\sigma}}\right). \tag{50}$$

(1) . With $\mathscr{D}(S) = \emptyset$, the outage probability can be expressed as

$$P_{out}(\emptyset) = P\left[C_S < C_{th} \mid \mathscr{D}(S) = \emptyset\right] P\left[\mathscr{D}(S) = \emptyset\right], \tag{51}$$

where $P[C_S < C_{th} \mid \mathscr{D}(S) = \emptyset]$ can also be derived as

$$\begin{aligned} &P\left[C_S < C_{th} \mid \mathscr{D}(S) = \emptyset\right] \\ &= P\left[\log_2(1 + y\gamma_S) < C_{th} \mid \mathscr{D}(S) = \emptyset\right] \\ &= P\left[y < \lambda_{th} \mid \mathscr{D}(S) = \emptyset\right] = Q\left(\frac{\widehat{\mu}_y - \xi \ln \lambda_{th}}{\widehat{\sigma}}\right), \end{aligned} \tag{52}$$

where $\lambda_{th} = (2^{C_{th}} - 1)/\gamma_S$.

(2) . The capacity can be expressed as

$$\begin{aligned} &C_{end}(\emptyset) \\ &\quad = E\left[\log_2(1 + y\gamma_S) \mid \mathscr{D}(S) = \emptyset\right] P\left[\mathscr{D}(S) = \emptyset\right], \end{aligned} \tag{53}$$

where $E[\log_2(1 + y\gamma_S) \mid \mathscr{D}(S) = \emptyset]$ can be expressed as

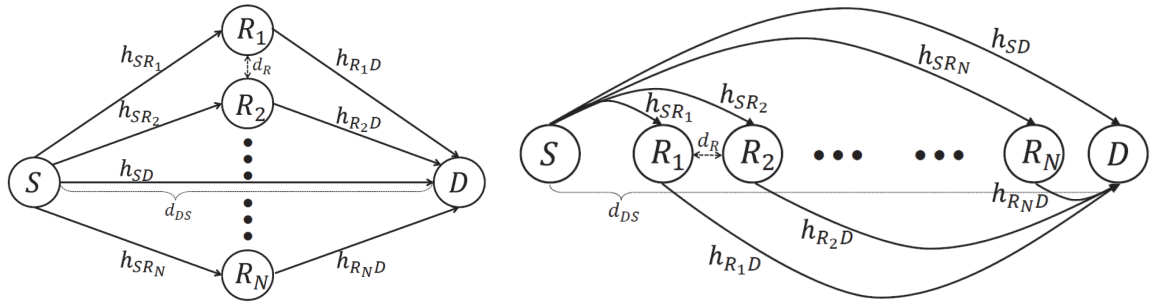
$$\begin{aligned} E\left[\log_2(1 + y\gamma_S) \mid \mathscr{D}(S) = \emptyset\right] = \int_0^{\infty} \log_2(1 + y\gamma_S) \\ \cdot \frac{\xi}{\sqrt{2\pi}\widehat{\sigma} y} \exp\left(-\frac{(\xi \ln y - \widehat{\mu}_S)^2}{2\widehat{\sigma}^2}\right) dx \end{aligned} \tag{54}$$

Following the procedure of deriving (33), we can have the numerical expression of (54) as

$$\begin{aligned} &E\left[\log_2(1 + y\gamma_S) \mid \mathscr{D}(S) = \emptyset\right] \\ &\quad \cong \sum_{\eta=1}^{N_H} \omega_{\eta} \log_2\left[1 + \gamma_S \exp\left(\frac{\sqrt{2}\widehat{\sigma} t_{\eta} + \widehat{\mu}_y}{\xi}\right)\right]. \end{aligned} \tag{55}$$

5. Numerical Results

In this section, the relay-assisted D2D and cellular networks are considered to evaluate the exactness of the analytical model and investigate the performance degradation caused



(a) Vertically deployed relays (b) Horizontally deployed relays

Figure 2: Relay-assisted D2D network with N (a) vertically and (b) horizontally deployed relays.

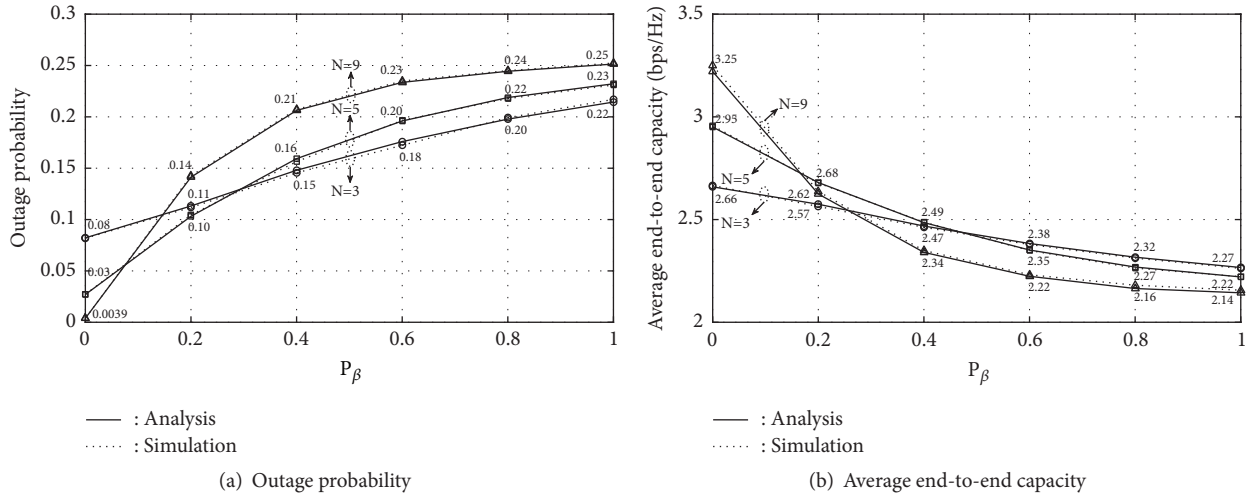
by the masquerading attack. In either scenario, the unit-variance Rayleigh fading is assumed. Also, the path loss exponent is 3.5 and the standard deviation of the Log-Normal shadowing is 6 in the dB domain. All the simulation results are obtained by averaging over 200,000 rounds.

5.1. D2D Network. Here, the vertical deployment of the relay network (as shown in Figure 2(a)) is firstly applied for investigating the impact of the masquerading attack. Then, the horizontal deployment of Figure 2(b) is used to quantitatively investigate the effect of the location of a single designated masquerader. As shown in the figures, the distance between S and D is $d_{DS} = 1000$ m; and that between two neighboring relays is $d_R = 50$ m. The transmission power of the source P_S is set so that the thermal noise outage (O_N) at the destination can be 0.2 [19]. Similarly, the transmission power of each relay P_R is set so that $O_N = 0.2$ can be achieved by the central relay (e.g., R_2 with $N = 3$ or R_3 with $N = 5$). Note that the required SNR corresponding to $O_N = 0.2$ is defined as 0 dB, whereas, for the purpose of evaluating the outage probability, the SNR threshold is 8 dB. Also, the capacity threshold C_{th} in Sections 2, 3, and 4 can be obtained by substituting the SNR threshold into the well-known equation of Shannon capacity.

Figure 6 shows the (a) outage probability and (b) average end-to-end capacity with respect to P_β for the relay-assisted D2D network under the CELN channel environment, where $P_\alpha = 0.5$; $N = 3$, $N = 5$, and $N = 9$ relays are placed according to the vertical deployment as illustrated in Figure 2(a). Apparently, the analytic and simulation results match with each other quite well. Most importantly, as demonstrated in the figures, the masquerading attack can cause significant performance degradation. For example, as the P_β increases from 0 to 0.4, the outage probability for the case with $N = 5$ can increase from 0.03 to 0.16. In addition, it can lead to 16% capacity loss (from 2.95 to 2.49 bps/Hz). Moreover, as P_β keeps growing, its impact becomes marginal. It should be noticed that the equivalent activity of the masquerading behavior for each relay is $P_\alpha \times P_\beta$, whereas the overall masquerading behavior across the whole network is $N \times P_\alpha \times P_\beta$. Thus, with $N = 5$, $P_\alpha = 0.5$, and $P_\beta = 0.2$, solely $P_\alpha \times P_\beta = 0.5 \times 0.2 = 10\%$ (or overall $5 \times 0.5 \times 0.2 = 50\%$) equivalent activity of the masqueraders can cause 9.2% capacity loss (from 2.95 to 2.68), while the outage probability can increase from 0.03 to 0.1. When the equivalent activity becomes $P_\alpha \times P_\beta = 0.5 \times 1 = 50\%$ (or overall $N \times P_\alpha \times P_\beta = 5 \times 0.5 \times 1 = 250\%$), it ends in 25% capacity loss and unacceptably high outage probability of 0.23 (667% rise).

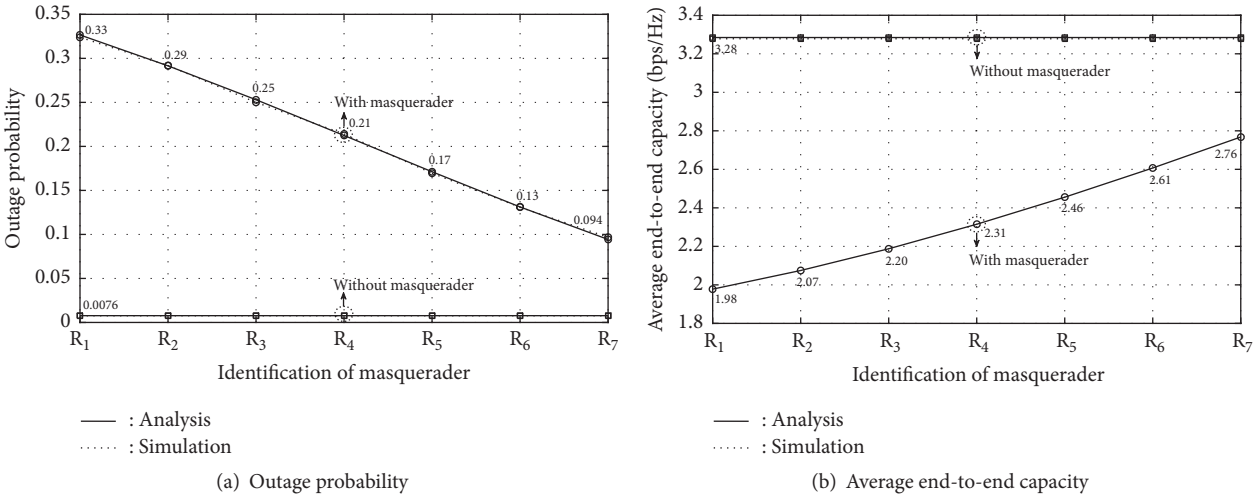
This phenomenon can become deteriorated when the number of relays increases. For example, comparing the curve of $N = 5$ at $P_\beta = 0.4$, using $N = 9$ relays can result in additional 6% capacity loss (from 2.49 to 2.34 bps/Hz), and higher outage probability (increasing from 0.16 to 0.21). Moreover, as P_β grows to one, 34% capacity loss can be resulted; and the outage probability can be extremely risen by 6310%. It should be noticed that, in general, using more relays can contribute to a better system performance. However, the masqueraders seriously dilute the diversity gain. Thus, how to tackle the issue of masqueraders could be an important issue for the future generation of hyperdense relay networks. Figure 3 shows the (a) outage probability and (b) average end-to-end capacity with respect to P_β for the relay-assisted D2D network under the CELN channel environment, where $P_\alpha = 0.5$; $N = 3$, $N = 5$, and $N = 9$ relays are placed according to the vertical deployment as illustrated in Figure 2(a).

Figure 4 shows the (a) outage probability and (b) average end-to-end capacity for the relay-assisted D2D network under the CELN environment with a single designated masquerader according to the horizontal deployment as illustrated in Figure 2(b), where $N = 7$ and $P_\beta = 1$. Note that the cases without masquerader mean that all the $N = 7$ relays are ordinary ones, whereas the cases with masquerader mean that there is only one masquerader indicated by the horizontal axis. In addition to the similar phenomenon observed from Figure 6 (i.e., the significant performance degradation caused by the masquerader), one can also find that the masquerader located farther from the destination can cause severer performance degradation. This explains the lowest capacity and highest outage probability for the case of the first relay (i.e., R_1) being the designated masquerader. Therefore, it can be expected that a masquerader can possibly incur a serious bottleneck effect on the multihop transmissions in the future generation of wireless communication systems.



(a) Outage probability (b) Average end-to-end capacity

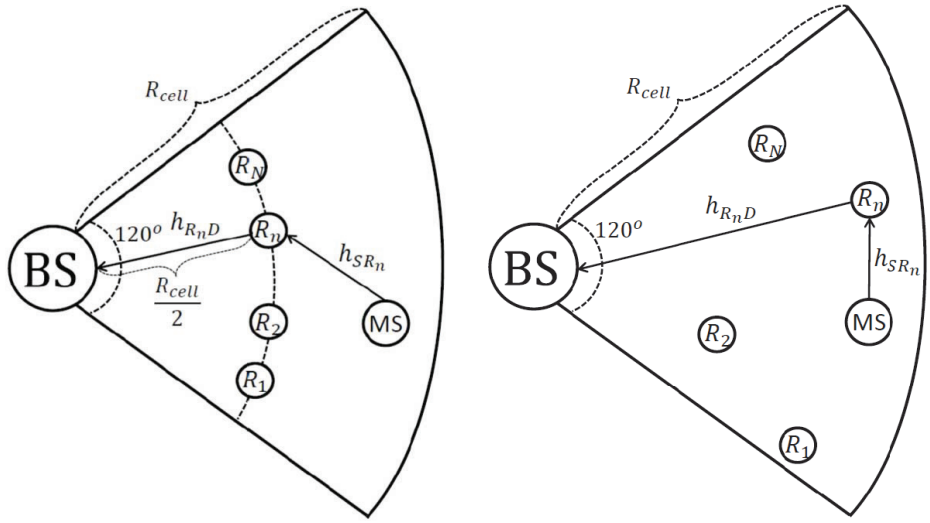
FIGURE 3: (a) Outage probability and (b) average end-to-end capacity with respect to P_β for the relay-assisted D2D network under the CELN channel environment, where $P_\alpha = 0.5$; $N = 3$, $N = 5$, and $N = 9$ relays are placed according to the vertical deployment as illustrated in Figure 2(a).



(a) Outage probability (b) Average end-to-end capacity

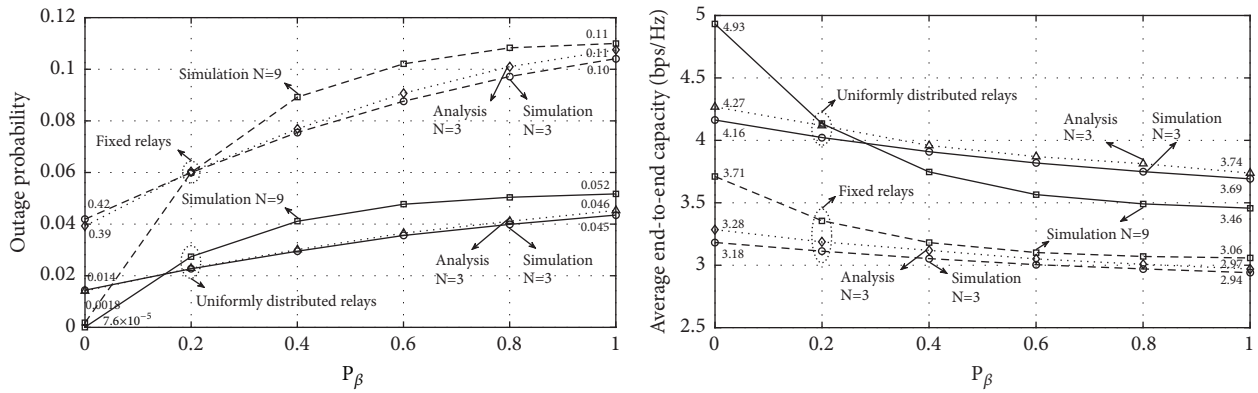
FIGURE 4: (a) Outage probability and (b) average end-to-end capacity for the relay-assisted D2D network under the CELN environment with a single designated masquerader according to the horizontal deployment as illustrated in Figure 2(b), where $N = 7$ and $P_\beta = 1$.

5.2. Cellular Network. In the cellular scenario, one cell with three 120° sectors is considered. As per the parameter setting in Figure 1, the simulation is conducted for the network topologies illustrated in Figures 5(a) and 5(b). Therein, $N = 3$ and 9 relays are fixed at the middles or uniformly distributed over its coverage area, respectively. In the latter case, the minimum distance between a relay and BS is 100 m. Also, in both cases, the location of MS is uniformly spread over the sector. Since the analytical results are obtained by averaging over 100 randomly generated network topologies, the time required to calculate all the cases discussed in Sections 3 and 4 can be prohibitively prolonged when $N \geq 7$. Thus, only $N = 3$ is considered for generating the analytical results. Firstly, the exactness of the analytical results can still be verified. Secondly, as observed in the D2D network, more stringent performance degradation can be incurred by the larger amount of relays. Thirdly, the masquerading attack can cause more significant performance degradation for the cases with uniformly distributed relays. For the example with $N = 9$ uniformly distributed relays, serious masquerading attack can cause 30% capacity loss (from 4.93 to 3.46 bps/Hz). However, the loss becomes 18% (from 3.71 to 3.05 bps/Hz) when the relays are fixed at the middles of the sector. Note that the larger diversity gain can be obtained when the relays are "not fixed" at the middles of the sector (which explains the better performance for the cases with uniformly distributed relays as well). However, the masquerading attack dilutes the achievable diversity gain and causes larger performance degradation for the cases with larger diversity gain (as aforementioned).



(a) A sector with fixed relays (b) A sector with uniformly distributed relays

FIGURE 5: A cellular sector with N (a) fixed relays and (b) uniformly distributed relays.



(a) Outage probability (b) Average end-to-end capacity

FIGURE 6: (a) Outage probability and (b) average end-to-end capacity with respect to P_β for the cellular networks with fixed and uniformly distributed relays under the CELN channel environment, where $P_\alpha = 0.5$; the numbers of relays are $N = 3$ and $N = 9$.

6. Conclusions

In this paper, we have defined the masquerading attack for the relay-assisted networks. For the purpose of numerically characterizing the masquerading attack, the mathematical expressions for the end-to-end capacity and outage probability have been derived. To make the discussions more complete, the CELN channel model was taken into account such that the geographic effects of the network topology can be captured. Moreover, the random masquerading behavior was considered as well, including the probability of a relay to become a masquerader and probability of a masquerader to become active. Via the analytical and simulation results, it was found that the masquerading attack can cause 34% and 30% capacity loss for considered D2D and cellular networks. Also, the corresponding outage probability can be extremely risen.

Nowadays, the necessity of relay-assisted transmission scheme for the next generation of wireless communication networks has been widely recognized. With the aid of relay, the performance of secondary users in the cognitive network can be improved [21]; the physical layer security in the large-scale fifth-generation network can be strengthened [22]; the energy efficiency and link reliability for the vehicular ad hoc networks can be enhanced [23]; the cellular coverage area can be extended via multihop D2D communications [6, 7, 24], especially for the millimeter-wave-based systems [25–27] and Internet-of-Things [28]; the high quality transmissions for the sensor network can be achieved [29] as well. However, based on the finding of this paper, the achievable diversity gain via relay transmissions will be seriously diluted under the masquerading attack. De facto, in addition to the DNPS protocol, any arbitrary relay networks (especially for the ones operating in the distributed mode) can encounter this

kind of threat, which hypocritically forwards packets and removes the diversity gain in silence. Thus, how to evaluate and alleviate the impact of the masqueraders could be a critical issue to fully utilize the advantages of relay-assisted transmissions. This paper can be recognized as a first step to inspire the investigation of the masquerading attack for the relay networks.

Data Availability

All the analytical and numerical results can be reproduced by using the source codes at http://140.116.92.1/SourceCode/WCMC/experiment. The Matlab codes used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Ministry of Science and Technology, Taiwan, under Contract 105-2221-E-006-034.

References

[1] J. Xu, J. Wang, Y. Zhu et al., "Cooperative distributed optimization for the hyper-dense small cell deployment," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 61–67, 2014.

[2] H. Shokri-Ghadikolaei, C. Fischione, P. Popovski, and M. Zorzi, "Design aspects of short-range millimeter-wave networks: A MAC layer perspective," *IEEE Network*, vol. 30, no. 3, pp. 88–96, 2016.

[3] T. E. Bogale and L. B. Le, "Massive MIMO and mmWave for 5G wireless HetNet: potential benefits and challenges," *IEEE Vehicular Technology Magazine*, vol. 11, no. 1, pp. 64–75, 2016.

[4] M. Peng, Y. Liu, D. Wei, W. Wang, and H. Chen, "Hierarchical cooperative relay based heterogeneous networks," *IEEE Wireless Communications Magazine*, vol. 18, no. 3, pp. 48–56, 2011.

[5] M. Cardone, D. Tuninetti, and R. Knopp, "On the optimality of simple schedules for networks with multiple half-duplex relays," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 62, no. 7, pp. 4120–4134, 2016.

[6] L. Wei, R. Hu, Y. Qian, and G. Wu, "Key elements to enable millimeter wave communications for 5G wireless systems," *IEEE Wireless Communications Magazine*, vol. 21, no. 6, pp. 136–143, 2014.

[7] J. Qiao, X. S. Shen, J. W. Mark, Q. Shen, Y. He, and L. Lei, "Enabling device-to-device communications in millimeter-wave 5G cellular networks," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 209–215, 2015.

[8] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, 2015.

[9] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 152–158, 2016.

[10] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 2, pp. 198–212, 2007.

[11] S. Dehnie and N. Memon, "Detection of misbehavior in cooperative diversity," in *Proceedings of theMilitary Communications Conference (MILCOM)*, pp. 1–5, 2008.

[12] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "Smart: a secure multilayer credit-based incentive scheme for delay-tolerant networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4628–4639, 2009.

[13] L.-C Lo and W.-J Huang, "Misbehavior detection without channel information in cooperative networks," in *Proceedings of the 2011 IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1–5, San Francisco, CA, USA, September 2011.

[14] Y.-M. Yi, L.-C. Lo, and W.-J. Huang, "On blind sequential detection of misbehaving relay," in *Proceedings of the Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, pp. 1–4, 2012.

[15] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659–672, 2006.

[16] R. Gangula and R. Bhattacharjee, "Performance of selection cooperation in the presence of a malicious relay," in *Proceedings of the 2010 7th International Symposium on Wireless Communication Systems, ISWCS'10*, pp. 408–412, September 2010.

[17] J. Zhang and J. G. Andrews, "Distributed antenna systems with randomness," *IEEE Transactions on Wireless Communications*, vol. 7, no. 9, pp. 3636–3646, 2008.

[18] W. Chang, "On the performance of the DNPS-based relay networks under attack by masquerader," in *Proceedings of the 2017 IEEE Wireless Communications and Networking Conference, (WCNC 2017)*, pp. 1–6, March 2017.

[19] G. L. Stuber, *Principles of Mobile Communications*, Kluwer Academic Publishers, 2nd edition, 2001.

[20] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, Dover Publications, New York, NY, USA, 9th edition, 1970.

[21] J. Van Hecke, P. Del Fiorentino, V. Lottici, F. Giannetti, L. Vandendorpe, and M. Moeneclaey, "Distributed Dynamic Resource Allocation for Cooperative Cognitive Radio Networks with Multi-Antenna Relay Selection," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1236–1249, 2017.

[22] C. Zhang, J. Ge, J. Li, F. Gong, and H. Ding, "Complexity-aware relay selection for 5g large-scale secure two-way relay systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5461–5465, 2017.

[23] D. Tian, J. Zhou, Z. Sheng, M. Chen, Q. Ni, and V. C. Leung, "Self-Organized Relay Selection for Cooperative Transmission in Vehicular Ad-Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9534–9549, 2017.

[24] J. Gui and J. Deng, "Multi-hop relay-aided underlay d2d communications for improving cellular coverage quality," *IEEE Access*, vol. 6, pp. 14318–14338, 2018.

[25] Y. Niu, L. Su, C. Gao, Y. Li, D. Jin, and Z. Han, "Exploiting Device-to-Device Communications to Enhance Spatial Reuse for Popular Content Downloading in Directional mmWave Small Cells," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp. 5538–5550, 2016.

[26] W. Chang and J.-C. Teng, "Energy efficient relay matching with bottleneck effect elimination power adjusting for full-duplex relay assisted D2D networks using mmWave technology," *IEEE Access*, vol. 6, 2018.

[27] K. Belbase, Z. Zhang, H. Jiang, and C. Tellambura, "Coverage analysis of millimeter wave decode-and-forward networks with best relay selection," *IEEE Access*, vol. 6, pp. 22670–22683, 2018.

[28] G. Chen, J. Tang, and J. P. Coon, "Optimal routing for multihop social-based d2d communications in the internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1880–1889, 2018.

[29] X. Li, J. Liu, L. Yan, S. Han, and X. Guan, "Relay selection for underwater acoustic sensor networks: a multi-user multi-armed bandit formulation," *IEEE Access*, vol. 6, pp. 7839–7853, 2018.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 2390834, 11 pages
https://doi.org/10.1155/2018/2390834

Research Article

Impact of Antenna Selection on Physical-Layer Security of NOMA Networks

Dan Deng[1], **Chao Li**[2], **Lisheng Fan**[2], **Xin Liu**[3] and **Fasheng Zhou**[4]

[1]*School of Information Engineering, Guangzhou Panyu Polytechnic, Guangzhou, 511483, China*
[2]*School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China*
[3]*School of Information and Communication Engineering, Dalian University of Technology, China*
[4]*School of Physics and Electronic Engineering, Guangzhou University, Guangzhou 510006, China*

Correspondence should be addressed to Lisheng Fan; lsfan@gzhu.edu.cn

Received 17 April 2018; Accepted 31 May 2018; Published 3 July 2018

Academic Editor: Li Sun

This paper studies the impacts of antenna selection algorithms in decode-and-forward (DF) cooperative nonorthogonal multiple access (NOMA) networks, where the secure information from the relay can be overheard by an eavesdropper in the networks. In order to ensure the secure transmission, an optimal antenna selection algorithm is proposed to choose one best relay's antenna to assist the secure transmission. We study the impact of antenna selection on the system secure communication through deriving the analytical expression of the secrecy outage probability along with the asymptotic expression in the high regime of signal-to-noise ratio (SNR) and main-to-eavesdropper ratio (MER). From the analytical and asymptotic expressions, we find that the system secure performance is highly dependent on the system parameters such as the number of antennas at the relay, SNR, and MER. In particular, the secrecy diversity order of the system is equal to the antenna number, when the interference from the second user is limited.

1. Introduction

In recent years, the wireless data rate has been explosively increasing [1–4], and many wireless services have been emerging, which requires the rapid development of wireless transmission [5–8]. As one of the most promising techniques, nonorthogonal multiple access (NOMA) provides superhigh data rate over the orthogonal multiple access, and hence it has been recognized as one candidate for the next-generation wireless communication networks [9, 10].

Moreover, NOMA has been demonstrated to be compatible with other emerging technologies [11–14]. In particular, the impact of imperfect self-interference cancellation for full-duplex cooperative NOMA is investigated in [12], while authors in [13] study the combination of NOMA and relay selection and results show that the proposed strategy can provide maximal diversity gain. Considering multiple sources, relay sharing scheme is proposed in [14] and results show that the proposed scheme outperforms OMA under perfect or imperfect SIC.

Due to the broadcast nature of wireless transmission, it is of vital importance to guarantee the transmission security from the application layer [15–19] to physical layer [20, 21]. The authors in [22] provided the framework of wiretap channels, which gives a general way to analyze and design the secure physical-layer security. In general, the performances of secure communications is affected by many wireless channel parameters, such as the channel correlation [23–25] and fading characteristics [26–28]. Recently, researchers turned to study the physical-layer security for NOMA communication systems. In [29], the authors proposed the transmission antenna selection for NOMA systems with multiple antennas, in order to ensure the secure communication. The authors in [30] optimized the secrecy sum rate of multiple users, in order to optimize the system design. Moreover, the authors in [31] investigated the downlink NOMA communication systems and proposed a secure beamforming algorithm to enhance the physical-layer security.

To further enhance the physical-layer security of NOMA systems, researchers proposed the spatial selection, such as

antenna selection or relay selection [32]. The authors in [33] extended this work into amplify-and-forward (AF) and decode-and-forward (DF) modes and devised a novel relay selection scheme which consists of two stages. The analytical results in this paper depicted that the proposed scheme outperformed the conventional relay selection schemes. The authors in [34] studied the NOMA system over Nakagami-m fading channels and verified that relay selection could enhance the wireless security for the fixed-gain relaying mode. In [13], the authors applied the relay selection technique into NOMA systems with multiple relays and demonstrated that the proposed scheme could achieve the maximum secrecy diversity gain. Moreover, the authors in [14] studied the NOMA systems with multiple sources, and devised a relay sharing scheme which was demonstrated to outperform the conventional OMA with either perfect or imperfect SIC. In [35], the authors studied the NOMA communication systems with AF relay, and derived the analytical outage expression for the cooperative NOMA networks.

However, as to the best of our knowledge, there are no literatures on the effects of the antenna selection algorithms on the secrecy outage probability for cooperative NOMA. Motivated by that, based on the optimal antenna selection algorithm, this paper studies the secrecy outage performance for decode-and-forward (DF) cooperative NOMA networks. (DF relay can decode the wireless signal before forwarding to the destination note, which can improve the link quality. While amplify-and-forward (AF) relay only amplifies its received signal and the link quality can not be improved. Considering the advantages of DF relay scheme compared with AF scheme, only DF cooperative network is studied in this paper.) By using NOMA protocol and with the help of the relay station, the source station transfers messages to two destinations simultaneously. The best antenna of relay is selected to assist the secure transmission from the source to the destinations. The impact of the system parameters is analyzed through deriving the exact analytical expressions on the secrecy outage performance as well as the asymptotic results with large SNR and main-to-eavesdropper ratio (MER). We find that the system secure performance is highly dependent on the system parameters such as the number of antennas at the relay, SNR, and MER. Specifically, the secrecy diversity order of the system is equal to the antenna number, when the interference from the second user is limited. Furthermore, simulation results are provided to validate the theoretical analysis.

The main contributions of this paper are summarized as follows:

(1) An optimal antenna selection for cooperative NOMA networks is proposed and the closed-form exact expressions and the asymptotic expressions on the secrecy outage performance are derived.

(2) According to the asymptotic analysis, the impacts of the system parameters on the secrecy outage probability are revealed. We find that, in the case of limited interference, the secrecy diversity order of the system is equal to the antenna number

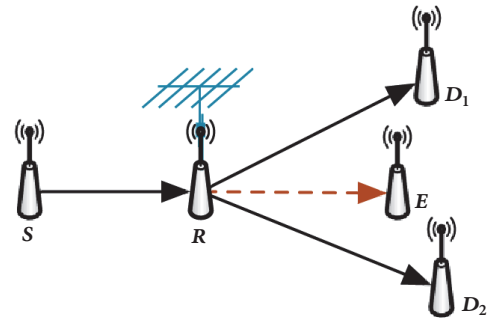


Figure 1: Secure antenna selection for cooperative NOMA networks.

Notations. We use the notations $\log_2(\cdot)$ and $\ln(\cdot)$ to represent the logarithms with the base of 2 and natural, respectively. Moreover, we use notations $f_X(x)$ and $F_X(x)$ to represent the probability density function and cumulative distribution function of the random variable X, respectively. Notation $\mathbb{E}(X)$ returns the expectation result of a random event X. In addition, $x \sim \mathcal{CN}(\mu, \sigma^2)$ indicates that the random variable x follows a circularly symmetric complex-valued Gaussian distribution of the mean μ and variance σ^2. We use the notation R-D to denote the link from R to D.

2. System Model and Selection Algorithm

The system model of two-slot decode-and-forward (DF) cooperative NOMA networks is given in Figure 1. The considered system consists of one source station, a DF relay with N antennas, two destinations, and one passive eavesdropper, denoted as S, R, $\{D_1, D_2\}$, and E, respectively. The relay station is equipped with N antennas, and we use $\{R_n, n \in [1, N]\}$ to denote the n-th antenna of R. It is assumed that perfect channel status information (CSI) of h_{SR_n}, $h_{R_nD_1}$, and $h_{R_nD_1}$ can be obtained by the relay station through dedicated feedback channel [36–39]. Since the eavesdropper does not transmit any signal all the time [40], the relay cannot obtain the CSI of the eavesdropping links. Due to the long distance or severe shadow fading [41–43], there exists no direct link between the source and the destinations. Then with the assistant of the relay station, the source station can transfer messages to two destinations by using the NOMA protocol. Meanwhile, the wireless signal from the relay station may be intercepted by the eavesdropper. Both S and D are assumed to be equipped with a single antenna and operate in the half-duplex time-division mode. To reduce the information leakage to the eavesdropper, the *best* antenna in R is selected to decode the signal and forward to the destinations. As mentioned before, the destinations share the wireless channel through NOMA protocol. In addition, all of the wireless channels are assumed to be quasi-static Rayleigh block fading and statistically independent of each other.

In the first slot, a mixture signal is transmitted from the source station to the selected relay's antenna. Thus, the received signal at n-th antenna of R can be expressed as

$$r_{R_n} = h_{SR_n}\left(\sqrt{\alpha_1 P_S}x_1 + \sqrt{\alpha_2 P_S}x_2\right) + n_{R_n}, \quad (1)$$

where x_1, x_2 are the messages transmitted from S to D_1 and D_2, respectively. $n_{R_n} \sim \mathcal{CN}(0, N_0)$ is the additive white Gaussian noise (AWGN) received at R_n. We use P_S to denote the total transmission power of the source station and use $h_{SR_n} \sim \mathcal{CN}(0, \lambda_0)$ to represent the instantaneous channel fading coefficient between S and R_n. The power allocation factors for x_1 and x_2 are denoted by α_1, α_2, respectively. According to the NOMA protocol [13], low rate and urgent traffic are carried by the first data stream, while the second data stream x_2 is used for opportunistic communications with long time tasks. To satisfy the total power requirement, α_1 and α_2 meet the following constraint: $\alpha_1 + \alpha_2 = 1$ and $\alpha_1 > \alpha_2$.

In this paper, we assume that perfect successive interference cancellation (SIC) receiver [44, 45] is used at R_n. Thus, x_2 is treated as interference before x_1 is decoded. Therefore, the SINRs for x_1 and x_2 at R_n can be obtained as

$$\mathrm{SINR}_{R_n}^{(1)} = \frac{\alpha_1 P_S \nu_n}{\alpha_2 P_S \nu_n + \sigma^2}, \tag{2}$$

and

$$\mathrm{SINR}_{R_n}^{(2)} = \frac{\alpha_2 P_S \nu_n}{\sigma^2}, \tag{3}$$

respectively, where $\nu_n = |h_{SR_n}|^2$ is used to denote the channel fading gain between S and R_n.

Consequently, the achievable rate for x_1 and x_2 at R_n can be expressed as follows:

$$\begin{aligned} C_{R_n}^{(1)} &= \frac{1}{2}\log_2\left(1 + \mathrm{SINR}_{R_n}^{(1)}\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\alpha_1 \nu_n}{\alpha_2 \nu_n + 1/\rho_S}\right), \end{aligned} \tag{4}$$

and

$$C_{R_n}^{(2)} = \frac{1}{2}\log_2\left(1 + \mathrm{SINR}_{R_n}^{(2)}\right) = \frac{1}{2}\log_2\left(1 + \alpha_2 \rho_S \nu_n\right), \tag{5}$$

where $\rho_S = P_S/N_0$.

Both of the data streams, i.e., x_1 and x_2, are decoded by the selected antenna in the second slot and forwarded to the destinations. Meanwhile, the wireless signal from the relay may be overheard by the passive eavesdropper. Given that R_n is selected and the received signal at D_2 and E can be given as

$$r_{D_2} = h_{R_n D_2}\left(\sqrt{\alpha_1 P_R}x_1 + \sqrt{\alpha_2 P_R}x_2\right) + n_{D_2}, \tag{6}$$

$$r_E = h_{R_n E}\left(\sqrt{\alpha_1 P_R}x_1 + \sqrt{\alpha_2 P_R}x_2\right) + n_E, \tag{7}$$

where $h_{R_n D_2} \sim \mathcal{CN}(0, \lambda_2)$, $h_{R_n E} \sim \mathcal{CN}(0, \lambda_E)$ are the instantaneous channel fading coefficient of R_n-D_2 and R_n-E links, respectively, P_R is the transmission power of R_n, $n_{D_2} \sim \mathcal{CN}(0, N_0)$, and $n_E \sim \mathcal{CN}(0, N_0)$ denote the AWGN received at D_2 and E, respectively.

Moreover, it is assumed that SIC receiver is used at both D_2 and E. That is, x_2 is treated as noise when they are trying to decode x_1. Thus, the achievable rates of x_1 at D_2 and E are given as (4)

$$\begin{aligned} C_{D_2}^{(1)} &= \frac{1}{2}\log_2\left(1 + \mathrm{SINR}_{D_2}^{(1)}\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\alpha_1 u_n}{\alpha_2 u_n + 1/\rho_R}\right), \end{aligned} \tag{8}$$

$$\begin{aligned} C_E^{(1)} &= \frac{1}{2}\log_2\left(1 + \mathrm{SINR}_E^{(1)}\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\alpha_1 g_n}{\alpha_2 g_n + 1/\rho_R}\right), \end{aligned} \tag{9}$$

where $u_n = |h_{R_n D_2}|^2$ and $g_n = |h_{R_n E}|^2$ denote the channel fading gain of links R_n-D_2 and R_n-E, respectively, and $\rho_R = P_R/N_0$.

Conditioned on that x_1 is decoded successfully, then the achievable rates of x_2 at D_2 and E can be expressed as

$$C_{D_2}^{(2)} = \frac{1}{2}\log_2\left(1 + \mathrm{SINR}_{D_2}^{(2)}\right) = \frac{1}{2}\log_2\left(1 + \alpha_2 \rho_R u_n\right), \tag{10}$$

and

$$C_E^{(2)} = \frac{1}{2}\log_2\left(1 + \mathrm{SINR}_E^{(2)}\right) = \frac{1}{2}\log_2\left(1 + \alpha_2 \rho_R g_n\right). \tag{11}$$

Thus, the secrecy capacity of the relaying system can be written as [46]

$$C_S = \left[C_{D_2}^{(2)} - C_E^{(2)}\right]^+, \tag{12}$$

where $[x]^+ = \max\{x, 0\}$.

Based on the theoretical analysis on the secrecy capacity, in order to minimize the secrecy outage probability of cooperative NOMA system, an optimal antenna selection algorithm is proposed in the following section.

The correctly decoding antenna subset is defined in the first step of the proposed algorithm as follows:

$$S_D = \left\{n : n \in [1, N], \mathrm{SINR}_{R_n}^{(1)} \geq \gamma_1, \mathrm{SINR}_{R_n}^{(2)} \geq \gamma_2\right\}, \tag{13}$$

with

$$\begin{aligned} \gamma_1 &= 2^{2R_1} - 1, \\ \gamma_2 &= 2^{2R_2} - 1, \end{aligned} \tag{14}$$

where R_1 and R_2 denote the minimum rate requirements for x_1 and x_2, respectively.

It is easy to prove that both $C_{D_2}^{(1)}$ and $C_{D_2}^{(2)}$ are monotone increasing functions with respect to u_n. In the second step of the selection algorithm, since the relay has no CSI of the eavesdropper, the optimal antenna selection algorithm can be performed as follows:

$$n^* = \arg\max_{n \in S_D} \{u_n\}. \tag{15}$$

3. Performance Analysis

In this section, the theoretical analysis on the secrecy outage probability for the cooperative NOMA networks will be derived, as well as the asymptotic results. From the analysis, a deep insight on the effects of the system parameters, such as the antenna number and the power allocation factors, on the outage performance is present.

3.1. Exact Expression on Secrecy Outage Probability. In this section, the outage probability of the first step in (13) is analyzed. Given that relay antenna R_n is randomly selected, H_n is defined as the probability that R_n belongs to the decoding antenna subset S_D. By substituting (4) and (5) into (13), we have

$$\begin{aligned} H_n &= \Pr\left[R_n \in S_D\right] = \Pr\left[\mathrm{SINR}_{R_n}^{(1)} \geq \gamma_1, \mathrm{SINR}_{R_n}^{(2)} \geq \gamma_2\right] \\ &= e^{-c_3/\rho_S\lambda_0}, \end{aligned} \tag{16}$$

with

$$\begin{aligned} c_1 &= \frac{\gamma_1}{\alpha_1 - \alpha_2\gamma_1}, \\ c_2 &= \frac{\gamma_2}{\alpha_2}, \\ c_3 &= \max\left\{c_1, c_2\right\}. \end{aligned} \tag{17}$$

Note that when $\gamma_1 \geq \alpha_1/\alpha_2$, no antenna can decode x_1 correctly, and the outage occurs definitely. Thus, we only need to consider the case that $\gamma_1 < \alpha_1/\alpha_2$.

We use $|S_D|$ to denote the size of subset S_D. Because of the statistical independence between $S - R_n$ links, the probability that $|S_D|$ equals M can be written as

$$\begin{aligned} \Pr\left\{\left|S_D\right| = M\right\} &= \binom{N}{M}\left(H_n\right)^M\left(1 - H_n\right)^{N-M} \\ &= \binom{N}{M}\left(e^{-c_3/\rho_S\lambda_0}\right)^M\left(1 - e^{-c_3/\rho_S\lambda_0}\right)^{N-M}. \end{aligned} \tag{18}$$

In particular, the outage probability that the size of S_D equals zero can be given as

$$\Pr\left[\left|S_D\right| = 0\right] = \left(1 - e^{-\gamma_m/\gamma_s\beta}\right)^N. \tag{19}$$

We turn to consider the performance of the second step in (15), given that R_n is selected. The scenarios of successful secrecy transmission can be divided into two cases as follows. The first case is that both D_2 and E can decode x_1 successfully, and the secrecy capacity is better than the minimum requirement simultaneously. The probability of the first case can be given as

$$\begin{aligned} P_{n,1} &= \Pr\left[C_{D_2}^{(1)} \geq R_1, C_E^{(1)} \geq R_1, C_S \geq R_S\right] \\ &= \Pr\left[C_{D_2}^{(1)} \geq R_1, C_E^{(1)} \geq R_1, C_{D_2}^{(2)} - C_E^{(2)} \geq R_S\right]. \end{aligned} \tag{20}$$

By applying necessary mathematical derivation and substituting (8), (9), (10), and (11) into (20), we obtain

$$P_{n,1} = \Pr\left[u_n \geq g_n\gamma_S + \frac{c_4}{\rho_R}, g_n \geq \frac{c_1}{\rho_R}\right], \tag{21}$$

where $\gamma_S = 2^{2R_S}$ and $c_4 = (\gamma_S - 1)/\alpha_2$.

The second case is that E cannot decode x_1 correctly, but D_2 can. In this case, the secrecy capacity equals the achievable rate of x_2 at D_2. The probability of the second case can be written as

$$P_{n,2} = \Pr\left[C_{D_2}^{(1)} \geq R_1, C_E^{(1)} < R_1, C_{D_2}^{(2)} \geq R_S\right]. \tag{22}$$

Similarly, substituting (8), (9), and (10) into (22), we obtain

$$P_{n,2} = \Pr\left[u_n \geq \frac{c_5}{\rho_R}, g_n < \frac{c_1}{\rho_R}\right]. \tag{23}$$

Using the full probability formula, the outage probability of this step can be calculated as

$$P_{O,n,M} = \left[1 - P_{n,1} - P_{n,2}\right], \tag{24}$$

where $M > 0$ is the size of the decoding antenna subset.

Thus, the secrecy outage probability of the cooperative NOMA system for R_n is

$$P_{O,n} = \Pr\left[\left|S_D\right| = 0\right] + \sum_{M=1}^{N}\Pr\left[\left|S_D\right| = M\right]P_{O,n,M}. \tag{25}$$

According to the order statistics [47], the CDF of u_{n^*} can be expressed as

$$F_{u_{n^*}}(x) = \Pr\left\{u_{n^*} < x\right\} = \Pr\left\{u_n < x, n \in S_D\right\}. \tag{26}$$

Due to the independence of channel fading gains u_n, the cumulative distribution function can be rewritten as

$$F_{u_{n^*}}(x) = \prod_{n=1}^{M}\Pr\left\{u_n < x\right\} = \left(1 - e^{-x/\lambda_2}\right)^M. \tag{27}$$

By using the binomial theorem on (27), we obtain

$$F_{u_{n^*}}(x) = 1 - \sum_{k=1}^{M}\binom{M}{k}(-1)^{k-1}e^{-kx/\lambda_2}. \tag{28}$$

Using the analysis result in (28), the probability density function of u_{n^*} can be expressed as

$$f_{u_{n^*}}(x) = \sum_{k=1}^{M}\binom{M}{k}(-1)^{k-1}\frac{k}{\lambda_2}e^{-kx/\lambda_2}. \tag{29}$$

Since u_n is independent of g_n, the PDF of g_{n^*} remains the same with that of g_n; i.e.,

$$f_{g_{n^*}}(x) = f_{g_n}(x) = \frac{1}{\lambda_E}e^{-x/\lambda_E}. \tag{30}$$

By applying (29) and (30) on (21) and (23), we have

$$P_{n^*,1} = \sum_{k=1}^{M} \binom{M}{k} \frac{(-1)^{k-1}}{c_{6,k}\lambda_E} e^{-c_{7,k}/\rho_R}, \tag{31}$$

with

$$\begin{aligned} c_{6,k} &= \frac{1}{\lambda_E} + \frac{k\gamma_S}{\lambda_2}, \\ c_{7,k} &= c_1 c_{6,k} + \frac{k c_4}{\lambda_2}, \end{aligned} \tag{32}$$

and

$$P_{n^*,2} = \left(1 - e^{-c_1/\rho_R\lambda_E}\right) \sum_{k=1}^{M} \binom{M}{k} (-1)^{k-1} e^{-kc_3/\rho_R\lambda_2}. \tag{33}$$

Using (31) and (33), $P_{O,n^*,M}$ in (24) and the secrecy outage probability in (25) for the optimal antenna selection can be expressed as in (34).

$$\begin{aligned} P_{O,n^*} &= \Pr\{|S_D| = 0\} + \sum_{M=1}^{N} \Pr\{|S_D| = M\} P_{O,n^*,M} \\ &= \Pr\{|S_D| = 0\} + \sum_{M=1}^{N} \Pr\{|S_D| = M\} \cdot \Bigg\{ 1 \\ &\quad - \left[\sum_{k=1}^{M} \binom{M}{k} \frac{(-1)^{k-1}}{c_{6,k}\lambda_E} e^{-c_{7,k}/\rho_R} \right] \\ &\quad - \left[\left(1 - e^{-c_1/\rho_R\lambda_E}\right) \sum_{k=1}^{M} \binom{M}{k} (-1)^{k-1} e^{-kc_3/\rho_R\lambda_2} \right] \Bigg\}. \end{aligned} \tag{34}$$

The details about the numerical computation and associated analysis can be found in the literature, such as the works [48–52] or [53–56].

3.2. Asymptotic Outage Probability Analysis. We present the asymptotic analysis in this section to reveal a deep insight on the effects of the system parameters on the outage probability. The asymptotic analysis focuses on the system behavior when the noise can be neglected. In this case, the main contribution or the bottleneck of the system performance can be revealed. Based on the asymptotic analysis, we can propose the optimization scheme on the system parameters. According to the asymptotic results, we can show behavior of the outage performance when both the transmission and the main-to-eavesdropper ratio (MER) are large enough.

Firstly, we give the definition of MER, which denotes the ratio of average fading power of $h_{R_n D_2}$ to that of $h_{R_n E}$; i.e.,

$$\mu = \frac{\lambda_2}{\lambda_E}. \tag{35}$$

Lemma 1. *Given the definition of function* $G(M,k) = \sum_{m=1}^{M} \binom{M}{m} (-1)^m m^k$*, we have the following equation:*

$$G(M,k) = 0, \quad \forall k = 1, 2, \ldots, (M-1). \tag{36}$$

Proof. See Appendix A. □

Lemma 2. *Given the definition of function* $A_N = \sum_{k=0}^{N} \binom{N}{k} ((-1)^k/(1+k\delta))$*, if* $\delta \to 0$*, we have the following approximation result:*

$$A_N \approx (-\delta)^N G(N,N). \tag{37}$$

Proof. See Appendix B. □

Consider the asymptotic expression of $P_{n^*,1}$ in (31). By using the approximation that $e^x = 1 + x$, we have

$$\begin{aligned} \widehat{P}_{n^*,1} &= 1 - P_{n^*,1} \approx 1 - \sum_{k=1}^{M} \binom{M}{k} \frac{(-1)^{k-1}}{c_{6,k}\lambda_E} \left(1 - \frac{c_{7,k}}{\rho_R}\right) \\ &= 1 - \sum_{k=1}^{M} \binom{M}{k} \frac{(-1)^{k-1}}{1 + k\left(\gamma_S\lambda_E/\lambda_2\right)} \left(1 - \frac{c_{7,k}}{\rho_R}\right). \end{aligned} \tag{38}$$

Then, by using Lemma 2, we obtain

$$\begin{aligned} \widehat{P}_{n^*,1} &= 1 - \sum_{k=1}^{M} \binom{M}{k} \frac{(-1)^{k-1}}{1 + k\left(\gamma_S\lambda_E/\lambda_2\right)} \left(1 - \frac{c_{7,k}}{\rho_R}\right) \\ &= \left(-\frac{\gamma_S}{\mu}\right)^M G(M,M) \\ &\quad + \sum_{k=1}^{M} \binom{M}{k} \frac{(-1)^k}{1 + k\left(\gamma_S/\mu\right)} \frac{c_{7,k}}{\rho_R} \\ &= \left(-\frac{\gamma_S}{\mu}\right)^M G(M,M) + \frac{c_1}{\rho_R\gamma_E}. \end{aligned} \tag{39}$$

Similarly, consider the asymptotic expression of $P_{n^*,2}$ in (33), and using the approximation $1 - e^{-x} = x$ yields

$$\begin{aligned} P_{n^*,2} &\approx \frac{c_1}{\rho_R\lambda_E} \sum_{k=1}^{M} \binom{M}{k} (-1)^{k-1} e^{-kc_3/\rho_R\lambda_2} \\ &\approx \left(\frac{c_1}{\rho_R\lambda_E}\right) \sum_{k=1}^{M} \binom{M}{k} (-1)^{k-1} \left(1 - \frac{kc_3}{\rho_R\lambda_2}\right) \\ &\approx \frac{c_1}{\rho_R\lambda_E} \sum_{k=1}^{M} \binom{M}{k} (-1)^{k-1} = \frac{c_1}{\rho_R\lambda_E}. \end{aligned} \tag{40}$$

When $\rho_S \to \infty$, the asymptotic result of (18) can be given as

$$\begin{aligned} \Pr\{|S_D| = M\} &\approx \binom{N}{M} \left(e^{-c_3/\rho_S\lambda_0}\right)^M \left(\frac{c_3}{\rho_S\lambda_0}\right)^{N-M} \\ &\approx \binom{N}{M} \left(\frac{c_3}{\rho_S\lambda_0}\right)^{N-M}. \end{aligned} \tag{41}$$

Specifically, when $M = 0$, we have

$$\Pr\{|S_D| = 0\} \approx \left(\frac{c_3}{\rho_S\lambda_0}\right)^N. \tag{42}$$

By substituting (39), (40), and (41) into (34), we can get the asymptotic expression on the outage probability

$$P_{O,n^*} = \left(\frac{c_3}{\rho_S \lambda_0}\right)^N + \sum_{M=1}^{N} \binom{N}{M} \left(\frac{c_3}{\rho_S \lambda_0}\right)^{N-M} \left(-\frac{\gamma_S}{\mu}\right)^M G(M,M). \quad (43)$$

Particularly, when the system is interference limited, i.e., $N_0 = 0$, we get

$$P_{O,n^*} \approx \sum_{M=1}^{N} \binom{N}{M} \left(\frac{c_3}{\rho_S \lambda_0}\right)^{N-M} \left(-\frac{\gamma_S}{\mu}\right)^M G(M,M) \approx \left(-\frac{\gamma_S}{\mu}\right)^N G(N,N). \quad (44)$$

From the asymptotic expression in (43) and (44), we can have the following remarks. (a) The asymptotic expression of the secrecy outage probability is jointly determined by the SNR, MER, and the antenna number. (b) For the interference limited system, the secrecy outage probability is only determined by the MER, and the diversity order of the outage probability equals the number of the antennas.

4. Simulation Results

In this section, we provide numerical results to verify the theoretical analysis, which shows the impacts of the system parameters, such as MER (μ), the number of antennas (N), the power allocation factor (α_1), and the rate requirement (R_S, R_2) on the secrecy outage probability as well as the asymptotic results. The Rayleigh fading channels are used in our simulation cases for all links in the NOMA relaying networks. Without loss of generality, in all simulation cases, we set that the transmission power of the relay is the same as that of the source station.

As a function of SNR (ρ_S), the effects of N on the outage probability is shown in Figure 2 with μ = 24dB. We set γ_S = 60dB, $R_1 = R_2$ = 1bps/Hz, R_S = 0.1bps/Hz, and λ_0 = 10, and the antenna number changes from 1 to 3. From this figure, we can see that large N can introduce extra freedom the wireless fading channels, which can improve the outage probability with low SNR region. Also, when SNR grows to be large enough, an error floor occurs for the outage probability, which is determined by the MER and the antenna number. The reason is that when SNR approaches infinity, the bottleneck of the system performance is the interference introduced by NOMA protocol.

Figure 3 shows the effects of λ_0 on the outage probability as a function of SNR. The value of λ_0 changes from 1, 5 to 10. From this figure, we find that large λ_0 means that the average fading power of the first slot is large, which can obviously enlarge the size of the decoding antenna subset S_D. Thus, the secrecy outage probability can be reduced.

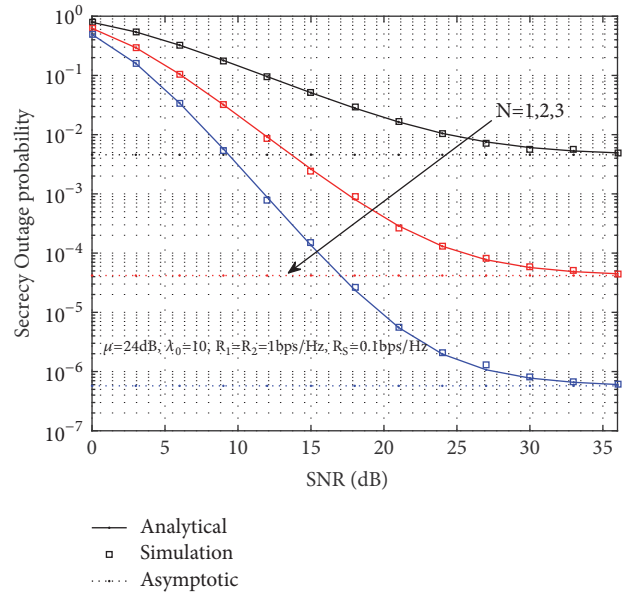


Figure 2: Secrecy outage probability versus SNR ρ_S with different N.

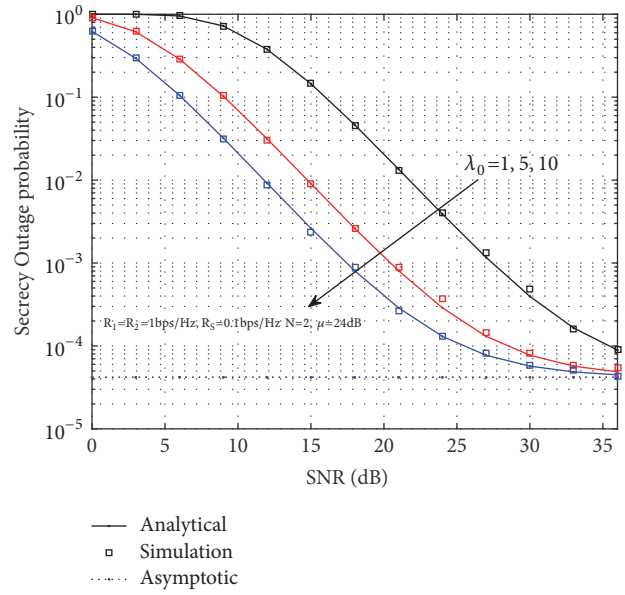


Figure 3: Secrecy outage probability versus SNR ρ_S with different λ_0.

Figure 4 shows the effects of power allocation factor α_1 on the outage probability as a function of SNR. The value of α_1 changes as 0.8, 0.9, and 0.95. Under this configuration, we can see that small α_1 can get better system performance. The reason is that, in this case, the bottleneck is the capacity of data stream x_2. Small α_1 means more power can be allocated for x_2, which can improve the secrecy outage probability.

The effects of R_2 on the outage probability are depicted in Figure 5 with R_S = 0.1bps/Hz as a function of SNR. The value of R_2 changes from 1.0 and 1.5 to 2.0 bps/Hz. Since small R_2

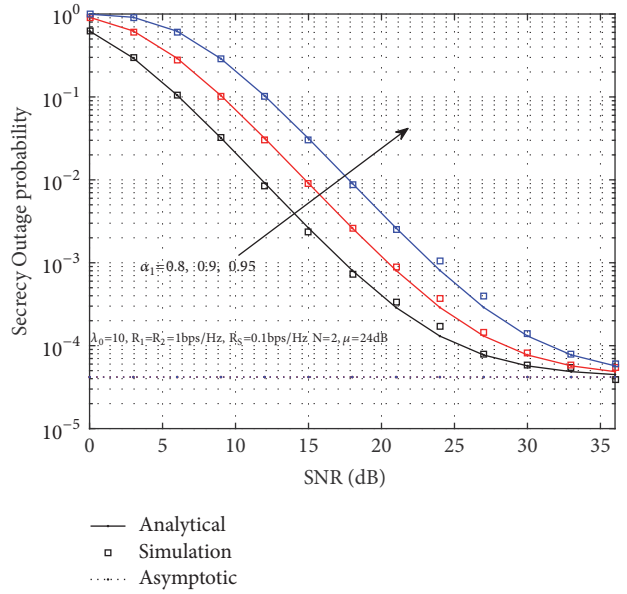


FIGURE 4: Secrecy outage probability versus SNR ρ_S with different α_1.

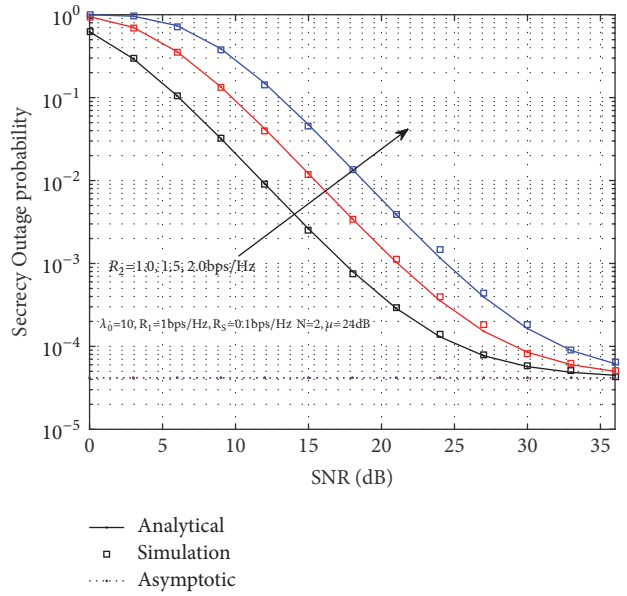


FIGURE 5: Secrecy outage probability versus SNR ρ_S with different R_2.

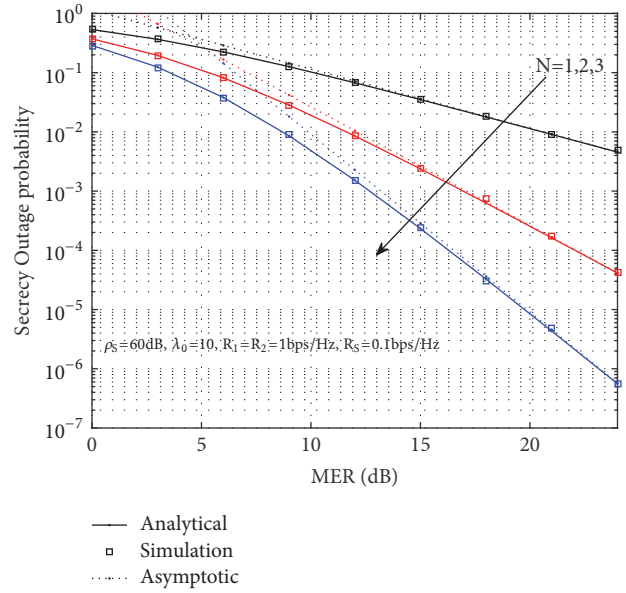


FIGURE 6: Secrecy outage probability versus MER μ.

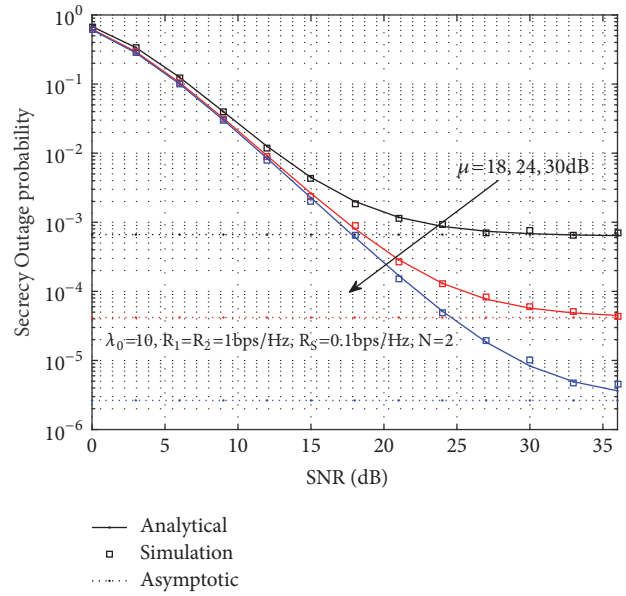


FIGURE 7: Secrecy outage probability versus SNR ρ_S with different μ.

can enlarge the size of S_D, large freedom for the second hop can be obtained to improve the secure performance. Thus, we can see from the figure that small R_2 can significantly improve the outage performance.

As a function of MER μ, the analytical SOP in (34) and (44) for cooperative NOMA system is present in Figure 6. Considering the interference limited scenarios, we set γ_S = 60dB, R_1 = R_2 = 1bps/Hz, R_S = 0.1bps/Hz, and λ_0 = 10, and the number of antennas N increases from 1 to 3. From this figure, it is seen that the analytical SOP curves match the simulation SOP curves well in all regions, while, in the high SNR region, the simulation SOP curves converge to that of the asymptotic line. The accuracy of the theoretical analysis can be verified in all the simulation cases. Furthermore, we find that the diversity order of the outage probability is equal to the number of the antennas.

The effects of μ on the outage probability with N = 2 is shown in Figure 7. We can see that, in high SNR region, all lines approach an error floor, and small μ results in worse outage performance. The reason is that μ denotes the average fading power of the main-to-eavesdropper ration, and large μ can lower the outage probability of the system.

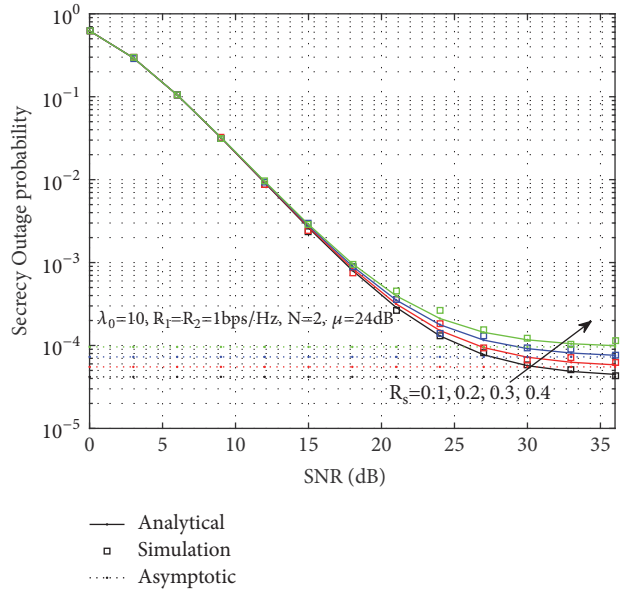


FIGURE 8: Secrecy outage probability versus SNR ρ_S with different R_S.

Figure 8 shows the effects of R_S on the outage probability with $\mu = 24$dB as a function of SNR. The other parameters are set as the same as Figure 7. The value of R_S is set as 0.1 and 0.4. We can see from the figure that small R_S can lower the outage probability, which is consistent with intuition.

5. Conclusion

In this paper, we propose an optimal antenna selection algorithm to enhance the secure performance for DF cooperative NOMA networks. The exact analytical expressions on the secrecy outage performance are derived, as well as the asymptotic results in the high regime of signal-to-noise ratio (SNR) and main-to-eavesdropper ratio (MER). From the analytical and asymptotic expressions, we find that the system secure performance is highly dependent on the system parameters such as the number of antennas at the relay, SNR, and MER. Specifically, the secrecy diversity order of the system is equal to the antenna number, when the interference from the second user is limited. In the future works, we will incorporate other wireless transmission techniques such as the works in [57–61], in order to further enhance the system performance and ensure the secure communications.

Appendix

A. Proof of Lemma 1

Considering the definition of $G(M,k)$, by using the binomial theorem, we can easily find that $G(M,0) = -1$. Applying variable substitution on $G(M,1)$, we have

$$\begin{aligned} G(M,1) &= \sum_{m=1}^{M} \binom{M}{m} (-1)^m m \\ &= -M \sum_{m=1}^{M} \binom{M-1}{m-1} (-1)^{m-1} \\ &= -M \sum_{m=0}^{M-1} \binom{M-1}{m} (-1)^m = 0. \end{aligned} \tag{A.1}$$

Similarly, we can prove $G(M,2) = 0$.

Generally, consider the definition of $G(M,k)$, and we have

$$\begin{aligned} G(M,k) &= \sum_{m=1}^{M} \binom{M}{m} (-1)^m m^k \\ &= -M \sum_{m=1}^{M} \binom{M-1}{m-1} (-1)^{m-1} m^{k-1} \\ &= -M \sum_{m=1}^{M} \binom{M-1}{m-1} (-1)^{m-1} (m-1+1)^{k-1}. \end{aligned} \tag{A.2}$$

By applying binomial theorem on $G(M,k)$, we have

$$\begin{aligned} &G(M,k) \\ &= -M \sum_{m=1}^{M} \binom{M-1}{m-1} (-1)^{m-1} \\ &\quad \cdot \left[1 + \sum_{j=1}^{k-1} \binom{k-1}{j} (m-1)^j \right] \\ &= -M \sum_{m=0}^{M-1} \binom{M-1}{m} (-1)^m \left[1 + \sum_{j=1}^{k-1} \binom{k-1}{j} (m)^j \right] \\ &= -M \sum_{m=0}^{M-1} \binom{M-1}{m} (-1)^m \sum_{j=1}^{k-1} \binom{k-1}{j} (m)^j \\ &= -M \sum_{j=1}^{k-1} \sum_{m=1}^{M-1} \binom{M-1}{m} (-1)^m \binom{k-1}{j} m^j \\ &= -M \sum_{j=1}^{k-1} \binom{k-1}{j} G(M-1,j). \end{aligned} \tag{A.3}$$

Since $G(M,1) = G(M,2) = 0$, according to (A.3), we obtain $G(M,3) = 0$. Furthermore, with mathematical induction, we can prove that $G(M,k) = 0$, $\forall k = 1,2,\ldots,(M-1)$.

Lemma 1 is proved.

B. Proof of Lemma 2

Proof. For $x \to 0$, using the series expansion equation that $1/(1+x) = \sum_{m=0}^{\infty}(-1)^m x^m$, we have

$$\begin{aligned} A_N &= \sum_{k=0}^{N} \binom{N}{k} \frac{(-1)^k}{1+k\delta} \\ &= \sum_{k=0}^{N} \binom{N}{k} (-1)^k \sum_{m=0}^{\infty} (-1)^m (k\delta)^m \\ &= \sum_{m=0}^{\infty} (-\delta)^m \sum_{k=0}^{N} \binom{N}{k} (-1)^k k^m. \end{aligned} \tag{B.1}$$

By using Lemma 1, we have

$$\begin{aligned} A_N &= \sum_{m=0}^{\infty} (-\delta)^m \sum_{k=1}^{N} \binom{N}{k} (-1)^k k^m \\ &= \sum_{m=0}^{\infty} (-\delta)^m G(N,m). \end{aligned} \tag{B.2}$$

Since $\delta \to 0$, we can ignore the high order items. Thus, A_N can be rewritten as

$$A_N \approx (-\delta)^N G(N,N). \tag{B.3}$$

Lemma 2 is proved. □

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

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

Acknowledgments

This work was supported in part by the Scientific Research Project of Education Department of Guangdong, China, under Grant 2017GKTSCX045, in part by the Science and Technology Program of Guangzhou, China, under Grant 201707010389, 201807010103 and 201804010127, in part by the Scientific Research Project of Guangzhou Municipal University under Grant 1201620439, in part by the Qingshanhu Young Scholar Program in GZPYP under Grant 2016Q001, and in part by Comba Research Funds under Grant H2017007, in part by the Guangdong Natural Science Funds for Distinguished Young Scholar under Grant 2014A030306027, in part by the Innovation Team Project of Guangdong Province University under Grant 2016KCXTD017.

References

[1] G. Huang, Q. Zhang, and J. Qin, "Joint Time Switching and Power Allocation for Multicarrier Decode-and-Forward Relay Networks with SWIPT," *IEEE Signal Processing Letters*, vol. 22, no. 12, pp. 2284–2288, 2015.

[2] H. Marshoud, P. C. Sofotasios, S. Muhaidat, G. K. Karagiannidis, and B. S. Sharif, "On the Performance of Visible Light Communication Systems with Non-Orthogonal Multiple Access," *IEEE Transactions on Wireless Communications*, vol. 16, no. 10, pp. 6350–6364, 2017.

[3] X. Liu, F. Li, and Z. Na, "Optimal Resource Allocation in Simultaneous Cooperative Spectrum Sensing and Energy Harvesting for Multichannel Cognitive Radio," *IEEE Access*, vol. 5, pp. 3801–3812, 2017.

[4] M. Shirvanimoghaddam, M. Condoluci, M. Dohler, and S. J. Johnson, "On the Fundamental Limits of Random Non-Orthogonal Multiple Access in Cellular Massive IoT," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2238–2252, 2017.

[5] G. Liu, H. Liu, H. Chen, C. Zhou, and L. Shu, "Position-based adaptive quantization for target location estimation in wireless sensor networks using one-bit data," *Wireless Communications and Mobile Computing*, vol. 16, no. 8, pp. 929–941, 2016.

[6] G. Huang and D. Tang, "Wireless Information and Power Transfer in Two-Way OFDM Amplify-and-Forward Relay Networks," *IEEE Communications Letters*, vol. 20, no. 8, pp. 1563–1566, 2016.

[7] W. Tan, M. Matthaiou, S. Jin, and X. Li, "Spectral Efficiency of DFT-Based Processing Hybrid Architectures in Massive MIMO," *IEEE Wireless Communications Letters*, 2017.

[8] X. Liu, X. Zhang, M. Jia, L. Fan, W. Lu, and X. Zhai, "5G-based green broadband communication system design with simultaneous wireless information and power transfer," *Physical Communication*, vol. 28, pp. 130–137, 2018.

[9] Z. Ding, P. Fan, and H. V. Poor, "Random Beamforming in Millimeter-Wave NOMA Networks," *IEEE Access*, vol. 5, pp. 7667–7681, 2017.

[10] J. Li, X. Jiang, Y. Yan, W. Yu, S. Song, and M. H. Lee, "Low Complexity Detection for Quadrature Spatial Modulation Systems," *Wireless Personal Communications*, vol. 95, no. 4, pp. 4171–4183, 2017.

[11] 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.

[12] 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.

[13] Z. Ding, H. Dai, and H. V. Poor, "Relay Selection for Cooperative NOMA," *IEEE Wireless Communications Letters*, vol. 5, no. 4, pp. 416–419, 2016.

[14] M. F. Kader, M. B. Shahab, and S. Y. Shin, "Exploiting Non-Orthogonal Multiple Access in Cooperative Relay Sharing," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1159–1162, 2017.

[15] Z. Huang, S. Liu, X. Mao, K. Chen, and J. Li, "Insight of the protection for data security under selective opening attacks," *Information Sciences*, vol. 412-413, pp. 223–241, 2017.

[16] J. Li, Z. Liu, X. Chen, F. Xhafa, X. Tan, and D. S. Wong, "L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing," *Knowledge-Based Systems*, vol. 79, pp. 18–26, 2015.

[17] T. Li, J. Li, Z. Liu, P. Li, and C. Jia, "Differentially private Naive Bayes learning over multiple data sources," *Information Sciences*, vol. 444, pp. 89–104, 2018.

[18] J. Li, X. Chen, X. Huang et al., "Secure distributed deduplication systems with improved reliability," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 64, no. 12, pp. 3569–3579, 2015.

[19] J. Li, X. Chen, S. S. Chow, Q. Huang, D. S. Wong, and Z. Liu, "Multi-authority fine-grained access control with accountability and its application in cloud," *Journal of Network and Computer Applications*, vol. 112, pp. 89–96, 2018.

[20] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying with Cochannel Interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1494–1505, 2016.

[21] X. Lai, J. Xia, M. Tang, H. Zhang, and J. Zhao, "Cache-aided multiuser cognitive relay networks with outdated channel state information," *IEEE Access*, vol. 6, pp. 21879–21887, 2018.

[22] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[23] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy Cooperative Networks with Outdated Relay Selection over Correlated Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7599–7603, 2017.

[24] H. Xu, L. Sun, P. Ren, Q. Du, and Y. Wang, "Cooperative Privacy Preserving Scheme for Downlink Transmission in Multiuser Relay Networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 825–839, 2017.

[25] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying over Correlated Fading Channels," *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 2811–2820, 2017.

[26] G. Pan, H. Lei, Y. Deng et al., "On Secrecy Performance of MISO SWIPT Systems with TAS and Imperfect CSI," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 3831–3843, 2016.

[27] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Communications*, vol. 14, no. 12, pp. 1–14, 2017.

[28] R. Zhao, Y. Yuan, L. Fan, and Y.-C. He, "Secrecy Performance Analysis of Cognitive Decode-and-Forward Relay Networks in Nakagami-m Fading Channels," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 549–563, 2017.

[29] H. Lei, J. Zhang, K.-H. Park et al., "On Secure NOMA Systems with Transmit Antenna Selection Schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.

[30] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access," *IEEE Communications Letters*, vol. 20, no. 5, pp. 930–933, 2016.

[31] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure Beamforming in Downlink MISO Nonorthogonal Multiple Access Systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7563–7567, 2017.

[32] D. Deng, L. Fan, X. Lei, W. Tan, and D. Xie, "Joint user and relay selection for cooperative NOMA networks," *IEEE Access*, vol. 2017, no. 5, pp. 20220–20227, 2017.

[33] Z. Yang, Z. Ding, Y. Wu, and P. Fan, "Novel relay selection strategies for cooperative NOMA," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 99, pp. 10114–10123, 2017.

[34] X. Yue, Y. Liu, S. Kang, and A. Nallanathan, "Performance Analysis of NOMA with Fixed Gain Relaying over Nakagami-m Fading Channels," *IEEE Access*, vol. 5, pp. 5445–5454, 2017.

[35] X. Liang, Y. Wu, D. W. K. Ng, Y. Zuo, S. Jin, and H. Zhu, "Outage Performance for Cooperative NOMA Transmission with an AF Relay," *IEEE Communications Letters*, vol. 21, no. 11, pp. 2428–2431, 2017.

[36] W. Tan, S. Jin, C. Wen, and T. Jiang, "Spectral efficiency of multi-user millimeter wave systems under single path with uniform rectangular arrays," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, 2017.

[37] X. Liu, M. Jia, X. Gu, and X. Tan, "Optimal periodic cooperative spectrum sensing based on weight fusion in cognitive radio networks," *Sensors*, vol. 13, no. 4, pp. 5251–5272, 2013.

[38] G. Huang and W. Tu, "Optimal resource allocation in wireless-powered OFDM relay networks," *Computer Networks*, vol. 104, pp. 94–107, 2016.

[39] D. Deng, M. Yu, J. Xia, Z. Na, J. Zhao, and Q. Yang, "Wireless powered cooperative communications with direct links over correlated channels," *Physical Communication*, vol. 28, pp. 147–153, 2018.

[40] J. Li, M. Wen, X. Jiang, and W. Duan, "Space-Time Multiple-Mode Orthogonal Frequency Division Multiplexing with Index Modulation," *IEEE Access*, vol. 5, pp. 23212–23222, 2017.

[41] X. Wang, H. Zhang, L. Fan, and Y. Li, "Performance of Distributed Switch-and-Stay Combining for Cognitive Relay Networks with Primary Transceiver," *Wireless Personal Communications*, vol. 97, no. 2, pp. 3031–3042, 2017.

[42] X. Liu, M. Jia, X. Gu, J. Yan, and J. Zhou, "Optimal spectrum sensing and transmission power allocation in energy-efficiency multichannel cognitive radio with energy harvesting," *International Journal of Communication Systems*, vol. 30, no. 5, p. e3044, 2017.

[43] J. Yuan, S. Jin, W. Xu, W. Tan, M. Matthaiou, and K.-K. Wong, "User-Centric Networking for Dense C-RANs: High-SNR Capacity Analysis and Antenna Selection," *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 5067–5080, 2017.

[44] X. Jiang, M. Wen, H. Hai, J. Li, and S. Kim, "Secrecy-Enhancing Scheme for Spatial Modulation," *IEEE Communications Letters*, vol. 22, no. 3, pp. 550–553, 2018.

[45] G. Huang and W. Tu, "Wireless Information and Energy Transfer in Nonregenerative OFDM AF Relay Systems," *Wireless Personal Communications*, vol. 94, no. 4, pp. 3131–3146, 2017.

[46] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[47] H. A. David and H. N. Nagaraja, *Order Statistics*, Wiley Online Library, 3rd edition, 2003.

[48] H. Wu, Y. Liao, Y. Ding, H. Wang, C. Peng, and S. Yin, "Engineering thermal and mechanical properties of multilayer aligned fiber-reinforced aerogel composites," *Heat Transfer Engineering*, vol. 35, no. 11-12, pp. 1061–1070, 2014.

[49] J. Deng, Z. John Ma, A. Liu, S. Cao, and B. Zhang, "Seismic Performance of Reinforced Concrete Bridge Columns Subjected to Combined Stresses of Compression, Bending, Shear, and Torsion," *Journal of Bridge Engineering*, vol. 22, no. 11, p. 04017099, 2017.

[50] Y. Liang, H. Wu, G. Huang, J. Yang, and H. Wang, "Thermal performance and service life of vacuum insulation panels with aerogel composite cores," *Energy and Buildings*, vol. 154, pp. 606–617, 2017.

[51] J. Deng, A. Liu, Q. Yu, and G. Peng, "Seismic performances of steel reinforced concrete bridge piers," *Steel and Composite Structures*, vol. 21, no. 3, pp. 661–677, 2016.

[52] J. Yang, H. Wu, M. Wang, and Y. Liang, "Prediction and optimization of radiative thermal properties of nano TiO2

assembled fibrous insulations," *International Journal of Heat and Mass Transfer*, vol. 117, pp. 729–739, 2018.

[53] J. Yang, H. Wu, M. Wang, S. He, and H. Huang, "Prediction and optimization of radiative thermal properties of ultrafine fibrous insulations," *Applied Thermal Engineering*, vol. 104, pp. 394–402, 2016.

[54] J. Deng, A. Liu, P. Huang, and X. Zheng, "Interfacial mechanical behaviors of RC beams strengthened with FRP," *Structural Engineering and Mechanics*, vol. 58, no. 3, pp. 577–596, 2016.

[55] J. Yang, H. Wu, S. He, and M. Wang, "Prediction of thermal conductivity of fiber/aerogel composites for optimal thermal insulation," *Journal of Porous Media*, vol. 18, no. 10, pp. 971–984, 2015.

[56] J. Deng, A. Liu, Z. Ma, P. Huang, and R. Zhou, "Interfacial behavior of RC beams strengthened with FRP under fatigue loading," *Advances in Structural Engineering*, vol. 18, no. 2, pp. 283–293, 2015.

[57] J. Xia, F. Zhou, X. Lai et al., "Cache Aided Decode-and-Forward Relaying Networks: From the Spatial View," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 5963584, 9 pages, 2018.

[58] X. Liu, Y. Wang, Y. Chen et al., "A Multichannel Cognitive Radio System Design and Its Performance Optimization," *IEEE Access*, vol. 6, pp. 12327–12335, 2018.

[59] F. Shi, L. Fan, X. Liu, Z. Na, and Y. Liu, "Probabilistic Caching Placement in the Presence of Multiple Eavesdroppers," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 2104162, 10 pages, 2018.

[60] X. Liu, M. Jia, X. Gu, F. Kong, and Q. Jing, "Optimal joint allocation of multislot spectrum sensing and transfer power in multichannel cognitive radio," *Journal of Sensors*, vol. 2014, Article ID 2104162, 9 pages, 2014.

[61] F. Zhou, L. Fan, X. Lei, G. Luo, H. Zhang, and J. Zhao, "Edge Caching With Transmission Schedule for Multiuser Multirelay Networks," *IEEE Communications Letters*, vol. 22, no. 4, pp. 776–779, 2018.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 9637610, 15 pages
https://doi.org/10.1155/2018/9637610

Research Article

Exploiting Uplink NOMA to Improve Sum Secrecy Throughput in IoT Networks

Zhongwu Xiang, Weiwei Yang, Yueming Cai, Yunpeng Cheng, Heng Wu, and Meng Wang

Army Engineering University of PLA, 210007, Nanjing, China

Correspondence should be addressed to Weiwei Yang; wwyang1981@163.com

Received 14 February 2018; Revised 17 May 2018; Accepted 5 June 2018; Published 2 July 2018

Academic Editor: Li Sun

This paper exploits nonorthogonal multiple access (NOMA) to enhance the uplink secure transmission in Internet of Things (IoT) networks. Considering the different intercept ability of eavesdroppers (Eve), secrecy performances of both strong and weak Eve wiretap scenarios have been investigated. In strong Eve wiretap scenario (SWS), Eve is assumed to be powerful enough to decode message without interference and, in weak Eve wiretap scenario (WWS), Eve is assumed to have significant demodulation capability constraint. The new closed-form expressions of joint connection outage probability (JCOP), joint secrecy outage probability (JSOP), and sum secrecy throughput (SST) are derived in these two scenarios to indicate the impact of parameters, i.e., transmit power, codeword rate, and the placement of devices, on security performance. In order to demonstrate the superiority of NOMA, we also investigate the secrecy performance of orthogonal multiple access (OMA) system as a benchmark. Analysis results show that the performance in WWS is always better than that in SWS and, in low signal-to-noise ratio (SNR) or high codeword rate region, the performances of these two scenarios are close. In addition, we present the condition that NOMA outperforms OMA in terms of SST. Moreover, the placements of devices are significant to the SST performance of NOMA system. The suboptimal device placement scheme has been designed to maximize SST. Analysis results demonstrate that when Eve is far away from legal users, the suboptimal results tend to optimal.

1. Introduction

Internet of Things (IoT) offers a challenging notion of creating a world where all the things are connected via smart devices [1]. Various scenarios can be served by IoT networks, many of them concerning confidential or privacy information, such as Mobile Payment and Smart Healthcare. Due to the openness of the wireless medium, wireless communication networks are particularly susceptible to be eavesdropped [2]. The security of wireless IoT networks is a critical issue [3, 4]. Furthermore, the nodes in IoT networks are comprised of large number of machine-type communication (MTC) devices with power constraint and limited signal processing capability [5]. Consequently, traditional cryptography requiring high computing complexity is not practical for IoT systems when the devices' communication resources are constrained.

Physical layer security (PLS) technology may be a promising solution for securing the IoT transmission. Compared with cryptography, it is a simple, lightweight, and efficient security scheme [6]. Various physical layer techniques have been proposed for improving security, such as relay selection transmission [7, 8] and artificial noise/jamming and beamforming [9, 10]. In particular, in resource-constrained system, [11] adopted energy harvesting to improve secrecy energy efficiency in physical layer. The study [12] improved secure spectrum efficiency and energy efficiency tradeoff by optimizing system parameters. The works [13] and [14] designed a lightweight secure modulation scheme and an on-off transmission scheme, respectively. And [15] introduced an opportunistic jamming scheme to enhance transmission security for low complexity devices. Recently, in IoT networks, PLS has become a popular technique for secure transmission. The study [5] provided some promising lightweight and low complexity PLS techniques for IoT. And [16] proposed a new compressed sensing security transmission model in IoT systems. Secrecy performance was analyzed in IoT networks under eavesdropper collusion [17]. The work [18]

focused on designing a transmission scheme for securing relay communications in IoT networks.

On the other hand, nonorthogonal multiple access (NOMA) has been presented as a promising solution to increase connectivity in massive IoT applications [19–21]. The study [20] designed a new multiple-input multiple-output NOMA scheme severing two users with different quality of service (QoS) demand, which share the same nonorthogonal resources by adopting NOMA protocol. An uplink NOMA-based multiple access strategy for cellular massive IoT was proposed in [21], in which multiple devices share the same subband and base station performs successive interference cancellation (SIC) to distinguish the messages from different devices. By adopting NOMA concept, the strict limitations of the amount of resources can be broken and enabling more devices to be supported in IoT networks. Furthermore, NOMA can be introduced as a low complexity solution to enhance secure downlink transmission [22–29]. Specifically, [27] demonstrated that the secrecy rate of a multiple-input single-output (MISO) NOMA system is higher than that of orthogonal multiple access (OMA) system. In addition, in a NOMA assisted multicast-unicast scheme, security unicasting rate achieved by NOMA is larger than or equal to that of OMA [28]. Moreover, [29] studied the performance gain of NOMA over OMA and indicated that the NOMA scheme always outperforms OMA scheme. However, to the best of our knowledge, there is no published work that studies the PLS in NOMA-based IoT networks.

NOMA can be applied in both uplink and downlink [30]. By using SIC, the receiver can detect the intended information from superposition signals [24, 28]. However, the process of SIC increases the signal processing complexity and imposes a high demand of detection capability at receiver. Notably, [24–29] all assumed that the SIC is performed ideally. It is overoptimistic, especially when the receivers have significant communication resources constraint. When adopting NOMA concept at uplink, the devices do not need to use SIC, which reduces its signal processing complexity. In addition, it becomes reasonable to assume that the SIC is applied perfectly, because the receiver is usually a base station or an access point with powerful detection capability in IoT networks. Significantly, it is a multiuser communication scenario which makes the analysis of PLS different from that in downlink NOMA systems. As far as we know, the PLS performance of uplink NOMA in IoT networks has not been investigated. The secure communication of uplink NOMA in IoT networks is worthy of our attention. Then, a fundamental question arises to be addressed: *Can NOMA enhance the secrecy performance in IoT networks?*

Because various scenarios are served by IoT networks, the wiretapping scenario also can be in variety. In this paper, two scenarios, i.e., strong eavesdropper (Eve) wiretap scenario (SWS) and weak Eve wiretap scenario (WWS), are considered according to the detection capability of Eve. In addition, we introduce uplink NOMA to enhance secure transmission of IoT networks in these two scenarios. Moreover, a low complexity device placement scheme is proposed to further enhance the security of uplink NOMA-based IoT networks. Our principal contributions are summarized as follows:

(i) We first exploit uplink NOMA to improve security performance in IoT networks. The new closed-form expressions of joint connection outage probability (JCOP), joint secrecy outage probability (JSOP), and sum secrecy throughput (SST) are derived both in SWS and WWS. The impact of different detection capability of Eve on secrecy performance is investigated. Analysis results show that the transmission in WWS is always securer than that in SWS and, in low signal-to-noise ratio (SNR) or high codeword rate region, secrecy performances in WWS and SWS are close.

(ii) The performance of OMA-based benchmark system is analyzed. We present the condition that NOMA outperforms OMA in terms of SST, which shows that in high SNR or low codeword rate region NOMA is likely outperforming OMA and when channel states (CS) of devices are very different, NOMA tends to get a high performance gain on OMA.

(iii) We introduce a device placement method and formulate it as an optimization problem for further improving SST. However, it is a multiparameter and nonconvex optimization problem which is challenging for results derivation. A practical scheme is provided and we propose an upper bound of the SST. In SWS, we can only obtain the suboptimal results. However, in WWS, optimal results are available in some cases. Analysis results show that when Eve is far away from legal users, SST obtained from our device placement scheme becomes close to its upper bound tightly, which indicates that the suboptimal results tend to be optimal.

(iv) By simulation, we confirm the accuracy of our analysis including security performance and device placement method. In addition, simulation results show that there is an optimal desired transmission SNR or codeword rate which maximizes the SST both in WWS and in SWS. Moreover, in low SNR region or high codeword rate region, results from our device placement scheme are also close to their upper bound tightly.

The rest of the paper is organized as follows. The uplink NOMA-based IoT networks and channel model are introduced in Section 2. In Section 3, we derive a set of closed-form expressions of secrecy performance in three scenarios. Section 4 introduces a security enhancing methods. We formulate the optimization problem of this method and give the suboptimal solutions. The security performance and optimal solutions are verified by numerical and simulation results in Section 5. Finally, Section 6 concludes the paper.

2. Network Model

In this paper, we consider an uplink NOMA-based IoT network. Considering a passive wiretap scenario, the detection capability of Eve is unknown. In addition, various scenarios served by IoT networks result in the variety kinds of Eve.

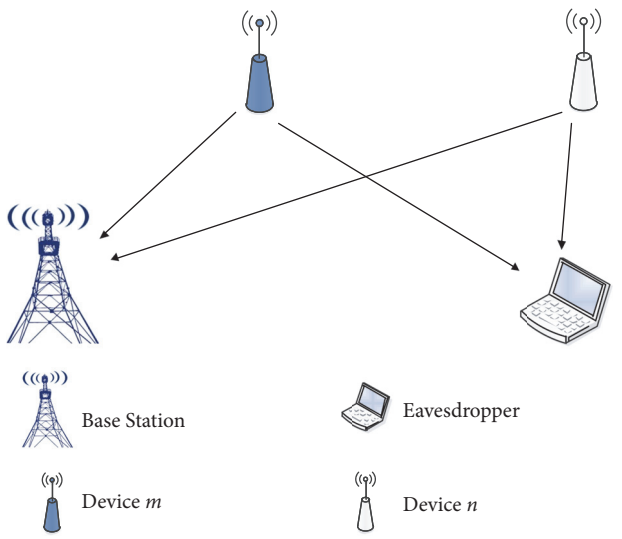


Figure 1: Network model for uplink NOMA IoT system.

For simplifying the analysis, we consider two extreme wiretap scenarios, i.e., strong Eve wiretap scenario and weak Eve wiretap scenario, according to the detection capability of Eve. Uplink NOMA scheme enables one receiver to serve multiple devices simultaneously. It is worth noticing that two users' scheme was selected for performing NOMA in 3GPP LTE Advanced [31]. We also consider a two users' uplink power-domain NOMA scheme in IoT networks. These two users denoted as device n and device m are grouped as a device pair. As shown in Figure 1, the pair devices transmit confidential message to a base station under the malicious attempt of the Eve. The received signal at base station (BS) and Eve can be expressed as

$$y_B = h_n s_n \sqrt{L(d_n) P_n} + h_m s_m \sqrt{L(d_m) P_m} + n_B, \quad (1)$$

$$y_e = h_{en} s_n \sqrt{L(d_{en}) P_n} + h_{em} s_m \sqrt{L(d_{em}) P_m} + n_e, \quad (2)$$

respectively, where P_m and P_n denote the transmit power of device m and device n and s_m, s_n are the normalized message for device m and device n, respectively. n_B, n_e denote the zero-mean additive white Gaussian noise (AWGN) at base station and Eve, which are assumed to have the same variance σ_n^2. d_m, d_n are the distance between devices and BS, respectively, and d_{em}, d_{en} are the distance between devices and Eve. $L(x) = 1/x^{\alpha}$ is the path loss with fading exponent α. h_m, h_n, h_{em}, h_{en} are small-scale fading coefficients, which are supposed to obey independent and identical complex Gaussian distribution with zero mean and variance is σ^2 [24]. We assume that transmit power of devices is fixed and equal; i.e., $P_n = P_m = P$.

2.1. Channel Capacity of Base Station. According to the protocol of NOMA, device m and device n transmit message to the BS at the same time and frequency. The nonorthogonal messages are overlapped and interfered by each other. In order to distinguish the mixing messages, SIC is widely adopted. Based on the principle of SIC, the message with stronger power is demodulated first under the interference from another device. And, then, remodulate the demodulated message and deduct it from the overlapping signal. In an ideal situation, the remained message is pure for another device [24]. The impact of the path loss is generally more dominant than small scaling fading effects. In addition, transmit powers of the two devices are assumed to be the same. Hence, the decoding order is dependent on the distances between the devices and BS. Without loss of generality, we assume that the location of device m is closer to BS and demodulated first. According to the Shannon channel capacity formula, the channel capacity of device m and device n at BS can be expressed as

$$C_m = \log_2 \left(1 + \frac{\rho L(d_m) |h_m|^2}{\rho L(d_n) |h_n|^2 + 1} \right), \quad (3)$$

$$C_n = \log_2 \left(1 + \rho L(d_n) |h_n|^2 \right), \quad (4)$$

respectively, where $\rho = P/\sigma_n^2$ denotes transmit SNR. Because device m is interfered by device n, when ρ tends to infinite, C_m tends to a finite value, however with C_n tending to infinite.

2.2. Channel Capacity of Strong Eve. We consider a strong Eve which has equal or superior capability of BS. By applying powerful multiuser detection techniques, the overlapping messages from devices can be distinguished by the Eve perfectly [24]. In SWS, the channel capacity of devices m and n can be written as

$$C_{em}^s = \log_2 \left(1 + \rho L(d_{em}) |h_{em}|^2 \right), \quad (5)$$

$$C_{en}^s = \log_2 \left(1 + \rho L(d_{en}) |h_{en}|^2 \right), \quad (6)$$

respectively. For an infinite transmission SNR ρ, both the channel capacities of device m and device n at Eve are infinite value for SWS. Based on (3), when ρ tends to be infinite, the capacity of device m in legal channel is a finite value. It demonstrates that SWS is really a detrimental scenario for secure transmission.

2.3. Channel Capacity of Weak Eve. In WWS, the Eve has significant demodulation capability constraint, which can also be seen as a malignant device [28]. Because of limited demodulation capability, the interference from each other cannot be eliminated. Consequently, in WWS, the channel capacity of devices m and n at Eve can be expressed as

$$C_{em}^w = \log_2 \left(1 + \frac{\rho L(d_{em}) |h_{em}|^2}{\rho L(d_{en}) |h_{en}|^2 + 1} \right), \quad (7)$$

$$C_{en}^w = \log_2 \left(1 + \frac{\rho L(d_{en}) |h_{en}|^2}{\rho L(d_{em}) |h_{em}|^2 + 1} \right), \quad (8)$$

respectively. Both the capacities of device m and device n at Eve are limited by the interference from each other. Comparing with (3) and (4), the interference in WWS deteriorates the illegal channel more seriously than that in SWS. It shows that WWS is a relative secure wiretap scenario.

3. Secrecy Performance Analysis

In this section, we will study the secrecy performance in SWS, WWS, and OMA-based benchmark system. Considering the limitation of devices' ability, we assume a fix transmission rate situation. Based on the well-known Wyner wiretap code theorem [32], codeword rates and confidential information rates are fixed. We suppose that the statistic channel state information (CSI) of legal and illegal channel is available by legal devices. By the way, this assumption is adopted by many literatures [24, 28, 29]. Under these assumptions, we first analyze the reliability performance in NOMA system. And, then, the secrecy performance is studied in WWS, SWS, and OMA-based benchmark system. Finally, we compare the security performance between NOMA and OMA in terms of SST.

3.1. Reliability Performance of NOMA. Connection outage probability (COP) is a popular metric for reliability performance, which denotes the probability of legal channel capacity dropping below to the codeword rate [11]. We define the joint connection outage probability for the device pair as that of either the device n or device m outage. JCOP can be expressed in the following equation:

$$P_{co}\left(R_{n,t}, R_{m,t}\right) = 1 - \Pr\left[C_n > R_{n,t}, C_m > R_{m,t}\right], \quad (9)$$

where $R_{m,t}$ and $R_{n,t}$ are codeword rate of device m and deice n, respectively. The closed-form expression of JCOP is written as

$$P_{co}\left(\theta_{n,t}, \theta_{m,t}\right) = 1 - \frac{1}{1+\theta_{m,t}k_t} e^{-\left(\theta_{n,t}/k_t \rho\sigma^2 L(d_m) + \theta_{m,t}(1+\theta_{n,t})/\rho\sigma^2 L(d_m)\right)}, \quad (10)$$

where $\theta_{m,t} = 2^{R_{m,t}} - 1$, $\theta_{n,t} = 2^{R_{n,t}} - 1$, and $k_t = L(d_n)/L(d_m)$ which denotes the path loss ratio of device n to device m at BS.

Proof. Substituting (3) and (4) into (9), we can obtain

$$\begin{aligned} P_{co}\left(R_{n,t}, R_{m,t}\right) &= 1 - \Pr\left[\log\left(1 + \frac{\rho L\left(d_m\right)\left|h_m\right|^2}{\rho L\left(d_n\right)\left|h_n\right|^2 + 1}\right)\right. \\ &\quad \left. \geq R_{m,t}, \log\left(1 + \rho L\left(d_n\right)\left|h_n\right|^2\right) \geq R_{n,t}\right], \\ &= 1 - \Pr\left[\frac{\rho L\left(d_m\right)\left|h_m\right|^2}{\rho L\left(d_n\right)\left|h_n\right|^2 + 1} \geq \theta_{m,t}, \rho L\left(d_n\right)\left|h_n\right|^2\right. \\ &\quad \left. \geq \theta_{n,t}\right], \\ &= 1 - \int_{\theta_m(1+\theta_n)}^{\infty} \int_{\theta_n}^{x/\theta_m - 1} \frac{e^{-\left(x/\rho\sigma^2 L(d_m) + y/\rho\sigma^2 L(d_n)\right)}}{\left(\rho\sigma^2\right)^2 L\left(d_m\right) L\left(d_n\right)} dy dx. \end{aligned} \quad (11)$$

After some mathematical manipulations, the desired result can be easily derived.

From (10) we can find that when ρ tends to be infinite, P_{co} tends to $1 - 1/(1+\theta_{m,t}k_t)$ instead of zero. It demonstrates that the effect of ρ is limited for improving reliability performance. In addition, when k_t tends to zero, i.e., device n far away from BS, JCOP tends to 1, because COP of device n is always one. Due to the fact that (10) is not a monotonic function with k_t, there may exist an optimal k_t for maximizing the reliability performance. □

3.2. Secrecy Performance in SWS. Secrecy outage probability (SOP) is widely used to evaluate the secrecy performance, which denotes the probability of illegal channel capacity growing up to the redundancy rate [11]. We define the joint secrecy outage probability for the device pair as that of either the device n or device m outage, which is similar to the definition in [24]. Based on Wyner wiretap code theorem, the JSOP of device pair in SWS can be written as follows:

$$\begin{aligned} &P_{so}^{s}\left(R_{n,t}, R_{n,s}, R_{m,t}, R_{m,s}\right) \\ &\quad = 1 - \Pr\left[C_{en}^{w} < R_{n,t} - R_{n,s}, C_{em}^{w} < R_{m,t} - R_{m,s}\right], \end{aligned} \quad (12)$$

where $R_{m,s}, R_{n,s}$ are secrecy rate of device m and device n, respectively. $R_{n,t} - R_{n,s}$ and $R_{m,t} - R_{m,s}$ are redundancy rate. The closed-form expression of P_{so}^{s} can be written as

$$P_{so}^{s}\left(\theta_{n,s}, \theta_{m,s}\right) = 1 - \left(1 - e^{-\theta_{n,s}/k_s\gamma}\right)\left(1 - e^{-\theta_{m,s}/\gamma}\right), \quad (13)$$

where $\theta_{n,s} = 2^{R_{n,t} - R_{n,s}} - 1$, $\theta_{m,s} = 2^{R_{m,t} - R_{m,s}} - 1$, $\gamma = \rho\sigma^2 L(d_{em})$, and $k_s = L(d_{en})/L(d_{em})$. γ denotes the average receiving SNR of device m at Eve and k_s represents the path loss ratio of device n to device m at Eve.

Proof. Substituting (5) and (6) into (12), we can obtain

$$\begin{aligned} P_{so}^{s}\left(\theta_{n,s}, \theta_{m,s}\right) &= 1 - \Pr\left[\rho L\left(d_{en}\right)\left|h_{en}\right|^2\right. \\ &\quad \left. < \theta_{n,s}, \rho L\left(d_{em}\right)\left|h_{em}\right|^2 < \theta_{m,s}\right]. \end{aligned} \quad (14)$$

Because of the independence between $|h_{en}|^2$ and $|h_{em}|^2$, $P_{so}^{s}(\theta_{n,s}, \theta_{m,s})$ can be written as

$$\begin{aligned} P_{so}^{s}\left(\theta_{n,s}, \theta_{m,s}\right) &= 1 - \Pr\left[\rho L\left(d_{en}\right)\left|h_{en}\right|^2 < \theta_{n,s}\right] \\ &\quad \cdot \Pr\left[\rho L\left(d_{em}\right)\left|h_{em}\right|^2 < \theta_{m,s}\right] \end{aligned} \quad (15)$$

After some mathematical manipulations, (13) is obtained.

Obviously, (13) shows that P_{so}^{s} is a monotonic increasing function with γ and when γ tends to be infinite, P_{so}^{s} tends to unity. It indicates that high average receiving SNR at Eve is detrimental for secure transmitting. When k_s tends to zero, i.e., device n far away from Eve, JSOP tends to $e^{-\theta_{m,s}/\gamma}$ which is SOP of device m. It demonstrates that the transmit security of device n is guaranteed and JSOP is only determined by the SOP of device m.

JCOP denotes the reliability performance and JSOP represents the secrecy performance, which are inadequate to evaluate the efficiency performance of NOMA. However, in our definition, we consider these two devices as an entirety

and investigate the joint secrecy performance. Nonzero SST can not be obtained when any one of devices undergo outage. Joint secrecy performance is more interesting when these two devices are related and sum secrecy throughput is adopted as the metric for device pair, which represents sum transmission rate of device pair under the constraints of joint reliability and security. SST can be expressed as

$$\eta_s = \left(1 - P_{co}\right)\left(1 - P_{so}^{s}\right)\left(R_{m,s} + R_{n,s}\right). \tag{16}$$

From the analysis above, we can find that P_{co} and P_{so}^{s} are independent. The product of $(1 - P_{co})$ and $(1 - P_{so}^{s})$ represents the reliable and secure connection probability. $R_{m,s} + R_{n,s}$ is sum secrecy rate. Under the above definition, nonzero SST can not be obtained when any one of the devices undergo outage.

After substituting (10) and (13) into (16), the closed-form expression of η_s can be written as

$$\begin{aligned}\eta_s = {} & \frac{\left(R_{m,s} + R_{n,s}\right)}{1 + \theta_{m,t}k_t}\left(1 - e^{-\theta_{n,s}/k_s\gamma}\right)\left(1 - e^{-\theta_{m,s}/\gamma}\right) \\ & \times e^{-\left(\theta_{n,t}/k_t\rho\sigma^2 L(d_m) + \theta_{m,t}(1+\theta_{n,t})/\rho\sigma^2 L(d_m)\right)}.\end{aligned} \tag{17}$$

Equation (17) shows that SST is jointly determined by JCOP and JSOP. JCOP is a decrease function about transmit power. However, JSOP is an increase function about transmit power. Thus, SST may not be a monotonous function about transmit power, which means an optimal transmit power existed for maximizing SST. In addition, SST is also not a monotonous function about $R_{m,s}$ or $R_{n,s}$ and the secrecy rate can be optimized can be optimized for achieving better performance. Furthermore, due to the interference between devices, the location of device n which is determined by k_t and k_s has significant impact on network performance which will be further studied in the next section. □

3.3. Secrecy Performance in WWS. Similarly, the JSOP in WWS can be written as

$$\begin{aligned}& P_{so}^{w}\left(R_{n,t}, R_{n,s}, R_{m,t}, R_{m,s}\right) \\ & \quad = 1 - \Pr\left[C_{en}^{w} < R_{n,t} - R_{n,s}, C_{em}^{w} < R_{m,t} - R_{m,s}\right].\end{aligned} \tag{18}$$

The closed-form expression of P_{so}^{w} is

$$\begin{aligned}& P_{so}^{w}\left(\theta_{n,s}, \theta_{m,s}\right) \\ & = \begin{cases} \dfrac{k_s}{k_s + \theta_{n,s}}e^{-\theta_{n,s}/k_s\gamma} + \dfrac{1}{1 + k_s\theta_{m,s}}e^{-\theta_{m,s}/\gamma} & \theta_{m,s}\theta_{n,s} \geq 1 \\ \dfrac{k_s}{k_s + \theta_{n,s}}e^{-\theta_{n,s}/k_s\gamma} + \dfrac{1}{1 + k_s\theta_{m,s}}e^{-\theta_{m,s}/\gamma} - \dfrac{k_s\left(1 - \theta_{m,s}\theta_{n,s}\right)}{\left(1 + k_s\theta_{m,s}\right)\left(k_s + \theta_{n,s}\right)}e^{-\left(k_s\theta_{m,s}(1+\theta_{n,s}) + \theta_{n,s}(1+\theta_{m,s})\right)/k_s\gamma(1-\theta_{m,s}\theta_{n,s})} & \theta_{m,s}\theta_{n,s} < 1. \end{cases}\end{aligned} \tag{19}$$

Proof. See Appendix A. □

Based on (19), there are two different results when transmit power tends to be infinite. When $\theta_{m,s}\theta_{n,s} < 1$ JSOP tends to 1 and when $\theta_{m,s}\theta_{n,s} \geq 1$ JSOP tends to $k_s/(k_s + \theta_{n,s}) + 1/(1 + k_s\theta_{m,s})$. This is because higher codeword redundancy rates can increase secrecy performance. Furthermore, when k_s tends to zero, i.e., device n far away from Eve, JSOP tends to $e^{-\theta_{m,s}/\gamma}$. It demonstrates that when k_s tends to zero, SOP of device m is the only parameter affecting JSOP.

Similar to (16), the SST in WWS can be expressed as

$$\eta_w = \left(1 - P_{co}\right)\left(1 - P_{so}^{w}\right)\left(R_{m,s} + R_{n,s}\right). \tag{20}$$

By substituting (10) and (19) into (20), the closed-form expression of η_w can be directly derived as

$$\begin{aligned}& \eta_w \\ & = \begin{cases} \left(1 - \dfrac{k_s}{k_s + \theta_{n,s}}e^{-\theta_{n,s}/k_s\gamma} - \dfrac{1}{1 + k_s\theta_{m,s}}e^{-\theta_{m,s}/\gamma}\right)\dfrac{\left(R_{m,s} + R_{n,s}\right)}{1 + \theta_{m,t}k_t}e^{-\left(\theta_{n,t}/k_t\rho\sigma^2 L(d_m) + \theta_{m,t}(1+\theta_{n,t})/\rho\sigma^2 L(d_m)\right)} & \theta_{m,s}\theta_{n,s} \geq 1 \\ \left(1 - \dfrac{k_s}{k_s + \theta_{n,s}}e^{-\theta_{n,s}/k_s\gamma} - \dfrac{1}{1 + k_s\theta_{m,s}}e^{-\theta_{m,s}/\gamma} + \dfrac{k_s\left(1 - \theta_{m,s}\theta_{n,s}\right)}{\left(1 + k_s\theta_{m,s}\right)\left(k_s + \theta_{n,s}\right)}e^{-\left(k_s\theta_{m,s}(1+\theta_{n,s}) + \theta_{n,s}(1+\theta_{m,s})\right)/k_s\gamma(1-\theta_{m,s}\theta_{n,s})}\right) & \\ \times\dfrac{\left(R_{m,s} + R_{n,s}\right)}{1 + \theta_{m,t}k_t}e^{-\left(\theta_{n,t}/k_t\rho\sigma^2 L(d_m) + \theta_{m,t}(1+\theta_{n,t})/\rho\sigma^2 L(d_m)\right)} & \theta_{m,s}\theta_{n,s} < 1. \end{cases}\end{aligned} \tag{21}$$

Similar to SWS, SST in WWS also is jointly determined by JCOP and JSOP and an optimal transmit power $R_{m,s}$, $R_{n,s}$ or location of device n may be found to maximize SST. The expression of SST is rather complicated and the further insights will be investigated by numerical results and simulations.

Remark 1. Comparing (5) with (7) and (6) with (8), we can find that the capacity of illegal channel in SWS is always bigger than that in WWS. It demonstrates that the message in WWS is securer than that in SWS. In (17) and (21), we can also find the impacts of parameters, i.e., transmit

power, codeword rate, and the placements of devices, on SST performance. Among them, the placements of devices are special for NOMA system, determined by k_s and k_t. SST can be enhanced by optimizing k_s and k_t and we propose a further researching in Section 4.

3.4. Secrecy Performance in OMA-Based Benchmark System. In OMA system, different orthogonal resources are allocated to different devices. In order to get a fairness and reasonable comparison, we consider a two users' situation and they are also named as device m and device n. The sum secrecy rate can be expressed as

$$R_s = \tau_1 R_{n,s} + \tau_2 R_{m,s}, \tag{22}$$

where τ_1 and τ_2 are resource allocation coefficients and $\tau_1 + \tau_2 = 1$. For time-division multiple access (TDMA) system, the resource is transmission time. However, for frequency-division multiple access (FDMA), the resource is bandwidth. Without loss of generality, we consider a TDMA system as OMA-based benchmark system. Specifically, the conventional TDMA scheme with equal time sharing is adopted by many studies [29]. In this paper, we also adopt equal time sharing scheme for convenience; i.e., $\tau_1 = \tau_2 = 1/2$. The other system parameters are the same as NOMA system.

In OMA system, there is no interference between devices. The channel capacity of device m and device n at BS can be written as

$$C_m^o = \frac{1}{2}\log_2\left(1 + \rho L\left(d_m\right)\left|h_m\right|^2\right), \tag{23}$$

$$C_n^o = \frac{1}{2}\log_2\left(1 + \rho L\left(d_n\right)\left|h_n\right|^2\right), \tag{24}$$

respectively. In an equal time sharing scheme, half of transmitting time is used by every device. Consequently, the average channel capacity is half of that in NOMA. Similar to NOMA system, JCOP in OMA system can be expressed as

$$P_{co}^o\left(R_{n,t}, R_{m,t}\right) = 1 - \Pr\left[C_n^o \geq \frac{1}{2}R_{n,t}, C_m^o \geq \frac{1}{2}R_{m,t}\right]. \tag{25}$$

Because the resources are equal and orthogonally used by devices, the codeword rate is half of that in NOMA system. The expression of P_{co}^o can be easily derived as follows:

$$P_{co}^o\left(\theta_{n,t}, \theta_{m,t}\right) = 1 - e^{-\left(\theta_{n,t}/k_t\rho\sigma^2 L(d_m) + \theta_{m,t}/\rho\sigma^2 L(d_m)\right)}. \tag{26}$$

Because of no interference between devices, when ρ tends to be infinite, P_{co}^o tends to zero. It demonstrates that the effect of ρ is not limited for improving reliability performance in OMA system.

In illegal channel, derivation of JSOP in OMA system is the same as the derivation of P_{co}^s. The expression of JSOP in OMA can be directly written as

$$P_{so}^o\left(\theta_{n,s}, \theta_{m,s}\right) = 1 - \left(1 - e^{-\theta_{n,s}/k_s\gamma}\right)\left(1 - e^{-\theta_{m,s}/\gamma}\right). \tag{27}$$

Obviously, when γ tends to be infinite, P_{so}^o tends to unity, which is the same as one-user OMA system.

According to the definition of SST in NOMA system, the SST in OMA can be expressed as

$$\eta_o = \frac{1}{2}\left(1 - P_{co}^o\right)\left(1 - P_{so}^o\right)\left(R_{m,s} + R_{n,s}\right). \tag{28}$$

Because resources are equally shared by devices in OMA system, the SST is half when compared with NOMA system. After substituting (26) and (27) into (28), η_o can be finally expressed as

$$\eta_o = \frac{\left(R_{m,s} + R_{n,s}\right)}{2}\left(1 - e^{-\theta_{n,s}/k_s\gamma}\right)\left(1 - e^{-\theta_{m,s}/\gamma}\right) \times e^{-\left(\theta_{n,t}/k_t\rho\sigma^2 L(d_m) + \theta_{m,t}/\rho\sigma^2 L(d_m)\right)}. \tag{29}$$

In two users' OMA system, k_s and k_t are also important parameters for SST. In (29), η_o is a decrease function about k_s and increase function about k_t, which show that being far away from Eve and close to BS can enhance performance. This conclusion is also the same as that in traditional one-user OMA system.

3.5. Secrecy Performance Comparison Between NOMA and OMA System. NOMA allows two devices to transmit message with nonorthogonal resources, which increases connectivity and also gives more chances to Eve for wiretapping. The performance comparison between NOMA and OMA is not straightforward. According to the analysis of Remark 1, the message in WWS is securer than that in SWS. Thus, it is reasonable to take the performance in SWS as benchmark to compare it with that in OMA scheme. Moreover, due to NOMA enabling massive connectivity supported in network, more devices can transmit credential message at the same time. Therefore, SST may be an appropriate comparison metric. Based on (17) and (29), the condition of NOMA outperforming OMA is directly given as follows:

$$\frac{1}{\theta_{m,t}k_t + 1}e^{-\theta_{m,t}\theta_{n,t}/\rho\sigma^2 L(d_m)} > \frac{1}{2}. \tag{30}$$

In (30), the expression in the left part of the inequality is a decrease function about $\theta_{m,t}$ and $\theta_{n,t}$. It shows that lower codeword rate makes NOMA more likely to outperform OMA. In addition, it is an increase function about ρ and $L(d_m)$. It indicates that increasing average receiving SNR makes NOMA tend to be superior than OMA. Especially, when k_t is small, i.e., the channel conditions of pair devices are very different, NOMA will likely obtain better performance than OMA.

4. Enhancing Security by Device Placement

In this section, a low complexity device placement method is proposed for uplink NOMA to enhance security performance in IoT networks. It is wort pointing out that this secrecy enhancement method does not increase the signal processing complexity and power consumption, which is suitable for the low cost IoT applications [5]. We have assumed that the statistic CSI of legal and illegal channel are available

by legal devices. Because multiple devices are served in uplink NOMA system, the statistic CSI of Eve is available by more than one device. Consequently, the location of Eve is also available. We assume a scenario where the locations of Eve and device m are fixed but the placement of device n which is determined by path loss ratios k_s and k_t is chosen under security constraint. Therefore, the optimal placement of device n can be obtained by optimizing k_s and k_t.

4.1. Optimization Problem of Device Placement. As it is analyzed in Section 3, optimization problem can be formulated as follows:

$$(k_s, k_t)^* = \underset{0<k_s,0<k_t,(k_s^{-1/\alpha}d_{em}+k_t^{-1/\alpha}d_m)/d_{BE}\geq 1,|k_s^{-1/\alpha}d_{em}-k_t^{-1/\alpha}d_m|/d_{BE}\leq 1}{\operatorname{argmax}} \eta(k_s, k_t), \quad (31)$$

where d_{BE} is the distance between BS and Eve and $\eta \in \{\eta_s, \eta_w\}$. Because the location of device n is determined by k_s and k_t, they have to satisfy the constraint of triangle inequality which is described in the shade area of Figure 2. Equation (31) is a two parameters' optimization problem. In addition, because of the constraint, it is a nonconvex problem in nature. For these reasons, solving the optimization problem is challenging. Naturally, it is more practicable when optimizing k_t and k_s separately. However, because of the triangle inequality constraint between k_t and k_s, the optimal results may not be obtained.

4.2. Suboptimal Scheme of Device Placement. We introduce an easy-to-accomplish scheme to simplify problem (31). From (16) and (20), we can find that P_{co} and P_{so} have independent expression in η. Inspired by this, we separate (31) into two parts and each part is a single-parameter optimization problem. The scheme is expressed as follows:

$$k_t^* = \underset{0<k_t}{\arg\min} P_{co}(k_t), \quad (32)$$

$$k_s^* = \underset{0<k_s,(k_s^{-1/\alpha}d_{em}+(k_t^*)^{-1/\alpha}d_m)/d_{BE}\geq 1,|k_s^{-1/\alpha}d_{em}-(k_t^*)^{-1/\alpha}d_m|/d_{BE}\leq 1}{\arg\min} P_{so}(k_s), \quad (33)$$

where $P_{so} \in \{P_{so}^s, P_{so}^w\}$. In this scheme, k_t is priority optimized without triangle inequality constraint, and k_s is optimized with triangle inequality constraint. Therefore, k_t^* and k_s^* can determine the location of device n. However, this scheme is a suboptimal method. It should be pointed out that this scheme is appropriate for the scenario where legal channels are stronger than wiretap channels and we will prove that the results obtained from this scheme tend to be optimal when Eve stays far away from legal channel.

Problem (32) can be solved directly and the following lemma gives a preliminary result of problem (33).

Lemma 2. *If $P_{so}(k_s)$ has at most one stationary point, k_s^* is formulated as*

$$k_s^* = \begin{cases} \left(\dfrac{d_{BE}+d_m(k_t^*)^{-1/\alpha}}{d_{em}}\right)^{-\alpha}, & (k_s^{opt})^{-1/\alpha} > \left(\dfrac{d_{BE}+d_m(k_t^*)^{-1/\alpha}}{d_{em}}\right) \\ \left(\dfrac{d_m(k_t^*)^{-1/\alpha}-d_{BE}}{d_{em}}\right)^{-\alpha}, & (k_s^{opt})^{-1/\alpha} < \left(\dfrac{d_m(k_t^*)^{-1/\alpha}-d_{BE}}{d_{em}}\right) \\ \left(\dfrac{d_{BE}-d_m(k_t^*)^{-1/\alpha}}{d_{em}}\right)^{-\alpha}, & (k_s^{opt})^{-1/\alpha} < \left(\dfrac{d_{BE}-d_m(k_t^*)^{-1/\alpha}}{d_{em}}\right) \\ k_s^{opt}, & else, \end{cases} \quad (34)$$

Where k_s^{opt} is the result of the following problem:

$$k_s^{opt} = \underset{0<k_s}{\arg\max} P_{so}(k_s). \quad (35)$$

If (k_t^*, k_s^{opt}) locates in feasible region 1 showed in Figure 2, the results from this scheme are optimal. However, the results are suboptimal when locating in other regions, i.e., regions 2, 3, and 4.

Proof. See Appendix B. □

Remark 3. When Eve is far away from legal channel, i.e., $d_{em} \longrightarrow \infty$, we can find that $\gamma \longrightarrow 0$. Based on (13) and (19), P_{so} tends to be zero. Consequently, problem (31) degrades to problem (32) which is optimized in our scheme. It demonstrates that the suboptimal results from our device placement scheme tend to be optimal. Significantly, the results from the proposed method are lower bound of SST and this is useful for robust secrecy design.

4.2.1. Optimization of k_t. The following lemma provides the closed-form expression of k_t^*.

Lemma 4. *According to the scheme, k_t^* is given by*

$$k_t^* = \frac{\theta_{m,t}\theta_{n,t} + \sqrt{(\theta_{m,t}\theta_{n,t})^2 + 4\rho\sigma^2\theta_{m,t}\theta_{n,t}L(d_m)}}{2\rho\sigma^2\theta_{m,t}L(d_m)}. \quad (36)$$

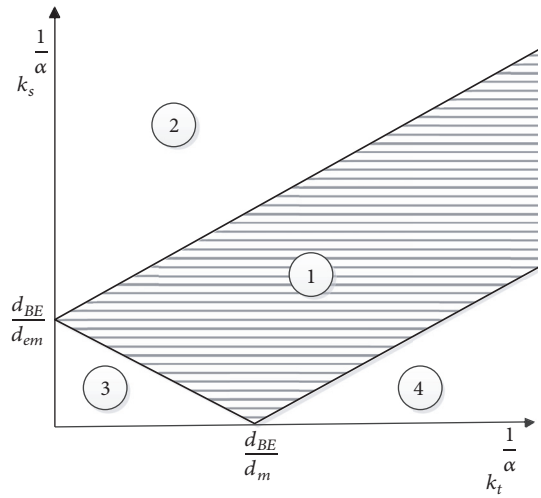


Figure 2: Feasible region for k_s and k_t.

Proof. The first-order partial derivative of P_{co} with respect to k_t can be written as

$$\frac{\partial P_{co}}{\partial k_t} = e^{-(\theta_{n,t}/k_t \rho\sigma^2 L(d_m)+\theta_{m,t}(1+\theta_{n,t})/\rho\sigma^2 L(d_m))} \times \left(\frac{\rho\sigma^2\theta_{m,t}L(d_m)k_t^2 - \theta_{m,t}\theta_{n,t}k_t - \theta_{n,t}}{k_t^2(\theta_{m,t}k_t+1)^2\rho\sigma^2 L(d_m)} \right). \tag{37}$$

By setting $\partial P_{co}/\partial k_t = 0$, we can obtain only one result in feasible region which is showed in (36). Furthermore, when $k_t \longrightarrow 0$, $\partial P_{co}/\partial k_t < 0$ and when $k_t \longrightarrow \infty$, $\partial P_{co}/\partial k_t > 0$. Therefore, $P_{co}(k_t^*)$ is the minimum of P_{co}. The proof is completed. □

The result of (32) is applicable for both SWS and WWS, because they have the identical expression of P_{co}. However, the results of problem (33) are different in SWS and WWS.

4.2.2. Optimization of k_s in SWS. The optimal result of k_s in SWS is given in following lemma.

Lemma 5. *The result of problem (33) in SWS is expressed as*

$$k_s^* = \left(\frac{d_{BE} + d_m (k_t^*)^{-1/\alpha}}{d_{em}} \right)^{-\alpha}. \tag{38}$$

Proof. The first-order partial derivative of P_{so}^s with respect to k_s can be written as

$$\frac{\partial P_{so}^s}{\partial k_s} = \frac{\theta_{n,s}}{\gamma k_s^2} e^{-\theta_{n,s}/k_s\gamma} \left(1 - e^{-\theta_{m,s}/\gamma}\right). \tag{39}$$

We can find that $\partial P_{so}^s/\partial k_s > 0$ for all k_s. It shows that $P_{so}^s(k_s)$ is an increase function, and $k_s^{opt} = 0$. According to Lemma 2, Lemma 5 can be obtained and the results are always suboptimal. □

4.2.3. Optimization of k_s in WWS. To derive the result of problem (33) in WWS, we first give the result of a special case in the following lemma.

Lemma 6. *Assuming a specific situation where $\theta_{n,s} = \theta_{m,s} = \theta$ and $\theta \geq 1$, the result of problem (33) in WWS is given by*

$$k_s^* = \begin{cases} \left(\dfrac{d_{BE} + d_m (k_t^*)^{-1/\alpha}}{d_{em}} \right)^{-\alpha}, & (k_s^{opt})^{-1/\alpha} > \left(\dfrac{d_{BE} + d_m (k_t^*)^{-1/\alpha}}{d_{em}} \right) \\ \left(\dfrac{d_m (k_t^*)^{-1/\alpha} - d_{BE}}{d_{em}} \right)^{-\alpha}, & (k_s^{opt})^{-1/\alpha} < \left(\dfrac{d_m (k_t^*)^{-1/\alpha} - d_{BE}}{d_{em}} \right) \\ \left(\dfrac{d_{BE} - d_m (k_t^*)^{-1/\alpha}}{d_{em}} \right)^{-\alpha}, & (k_s^{opt})^{-1/\alpha} < \left(\dfrac{d_{BE} - d_m (k_t^*)^{-1/\alpha}}{d_{em}} \right) \\ k_s^{opt}, & else, \end{cases} \tag{40}$$

where k_s^{opt} is the result of the following equation:

$$\left(\frac{1}{k_s^{opt}\gamma\left(k_s^{opt}+\theta\right)}+\frac{1}{\left(k_s^{opt}+\theta\right)^2}\right)e^{-1/k_s^{opt}\gamma} = \frac{1}{\left(1+k_s^{opt}\theta\right)^2}e^{-1/\gamma}. \tag{41}$$

Proof. See Appendix C. □

The key to problem (33) is the derivation of k_s^{opt}. When $0 < \theta < 1$ or $\theta_{n,s} \neq \theta_{m,s}$, solving problem (35) in WWS is quite challenging. Instead, we investigate k_s^{opt} by detailed simulations and numerical calculations repeatedly in different parameters and find that k_s^{opt} can be obtained by solving the following equation:

$$\frac{\partial P_{so}^{w}}{\partial k_s} = 0. \tag{42}$$

Although it does not formally identify the globally optimal solution, it identifies a locally optimal solution [33]. Combining with (40), we can get a suboptimal result.

4.3. Upper Bound of Optimization Problem. To show the performance of our scheme, the benchmark is required. However, getting the result of problem (31) needs a two-dimension searching method, which is complicated and time-consuming. We introduce an easy-to-implement upper bound of problem (31), which is formulated as follows:

$$\left(k_s, k_t\right)^* = \arg\max_{0<k_s,0<k_t} \eta\left(k_s, k_t\right). \tag{43}$$

It is the form of problem (31) without triangle constraint. Thus, the feasible region of k_s and k_t is the sum area of regions 1 to 4 showed in Figure 2. It demonstrates that the SST achieved by (43) is always equal to or bigger than that achieved by (31).

Problem (43) can be equally separated into two parts. They are formulated as follows:

$$k_t^* = \arg\min_{0<k_t} P_{co}\left(k_t\right), \tag{44}$$

$$k_s^* = \arg\min_{0<k_s} P_{so}\left(k_s\right). \tag{45}$$

We can find that (44) is equal to (32) and they have the same result expressed in (36). For (45), in SWS, according to Lemma 5, $k_s^* = 0$. Besides, in WWS, based on Lemma 6, $k_s^* = k_s^{opt}$. Because k_t^* and k_s^* are obtained without triangle constraint, the location of device n can not be determined by k_t^* and k_s^*. Although it is not practical, we can regard the SST obtained from (43) as a benchmark to show the performance of our suboptimal device placement scheme.

According to the definition, k_t^* and k_s^* represent the path loss ratio, which denotes the distance relationship of devices to BS and devices to Eve, respectively. The locations of device m and Eve are assumed to be known by BS. According to k_t^* and k_s^*, the location of device n can be determined. If the result is optimal, there may be one or two optimal locations for device n. However, there only exists one location for device n when the result is suboptimal.

Table 1: Table of parameters.

Parameters	values
Monte Carlo simulation repeated	10^6 times
The distance between BS and device m	$d_m = 5m$
The distance between BS and Eve	$d_{BE} = 15m$
Rayleigh fading variance	$\sigma^2 = 1$
The path loss exponent	$\alpha = 2.7$
Expected secrecy rate	$R_{n,s} = R_{m,s} = 0.2$BPCU

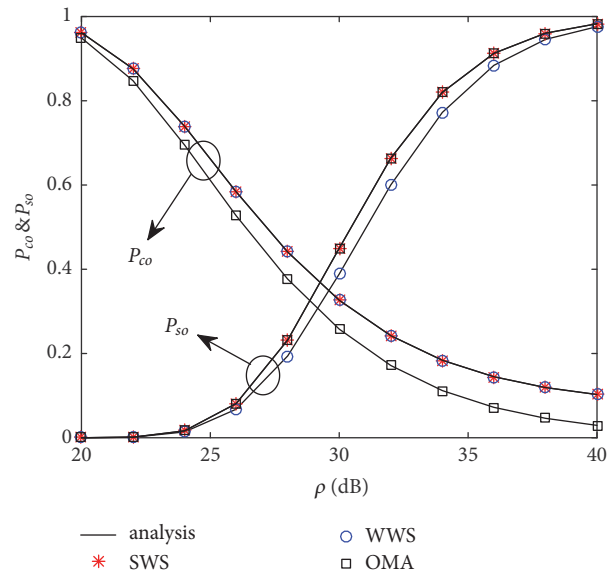


Figure 3: P_{co} and P_{so} versus ρ with $k_t = 0.15$, $k_s = 0.55$, $d_{em} = 20m$, and $R_t = 0.6$BPCU.

5. Numerical Results

In this section, we present the numerical results for verifying our analysis. Unless otherwise stated, some of the simulation parameters are in Table 1. We introduce bit per channel use (BPCU) as the unit of transmitting rate. The distances between each other are set to be small values, which do not lose the generality, and also adopted in [24, 30].

Figure 3 plots P_{co} and P_{so} versus ρ with $k_t = 0.15$, $k_s = 0.55$, $d_{em} = 20m$, and $R_t = 0.6$BPCU ($R_t = R_{n,t} = R_{m,t}$). The analysis curves of P_{co} are calculated from (10) and (26) and theoretic results of P_{so} are calculated from (13), (19), and (27). In this figure, we first observe that the simulations precisely match the theoretic curves, which validates our analysis. And, then, we observe that the curves of P_{co} decrease and the curves of P_{so} increase as the increasing of ρ. In addition, the curve of P_{co} in SWS is the same as that in WWS and P_{so} of strong Eve and OMA system are also the same, which correspond to our analysis. Moreover, due to no interference in OMA system,

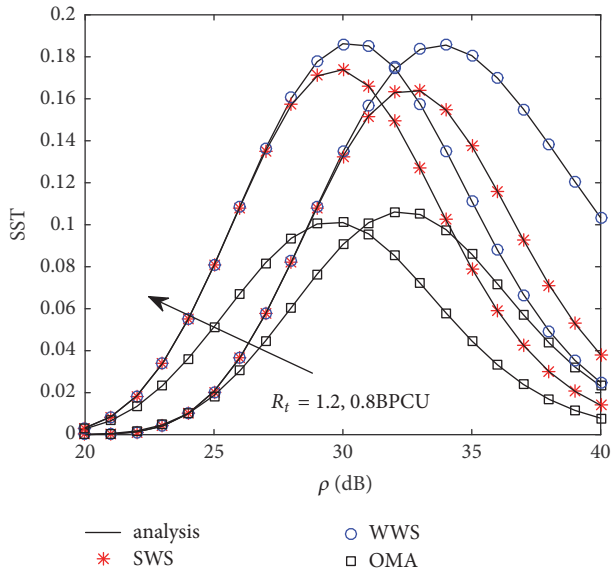


FIGURE 4: The SST versus ρ with $k_t = 0.15$, $k_s = 0.55$, and $d_{em} = 20m$.

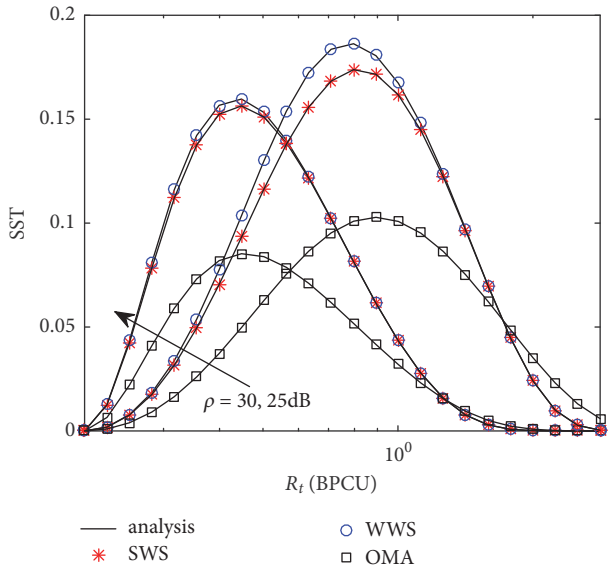


FIGURE 5: The SST versus R_t with $k_t = 0.15$, $k_s = 0.55$, and $d_{em} = 20m$.

it has lower COP than NOMA and as, with the increasing of ρ, COP of OMA tends to zero. In particular, P_{so} in WWS is always lower than that in SWS and OMA system because ability limited Eve is interfered by devices in WWS.

Figure 4 plots the SST of NOMA and OMA system versus transmit SNR ρ with $k_t = 0.15$, $k_s = 0.55$, and $d_{em} = 20m$ for $R_t = 1.2, 0.8$BPCU. The analysis curves are obtained from (17), (21), and (29). Significantly, we find that the Monte Carlo simulation points match precisely with the analytical curves, which certifies to the accuracy of our analysis. We first observe that for both NOMA and OMA system the curves of SST first increase and then decrease as the increasing of ρ. ρ can be optimized for maximizing SST, however, which is beyond the scope of this work. Secondly, we can find that NOMA system is outperforming OMA system in high SNR region, which is correspond to the analysis of (30). In addition, SST is always bigger in WWS than that in SWS, which confirms the analysis in Section 4. We also find that at low ρ region the SST is nearly equal in SWS and WWS. This is because, at low SNR region, the effect of interference at Eve is negligible, so the security performance in SWS is close to that in WWS.

Figure 5 plots the SST versus R_t with $k_t = 0.15$, $k_s = 0.55$, and $d_{em} = 20m$ for $\rho = 30$dB and 25dB. Firstly, we observe that the curves of SST first increase and then decrease with the increasing of R_t for different ρ. There may also exist an optimal R_t which makes the system achieve maximum SST. There are many literatures about finding the optimal R_t [33] and this work is beyond the scope of this paper. In addition, when R_t is bigger enough, the gap of SST between WWS and SWS tends to be zero. This is due to the fact that increasing R_t enhances the ability of resisting wiretapping. When R_t is bigger enough, P_{so} is negligible; the key restriction of SST is P_{co} which is the same in WWS and SWS. Moreover, we give a performance comparison between $\rho = 35$dB and 30dB,

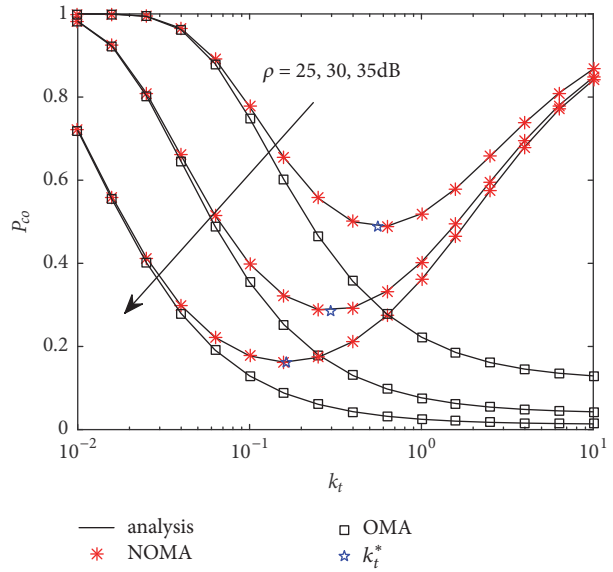


FIGURE 6: P_{co} versus k_t with $R_t = 0.6$BPCU and $d_{em} = 20m$.

which shows the similar trends as the increasing of R_t. By the way, we can get the similar characteristics when SST is versus $R_{n,t}$ or $R_{m,t}$. Ultimately, we can find that when R_t is high enough, the security performance of OMA system outperforms that in NOMA system, which is proved by (30).

Figure 6 plots P_{co} versus k_t with $R_t = 0.6$BPCU, for $\rho = 35, 30$ and 25dB. Firstly, we can observe that P_{co} of NOMA system first decrease and then increase as the increasing of k_t for different ρ. However, P_{co} in OMA system is a decrease function about k_t. This is because in NOMA system when device n becomes close to device m, the CS of device n is improved but deteriorating the CS of device m; however, it only improves the CS of device n in OMA system. Besides, k_t^*, obtained from (36), always stand for the minimum point

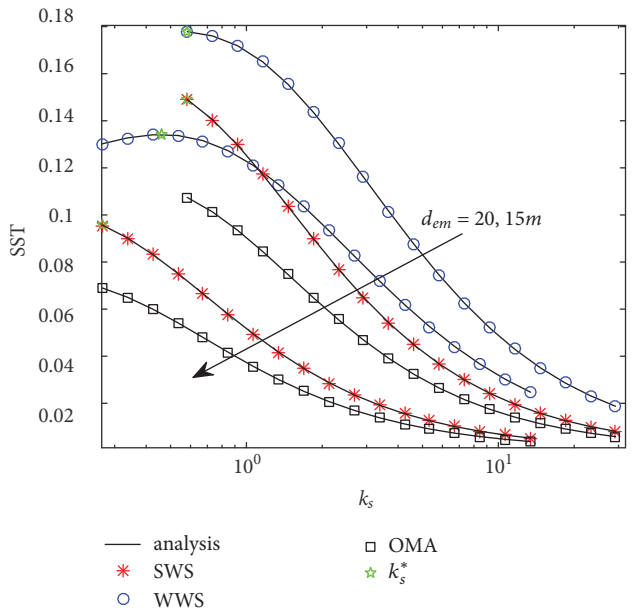


FIGURE 7: SST versus k_s with $k_t = k_t^*$, ρ = 35dB, and R_t = 1.5BPCU.

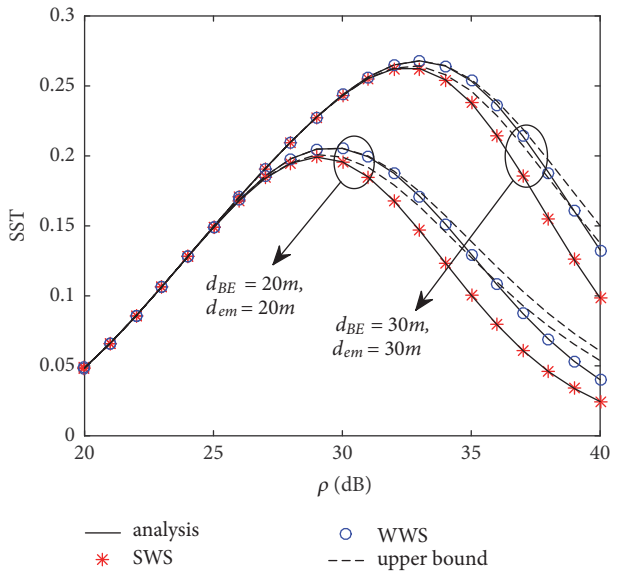


FIGURE 8: The SST versus ρ with $k_t = k_t^*$, $k_s = k_s^*$, and R_t = 0.8BPCU.

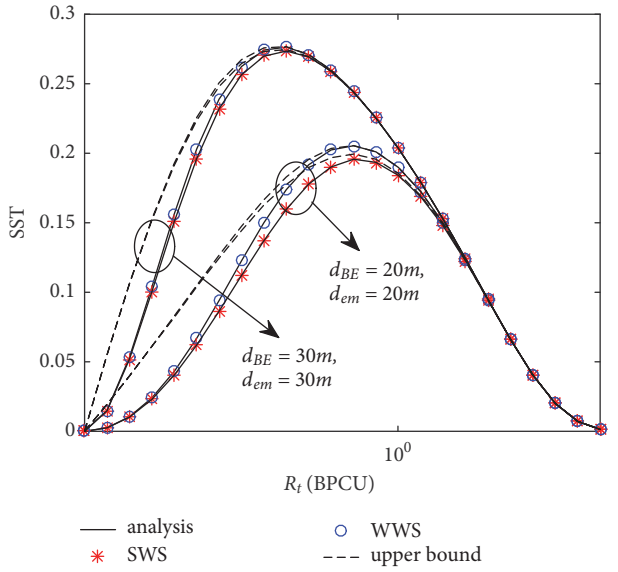


FIGURE 9: The SST versus R_t with $k_t = k_t^*$, $k_s = k_s^*$, and ρ = 30dB.

of P_{co} in NOMA system precisely which verifies Lemma 4. Moreover, as the increasing of ρ, P_{co} is decreasing, which corresponds to Figure 3. In addition, as the increasing of ρ, k_t^* also decreases, because far away from device m can reduce its interference. Ultimately, When k_t is small, P_{co} of OMA and that of NOMA system are close. It verifies that pairing users whose CS are very different achieves high transmission efficiency gain on OMA.

Figure 7 plots SST versus k_s with $k_t = k_t^*$, ρ = 35dB, and R_t = 1.5BPCU for different d_{em} in their feasible region. We first observe that k_s^* always stand for the maximum point of SST in NOMA system in their feasible region, which verifies Lemma 2. In addition, k_s^* are always standing for the suboptimal results in SWS for different d_{em}, which is proved by Lemma 5. In WWS, when $d_{em} = 20m$, (k_t^*, k_s^{opt}) is located in region 2, k_s^* is suboptimal result; when $d_{em} = 15m$, (k_t^*, k_s^{opt}) is located in region 1, we can observe that k_s^* is optimal result.

Figures 8 and 9 plot SST versus ρ and R_t, respectively, with $k_t = k_t^*$ and $k_s = k_s^*$. In these figures, k_s and k_t are adaptively changed due to the increasing of ρ or R_t according to Lemmas 2 and 4, respectively. In Figure 8, we find that, in low SNR region, our results are very close to the upper bound. In Figure 9, we observe that, in high R_t region, our results are also close to their upper bounds tightly. As both in low SNR region and in high R_t region, the security outage performance can be ensured and SST is restricted by P_{co} principally which is optimized in our method. Consequently, the results from our method tend to be optimal. Both Figures 8 and 9 show that the curves of WWS are closer to their upper bounds than that of SWS since by our scheme only suboptimal result can be obtained in SWS. In particular, when Eve is away from legal channel, i.e., increasing d_{BE} and d_{em}, our results approach their upper bounds closer in both Figures 8 and 9. It certificates our analysis in Remark 3.

6. Conclusion

In this paper, we have first exploited uplink NOMA to enhance PLS in IoT networks. The closed-form expressions of JCOP, JSOP, and SST are derived in SWS and WWS. Analysis results show that the secrecy performance in WWS is always better than that in SWS and the two scenarios have similar performance in low SNR region or high R_t region. In addition, we also have studied the security performance of TDMA system as a benchmark to show superiority of NOMA. The condition that NOMA outperforms OMA in terms of SST is provided. Moreover, we formulate an easy-to-implement scheme of device placement. Although the scheme obtains optimal results only in some cases, when

Eve is far away from legal users, the suboptimal results tend to be optimal. In addition, simulation results show that, in low SNR region and high R_t region, our results also tend to be optimal. Besides, by simulation, we find that there exists an optimal desired transmission power or codeword rate, which maximizes the SST both in SWS and in WWS. The optimization of those parameters may be a future research direction. Furthermore, we assume that statistic CSI of Eve is available by legal users. In reality, it is impractical especially for a totally passive Eve. Moreover, the massive devices are randomly distributed in IoT networks. Using stochastic geometry approach for modeling the positions of devices and Eve may be another promising research direction.

Appendix

A. The Proof of (19)

To derive P_{so}^{w}, based on (18), we can formulate

$$\begin{aligned} P_{so}^{w}\left(\theta_{m,s},\theta_{n,s}\right) &= 1-\Pr\left[\frac{\rho L\left(d_{em}\right)\left|h_{em}\right|^{2}}{\rho L\left(d_{en}\right)\left|h_{en}\right|^{2}+1}\right. \\ &\left.<\theta_{m,s},\frac{\rho L\left(d_{en}\right)\left|h_{en}\right|^{2}}{\rho L\left(d_{em}\right)\left|h_{em}\right|^{2}+1}<\theta_{n,s}\right]=1 \\ &-\Pr\left[\frac{\lambda k_s\left|h_{en}\right|^{2}}{\theta_{n,s}}-1<\lambda\left|h_{em}\right|^{2}\right. \\ &\left.<\theta_{m,s}\left(\lambda k_s\left|h_{en}\right|^{2}+1\right)\right], \end{aligned} \tag{A.1}$$

where $\lambda=\rho L(d_{em})$. For obtaining a practical value, we let

$$\frac{\lambda k_s\left|h_{en}\right|^{2}}{\theta_{n,s}}-1<\theta_{m,s}\left(\lambda k_s\left|h_{en}\right|^{2}+1\right). \tag{A.2}$$

After some simplification manipulations, we can obtain

$$\frac{1-\theta_{n,s}\theta_{m,s}}{\theta_{n,s}}\lambda k_s\left|h_{en}\right|^{2}<\theta_{m,s}+1. \tag{A.3}$$

When $\theta_{n,s}\theta_{m,s}\geq 1$, we can formulate

$$\begin{aligned} &P_{so}^{w}\left(\theta_{m,s},\theta_{n,s}\right) \\ &=1-\int_{0}^{\theta_{n,s}}\int_{0}^{\theta_{m,s}(1+y)}\frac{1}{k_s\gamma^{2}}e^{-(x/\gamma+y/k_s\gamma)}dxdy \\ &\quad-\int_{\theta_{n,s}}^{\infty}\int_{y/\theta_{n,s}-1}^{\theta_{m,s}(1+y)}\frac{1}{k_s\gamma^{2}}e^{-(x/\gamma+y/k_s\gamma)}dxdy, \end{aligned} \tag{A.4}$$

where $\gamma=\lambda\sigma^{2}$. After some mathematical manipulations, we can obtain

$$\begin{aligned} P_{so}^{w}\left(\theta_{m,s},\theta_{n,s}\right) &= \frac{k_s}{k_s+\theta_{n,s}}e^{-\theta_{n,s}/k_s\gamma} \\ &\quad+\frac{1}{1+k_s\theta_{m,s}}e^{-\theta_{m,s}/\gamma}. \end{aligned} \tag{A.5}$$

When $\theta_{n,s}\theta_{m,s}<1$, we can formulate

$$\begin{aligned} P_{so}^{w}\left(\theta_{m,s},\theta_{n,s}\right) &= 1-\int_{0}^{\theta_{n,s}}\int_{0}^{\theta_{m,s}(1+y)}\frac{1}{k_s\gamma^{2}}e^{-(x/\gamma+y/k_s\gamma)}dxdy \\ &\quad-\int_{\theta_{n,s}}^{\theta_{n,s}(1+\theta_{m,s})/(1-\theta_{n,s}\theta_{m,s})}\int_{y/\theta_{n,s}-1}^{\theta_{m,s}(1+y)}\frac{1}{k_s\gamma^{2}}e^{-(x/\gamma+y/k_s\gamma)}dxdy. \end{aligned} \tag{A.6}$$

After some mathematical manipulations, we can obtain

$$\begin{aligned} P_{so}^{w}\left(\theta_{m,s},\theta_{n,s}\right) &= \frac{k_s}{k_s+\theta_{n,s}}e^{-\theta_{n,s}/k_s\gamma}+\frac{1}{1+k_s\theta_{m,s}} \\ &\quad\cdot e^{-\theta_{m,s}/\gamma}-\frac{k_s\left(1-\theta_{m,s}\theta_{n,s}\right)}{\left(1+k_s\theta_{m,s}\right)\left(k_s+\theta_{n,s}\right)} \\ &\quad\cdot e^{-k_s\theta_{m,s}(1+\theta_{n,s})+\theta_{n,s}(1+\theta_{m,s})/k_s\gamma(1-\theta_{m,s}\theta_{n,s})}. \end{aligned} \tag{A.7}$$

Above all, (19) is derived.

B. The Proof of Lemma 2

In order to find the optimal k_s, the general idea is investigating the monotonicity of target function in its feasible region which is determined by its extreme point. When the considered target function has at most one stationary point, the problem becomes explicit. If the extreme point is located in the feasible region, the optimal point is the extreme point. If the extreme point is located in the sides of the feasible region, the target function is a monotonic function and the optimal point locates at the boundary of the feasible region. According to Figure 2 and the value of k_t^{*}, four cases based on the location of extreme point should be considered to discuss the result of optimal k_s.

We first obtain k_t^{*} and k_s^{opt}, where $k_t^{*}=\arg\min_{0<k_t}P_{co}(k_t)$ and $k_s^{opt}=\arg\min_{0<k_s}P_{so}(k_s)$. Thus, k_s^{opt} is the extreme point of $P_{so}(k_s)$. In addition, we assume that $P_{so}(k_s)$ has at most one stationary point. Thus, when $k_s<k_s^{opt}$, $P_{so}(k_s)$ is monotonic decrease function about k_s and when $k_s>k_s^{opt}$, $P_{so}(k_s)$ is monotonic increase function about k_s. The four cases are discussed as follows.

If (k_t^{*},k_s^{opt}) locates in region 1, i.e.,

$$\frac{k_s^{-1/\alpha}d_{em}+\left(k_t^{*}\right)^{-1/\alpha}d_m}{d_{BE}}\geq 1, \tag{B.1}$$

and

$$\frac{\left|k_s^{-1/\alpha}d_{em}-\left(k_t^{*}\right)^{-1/\alpha}d_m\right|}{d_{BE}}\leq 1, \tag{B.2}$$

k_s^{opt} satisfies the triangle inequality constraint. $k_s^{*}=k_s^{opt}$ and the result is optimal. However, when (k_t^{*},k_s^{opt}) does not locate in region 1, i.e., k_s^{opt} does not satisfy the triangle inequality constraint, $k_s^{*}\neq k_s^{opt}$ and the results are suboptimal.

If (k_t^{*},k_s^{opt}) is located in region 2, i.e.,

$$d_{BE}-d_m\left(k_t^{*}\right)^{-1/\alpha}>0, \tag{B.3}$$

and

$$\left(\frac{d_{BE}+d_m\left(k_t^*\right)^{-1/\alpha}}{d_{em}}\right)^{-\alpha}>k_s^{opt}, \tag{B.4}$$

$P_{so}(k_s)$ is monotonic increase function about k_s and the feasible region is expressed as

$$k_s\in\left[\left(\frac{d_{BE}+d_m\left(k_t^*\right)^{-1/\alpha}}{d_{em}}\right)^{-\alpha},\left(\frac{d_{BE}-d_m\left(k_t^*\right)^{-1/\alpha}}{d_{em}}\right)^{-\alpha}\right]. \tag{B.5}$$

Therefore $k_s^*=((d_{BE}+d_m(k_t^*)^{-1/\alpha})/d_{em})^{-\alpha}$.

If (k_t^*,k_s^{opt}) is located in region 3, i.e.,

$$d_{BE}-d_m\left(k_t^*\right)^{-1/\alpha}>0, \tag{B.6}$$

and

$$\left(\frac{d_{BE}-d_m\left(k_t^*\right)^{-1/\alpha}}{d_{em}}\right)^{-\alpha}<k_s^{opt}, \tag{B.7}$$

$P_{so}(k_s)$ is monotonic decrease function about k_s and the feasible region can be written as

$$k_s\in\left[\left(\frac{d_{BE}+d_m\left(k_t^*\right)^{-1/\alpha}}{d_{em}}\right)^{-\alpha},\left(\frac{d_{BE}-d_m\left(k_t^*\right)^{-1/\alpha}}{d_{em}}\right)^{-\alpha}\right]. \tag{B.8}$$

Therefore, $k_s^*=((d_{BE}-d_m(k_t^*)^{-1/\alpha})/d_{em})^{-\alpha}$.

If (k_t^*,k_s^{opt}) is located in region 4, i.e.,

$$d_m\left(k_t^*\right)^{-1/\alpha}-d_{BE}>0, \tag{B.9}$$

and

$$\left(\frac{d_m\left(k_t^*\right)^{-1/\alpha}-d_{BE}}{d_{em}}\right)^{-\alpha}<k_s^{opt}. \tag{B.10}$$

$P_{so}(k_s)$ is monotonic decrease function about k_s and the feasible region is expressed as

$$k_s\in\left[\left(\frac{d_{BE}+d_m\left(k_t^*\right)^{-1/\alpha}}{d_{em}}\right)^{-\alpha},\left(\frac{d_m\left(k_t^*\right)^{-1/\alpha}-d_{BE}}{d_{em}}\right)^{-\alpha}\right]. \tag{B.11}$$

Therefore, $k_s^*=((d_m(k_t^*)^{-1/\alpha}-d_{BE})/d_{em})^{-\alpha}$.

Combining the above four cases, we obtain Lemma 2.

C. The Proof of Lemma 6

When $\theta_{m,s}=\theta_{n,s}=\theta$, and $\theta\geq 1$, based on (19), P_{so}^w can be expressed as

$$P_{so}^w=\frac{k_s}{k_s+\theta}e^{-\theta/k_s\gamma}+\frac{1}{1+k_s\theta}e^{-\theta/\gamma}. \tag{C.1}$$

The first-order partial derivative of P_{so}^w with respect to k_s can be written as

$$\frac{\partial P_{so}^w}{\partial k_s}=\underbrace{\left(\frac{\theta}{k_s\gamma\left(k_s+\theta\right)}+\frac{\theta}{\left(k_s+\theta\right)^2}\right)}_{\Xi_1}e^{-\theta/k_s\gamma}-\frac{\theta}{\left(1+k_s\theta\right)^2}e^{-\theta/\gamma}. \tag{C.2}$$

From (C.2), we can find that when k_s tends to be zero, $\partial P_{so}^w/\partial k_s<0$; when $k_s=1$, $\partial P_{so}^w/\partial k_s>0$. So at least existing one k_s make $\partial P_{so}^w/\partial k_s=0$. If there is only one k_s indicated as k_s^{opt}, it is the optimal result of (35). We will prove that only one k_s makes $\partial P_{so}^w/\partial k_s=0$ below.

The second-order partial derivative of P_{so}^w with respect to k_s can be expressed as

$$\frac{\partial^2 P_{so}^w}{\partial k_s^2}=\frac{2\theta^2}{\left(1+k_s\theta\right)^3}e^{-\theta/\gamma}+\left(\frac{\theta^2}{k_s^3\gamma^2\left(k_s+\theta\right)}-\frac{2\theta}{k_s\gamma\left(k_s+\theta\right)^2}-\frac{2\theta}{\left(k_s+\theta\right)^3}\right)\cdot e^{-\theta/k_s\gamma}. \tag{C.3}$$

When k_s tends to zero, $\partial^2 P_{so}^w/\partial k_s^2>0$. It shows that, with the increasing of k_s, $\partial P_{so}^w/\partial k_s$ first increases. When $\partial P_{so}^w/\partial k_s$ begins to decrease, i.e., $\partial^2 P_{so}^w/\partial k_s^2<0$, which can be further expressed as

$$\frac{\partial^2 P_{so}^w}{\partial k_s^2}=\left(\frac{\theta^2}{k_s^3\gamma^2\left(k_s+\theta\right)}-\frac{2\theta}{k_s\gamma\left(k_s+\theta\right)^2}-\frac{2\theta}{\left(k_s+\theta\right)^3}\right)\cdot e^{-\theta/k_s\gamma}+\frac{2\theta^2}{\left(1+k_s\theta\right)^3}e^{-\theta/\gamma}<0. \tag{C.4}$$

After some calculations, we can obtain

$$\underbrace{\frac{\left(1+k_s\theta\right)}{2k_s^3\gamma^3\left(k_s+\theta\right)^3}\left(2\gamma^2k_s^2\left(k_s+\theta\right)-\theta\gamma\left(k_s+\theta\right)^2+2\gamma^3k_s^3\right)e^{-\theta/k_s\gamma}}_{\Xi_2}-\frac{\theta}{\left(1+k_s\theta\right)^2}e^{-\theta/\gamma}>0. \tag{C.5}$$

We investigate the result of $\Xi_1 - \Xi_2$, i.e.,

$$\begin{aligned}\Xi_1 - \Xi_2 &= \frac{1}{2k_s^3\gamma^3\left(k_s+\theta\right)^3}\left\{2\theta k_s^2\gamma^2\left(k_s+\theta\right)^2\right.\\&+2\theta k_s^3\gamma^3\left(k_s+\theta\right)+\left(1+k_s\theta\right)\\&\cdot\left.\left(\theta\gamma\left(k_s+\theta\right)^2-2\gamma^2k_s^2\left(k_s+\theta\right)-2\gamma^3k_s^3\right)\right\}\\&=\frac{1}{2k_s^3\gamma^2\left(k_s+\theta\right)^3}\left\{2k_s^3\left(\theta\left(k_s+\theta\right)-\left(1+k_s\theta\right)\right)\right.\\&\cdot\gamma^2+2k_s^2\left(k_s+\theta\right)\left(\theta\left(k_s+\theta\right)-\left(1+k_s\theta\right)\right)\gamma\\&+\left.\theta\left(1+k_s\theta\right)\left(k_s+\theta\right)^2\right\}.\end{aligned} \tag{C.6}$$

Introducing a function

$$\begin{aligned}F\left(\gamma\right)&=2k_s^3\left(\theta\left(k_s+\theta\right)-\left(1+k_s\theta\right)\right)\gamma^2\\&+\theta\left(k_s+\theta\right)^2\left(1+k_s\theta\right)\\&+\left(2\theta k_s^2\left(k_s+\theta\right)^2-2k_s^2\left(k_s+\theta\right)\left(1+k_s\theta\right)\right)\gamma,\end{aligned} \tag{C.7}$$

we find that

$$\frac{\partial F\left(\gamma\right)}{\partial\gamma}=\left(\theta^2-1\right)\left(4k_s^3\gamma+2\left(k_s+\theta\right)k_s^2\right)\geq 0. \tag{C.8}$$

Thus, we can obtain

$$F_{\min}\left(\gamma\right)=F_{\min}\left(0\right)=\theta\left(k_s+\theta\right)^2\left(1+k_s\theta\right)>0. \tag{C.9}$$

So,

$$\begin{aligned}&\Xi_1e^{-\theta/k_s\gamma}-\frac{\theta}{\left(1+k_s\theta\right)^2}e^{-\theta/\gamma}\\&>\Xi_2e^{-\theta/k_s\gamma}-\frac{\theta}{\left(1+k_s\theta\right)^2}e^{-\theta/\gamma}>0.\end{aligned} \tag{C.10}$$

The result shows that when $\partial^2P_{so}^w/\partial k_s^2<0$, $\partial P_{so}^w/\partial k_s>0$. Based on the above two results, $\partial P_{so}^w/\partial k_s$ first increases and when it begins to decrease it always stays positive value. It further demonstrates that $\partial P_{so}^w/\partial k_s=0$ have only one result k_s^{opt} which is expressed in (41).

Based on (34), Lemma 6 is obtained.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61771487, no. 61471393, and no. 61371122).

References

[1] Y. Chen, F. Han, Y.-H. Yang et al., "Time-reversal wireless paradigm for green internet of things: an overview," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 81–98, 2014.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[3] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[4] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2017.

[5] A. Mukherjee, "Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[6] L. Sun, Q. Du, P. Ren, and Y. Wang, "Two birds with one stone: towards secure and interference-free D2D transmissions via constellation rotation," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8767–8774, 2016.

[7] Y. Zou, J. Zhu, B. Zheng, and Y.-D. Yao, "An adaptive cooperation diversity scheme with best-relay selection in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 58, no. 10, pp. 5438–5455, 2010.

[8] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[9] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Transactions on Signal Processing*, vol. 63, no. 1, pp. 206–220, 2015.

[10] H. Yu, T. Kim, and H. Jafarkhani, "Wireless Secure Communication With Beamforming and Jamming in Time-Varying Wiretap Channels," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2087–2100, 2018.

[11] W. Yang, W. Mou, X. Xu, W. Yang, and Y. Cai, "Energy efficiency analysis and enhancement for secure transmission in SWIPT systems exploiting full duplex techniques," *IET Communications*, vol. 10, no. 14, pp. 1712–1720, 2016.

[12] X. Xu, W. Yang, Y. Cai, and S. Jin, "On the Secure Spectral-Energy Efficiency Tradeoff in Random Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 10, pp. 2706–2722, 2016.

[13] B. Chen, C. Zhu, L. Shu et al., "Securing uplink transmission for lightweight single-antenna UEs in the presence of a massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 5374–5384, 2016.

[14] J. Hu, W. Yang, N. Yang, X. Zhou, and Y. Cai, "On–Off-Based Secure Transmission DesignWith Outdated Channel State Information," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6075–6088, 2016.

[15] J. Choi, "Physical Layer Security for Channel-Aware Random Access with Opportunistic Jamming," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2699–2711, 2017.

[16] N. Wang, T. Jiang, W. Li, and S. Lv, "Physical-layer security in Internet of Things based on compressed sensing and frequency selection," *IET Communications*, vol. 11, no. 9, pp. 1431–1437, 2017.

[17] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On Secure Wireless Communications for IoT under Eavesdropper Collusion," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1281–1293, 2016.

[18] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.

[19] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive Non-Orthogonal Multiple Access for Cellular IoT: Potentials and Limitations," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 55–61, 2017.

[20] Z. Ding, L. Dai, and H. V. Poor, "MIMO-NOMA Design for Small Packet Transmission in the Internet of Things," *IEEE Access*, vol. 4, pp. 1393–1405, 2016.

[21] M. Shirvanimoghaddam, M. Condoluci, M. Dohler, and S. J. Johnson, "On the Fundamental Limits of Random Non-Orthogonal Multiple Access in Cellular Massive IoT," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2238–2252, 2017.

[22] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial Noise Aided Secure Cognitive Beamforming for Cooperative MISO-NOMA Using SWIPT," *IEEE Journal on Selected Areas in Communications*, 2018, to be published.

[23] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA Transmission With Artificial Noise," *IEEE Transactions on Vehicular Technology*, pp. 1-1.

[24] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.

[25] H. Lei, J. Zhang, K.-H. Park et al., "On Secure NOMA Systems with Transmit Antenna Selection Schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.

[26] L. Xu, A. Nallanathan, X. Pan, J. Yang, and W. Liao, "Security-Aware Resource Allocation with Delay Constraint for NOMA-Based Cognitive Radio Network," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 366–376, 2018.

[27] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure Beamforming in Downlink MISO Nonorthogonal Multiple Access Systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7563–7567, 2017.

[28] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the Spectral Efficiency and Security Enhancements of NOMA Assisted Multicast-Unicast Streaming," *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 3151–3163, 2017.

[29] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the Design of Secure Non-Orthogonal Multiple Access Systems," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2196–2206, 2017.

[30] Z. Ding, R. Schober, and H. V. Poor, "A General MIMO Framework for NOMA Downlink and Uplink Transmission Based on Signal Alignment," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4438–4454, 2016.

[31] Z. Yang, Z. Ding, P. Fan, and N. Al-Dhahir, "A General Power Allocation Scheme to Guarantee Quality of Service in Downlink and Uplink NOMA Systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7244–7257, 2016.

[32] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[33] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of Code Rates in SISOME Wiretap Channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 11, pp. 6377–6388, 2015.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 6869189, 14 pages
https://doi.org/10.1155/2018/6869189

Research Article

On Secrecy Outage Probability and Average Secrecy Rate of Large-Scale Cellular Networks

Liwei Tao, Weiwei Yang, Yueming Cai, and Dechuan Chen

College of Communication Engineering, Army Engineering University of PLA, 210007 Nanjing, China

Correspondence should be addressed to Weiwei Yang; wwyang1981@163.com

Received 14 February 2018; Revised 22 April 2018; Accepted 30 April 2018; Published 7 June 2018

Academic Editor: Lu Wei

We investigate the secrecy performance in large-scale cellular networks, where both Base Stations (BSs) and eavesdroppers follow independent and different homogeneous Poisson point processes (PPPs). Based on the distances between the BS and user, the intended user selects the nearest BS as serving BS to transmit the confidential information. We first derive closed-formed expressions of secrecy outage probability and average secrecy rate of a single-antenna system for both noncooperative and cooperative eavesdroppers scenarios. Then, to further improve the secrecy performance through additional spatial degrees of freedom, the above analyses generalize to the multiantenna scenario, where BSs employ the transmit antenna selection (TAS) scheme. Finally, the results show the small-scale fading has a considerable effect on the secrecy performance in certain density of eavesdroppers and small path loss exponent environment, and when the interference caused by BS is considered, the secrecy performance will be reduced. Moreover, the gap of secrecy performance between noncooperative and cooperative eavesdroppers cases is nearly invariable as the number of antennas increases.

1. Introduction

Due to the broadcast nature of physical propagation channel, wireless communication networks are particularly vulnerable to be wiretapped and attacked by malicious users. Traditionally, protecting the secret information transmission relies heavily on cryptographic encryption and decryption technologies. However, because of the high complexity caused by key distribution and management, cryptographic technologies may not be suitable for large-scale wireless networks. Against this background, physical layer security (PLS), which takes advantage of the inherent randomness of wireless channels, including noise, channel fading, and interference to achieve secure transmission for wireless networks, has aroused wide attention after Shannon and Wyner's pioneering works [1, 2].

1.1. Background. A significant amount of PLS techniques in wireless networks, such as artificial-noise-aided security [3], security-oriented beamforming [4], cooperation based secure transmission [5], and power control and resource allocation [6], has been developed by researchers. An important information conveyed by [7, 8] is that PLS techniques have enormous potential in future 5th-generation (5G) secure communications. However, most of these works are based on point-to-point communications, where the node locations and topology of networks are determined and static. Moreover, these works only consider small-scale fading in the process of information transmission. However, in reality, the uncertain node locations has significant impact on the secure communication, especially in future 5G wireless networks where the node locations and topological structure are becoming more and more randomized and dynamic. The difficulty of researching the secrecy performance in such wireless networks is how to model the random locations distribution of nodes accurately. Fortunately, stochastic geometry has provided a powerful tool to address this difficulty and achieved great success in ad hoc networks [9, 10], random cognitive radio networks [11, 12], and large-scale cellular networks [13–19].

Stochastic geometry has facilitated the investigation of the influence of randomly located eavesdroppers on secrecy

performance. Specially, for describing the locations distribution of unknown eavesdroppers, the Poisson point process (PPP) is an efficient model. In [13], the authors derived the secrecy outage probability in the scenario where a transmitter transmits confidential information to an intended receiver in the presence of PPP distributed eavesdroppers. In order to further enhance physical layer security of networks, the researchers exploited various signal processing technologies, e.g., beamforming [14], transmit antenna selection (TAS) [15], regularized channel inversion linear precoding [16], and artificial noise (AN) [17], and designed different transmission schemes, e.g., on-off transmission [18] and secrecy guard zone [19]. It is worth noting that [14, 15] simultaneously considered the noncooperative and cooperative eavesdroppers cases and analyzed the secrecy performance under various network factors. Comparing the two different eavesdropping cases, it can be concluded that cooperative eavesdroppers had more serious damage to the security of networks. The recently work [20] investigated the secrecy outage probability in random wireless networks, and the authors utilized TAS to enhance secrecy performance and proposed two metrics to order the users.

The aforementioned papers only take the single cell into account. Considering the mobility of users, users may communicate with different BSs in different locations. Hence, in order to conform to more realistic scenes, it is necessary to consider the impacts caused by the multiple cells in large-scale cellular networks. Due to the uneven distribution of BSs, particularly in remote areas, the cellular structure presents the irregular features. It has proved that the BSs modeled as PPP can track in real deployment as accurately as the traditional grid model [21]. Based on [21], the placement of BSs and eavesdroppers was modeled as mutually independent PPPs in [22, 23]. The authors in [23] specially evaluated the secrecy rate in large-scale cellular networks where BSs can exchange partial or complete information according to the eavesdroppers' location information. This work was extended to [24, 25] which proposed a regularized channel inversion linear precoding approach to improve the average secrecy rate. Furthermore, [26] considered the PLS in heterogeneous cellular networks where the BSs in every tier are spatially distributed according to a homogeneous PPP with different density.

1.2. Motivation. In large-scale cellular networks where BSs and eavesdroppers are random distribution [22, 23], only the large-scale fading is considered. In fact, small-scale fading caused by multipath components produces the harmful or even fatal impact for wireless communications. Hence, considering small-scale fading is more practical for analyzing secrecy performance. On the other hand, when the density of BSs is large enough, the distance between BSs and user will become small. For this short distance transmission, small-scale fading may be the main factor that affects the secrecy performance. Therefore, it is significant to research the effects on secrecy performance caused by the small-scale fading in addition to the large-scale fading in large-scale cellular networks. This work has been studied partly in our prior work [27]. However, the system that it considered is a single-antenna system, and the interference caused by BS has been ignored. In this paper, the influence of interference has been considered in single-antenna scenario. In addition, in future cellular networks, the BS may equip multiple antennas to enhance information transmission. Therefore, we extend the research to multiantenna scenario.

TAS technology with low-cost and low-computational can effectively enhance secrecy performance, and it achieves full diversity while maintaining low feedback overhead and requiring minimal transceiver circuitry. Although it has been applied in [15], it is important to know that [15] considered such a scenario where a transmitter communicated with an intended user in the presence of randomly distributed eavesdroppers. However, we focus on a more realistic and complex cellular network where BSs and eavesdroppers both are randomly distributed. It is significant to study how the network parameters, i.e., node density, the number of antennas, and path loss exponent, affect the secrecy performance, especially the performance difference between noncooperative and cooperative eavesdroppers cases, and these are beneficial for understanding and designing such wireless networks.

1.3. Contributions. In this paper, we investigate the secrecy outage probability and average secrecy rate of large-scale cellular networks subject to Rayleigh fading, coexisting with PPP distributed BSs and eavesdroppers. Comparing the work with [23], we consider both large-scale and small-scale fading simultaneously in the process of transmitting confidential information. Hence, our results in this paper are more general and realistic. In addition, through analyzing the secrecy performance in the large-scale cellular networks, we find that the results of [23] can be regarded as the bound of our results, and it can be concluded that the small-scale fading has a considerable effect on secrecy performance in certain density of eavesdroppers and small path loss exponent. And the impact on secrecy performance caused by the small-scale fading will decrease with the increasing of path loss exponent.

Especially, on the basis of considering the small-scale fading, we consider the interference caused by BS in the single-antenna scenario. In such case, the closed-form expressions of the secrecy outage probability and average secrecy rate are derived and the numerical results are also given in simulation section. On the other hand, we consider both noncooperative and cooperative eavesdroppers cases and derive an accurate expression as well as a closed-form bound on secrecy performance for the noncooperative eavesdroppers case and a closed-form solution for the cooperative eavesdroppers case, respectively. In the simulations section, the effects on secrecy performance in various network parameters have been given, which can help us design and optimize the network performance. An interesting finding is that increasing of the number of antennas has a little effect on the difference between noncooperative and cooperative eavesdroppers cases.

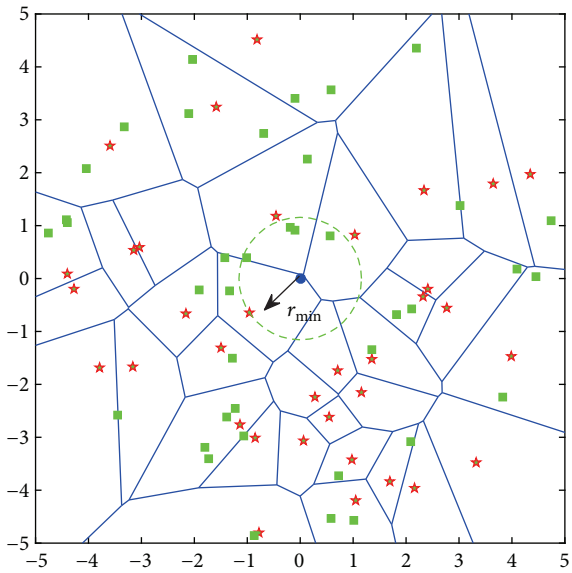


FIGURE 1: Illustration of Poisson distributed BSs cell boundaries. A typical user chooses the nearest BS to be the serving BS. BSs and eavesdroppers (respectively, represented by red five-pointed star and green squares) are distributed according to homogeneous PPPs.

2. System and Channel Model

As shown in Figure 1, we consider a downlink secure transmission in large-scale cellular networks, where one of stochastic distributed BSs is chosen to serve an intended mobile user in the presence of multiple malicious eavesdroppers. Without loss of generality, the intended mobile user is located at the origin in R^2 as the typical user by Slivnyak theorem [28]. In this paper, both the locations of BSs and eavesdroppers are modeled as independent homogeneous PPPs Φ_b and Φ_e of intensity λ_b and λ_e, respectively. First of all, we assume the BSs, the typical user, and eavesdroppers are equipped with a single antenna each. Furthermore, in Section 5, we extend to the multiantenna scenario where BSs are equipped with multiple antennas and use TAS technology to further enhance the secrecy performance.

We consider both large-scale and small-scale fading for the wireless channels. For the large-scale fading, we adopt the standard path loss model $l_{xy}^{-\alpha}$, where l_{xy} denotes the distance between transmitter x and receiver y, and $\alpha > 2$ is path loss exponent. Small-scale fading is caused by the coherent superposition of a great number of multipath components at the receiver. It heavily leads to the fragility of wireless communication. For the small-scale fading, a quasi-static Rayleigh fading is assumed, which is ignored by prior research in this research field [23]. And in the scenario of passive eavesdroppers, it is difficult to obtain the instantaneous channel state information (CSI) and locations of eavesdroppers. Nevertheless, we assume that their small-scale channel distributions are available. Let h_{ij} represent the Rayleigh fading coefficient between node i and node j in the cellular network. Meanwhile, we assume that the Rayleigh fading coefficient follows a zero-mean complex Gaussian distribution with unit variance, i.e., $\mathcal{CN}(0, 1)$.

Similar to [15, 23], in order to reduce feedback and computational complexity, we select the serving BS for the intended user only depending on the large-scale fading, i.e., $l_{B_iU}^{-\alpha}$. For a given α and channel model, serving BS is equivalent as the nearest BS. Hence the serving BS can be selected as $B^* = \arg\min_{B_i \in \Phi_b}(l_{B_iU})$. Based on [29], the probability density function (PDF) of l_{B^*U} is $f_{l_{B^*U}}(l) = 2\pi\lambda_b l e^{-\pi\lambda_b l^2}$, where l_{B^*U} is the distance between the serving BS and the typical user.

In this work, we adopt two assumptions; one is that the downlink receiver has no in-band interference [23]. It is justifiable when the interfering BSs are far away from the serving BS, so that a carefully planned frequency reuse pattern can be adopted. Moreover, the constant noise power can comprise interference of networks. Another assumption is that the interference caused by BS is considered in the process of information transmission [24, 25].

3. Secrecy Performance of Single-Antenna System

In this section, we investigate the secrecy outage probability and average secrecy rate at the typical user under the assumption that all nodes are equipped with a single antenna. The received signal-noise-ratio (SNR) at the typical user can be expressed as $\gamma_{B^*U} = P_{BS}|h_{B*U}|^2 l_{B*U}^{-\alpha}/\sigma^2$, and the SNR of an arbitrary eavesdropper e is $\gamma_{B^*e} = P_{BS}|h_{B^*e}|^2 l_{B^*e}^{-\alpha}/\sigma^2$, where σ^2 is the variance of zero-mean Additive White Gaussian Noise (AWGN) at each receiver, and P_{BS} is the transmit power of the serving BS.

3.1. Noncooperative Eavesdroppers. In this subsection, considering that there is no cooperation among eavesdroppers and each eavesdropper decodes information independently, in such case, we evaluate the secrecy outage probability and average secrecy rate of the intended user in cellular networks.

3.1.1. Secrecy Outage Probability. The secrecy outage probability is defined as the probability that the achievable secrecy rate is less than a given secrecy code rate which is nonnegative.

Based on the model described above, the channel capacity of the serving BS to the typical user can be written as

$$C_{B^*U} = \log_2(1 + \gamma_{B^*U}) = \log_2\left(1 + \frac{P_{BS}|h_{B^*U}|^2 l_{B^*U}^{-\alpha}}{\sigma^2}\right). \quad (1)$$

In order to design the optimal network parameters to achieve the maximum level of security in the presence of multiple noncooperative eavesdroppers, we consider the most detrimental eavesdropper which has the worst impact on secrecy performance of networks. The channel capacity at the most detrimental eavesdropper can be expressed as

$$\begin{aligned} C_{B^*e} &= \log_2\left(1+\max_{e\in\Phi_e}\left(\gamma_{B^*e}\right)\right) \\ &= \log_2\left(1+\max_{e\in\Phi_e}\left(\frac{P_{BS}\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}}{\sigma^2}\right)\right). \end{aligned} \tag{2}$$

The achievable maximum secrecy rate at the typical user is given by $R_s = [C_{B^*U} - C_{B^*e}]^+$, so the secrecy outage probability can be given as

$$\begin{aligned} P_{so}^{NC}(R_0) &= \mathbb{P}(R_s < R_0) = \mathbb{P}\left(C_{B^*U} - C_{B^*e} < R_0\right) \\ &= \mathbb{P}\left(\log_2\left(\frac{1+P_{BS}\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}/\sigma^2}{1+\max_{e\in\Phi_e}\left(P_{BS}\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}/\sigma^2\right)}\right)\right. \\ &\left. < R_0\right) \overset{a}{\simeq} \mathbb{P}\left(\frac{\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right), \end{aligned} \tag{3}$$

where $[X]^+ = \max(0, x)$ and $R_0 \geq 0$ denotes the secrecy rate threshold. Step (a) is based on that the typical user and eavesdroppers operate in moderate-to-high SNR regime [18, 23].

Proposition 1. *The secrecy outage probability for the scenario of noncooperative eavesdroppers can be expressed as*

$$\begin{aligned} &P_{so}^{NC}(R_0) \\ &\simeq \sum_{k=1}^{\infty}\left(\frac{-\lambda_b\alpha}{2\lambda_e\Gamma(2/\alpha)\left(2^{R_0}\right)^{2/\alpha}}\right)^{k-1}\Gamma\left(\frac{2}{\alpha}(k-1)+1\right). \end{aligned} \tag{4}$$

Proof. According to the definition of the secrecy outage probability in (3), we can derive the secrecy outage probability as

$$\begin{aligned} P_{so}^{NC}(R_0) &\simeq \mathbb{P}\left(\frac{\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) \\ &= \mathbb{E}_{\Phi_b,\Phi_e}\left(\mathbb{P}\left(\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right) > \frac{\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}}{2^{R_0}} \mid \Phi_b, \Phi_e\right)\right) \\ &= 1-\mathbb{E}_{\Phi_b,\Phi_e}\left(\prod_{e\in\Phi_e}\mathbb{P}\left(\left|h_{B^*e}\right|^2 < \frac{\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}}{2^{R_0}} l_{B^*e}^{\alpha} \mid \Phi_b, \Phi_e\right)\right) \overset{a}{=} 1 \\ &\quad - \mathbb{E}_{\Phi_b}\left(\exp\left(-\lambda_e\int_0^{2\pi}\int_0^{\infty} e^{(\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}/2^{R_0})r^{\alpha}} r dr d\theta\right) \mid \right. \\ &\quad \left.\Phi_b\right) \overset{b}{=} 1-\mathrm{E}_{\Phi_b}\left(\exp\left(-\frac{2\pi\lambda_e 2^{R_0}}{\alpha\left|h_{B^*U}\right|^{2/\alpha} l_{B^*U}^{-2}}\Gamma\left(\frac{2}{\alpha}\right)\right) \mid \right. \\ &\quad \left.\Phi_b\right) = 1 \\ &\quad - \mathrm{E}_{|h_{B^*U}|^2}\left(\int_0^{\infty}\exp\left(-\frac{2\pi\lambda_e\left(2^{R_0}\right)^{2/\alpha}}{\alpha\left|h_{B^*U}\right|^{2/\alpha} l_{B^*U}^{-2}}\times\Gamma\left(\frac{2}{\alpha}\right)\right)\right. \\ &\quad \left.\cdot f_{l_{B^*U}}(l)\,dl \mid \left|h_{B^*U}\right|^2\right) \\ &\quad \overset{c}{=} \int_0^{\infty}\left(\frac{2\lambda_e\Gamma(2/\alpha)\left(2^{R_0}\right)^{2/\alpha}e^{-x}}{\lambda_b\alpha x^{2/\alpha}+2\lambda_e\Gamma(2/\alpha)\left(2^{R_0}\right)^{2/\alpha}}\right)dx \\ &\quad \overset{d}{=} \sum_{k=1}^{\infty}\left(-\frac{\lambda_b\alpha}{2\lambda_e\Gamma(2/\alpha)\left(2^{R_0}\right)^{2/\alpha}}\right)^{k-1}\Gamma\left(\frac{2}{\alpha}(k-1)+1\right), \end{aligned} \tag{5}$$

where step (a) is based on the probability generating functional (PGFL) of PPPs Φ_b and Φ_e [30], and step (b) holds by using [31, eq. (3.326.2)]. In addition, step (c) is based on the exponential distribution of channel gain $|h_{B^*U}|^2$ and the PDF of l_{B^*U}, and step (d) follows polynomial expansion [31, eq. (1.112.1)] and integral formula [31, eq. (3.326.2)].

From (4), we know that if the density of eavesdroppers increases or the density of BSs decreases, the secrecy outage probability will increase. Additionally, the secrecy outage probability increases as the threshold value R_0 or α increases. In order to make the result easy to analyze, we derive the lower bound of the secrecy outage probability as

$$P_{so}^{NC}(R_0) \geq P_{so}^{NC-lower}(R_0) = \frac{\lambda_e\left(2^{R_0}\right)^{2/\alpha}}{\lambda_b+\lambda_e\left(2^{R_0}\right)^{2/\alpha}} \tag{6}$$

□

Proof. Beginning with the basic definition of the secrecy outage probability, it can be derived as follows:

$$
\begin{aligned}
P_{so}^{NC}(R_0) &= \mathbb{E}_{\Phi_b,\Phi_e}\left(\mathbb{P}\left(l_{B^*U} > \left(\frac{\left|h_{B^*U}\right|^2}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} \times \frac{1}{2^{R_0}}\right)^{1/\alpha} \mid \Phi_b,\Phi_e\right)\right) \\
&\overset{a}{\geq} \mathbb{E}_{l_{B^*U},l_{B^*e}}\left(\mathbb{P}\left(l_{B^*U} > \left(\mathbb{E}_{|h_{B^*U}|^2,|h_{B^*e}|^2}\left(\frac{1}{2^{R_0}} \times \frac{\left|h_{B^*U}\right|^2}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} \mid \left|h_{B^*U}\right|^2, \left|h_{B^*e}\right|^2\right)\right)^{1/\alpha}\right) \mid l_{B^*U},l_{B^*e}\right) \\
&= \mathbb{E}_{l_{B^*U},l_{B^*e}}\left(\mathbb{P}\left(l_{B^*U} > \frac{1}{\max_{e\in\Phi_e}\left(l_{B^*e}^{-\alpha}\right)\left(2^{R_0}\right)^{1/\alpha}}\right) \mid l_{B^*U},l_{B^*e}\right) \\
&= \mathbb{E}_{l_{B^*U},l_{B^*e}}\left(\mathbb{P}\left(\min_{e\in\Phi_e}\left(l_{B^*e}\right) < \left(2^{R_0}\right)^{1/\alpha} l_{B^*U}\right) \mid l_{B^*U},l_{B^*e}\right) \overset{b}{=} 1 - \int_0^\infty \exp\left(-\pi\lambda_e\left(2^{R_0}\right)^{2/\alpha} y^2\right) f_{l_{B^*U}}(l)\, dl \\
&= \frac{\lambda_e\left(2^{R_0}\right)^{2/\alpha}}{\lambda_b + \lambda_e\left(2^{R_0}\right)^{2/\alpha}},
\end{aligned}
\tag{7}
$$

where step (a) is derived by employing the Jensen inequality $E(\varphi(x)) \geq \varphi(E(x))$, and step (b) follows the PPPs void probability and the PDF of l_{B^*U}. □

Remark 2. It should be noticed that the result in (6) can be compared with scenario 1 in [23] where mobile users to be served by the nearest BS and the full location information of eavesdroppers can be obtained by BS. In that paper, it gave the complementary cumulative distribution function (CCDF) of R_s as $\overline{F}_{R_s}(R_0) = \mathbb{P}(R_s > R_0)$ without considering the impact of the small-scale fading. We can find that the result in [23] is the same as the lower bound in essence. Therefore, it provides a bound for our result. Because we take the small-scale fading into account, the result presented in this paper is more realistic and general.

3.1.2. Average Secrecy Rate. In the following, we study the average secrecy rate $\overline{R}_s$ of the cellular network in the presence of noncooperative eavesdroppers. By calculating the expectation of secrecy rate, we can derive the expression of average secrecy rate as

$$
\begin{aligned}
\overline{R}_s &= \int_0^\infty R_s f(R_s)\, dR_s = \int_0^\infty \left(\int_0^{R_s} dy\right) f(R_s)\, dR_s \\
&= \int_0^\infty \int_y^\infty f(R_s)\, dR_s dy = \int_0^\infty \left(1 - F(R_s)\right) dy,
\end{aligned}
\tag{8}
$$

where $f(R_s)$ and $F(R_s)$ are the PDF and the cumulative distribution function (CDF) of R_s, respectively. And, the secrecy outage probability can be regarded as the distribution function of the achievable maximum secrecy rate R_s. Therefore, based on Proposition 1, we can derive the expression of average secrecy rate as $\overline{R}_s = \int_0^\infty (1 - P_{so}(R_0)) dR_0$.

Corollary 3. *The average secrecy rate is provided by*

$$
\overline{R}_s^{NC} = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}\alpha}{2k\ln 2}\left(\frac{\alpha\lambda_b}{2\lambda_e\Gamma(2/\alpha)}\right)^k \Gamma\left(\frac{2}{\alpha}k + 1\right) \tag{9}
$$

Proof. From Proposition 1 and the definition of $\overline{R}_s$, the average secrecy rate can be expressed as

$$
\begin{aligned}
\overline{R}_s^{NC} &= \int_0^\infty \int_0^\infty \left(\frac{\lambda_b \alpha x^{2/\alpha} e^{-x}}{\lambda_b \alpha x^{2/\alpha} + 2\lambda_e \Gamma(2/\alpha)\left(2^{R_0}\right)^{2/\alpha}}\right) dx dR_0 \\
&\overset{a}{=} \int_0^\infty \frac{e^{-x}}{\ln\left(2^{2/\alpha}\right)}\left[\ln\left(\frac{\exp\left(\ln\left(2^{2/\alpha}\right)R_0\right)}{\lambda_b \alpha x^{2/\alpha} + 2\lambda_e\Gamma(2/\alpha)} \times \frac{\lambda_b \alpha x^{2/\alpha}}{\exp\left(\ln\left(2^{2/\alpha}\right)R_0\right)}\right)\right]_0^\infty dx \\
&= \int_0^\infty \left(\frac{\alpha e^{-x}}{2\ln 2}\ln\left(1 + \frac{\alpha\lambda_b x^{2/\alpha}}{2\lambda_e\Gamma(2/\alpha)}\right)\right) dx \overset{b}{=} \frac{\alpha^2\lambda_b}{4\ln 2\lambda_e\Gamma(2/\alpha)} \int_0^\infty \frac{e^{-t^{2/\alpha}}}{1 + \left(\alpha\lambda_b/2\lambda_e\Gamma(2/\alpha)\right)t} dt \\
&\overset{c}{=} \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{\ln 2}\left(\frac{\alpha\lambda_b}{2\lambda_e\Gamma(2/\alpha)}\right)^k \Gamma\left(\frac{2k}{\alpha} + 1\right),
\end{aligned}
\tag{10}
$$

where step (a) follows the integral result based on the integrand herein [32, eq. (5.1.2.4.2)], and step (b) is based on the integration by parts. In addition, step (c) uses the power of binomials [31, eq. (1.112.1)].

From (9), the average secrecy rate $\overline{R}_s$ at the typical user decreases when the value λ_e increases. Also, with the increasing of path loss exponent α, the average secrecy rate increases. So the large path loss exponent has a positive impact on the average secrecy rate. □

Remark 4. Utilizing the lower bound of secrecy outage probability in Proposition 1, the upper bound of the average secrecy rate is written as

$$\begin{aligned}\overline{R}_s^{NC} \le \overline{R}_s^{NC-upper} &= \int_0^{\infty} \left(1 - P_{so}^{NC-lower}\left(R_0\right)\right) dR_0 \\ &= \frac{\alpha}{2\ln 2} \ln\left(1 + \frac{\lambda_b}{\lambda_e}\right).\end{aligned} \tag{11}$$

We can find that the upper bound of the average secrecy rate is the same with the result in [23] where it considered a noncooperative eavesdroppers case and only taken lager-scale fading into account but ignored the effect caused by the small-scale fading. From (11), it is obvious that the large α and λ_b/λ_e are beneficial to improve the secrecy performance in the large-scale cellular network.

3.1.3. Security Outage Probability When Considering Interference. In this section, we consider the typical user will be interfered by the other BSs except the serving BS. In addition, the secrecy indeed becomes better when the eavesdropping channel is degraded under the effect of interference. In this paper, we focus on the worst-case scenario of eavesdropping, where all the eavesdroppers can mitigate the interference. In fact, eavesdroppers are usually assumed to have strong ability, and they may cooperate to cancel the interference, as seen in [33]. In this scenario, the security outage probability at the typical user is written as

$$\begin{aligned}P_{so}^{I}\left(R_0\right) &= \mathbb{P}\left(C_s < R_0\right) = \mathbb{P}\left(C_{B^*U} - C_{B^*e} < R_0\right) \\ &= \mathbb{P}\left(\log_2 \frac{1+\gamma_{B^*U}}{1+\gamma_{B^*e}} < R_0\right) \simeq \mathbb{P}\left(\frac{\gamma_{B^*U}}{\gamma_{B^*e}} < \beta\right) \\ &= \int_0^{\infty} \int_0^{\beta\gamma_{B^*e}} f_{\gamma_{B^*U}}(x)\, f_{\gamma_{B^*e}}(y)\, dxdy \\ &= \int_0^{\infty} F_{\gamma_{B^*U}}(\beta y)\, f_{\gamma_{B^*e}}(y)\, dy,\end{aligned} \tag{12}$$

where $\beta = 2^{R_0}$.

The CDF of γ_{B^*U} is derived as

$$\begin{aligned}F_{\gamma_{B^*U}}(x) &= \mathbb{P}\left(\gamma_{B^*U} < x\right) \\ &= \mathbb{P}\left(\frac{P_{BS} h_{B^*U} l_{B^*U}^{-\alpha}}{\sum_{i\in\Phi_b/\{s\}} P_{BS} h_{B_iU} l_{B_iU}^{-\alpha} + \sigma^2} < x\right) \\ &= \mathbb{P}\left(\frac{P_{BS} h_{B^*U} l_{B^*U}^{-\alpha}}{I + \sigma^2} < x\right) \\ &\overset{a}{\approx} \mathbb{P}\left(\frac{P_{BS} h_{B^*U} l_{B^*U}^{-\alpha}}{I} < x\right) = 1 - \mathrm{E}_{\Phi_b}\left(e^{-(xI/P_{BS}) l_{B^*U}^{-\alpha}}\right) \\ &= 1 - L_I\left(\frac{l_{B^*U}^{\alpha} x}{P_{BS}}\right) \\ &\overset{b}{=} 1 - \exp\left(-\pi l_{B^*U}^2 \lambda_b \Gamma\left(1 + \frac{2}{\alpha}\right)\Gamma\left(1 - \frac{2}{\alpha}\right) x^{2/\alpha}\right),\end{aligned} \tag{13}$$

where $I = \sum_{i\in\Phi_b/\{s\}} P_{BS} h_{B_iU} l_{B_iU}^{-\alpha}$. Step (a) is based on the the assumption that this is an interference limited system, and step (b) follows the Laplace transform of I [34].

Next, we can give the CDF of γ_{B^*e} as

$$\begin{aligned}F_{\gamma_{B^*e}}(x) &= \mathbb{P}\left(\gamma_{B^*e} < x\right) = \mathbb{P}\left(\max_{e\in\Phi_e} P h_{B^*e} l_{B^*e}^{-\alpha} < x\right) \\ &= \mathbb{E}_{\Phi_e}\left(\prod\left(P\left(h_{B^*e} < \frac{x l_{B^*e}^{\alpha}}{P}\right)\right)\right) \\ &= \exp\left(-2\pi\lambda_e \int_0^{\infty} e^{-xr^{\alpha}/P} r dr\right) \\ &= \exp\left(-2\pi\lambda_e \frac{\Gamma(2/\alpha)\, P^{2/\alpha}}{\alpha x^{2/\alpha}}\right),\end{aligned} \tag{14}$$

where $P = P_{BS}/\sigma^2$. Then, the PDF is

$$\begin{aligned}f_{\gamma_{B^*e}}(x) = &-\frac{4\pi\lambda_e \Gamma(2/\alpha)\, P^{2/\alpha}}{\alpha^2} x^{-2/\alpha-1} \\ &\cdot \exp\left(-2\pi\lambda_e \frac{\Gamma(2/\alpha)\, P^{2/\alpha}}{\alpha x^{2/\alpha}}\right),\end{aligned} \tag{15}$$

Submit (15) and (13) to (12), we can get the expression of secrecy outage probability

$$\begin{aligned}P_{so}^{I}\left(R_0\right) &\simeq \int_0^{\infty} 1 - \exp\left(-\pi l_0^2 \lambda_b \Gamma\left(1 + \frac{2}{\alpha}\right)\Gamma\left(1 - \frac{2}{\alpha}\right)(\beta y)^{2/\alpha}\right) \times f_{\gamma_{B^*e}}(y)\, dy \\ &= \int_0^{\infty} \int_0^{\infty} \left(1 - \exp\left(-\pi l_0^2 \lambda_b \Gamma\left(1 + \frac{2}{\alpha}\right)\Gamma\left(1 - \frac{2}{\alpha}\right)(\beta y)^{2/\alpha}\right)\right) \times 2\pi\lambda_b l_0 e^{-\pi\lambda_b l_0^2 d_{l_0} f_{\gamma_e}(y)} dy \\ &= \int_0^{\infty} \left(1 - 2\pi\lambda_b l_0 e^{-\pi\lambda_b l_0^2 - \pi l_0^2 \lambda_b \Gamma(1+2/\alpha)\Gamma(1-2/\alpha)(\beta y)^{2/\alpha}}\right) d_{l_0} f_{\gamma_e}(y)\, dy\end{aligned}$$

$$= 1 - \int_0^\infty \left(\frac{1}{1 + (\beta y)^{2/\alpha} \Gamma(1 + 2/\alpha) \Gamma(1 - 2/\alpha)} \right) f_{\gamma_e}(y)\, dy$$
$$= 1 + C_1 \int_0^\infty \frac{1}{1 + C_2 y^{2/\alpha}} \times \frac{1}{y^{2/\alpha+1}} \exp\left(-C_3 y^{-2/\alpha}\right) dy, \tag{16}$$

where $C_1 = 4\pi\lambda_e \Gamma(2/\alpha) P^{2/\alpha}/\alpha^2$, $C_2 = \beta^{2/\alpha}\Gamma(1 + 2/\alpha)\Gamma(1 - 2/\alpha)$, and $C_3 = 2\pi\lambda_e(\Gamma(2/\alpha)P^{2/\alpha}/\alpha)$.

Using the approach of equivalent substitution, the expression can be simplified as

$$\begin{aligned} P_{so}^I(R_0) &= 1 + C_1 \int_0^\infty \frac{1}{1 + C_2 t} \\ &\times \frac{1}{t^{1+2/\alpha}} \exp\left(-C_3 t^{-1}\right) \frac{dt}{(2/\alpha)(t)^{1-\alpha/2}} = 1 + \frac{\alpha}{2} \\ &\cdot C_1 \int_0^\infty \frac{1}{1 + C_2 t} \frac{1}{t^2} \exp\left(-C_3 t^{-1}\right) dt = 1 - \frac{\alpha}{2} \\ &\cdot C_1 \int_0^\infty \frac{x}{x + C_2} \exp(-C_3 x)\, dx \overset{a}{=} 1 - \frac{\alpha}{2} \\ &\cdot C_1 C_2 e^{C_2 C_3} \Gamma(2)\, \Gamma(-1, C_2 C_3), \end{aligned} \tag{17}$$

where $\Gamma(\alpha, x)$ is the incomplete gamma function and step (a) is based on [31, eq. (3.381.10)].

3.1.4. Average Secrecy Rate When Considering Interference. In this section, the average secrecy rates are derived when the interference caused by BSs is considered. According to the expression of average secrecy rate $\overline{R}_s = \int_0^\infty (1 - P_{so}(R_0))dR_0$, the average secrecy rate can be calculated as follows:

$$\begin{aligned} \overline{R}_s^I &= \int_0^\infty \left(\frac{\alpha}{2} C_1 C_2 e^{C_2 C_3} \Gamma(2)\, \Gamma(-1, C_2 C_3) \right) dR_0 \\ &= \frac{\alpha\Gamma(2)}{2} C_4 C_1 \int_0^\infty \left(\beta^{2/\alpha} e^{\beta^{2/\alpha} C_0} \Gamma\left(-1, \beta^{2/\alpha} C_0\right) \right) dR_0 \\ &= \frac{\alpha\Gamma(2)}{2\ln 2} C_4 C_1 \int_0^\infty \left(\beta^{2/\alpha - 1} e^{\beta^{2/\alpha} C_0} \Gamma\left(-1, \beta^{2/\alpha} C_0\right) \right) d\beta \\ &\overset{a}{=} \frac{\alpha^2\Gamma(2)}{4\ln 2} C_4 C_1 \int_0^\infty e^{C_0 t} \Gamma(-1, C_0 t)\, dt \\ &= \frac{\alpha^2\Gamma(2)}{4\ln 2} C_4 C_1 F(C_0), \end{aligned} \tag{18}$$

where $C_0 = (2\pi\lambda_e\Gamma(2/\alpha)P^{2/\alpha}/\alpha)\Gamma(1 + 2/\alpha)\Gamma(1 - 2/\alpha)$, $C_4 = \Gamma(1 + 2/\alpha)\Gamma(1 - 2/\alpha)$, and $F(x) = \int_0^\infty e^{xt}\Gamma(-1, xt)dt$. Step (a) is based on the variable substitution.

3.2. Cooperative Eavesdroppers. In this subsection, for a strongly robust analysis, we consider the worst case that all eavesdroppers can share the message with each other, and eavesdroppers are capable of combining their signals in an optimal manner to decode confidential information.

3.2.1. Secrecy Outage Probability. It is easy to know that the main channel capacity C_{B^*U} is the same as the scenario of noncooperative eavesdroppers. In cooperative eavesdroppers case, multiple eavesdroppers can be regarded as a single eavesdropper with multiple distributed antennas. Considering that the maximal ratio combining (MRC) scheme is employed, the equivalent eavesdropping channel capacity can be derived as

$$\begin{aligned} C_{B^*e} &= \log_2\left(1 + \sum_{e\in\Phi_e} (\gamma_{B^*e})\right) \\ &= \log_2\left(1 + \sum_{e\in\Phi_e} \left(\frac{P_{BS} \left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}}{\sigma^2} \right)\right). \end{aligned} \tag{19}$$

The secrecy outage probability $P_{so}^C(R_0)$ in the presence of multiple cooperative eavesdroppers can be calculated by

$$\begin{aligned} P_{so}^C(R_0) &= \mathbb{P}\left(C_{B^*U} - C_{B^*e} < R_0\right) \\ &= \mathbb{P}\left(\log_2\left(\frac{1 + P_{BS}\left|h_{B*U}\right|^2 l_{B*U}^{-\alpha}/\sigma^2}{1 + \sum_{e\in\Phi_e}\left(P_{BS}\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}/\sigma^2\right)} \right) \right. \\ &\left. < R_0 \right) \simeq \mathbb{P}\left(\frac{\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}}{\sum_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0} \right) \end{aligned} \tag{20}$$

Proposition 5. *The secrecy outage probability for the scenario of cooperative eavesdroppers can be given as*

$$P_{so}^C(R_0) \simeq \frac{2\lambda_e \left(2^{R_0}\right)^{2/\alpha} \Gamma(1 - 2/\alpha)\, \Gamma(2/\alpha)}{\alpha\lambda_b + 2\lambda_e \left(2^{R_0}\right)^{2/\alpha} \Gamma(1 - 2/\alpha)\, \Gamma(2/\alpha)} \tag{21}$$

Proof. Based on the definition of the secrecy outage probability (10) of the cooperative eavesdroppers case, the secrecy outage probability can be obtained as follows:

$$
\begin{aligned}
P_{so}^{C}(R_0) &\simeq \mathbb{P}\left(\frac{|h_{B^*U}|^2 l_{B^*U}^{-\alpha}}{\Sigma_{e\in\Phi_e}\left(|h_{B^*e}|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) \\
&\overset{a}{=} \int_0^{\infty} \mathbb{E}_{\Phi_e}\left(\mathbb{P}\left(|h_{B^*U}|^2 < 2^{R_0} l_{B^*U}^{\alpha} Z_{\Phi_e} \mid \Phi_e\right)\right) \\
&\cdot f_{l_{B*U}}(l)\, dl = \int_0^{\infty} \mathbb{E}_{\Phi_e}\left(1\right. \\
&\left. - \exp\left(-2^{R_0} l_{B^*U}^{\alpha} Z_{\Phi_e}\right)\right) f_{l_{B*U}}(l)\, dl \overset{b}{=} 1 \\
&- \int_0^{\infty} \exp\left(\frac{-2\pi\lambda_e \left(2^{R_0}\right)^{2/\alpha} \Gamma(1-2/\alpha)\Gamma(2/\alpha)}{\alpha}\right. \\
&\left. \cdot\, l_{B^*U}^{2}\right) f_{l_{B^*U}}(l)\, dl \\
&\overset{c}{=} \frac{2\lambda_e \left(2^{R_0}\right)^{2/\alpha} \Gamma(1-2/\alpha)\Gamma(2/\alpha)}{\alpha\lambda_b + 2\lambda_e \left(2^{R_0}\right)^{2/\alpha} \Gamma(1-2/\alpha)\Gamma(2/\alpha)}
\end{aligned}
\tag{22}
$$

where $Z_{\Phi_e} = \Sigma_{e\in\Phi_e}|h_{B^*e}|^2 l_{B^*e}^{-\alpha}$. Step (a) is derived based on the independence between Φ_b and Φ_e, and step (b) is the Laplace transform of Z_{Φ_e} given by $\mathbb{E}_{\Phi_e}(e^{-sZ_{\Phi_e}}) = \exp(-2\pi\lambda_e s^{2/\alpha}\Gamma(1-2/\alpha)\Gamma(2/\alpha)/\alpha)$ [34]. Step (c) utilizes the integral of exponential functions [31, eq. (3.326.2)].

From (21), it is easy to know that, with the increasing of the density of eavesdroppers, the secrecy outage probability increases, and the secrecy outage probability increases as the threshold R_0 increases. □

3.2.2. Average Secrecy Rate. In the scenario of cooperative eavesdroppers, the average secrecy rate at the typical user $\overline{R}_s^C$ can also be calculated by the integral over all possible values of R_s as stated in Proposition 5. Thus, we obtain $\overline{R}_s^C = \int_0^{\infty}(1 - P_{so}^{C}(\mathrm{R}_0))dR_0$.

Corollary 6. *The average secrecy rate at the typical user is provided by*

$$
\begin{aligned}
\overline{R}_s^C &= \int_0^{\infty} \frac{\alpha\lambda_b}{\alpha\lambda_b + 2\lambda_e \left(2^{R_0}\right)^{2/\alpha} \Gamma(1-2/\alpha)\Gamma(2/\alpha)} dR_0 \\
&= \int_0^{\infty} \frac{\alpha\lambda}{\alpha\lambda_b + 2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha)\, e^{(2\ln 2/\alpha)R_0}} dR_0 \\
&\overset{a}{=} \frac{\alpha}{2\ln 2} \cdot \ln\left(1 + \frac{\alpha\lambda_b}{2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha)}\right),
\end{aligned}
\tag{23}
$$

where step (a) follows the integral result for the form of integrand herein, which can be found in [32, eq. (5.1.2.4.2)].

When α increases, the typical user will achieve a larger average secrecy rate from formula (23). It is the same as the scenario of noncooperative eavesdropping. And the large density of eavesdroppers can reduce the average secrecy rate.

4. Secrecy Performance of Multiantenna System

In this section, comparing with the single-antenna system, we assume that the BS are equipped with multiple antennas and the typical user and each eavesdropper are equipped with a single antenna. Furthermore, we assume that the serving BS employs the TAS scheme to enhance secrecy performance in the cellular network. In this case, the typical user first gives feedback to the index of the antenna that maximizes its SNR. Then, the serving BS uses the selected antenna to broadcast the signal. Therefore, the selected s^{th} antenna can be expressed as

$$
s = \arg\max_{k\in[1,L]} \left(\left|h_{B_k^*U}\right|^2\right), \tag{24}
$$

where $h_{B_k^*U}$ is the channel between the k^{th} antenna at the serving BS and the typical user [35].

We consider that all the channels undergo independent Rayleigh fading channels. Thus, the PDF of $|h_{B_k^*U}|^2$ follows the form of exponential distribution, i.e.,

$$
f_{|h_{B_k^*U}|^2}(x) = \frac{1}{\overline{\gamma}} \exp\left(-\frac{x}{\overline{\gamma}}\right), \tag{25}
$$

where $\overline{\gamma} = \mathbb{E}[|h_{B_k^*U}|^2]$. Furthermore, we can derive the CDF of $|h_{B_k^*U}|^2$ as

$$
F_{|h_{B_k^*U}|^2}(x) = 1 - \exp\left(-\frac{x}{\overline{\gamma}}\right). \tag{26}
$$

According to the relationship given in (24), the CDF of $|h_{B_s^*U}|^2$ can be found using order statistics, i.e., $F_{|h_{B_s^*U}|^2}(x) = [F_{|h_{B_k^*U}|^2}(x)]^L$, which can be derived by (26) Relying on the binomial theorem, followed by some algebraic manipulations; the CDF of $|h_{B_s^*U}|^2$ can be reexpressed as

$$
F_{|h_{B_s^*U}|^2}(x) = \sum_{n=0}^{L} (-1)^n \binom{L}{n} \exp\left(-\frac{nx}{\overline{\gamma}}\right). \tag{27}
$$

Hence, the PDF of $|h_{B_s^*U}|^2$ can be calculated as

$$
f_{|h_{B_s^*U}|^2}(x) = \sum_{n=0}^{L} (-1)^{n+1} \frac{n}{\overline{\gamma}} \binom{L}{n} \exp\left(-\frac{nx}{\overline{\gamma}}\right). \tag{28}
$$

In the following analysis, we assume $\overline{\gamma} = 1$ to simplify calculation.

4.1. Noncooperative Eavesdroppers. In this section, we still use two secrecy performance metrics, i.e., the secrecy outage probability and average secrecy rate, to evaluate the security of cellular network.

4.1.1. Secrecy Outage Probability. The secrecy outage probability under the TAS scheme can be calculated by

$$P_{so}^{NC}(R_0) = \mathbb{P}\left(\frac{\left|h_{B_s^*U}\right|^2 l_{B^*U}^{-\alpha}}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) \tag{29}$$

Proposition 7. *The secrecy outage probability for the scenario of noncooperative eavesdroppers can be expressed as*

$$\begin{aligned} &P_{so}^{NC}(R_0) \\ &\simeq \sum_{n=0}^{L}\sum_{k=1}^{\infty}(-1)^{n+1}\binom{L}{n}\frac{\Gamma\left((2/\alpha)(k-1)+1\right)}{n^{(2/\alpha)(k-1)}} \\ &\times\left(\frac{-\lambda_b\alpha}{2\lambda_e\Gamma(2/\alpha)\left(2^{R_0}\right)^{2/\alpha}}\right)^{k-1} \end{aligned} \tag{30}$$

Proof. Based on the definition of the secrecy outage probability, the secrecy outage probability can be obtained as follows:

$$\begin{aligned} P_{so}^{NC}(R_0) &\simeq \mathbb{P}\left(\frac{\left|h_{B_s^*U}\right|^2 l_{B^*U}^{-\alpha}}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) = 1 \\ &- \mathbb{E}_{\Phi_b,\Phi_e}\left(\prod_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2\right.\right. \\ &\left.\left.< \frac{\left|h_{B_s^*U}\right|^2 l_{B^*U}^{-\alpha}}{2^{R_0}} l_{B^*e}^{\alpha} \mid \Phi_b,\Phi_e\right)\right) \overset{a}{=} 1 \\ &- \mathrm{E}_{\Phi_b}\left(\exp\left(-\frac{2\pi\lambda_e 2^{R_0}}{\alpha\left|h_{B^*U}\right|^{2/\alpha} l_{B^*U}^{-2}}\Gamma\left(\frac{2}{\alpha}\right)\right) \mid \Phi_b\right) \\ &= 1 \\ &- \mathrm{E}_{|h_{B^*U}|^2}\left(\int_0^{\infty}\exp\left(-\frac{2\pi\lambda_e\left(2^{R_0}\right)^{2/\alpha}}{\alpha\left|h_{B^*U}\right|^{2/\alpha} l_{B^*U}^{-2}}\times\Gamma\left(\frac{2}{\alpha}\right)\right)\right. \\ &\left.\cdot f_{l_{B^*U}}(l)\,dl \mid \left|h_{B^*U}\right|^2\right) \overset{b}{=} \sum_{n=0}^{L}(-1)^{n+1} \\ &\cdot n\binom{L}{n} \\ &\cdot\int_0^{\infty}\left(\frac{2\lambda_e\Gamma(2/\alpha)\left(2^{R_0}\right)^{2/\alpha}e^{-nx}}{\lambda_b\alpha x^{2/\alpha}+2\lambda_e\Gamma(2/\alpha)\left(2^{R_0}\right)^{2/\alpha}}\right)dx \\ &\overset{c}{=} \sum_{n=0}^{L}\sum_{k=1}^{\infty}\frac{\binom{L}{n}}{(-1)^{-n+1}} \\ &\cdot\frac{\Gamma\left((2/\alpha)(k-1)+1\right)}{n^{(2/\alpha)(k-1)}}\left(\frac{-\lambda_b\alpha}{2\lambda_e\Gamma(2/\alpha)\left(2^{R_0}\right)^{2/\alpha}}\right)^{k-1}, \end{aligned} \tag{31}$$

where step (a) is based on the PGFL of PPPs Φ_e, and step (b) follows the PDF of l_{B^*U} and $|h_{B_s^*U}|^2$. Step (c) is derived by the exponential function [31, eq. (1.211.1)]. □

4.1.2. Average Secrecy Rate. Based on the $P_{so}^{NC}(R_0)$ in Proposition 7, the average secrecy rate at the typical user can be derived by $\overline{R}_s^{NC} = \int_0^{\infty}(1 - P_{so}^{NC}(R_0))dR_0$.

Corollary 8. *The average secrecy rate is provided by*

$$\begin{aligned} &\overline{R}_s^{NC} \\ &= \sum_{n=0}^{L}\sum_{k=1}^{\infty}\binom{L}{n}\frac{(-1)^{n+k}}{n^{2k/\alpha-1}\ln 2}\left(\frac{\alpha\lambda_b}{2\lambda_e\Gamma(2/\alpha)}\right)^k\Gamma\left(\frac{2k}{\alpha}\right) \end{aligned} \tag{32}$$

Proof. With the help of (25), the desired results can be easily derived by following the similar procedures as the single-antenna scenario. □

4.2. Cooperative Eavesdroppers. In this subsection, the effect of cooperative eavesdroppers on secrecy performance under different network parameters is given for the multiantenna scenario.

4.2.1. Secrecy Outage Probability. Similar to (20), the secrecy outage probability $P_{so}^{C}(R_0)$ under the TAS scheme can be calculated by

$$P_{so}^{C}(R_0) = \mathbb{P}\left(\frac{\left|h_{B_s^*U}\right|^2 l_{B*U}^{-\alpha}}{\sum_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) \tag{33}$$

Proposition 9. *The secrecy outage probability for the scenario of cooperative eavesdroppers can be given as*

$$\begin{aligned} P_{so}^{C}(R_0) &\simeq \sum_{n=0}^{L}\left(\binom{L}{n}(-1)^n\right. \\ &\left.\times\frac{\alpha\lambda_b}{\alpha\lambda_b+2\lambda_e\Gamma(1-2/\alpha)\Gamma(2/\alpha)n^{2/\alpha}\left(2^{R_0}\right)^{2/\alpha}}\right) \end{aligned} \tag{34}$$

Proof. In multiantenna system, the secrecy outage probability can be expressed as (21). From the definition, we can derive the secrecy outage probability as follows:

$$\begin{aligned} P_{so}^{C}(R_0) &\simeq \mathbb{P}\left(\frac{\left|h_{B_s^*U}\right|^2 l_{B^*U}^{-\alpha}}{\Sigma_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) \\ &= \int_0^{\infty}\mathbb{E}_{\Phi_e}\left(\mathbb{P}\left(\left|h_{B_s^*U}\right|^2 < 2^{R_0} l_{B^*U}^{\alpha} Z_{\Phi_e} \mid \Phi_e\right)\right) \\ &\cdot f_{l_{B^*U}}(l)\,dl \overset{a}{=} \mathbb{E}_{\Phi_e}\left(1 - e^{-2^{R_0} l_{B^*U}^{\alpha} Z_{\Phi_e}}\right)^L \end{aligned}$$

$$\overset{b}{=} \sum_{n=0}^{L} \binom{L}{n} (-1)^n \mathbb{E}_{\Phi_e}\left(e^{-2^{R_0} l_{B^*U}^{\alpha} Z_{\Phi_e} n}\right)$$

$$\overset{c}{=} \sum_{n=0}^{L} \binom{L}{n} (-1)^n \cdot \frac{\alpha\lambda_b}{\alpha\lambda_b + 2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha) n^{2/\alpha} \left(2^{R_0}\right)^{2/\alpha}} \tag{35}$$

where $Z_{\Phi_e} = \Sigma_{e\in\Phi_e} |h_{B^*e}|^2 l_{B^*e}^{-\alpha}$. Step (a) is derived based on the CDF of $|h_{B_s^*U}|^2$, and according to the polynomial expansion [32, eq. (1.1.10)], step (b) can be obtained. In addition, step (c) is the Laplace transform of Z_{Φ_e} [34]. □

4.2.2. Average Secrecy Rate. Combining Proposition 9 and the integral formula in [32, eq. (5.1.2.4.2)], we can obtain the average secrecy rate at the typical user as follows.

Corollary 10. *The average secrecy rate is provided by*

$$\overline{R}_s^C = \sum_{n=1}^{L} \binom{L}{n} \cdot \frac{(-1)^{n+1}\alpha}{2\ln 2} \ln\left(1 + \frac{\alpha\lambda_b}{2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha) n^{2/\alpha}}\right) \tag{36}$$

Proof. Using the definition of the average secrecy rate, we can obtain the expression as follows:

$$\overline{R}_s^C = \int_0^{\infty} \sum_{n=0}^{L} \frac{(-1)^n \binom{L}{n} \alpha\lambda_b}{\alpha\lambda_b + 2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha) n^{2/\alpha} \left(2^{R_0}\right)^{2/\alpha}} dR_0$$

$$= \sum_{n=0}^{L} \frac{\binom{L}{n}}{(-1)^{-n}} \cdot \int_0^{\infty} \frac{\alpha\lambda_b dR_0}{\alpha\lambda_b + 2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha) n^{2/\alpha} \left(2^{R_0}\right)^{2/\alpha} e^{(2\ln 2/\alpha)R_0}} \tag{37}$$

$$\overset{a}{=} \sum_{n=0}^{L} \binom{L}{n} \frac{(-1)^{n+1}\alpha}{2\ln 2} \cdot \ln\left(1 + \frac{\alpha\lambda_b}{2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha) n^{2/\alpha}}\right)$$

where step (a) is based on the integral formula in [32, eq. (5.1.2.4.2)].

For the secrecy outage probability, we find that P_{so}^{NC} and P_{so}^{C} are a function of various factors, e.g., L, λ_e, λ_b, R_0, α. For any given L, λ_b, R_0, α, the secrecy outage probability solely depends on eavesdroppers' density. And a large α and L can decrease the secrecy outage probability in both cooperative and noncooperative eavesdroppers. As to the average secrecy rates $\overline{R}_S^{NC}$ and $\overline{R}_S^{C}$, the more number of antennas L and large path loss exponent α is also beneficial for improving the average secure transmission rate. Detailed analysis on the impacts of these factors to the security can be seen in Section 5. □

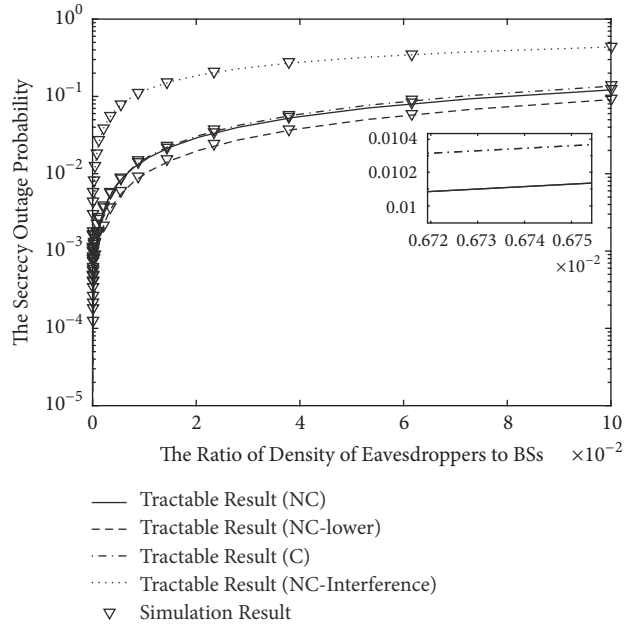


Figure 2: The secrecy outage probability as a function of λ_e/λ_b.

5. Numerical Results and Discussion

In this section, we provide simulation results to verify our analyses for different scenarios as mentioned above. We show the secrecy outage probability and the average secrecy rate as functions of λ_e/λ_b, α, R_0, and L. In the simulation analysis, we assume the transmit SNR $P_{BS}/\sigma^2 = 20dB$. In the following figures, NC and C denote the noncooperative eavesdroppers and cooperative eavesdroppers, respectively. In addition, the NC-lower and NC-upper corresponded, respectively, to the lower bound of the secrecy outage probability and the upper bound of the average secrecy rate under the noncooperative eavesdroppers scenarios, and NC-Interference is the secrecy performance in the noncooperative eavesdropping case with considering interference.

Figure 2 verifies the secrecy outage probability for two different scenarios as a function of λ_e/λ_b. We observe that the secrecy outage probability increases as the density of eavesdroppers increases. This is because large λ_e can reduce the distance between eavesdropper and BS. When the interference is considered, the secrecy outage probability has a large increase comparing to the noninterference case in noncooperative eavesdropping scenario. This indicates that the interference has an important effect for the secrecy performance in such a scenario. Moreover, with the increasing of λ_e, the lower bound of the secrecy outage probability is different from the performance of the exact analytical expression in (4). This difference shows that the impact of small-scale fading is considerable in certain λ_e regime. And the secrecy outage probability of the scenario of noncooperative eavesdroppers is always lower than that of cooperative eavesdroppers, because sharing information among eavesdroppers makes it easier to decode the confidential message.

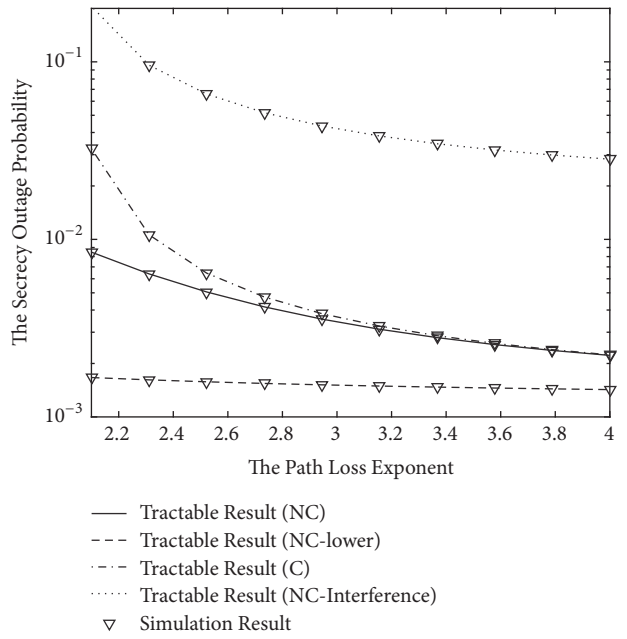


FIGURE 3: The secrecy outage probability as a function of α.

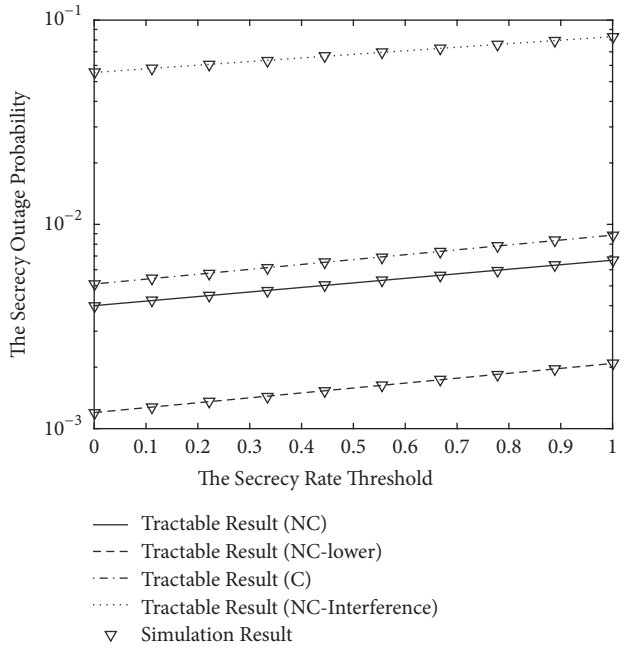


FIGURE 4: The secrecy outage probability as a function of R_0.

Figures 3 and 4 demonstrate the secrecy outage probability as a function of path loss exponent α and threshold R_0, respectively. It is easy to find that the secrecy outage probability decreases with the increasing of α and increases with the increasing of R_0. This is because larger path loss exponent indicates worse signal condition for both eavesdroppers and the typical user, whereas the impact on the former is turned out to be more influential on the secrecy outage probability. And the large threshold R_0 requires larger channel difference between legal and illegal links, so it is more likely to be easily interrupted for the transmission. Another fact is that the large value of α makes the difference on secrecy performance between the lower bound and the exact analytical expression become small. This explains that the effect of secrecy performance caused by small-scale fading cannot be ignored in small α environment. In addition, when the interference caused by BSs is considered, the secrecy performance is the worst in these scenarios.

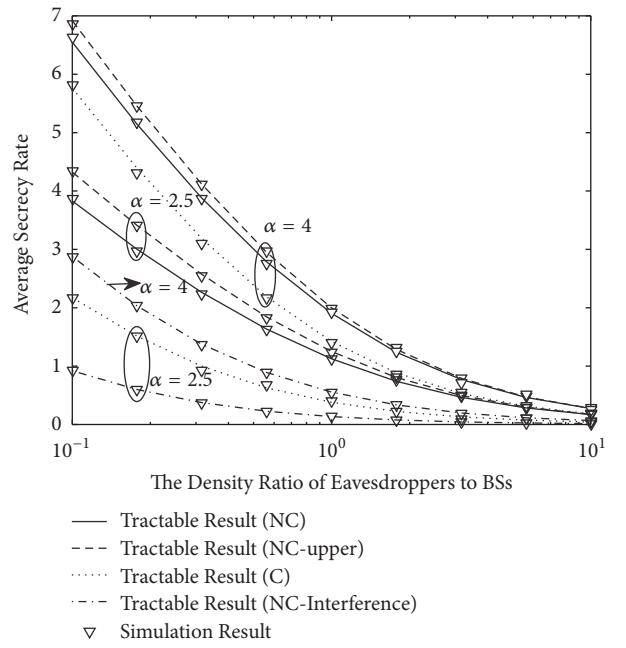


FIGURE 5: The average secrecy rate as a function of λ_e/λ_b for two different scenarios.

Figure 5 shows the average secrecy rate as a function of λ_e/λ_b under various path loss exponents α. The result shows that the average secrecy rate decreases as the density of eavesdroppers λ_e/λ_b increases. For a given λ_e/λ_b, the large path loss exponent α can improve the average secrecy rate. And the average secrecy rate is the lowest when interference is considered. This is because the interference reduces the channel capacity of legal link. At the same time, we can observe that the gap of the average secrecy rate between the scenarios of noncooperative eavesdroppers and cooperative eavesdroppers is becoming narrower with the increasing of λ_e/λ_b, especially the gap between the upper bound of the average secrecy rate with the exact analytical expression in (9). The reason is that the large-scale fading is gradually becoming the main cause on secrecy performance. Moreover, because eavesdroppers can exchange information with each other in the scenario of cooperative eavesdroppers, the secrecy performance is always worse than the scenario of noncooperative eavesdroppers.

Figure 6 illustrates the secrecy outage probability as a function of the number of antennas L. We can know that a slight increase of L effectively decreases the secrecy outage probability. This is because more antennas make BS transmit message in a better channel quality with a large probability. When λ_e becomes very small or large, the gap of secrecy

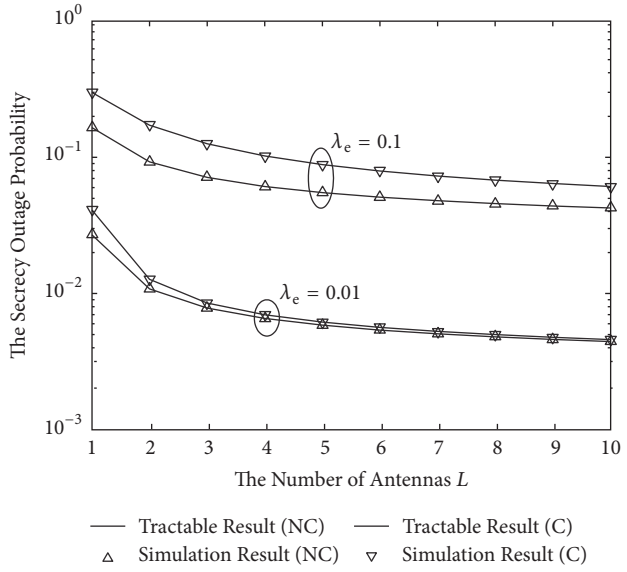


FIGURE 6: The secrecy outage probability as a function of L with $\lambda_e = 0.01$, $\lambda_e = 0.1$.

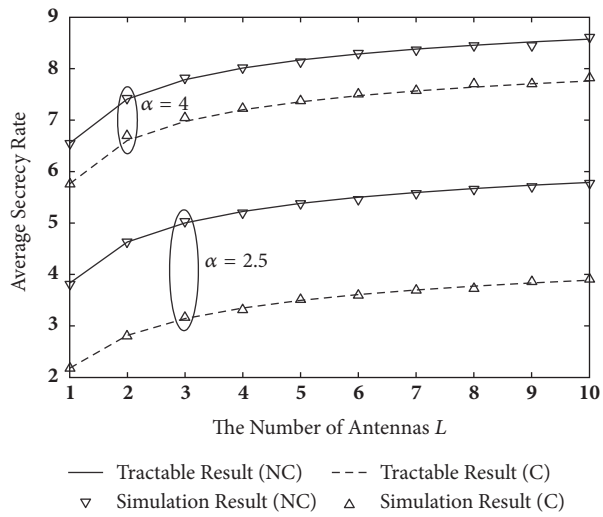


FIGURE 7: The average secrecy rate as a function of L with $\alpha = 2.5$, $\alpha = 4$.

outage probability between the scenarios of noncooperative and cooperative eavesdroppers will become narrower. This can be explained as follows: a smaller λ_e decreases the average number of eavesdroppers in a certain area, which naturally makes fewer eavesdroppers share information. In addition, a larger λ_e means eavesdroppers are closer to BSs, which leads to the worst eavesdropper being capable enough of intercepting the information transmission. In this case, whether or not eavesdroppers can cooperate has no significant effect on secrecy performance. Moreover, an interesting finding is that the gap between cooperative and noncooperative eavesdroppers does not change obviously as L increases. When the density of eavesdroppers is large, increasing the number of antennas has litter improvement on the secrecy outage probability. This is because the number of eavesdroppers has become the main influence factor to damage the secrecy performance.

In Figure 7, the average secrecy rate $\overline{R}_S^{NC}$ in (32) and $\overline{R}_S^{C}$ in (36) versus the number of antennas L with different path loss exponent α is presented. Both average secrecy rate in noncooperative and cooperative eavesdroppers scenarios monotonically increase with the increasing of L, with the benefit being brought by multiple antennas. But there is no obvious change in the gap between $\overline{R}_S^{NC}$ and $\overline{R}_S^{C}$ for $\alpha = 4$ and $\alpha = 2.5$ with an increasing of L, which indicates that multiple antenna has equal effects on the improvement of the secrecy rate in noncooperative and cooperative eavesdroppers scenarios. We also find that the average secrecy rate is smaller than that with $\alpha = 4$, which is the same as shown in Figure 4. Comparing to a small $\alpha = 2.5$, the average secrecy rate $\overline{R}_S^{NC}$ is closer to $\overline{R}_S^{C}$ when $\alpha = 4$. In other words, the cooperative eavesdroppers provides less additional degradation on the secrecy performance compared with the noncooperative eavesdroppers when α becomes larger. The reason is that more severe path loss makes the influence of the worst eavesdroppers more significant compared with other eavesdroppers, which has weakened the impact of eavesdroppers' cooperation.

6. Conclusion

In this paper, the exact expressions for the secrecy outage probability and average secrecy rate at the typical user are presented by using the tool of stochastic geometry in large-scale cellular networks. These results are represented by numerical simulations. Our results show that, with the increasing of density ratio of eavesdroppers to BSs, the secrecy performance decreases in both scenarios of noncooperative and cooperative eavesdroppers, and the typical user can achieve better secrecy performance in the environment with large path loss exponent. Furthermore, the secrecy performance in the scenario of noncooperative eavesdroppers is always better than that of cooperative eavesdroppers, and the interference caused by BS will damage the secrecy performance. Moreover, we give more accurate results than predecessors, because of considering both of the large-scale and small-scale fading. At the same time, we know that the small-scale fading cannot be ignored in eavesdroppers with certain density regime and small loss path exponent environment. Finally, using the TAS technology can effectively enhance the secrecy performance compared to single-antenna system, but it cannot obviously improve the difference on secrecy performance between the scenarios of noncooperative and cooperative eavesdroppers.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61471393 and no. 61771487). This paper was presented in part at the IEEE 3rd International Conference on Computer and Communications (ICCC 2017), Chengdu, China, Dec. 2017.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 2067–2076, 2011.

[4] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Processing Letters*, vol. 19, no. 2, pp. 71–74, 2012.

[5] L. Dong, Z. Han, A. P. Petropulu, and H. . Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, part 2, pp. 1875–1888, 2010.

[6] B. He and X. Zhou, "Secure On-Off transmission design with channel estimation errors," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1923–1936, 2013.

[7] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[8] L. Sun and Q. Du, "Physical layer security with its application in 5g networks: A review," *China Comunications*, vol. 14, no. 12, p. 14, 2017.

[9] S. Weber, J. G. Andrews, and N. Jindal, "The effect of fading, channel inversion, and threshold scheduling on ad hoc networks," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4127–4149, 2007.

[10] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2764–2775, 2011.

[11] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure Transmission Design for Cognitive Radio Networks With Poisson Distributed Eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 373–387, 2016.

[12] X. Xu, W. Yang, Y. Cai, and S. Jin, "Secure Transmission Design for Cognitive Radio Networks With Poisson Distributed Eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 34, no. 10, pp. 2706–2722, 2016.

[13] S. Vuppala and G. Abreu, "Secrecy outage in random wireless networks subjected to fading," in *Proceedings of the 2013 IEEE 24th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 446–450, London, September 2013.

[14] T.-X. Zheng, H.-M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Communications Letters*, vol. 18, no. 8, pp. 1299–1302, 2014.

[15] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy Outage Analysis for Downlink Transmissions in the Presence of Randomly Located Eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1195–1206, 2017.

[16] H. Chen, X. Tao, N. Li, and X. Li, "Secrecy performance of the artificial noise assisted broadcast channel with confidential messages and external eavesdroppers," in *Proceedings of the ICC 2016 - 2016 IEEE International Conference on Communications*, pp. 1–6, Kuala Lumpur, Malaysia, May 2016.

[17] T. Zheng, H. Wang, R. Huang, and P. Mu, "Adaptive artificial noise transmission against randomly distributed eavesdroppers," in *Proceedings of the 2015 10th International Conference on Communications and Networking in China (ChinaCom)*, pp. 248–253, Shanghai, China, August 2015.

[18] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Transactions on Communications*, vol. 63, no. 11, pp. 4347–4362, 2015.

[19] L. Zhang, H. Zhang, D. Wu, and D. Yuan, "Improving Physical Layer Security for MISO Systems via Using Artificial Noise," in *Proceedings of the GLOBECOM 2015 - 2015 IEEE Global Communications Conference*, pp. 1–6, San Diego, CA, USA, December 2015.

[20] G. Chen and J. P. Coon, "Secrecy Outage Analysis in Random Wireless Networks with Antenna Selection and User Ordering," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 334–337, 2017.

[21] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 3122–3134, 2011.

[22] H. Wang, X. Zhou, and M. C. Reed, "On the physical layer security in large scale cellular networks," in *Proceedings of the 2013 IEEE Wireless Communications and Networking Conference, WCNC 2013*, pp. 2462–2467, chn, April 2013.

[23] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2776–2787, 2013.

[24] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "A new model for physical layer security in cellular networks," in *Proceedings of the 2014 1st IEEE International Conference on Communications, ICC 2014*, pp. 2147–2152, aus, June 2014.

[25] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 6, pp. 2006–2021, 2014.

[26] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204–1219, 2016.

[27] L. Tao, W. Yang, Y. Cai, and D. Chen, "Secrecy performance analysis in large-scale cellular networks via stochastic geometry," in *Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pp. 1444–1449, Chengdu, December 2017.

[28] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications*, Wiley Series in Probability and Mathematical Statistics: Applied Probability and Statistics, John Wiley & Sons, Ltd., Chichester, New York, NY, USA, 1995.

[29] M. Haenggi, "On distances in uniformly random networks," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 51, no. 10, pp. 3584–3586, 2005.

[30] M. Haenggi, *Stochastic Geometry for Wireless Networks*, Cambridge University Press, 2012.

[31] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, New York, NY, USA, 7th edition, 2007.

[32] A. Jeffrey and H.-H. Dai, *Handbook of Mathematical Formulas and Integrals*, Academic Press of Elsevier, Burlington, Amsterdam, Netherlands, 4th edition, 2008.

[33] Y. Zhu, L. Wang, K. Wong, and R. W. Heath, "Physical Layer Security in Large-Scale Millimeter Wave Ad Hoc Networks," in *Proceedings of the GLOBECOM 2016 - 2016 IEEE Global Communications Conference*, pp. 1–6, Washington, DC, USA, December 2016.

[34] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks?" *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 624–632, 2014.

[35] N. S. Ferdinand, D. B. Da Costa, A. L. F. De Almeida, and M. Latva-Aho, "Physical layer secrecy performance of TAS wiretap channels with correlated main and eavesdropper channels," *IEEE Wireless Communications Letters*, vol. 3, no. 1, pp. 86–89, 2014.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 2104162, 10 pages
https://doi.org/10.1155/2018/2104162

Research Article

Probabilistic Caching Placement in the Presence of Multiple Eavesdroppers

Fang Shi,[1] Lisheng Fan,[1] Xin Liu,[2] Zhenyu Na,[3] and Yanchen Liu[4]

[1]*School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China*
[2]*School of Information and Communication Engineering, Dalian University of Technology, Dalian, China*
[3]*School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China*
[4]*Department of Building Science, Tsinghua University, Beijing 100084, China*

Correspondence should be addressed to Lisheng Fan; lsfan@gzhu.edu.cn

Received 1 February 2018; Accepted 1 April 2018; Published 8 May 2018

Academic Editor: Li Sun

The wireless caching has attracted a lot of attention in recent years, since it can reduce the backhaul cost significantly and improve the user-perceived experience. The existing works on the wireless caching and transmission mainly focus on the communication scenarios without eavesdroppers. When the eavesdroppers appear, it is of vital importance to investigate the physical-layer security for the wireless caching aided networks. In this paper, a caching network is studied in the presence of multiple eavesdroppers, which can overhear the secure information transmission. We model the locations of eavesdroppers by a homogeneous Poisson Point Process (PPP), and the eavesdroppers jointly receive and decode contents through the maximum ratio combining (MRC) reception which yields the worst case of wiretap. Moreover, the main performance metric is measured by the average probability of successful transmission, which is the probability of finding and successfully transmitting all the requested files within a radius R. We study the system secure transmission performance by deriving a single integral result, which is significantly affected by the probability of caching each file. Therefore, we extend to build the optimization problem of the probability of caching each file, in order to optimize the system secure transmission performance. This optimization problem is nonconvex, and we turn to use the genetic algorithm (GA) to solve the problem. Finally, simulation and numerical results are provided to validate the proposed studies.

1. Introduction

The arrival of big data era has led to a growing communication business, and the demand for wireless data rates becomes higher and higher. In order to reduce the transmission load and capacity crunch, caching is emerging as an important technology in the next generating wireless networks. The main idea behind caching is to store parts of the popular contents in caching helpers' memory and leverage the locally stored content to reduce transmission links, thereby reducing the transmission load and speeding up the transmission of requested content. And the different cache strategies have been well studied [1–9]. Specifically in [1], the authors considered a cluster-centric small-cell networks with combined design of cooperative caching and transmission policy and proposed a combined caching scheme to increase the local content diversity. The distributed caching placement has been studied in [2, 3], and in [3], the authors proposed to combine two recent schemes, distributed caching of content in small cells and cooperative transmissions from nearby base stations/BSs to achieve unprecedented content delivery speeds while reducing backhaul cost and delay. The probabilistic caching placement was studied in [4–7]. Departing from the conventional cache hit optimization in cache-enabled wireless networks, the authors in [4] considered an alternative optimization approach for the probabilistic caching placement in stochastic wireless D2D caching networks, proposed the cache-aided throughput, and provided a closed-form approximation of cache-aided throughput. Different from [4], the authors in [5] studied a probabilistic small-cell caching strategy and considered two kinds of network architectures: the small-cell base stations (SBSs) are always

active and the SBSs are activated on demand by mobile users (MUs). The authors in [6, 7] proposed to use different optimization strategies to optimize the probabilistic caching placement. In addition, in paper [8], the analysis, design, and optimization of geographic caching were presented; and in paper [9], a hybrid caching scheme was studied which was jointly optimized with the transmission schemes to achieve a fine balance between the signal cooperation gain and the caching diversity gain.

The emergence of cache and wireless devices has solved a lot of problems, such as reducing transmission load, traffic, and energy consumption of the backhaul. The existing works on the wireless caching and transmission mainly focus on the communication scenarios without eavesdroppers, for instance, [4–9]. But when the eavesdroppers appear, it is of vital importance to investigate the physical-layer security for the wireless caching aided networks. In recent years, some researchers also have took into account the problem of secure caching, such as [10–13]. Specially, in [10], the problem of secure caching in the presence of an external wiretapper for both centralized and decentralized cache placement was analyzed. In [11], unmanned aerial vehicles assisted secure transmission for scalable videos in hyperdense networks via caching was studied. The authors in [12] studied a cooperative network with caching relays to reduce the transmission links overheard by the eavesdropper. Moreover, a novel hybrid cache placement was proposed to cache the popular contents, and the closed expressions of the secrecy outage probability and average secrecy capacity were obtained. The authors in [13] studied a framework of communication, caching, and computing- (3C-) oriented small-cell networks with interference alignment, in which caching and computing are exploited to simplify the network topology, improve the throughput, reduce the backhaul load, and guarantee the quality of experience of users.

The works about the physical-layer security have been studied such as the works in [14–16]. In [14], Wyner proved that the secure communication is feasible without cryptography technology as long as the eavesdropper's instantaneous channel is worse than the legitimate user's instantaneous channel. Based on Wyner's wiretap channel model, the authors in [15] studied the secrecy capacity over Gaussian channel. And the knowledge about the wireless information-theoretic security has been studied in [16]. In addition, the secrecy performance of wireless communication has been studied in [17–19]. Specifically in [17], the impact of cochannel interference and wiretap on the security performance of multiple amplify-and-forward (AF) relaying networks has been studied. In [18], the physical-layer security of a multiantenna transmission system in the presence of Poisson distributed eavesdroppers was analyzed, and the two different cases including the eavesdroppers being colluding and noncolluding were also analyzed in the paper. The relaying techniques for enhancing the physical-layer security have been studied in [19–26].

According to the above analysis, the main idea of this paper is to design, analyze, and optimize the probabilistic caching placement based on the security of transmission. Without loss of generality, the locations of relays are modeled by a homogeneous PPP. Moreover, considering the randomness of eavesdroppers' positions, we also model the locations of eavesdroppers by a homogeneous PPP, and the eavesdroppers jointly receive and decode contents through MRC reception which yields the worst case of wiretap. In addition, the main performance metric is measured by the average probability of successful transmission; the analytical result and analytical lower bound of the average probability of successful transmission are presented in the performance analysis. Due to the nonconvex nature and the complication of the average probability of successful transmission, it is too complicated to get a closed-form solution. Therefore, the GA is used to find the optimal solution instead of deriving a closed-form solution. And in order to better evaluate the proposed caching placement, we use the most popular content (MPC) caching placement as a standard for comparison, where the method of MPC caching placement is to cache the most popular contents in all relays. Finally, the numerical and simulation results are provided to validate the proposed studies.

The novelties and main contributions of this paper can be summarized as follows:

(i) Based on the security of transmission, the probabilistic caching placement is designed in the presence of multiple eavesdroppers which follow the homogeneous PPP.

(ii) The main performance metric is measured by the average probability of successful transmission, and both the analytical result and the analytical lower bound of the average probability of successful transmission are presented. Moreover, GA is used to optimize the average probability of successful transmission to maximize the system performance.

(iii) The simulation results are provided to demonstrate the studies that the optimized probabilistic caching placement is superior to the MPC caching placement, and the system secure performance can be improved by increasing the transmit power, the cache size, and the intensity of relays but will deteriorate with larger intensity of eavesdroppers.

The rest of this paper is organized as follows. In Section 2, we introduce the system model and study the probabilistic caching placement and the file transmission. In Section 3, the system performance is analyzed. And the optimization of probabilistic caching placement is presented in Section 4. The numerical and simulation results are provided in Section 5. The conclusions are presented in Section 6.

Notations. In this paper, we use P_i^{find} and P_i^{suc} to represent the probability of finding the requested file i and the successful probability of transmitting the file i, respectively. Moreover, we use $\overline{P}_{\text{suc}}$ to represent the average probability of successful transmission and use $\overline{P}_{\text{low}}^{\text{suc}}$ to represent the lower bound of average probability of successful transmission.

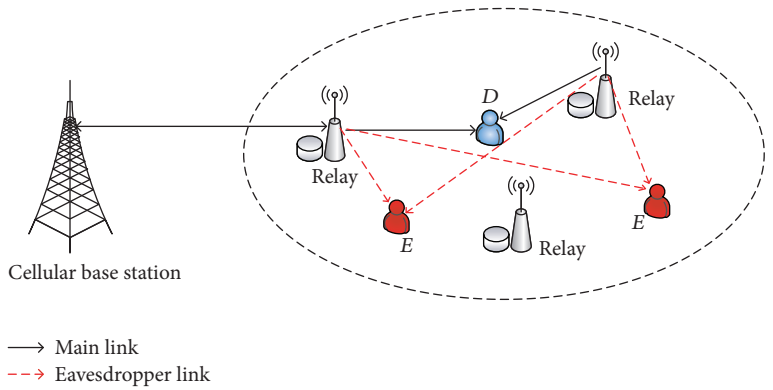


Figure 1: System model.

2. System Model

Figure 1 depicts the system model of a wireless caching network, which comprises a cellular base station (BS), a random legitimate user (D), multiple DF relays $\{R_k \mid k = 1, 2, \ldots, K\}$ with cache capacity, and multiple eavesdroppers $\{E_l \mid l = 1, 2, \ldots, L\}$ which can overhear messages and bring out the issue of information security [27–30]. Without loss of generality, the locations of relays are modeled by the homogeneous PPP Φ_r with intensity λ_r and the eavesdroppers' positions also follow the homogeneous PPP Φ_e with intensity λ_e.

In this system model, we consider BS has no direct link with D and eavesdroppers [31–33], the transmission is performed only via relays [34–36], and all relays can successfully send the files in their local cache to D within radius R. For legitimate D, if the requested file can be found in relays, the nearest relay directly transfers the file to D; otherwise, the file will be transmitted from BS to the nearest base station and then transmitted to D. Moreover, all wireless links are subjected to Rayleigh flat fading channel with a path loss governed by the exponent $\alpha > 2$ [37–39].

2.1. Cache Placement. We assume that there are N files that have been requested to D, which all have the same size. The case of unequal size will not be considered in this paper, but we can always assume that any file can be divided into blocks of the same size, so the similar analysis also can still be applied. In this paper, the files are characterized by their popularity, namely, the probability that a file is requested by the user. The request probability follows the Zipf distribution, which has been widely used in the literature [1–9]; that is, the request probability of ith file is

$$f_i = \frac{i^{-\gamma}}{\sum_{j=1}^{N} j^{-\gamma}}, \tag{1}$$

where γ is the Zipf parameter with the popularity skewness. According to the request probability, we can find that $f_1 \geq f_2 \geq \cdots \geq f_N$ and $\sum_{i=1}^{N} f_i = 1$.

In this paper, we consider each relay has the same cache memory size C_R ($C_R < N$) and the unit of storage/size is file. Because relays cannot store all files ($KC_R < N$), relays need to judiciously choose which files to store. Thus, we apply the probabilistic caching placement to the file's cache placement and by optimizing the cache placement to prove the system performance.

In the probabilistic model, the contents are independently placed in the cache memories of different relays, according to the same distribution. Therefore, if each relay caches ith file with a certain probability q_i ($0 \leq q_i \leq 1$) independently, we denote by $\mathbf{q} = [q_1, \ldots, q_N]$ the caching probabilities of file $i \in [1, N]$, and due to the cache storage limit, we have

$$\sum_{i=1}^{N} q_i \leq C_R. \tag{2}$$

In this paper, in order to alleviate the traffic and decline the transmission links, our goal is to find an optimal local caching strategy to optimize the system performance. Therefore, we only consider the secure transmission in local devices.

2.2. File Transmission. When a file request occurs, and there is at least one relay that stored the requested file within the radius r, the request would be satisfied and the relay would directly transmit the file to D. If there is more than one relay which has the requested file, the file will be transmitted from the nearest one. In the case where the requested file can not be found in relays, the file must be forwarded from core network to D assisted by nearest relay. Because we only consider the secure transmission in local devices, in the following, we will only analyze the local transmission.

We assume the channel state information (CSI) is known to D; therefore, when D sends the request, the nearest relay R_k ($k \in K$) which has cached the requested file directly transmits the file to D. According to [18], the received SNR at D can be shown as follows:

$$\mathsf{SNR}^D = \rho \eta_d, \tag{3}$$

where $\rho = p_r/\sigma^2$, p_r is the transmit power at relay, σ^2 is the noise power, $\eta_d \triangleq |h_{R_k,D}|^2 r_{R_k,D}^{-\alpha}$ is the channel gains for D, $h_{R_k,D}$ denotes the channel parameters of $R_k \to D$, and $r_{R_k,D}$ represents the distance from D to the nearest relay R_k.

The received SNR at a random eavesdropper E_l is given by

$$\mathrm{SNR}^{E_l} = \rho \eta_{e_l}, \tag{4}$$

where $\eta_{e_l} \triangleq |h_{R_k,E_l}|^2 r_{R_k,E_l}^{-\alpha}$, h_{R_k,E_l} denotes the channel parameters of $R_k \to E$, and r_{R_k,E_l} represents the distance from R_k to E_l.

3. Performance Analysis

In this section, we will analyze the cache hit probability and the average probability of successful transmission, and the average probability of successful transmission is defined as the main performance metric. Moreover, the analytical result and the analytical lower bound of the average probability of successful transmission are presented in this section.

3.1. Cache Hit Probability. In this paper, we define the cache hit probability as a probability that the user D successfully finds the requested file in a given area. From the system model, we know that relays are modeled by a PPP Φ_r with intensity λ_r, so the relays caching the ith file also follow a PPP with density $q_i\lambda_r$. According to the notion of stochastic geometry, in a given area within the radius r, the expected number of relays caching the ith file can be calculated as

$$E[K] = q_i \lambda_r \pi r^2. \tag{5}$$

And from [3–7], we find that, for a PPP distribution with density λ, the probability that there are n nodes in an area within the radius r is

$$F(n, r, \lambda) = \frac{\left(\pi r^2 \lambda\right)^n}{n!} e^{-\pi r^2 \lambda}. \tag{6}$$

Therefore, if we assume user D is located at the origin and find the requested file in an area within the radius R, the probability of finding at least one relay caching the ith file within a radius R is

$$P_i^{\mathrm{find}} = 1 - F\left(0, R, q_i\lambda_r\right) = 1 - e^{-\pi q_i \lambda_r R^2}. \tag{7}$$

3.2. Probability of Successful Transmission. In this paper, we define the probability of successful transmission as the probability of finding and then successfully transmitting the requested file within a radius R. In order to analyze the probability of successful transmission, we firstly analyze the secrecy capacity which is the difference between the capacities of the legitimate channel C_D and the equivalent wiretap channel C_E. Based on the system model, the secrecy capacity can be expressed as [40–43]

$$C_s = \left[\log_2\left(1 + \mathrm{SNR}^D\right) - \log_2\left(1 + \mathrm{SNR}^E\right)\right]^+, \tag{8}$$

where $[x]^+$ returns $\max(0, x)$, $\mathrm{SNR}^E = \rho\eta_e$, and $\eta_e = \sum_{E_l \in \Phi_e} \eta_{e_l}$ is equivalent wiretap channel gain.

Therefore, when the ith file is requested by D, we use r_i to represent the distance to the nearest relay which has cached ith file. The probability of successful transmission can be shown as follows [44–47]:

$$\begin{aligned} P_i^{\mathrm{suc}} &= \Pr\left\{\left[\log_2\left(1 + \mathrm{SNR}^D\right) - \log_2\left(1 + \mathrm{SNR}^E\right)\right] > R_s\right\} \\ &= \Pr\left\{\eta_d > M + \tau\eta_e\right\} \\ &= E_{r_i}\left[\int_0^\infty \int_{M+\tau y}^\infty f_{\eta_d}(x)\, f_{\eta_e}(y)\, d(x)\, d(y)\right], \end{aligned} \tag{9}$$

where R_s is the target secrecy rate, $M = (2^{R_s} - 1)/\rho$, $\tau = 2^{R_s}$, and f_{η_e} and f_{η_d} are the probability distribution function (PDF) of η_e and η_d, respectively.

Because eavesdroppers jointly receive and decode contents with MRC reception, we have $\eta_e = \sum_{E_l \in \Phi_e} \eta_{e_l}$. But since the randomness of eavesdroppers' positions, the exact closed-form expression for the PDF of η_e is difficult to obtain. However, by using the result from [48] and applying the PDF of η_d as $f_{\eta_d}(x) = r_i^\alpha e^{-r_i^\alpha x}$, we can calculate the successful probability of transmitting ith file P_i^{suc} as follows:

$$\begin{aligned} P_i^{\mathrm{suc}} &= E_{r_i}\left[e^{-r_i^\alpha M} \int_0^\infty e^{-r_i^\alpha \tau y} f_{\eta_e}(y)\, dy\right] \\ &= E_{r_i}\left[e^{-r_i^\alpha M} \mathscr{L}_{\eta_e}(s)\right] = \int_0^\infty e^{-r_i^\alpha M} \mathscr{L}_{\eta_e}(s)\, f_{r_i} d_{r_i}, \end{aligned} \tag{10}$$

where $s = r_i^\alpha \tau$ and $\mathscr{L}_{\eta_e}(s)$ is the Laplace transform of η_e. According to [48], we have

$$\begin{aligned} \mathscr{L}_{\eta_e}(s) &= E_{\Phi_e}\left[e^{-s\eta_e}\right] = E_{\Phi_e}\left[\exp\left(-s\sum_{e_l \in \Phi_e} \eta_{e_l}\right)\right] \\ &= E_{\Phi_e}\left[\prod_{e_l \in \Phi_e} E_{|h_{e_l}|}\left(\exp\left(-s\left|h_{e_l}\right|^2 r_{e_l}^{-\alpha}\right)\right)\right] \\ &\overset{(a)}{=} \exp\left\{-E_{|h_{e_l}|}\left(\int_0^\infty \lambda_e \left(1 - \exp\left(-s\left|h_{e_l}\right|^2 r_{e_l}^{-\alpha}\right)\right) 2\pi r_{e_l} d_{r_{e_l}}\right)\right\} \\ &\overset{(b)}{=} \exp\left(-\lambda_e \pi E_{h_{e_l}}\left[\left|h_{e_l}\right|^{4/\alpha}\right] \Gamma\left(1 - \frac{2}{\alpha}\right) s^{2/\alpha}\right), \end{aligned} \tag{11}$$

where step (a) holds for the probability generating functional lemma (PGFL) over PPP [48], step (b) holds for the integration formula $\int_0^\infty x^m \exp(-\beta x^n) d_x = \Gamma(\gamma)/(n\beta^\gamma)$, $\gamma = (m+1)/n$, $E_{h_{e_l}}[|h_{e_l}|^{4/\alpha}]$ can be calculated as

$$E_{h_{e_l}}\left[\left|h_{e_l}\right|^{4/\alpha}\right] = \int_0^\infty x^{2/\alpha} f_{|h_{e_l}|^2}(x)\, d_x = \Gamma\left(1 + \frac{2}{\alpha}\right), \tag{12}$$

and $f_{|h_{e_l}|^2}(x) = e^{-x}$ is the PDF of wiretap channel gain $|h_{R_k,E_l}|$. Therefore, substitute

$$\mathscr{L}_{\eta_e}(s) = \exp\left(-\beta s^{2/\alpha}\right), \tag{13}$$

where $\beta = \lambda_e \pi \Gamma(1 + 2/\alpha)\Gamma(1 - 2/\alpha)$. In this paper, we assume conditioning on $r_i \le R$ as a result of the maximum distance, and the PDF of r_i is given by

$$f_{r_i} = \begin{cases} \dfrac{2\pi q_i \lambda_r r_i}{1 - e^{-\pi q_i \lambda_r R^2}} e^{-\pi q_i \lambda_r r_i^2} & 0 \le r_i \le R \\ 0 & r_i > R. \end{cases} \tag{14}$$

Substituting (13) and (14) in (10), the successful probability of transmitting the file i is given by

$$P_i^{\text{suc}} = \int_0^{\infty} \exp\left(-r_i^{\alpha} M - \beta\tau^{2/\alpha} r_i^2\right) \times \frac{2\pi q_i \lambda_r r_i}{1 - e^{-\pi q_i \lambda_r R^2}} \exp\left(-\pi q_i \lambda_r r_i^2\right) d_{r_i}. \tag{15}$$

3.3. The Average Probability of Successful Transmission. In this paper, we define the average probability of successful transmission as the probability of finding and then successfully transmitting all the requested files within a radius R. Therefore, based on the above analysis, the average probability of successful transmission is given by

$$\overline{P}_{\text{suc}} = \sum_{i=1}^{N} f_i P_i^{\text{find}} P_i^{\text{suc}} = \sum_{i=1}^{N} f_i \left(1 - e^{-\pi q_i \lambda_r R^2}\right) \times \int_0^{\infty} \exp\left(-r_i^{\alpha} M - \beta\tau^{2/\alpha} r_i^2\right) \times \frac{2\pi q_i \lambda_r r_i}{1 - e^{-\pi q_i \lambda_r R^2}} \exp\left(-\pi q_i \lambda_r r_i^2\right) d_{r_i}, \tag{16}$$

following constraints

$$\sum_{i=1}^{N} q_i \le C_R, \quad q_i \in [0,1],\ i \in [1,N]. \tag{17}$$

From (16), we can find $\overline{P}_{\text{suc}}$ is a function of various factors, for example, r_i, α, R_s, q_i, R, λ_r as well as λ_e. For any given r_i, α, R_s, R, λ_r, and λ_e, $\overline{P}_{\text{suc}}$ solely depends on the caching probability q_i. But since the complication of $\overline{P}_{\text{suc}}$, it is complicated to obtain a closed-form expression for $\overline{P}_{\text{suc}}$. Thus, in this subsection, we derive its analytical lower bound. The analytical lower bound presents a conservative estimation of $\overline{P}_{\text{suc}}$. If the lower bound is higher than the success threshold, the exact $\overline{P}_{\text{suc}}$ can be definitely guaranteed. The details about the analytical lower bound are shown as follows. We rewrite (10) as

$$P_i^{\text{suc}} = E_{r_i}\left[\exp\left(-r_i^{\alpha} M\right) \exp\left(-\beta\tau^{2/\alpha} r_i^2\right)\right] = E_{r_i}\left[\exp\left(-r_i^{\alpha} M\right)\right] E_{r_i}\left[\exp\left(-\beta\tau^{2/\alpha} r_i^2\right)\right]. \tag{18}$$

According to Jensen's inequality, we have

$$P_i^{\text{suc}} \ge \exp\left(-M E_{r_i}\left[r_i^{\alpha}\right]\right) \exp\left(-\beta\tau^{2/\alpha} E_{r_i}\left[r_i^2\right]\right). \tag{19}$$

Based on the PDF of r_i in (14), $E_{r_i}[r_i^{\alpha}]$ can be calculated as

$$E_{r_i}\left[r_i^{\alpha}\right] = \int_0^{\infty} r_i^{\alpha} \frac{2\pi q_i \lambda_r r_i}{1 - e^{-\pi q_i \lambda_r R^2}} \exp\left(-\pi q_i \lambda_r r_i^2\right) d_{r_i} = \frac{\pi q_i \lambda_r}{1 - e^{-\pi q_i \lambda_r R^2}} \times \frac{\Gamma(1 + \alpha/2)}{\left(\pi q_i \lambda_r\right)^{1+\alpha/2}}. \tag{20}$$

$E_{r_i}[r_i^2]$ can be calculated as

$$E_{r_i}\left[r_i^2\right] = \int_0^{\infty} r_i^2 \frac{2\pi q_i \lambda_r r_i}{1 - e^{-\pi q_i \lambda_r R^2}} \exp\left(-\pi q_i \lambda_r r_i^2\right) d_{r_i} = \frac{\Gamma(2)}{\pi q_i \lambda_r \left(1 - e^{-\pi q_i \lambda_r R^2}\right)}. \tag{21}$$

Substituting (20) and (21) in (19), we can obtain the closed-form expression of the lower bound $P_{i_{\text{low}}}^{\text{suc}}$ as

$$P_{i_{\text{low}}}^{\text{suc}} = \exp\left(-\frac{M\pi q_i \lambda_r}{1 - e^{-\pi q_i \lambda_r R^2}} \times \frac{\Gamma(1 + \alpha/2)}{\left(\pi q_i \lambda_r\right)^{1+\alpha/2}}\right) \times \exp\left(-\frac{\beta\tau^{\alpha/2}\Gamma(2)}{\pi q_i \lambda_r \left(1 - e^{-\pi q_i \lambda_r R^2}\right)}\right). \tag{22}$$

Therefore, the closed-form expression of the lower bound $P_{\text{low}}^{\text{suc}}$ is given by

$$\overline{P}_{\text{low}}^{\text{suc}} = \sum_{i=1}^{N} f_i P_i^{\text{find}} P_{i_{\text{low}}}^{\text{suc}} = \sum_{i=1}^{N} f_i \left(1 - e^{-\pi q_i \lambda_r R^2}\right) \times \exp\left(-\frac{M\pi q_i \lambda_r}{1 - e^{-\pi q_i \lambda_r R^2}} \times \frac{\Gamma(1 + \alpha/2)}{\left(\pi q_i \lambda_r\right)^{1+\alpha/2}}\right) \times \exp\left(-\frac{\beta\tau^{2/\alpha}\Gamma(2)}{\pi q_i \lambda_r \left(1 - e^{-\pi q_i \lambda_r R^2}\right)}\right). \tag{23}$$

4. Optimization of Probabilistic Caching Placement

From the performance analysis, it can be seen that the caching parameter q_i affects the system secure performance significantly. Therefore, in this section, the optimization of probabilistic caching placement is to find the optimal caching probability q_i^* ($i \in [1, N]$). But due to the nonconvex nature and the complication of $\overline{P}_{\text{suc}}$, it is too complicated to get a closed-form solution of q_i^*. Based on the above considerations, we utilize the GA to find the optimal solution of q_i^* instead of deriving a closed-form solution. The details about the optimization of genetic algorithm are shown in Algorithm 1.

Notation. N denotes the number of total files, λ_r denotes the intensity of relays, λ_e denotes the intensity of eavesdroppers, p_r denotes the transmit power at relay, and $p_{r_{\min}}$ and $p_{r_{\max}}$ represent the minimum of transmit power and the maximum of transmit power, respectively. In addition, q^* represents the optimal caching probability of the ith file, $\overline{P}_{\text{suc}}^*$ represents the average probability of all files successful transmission, and LB and UB represent the lower bound and upper bound of variables, respectively.

Input: input parameters N, λ_r, λ_e, p_r, $p_{r_{\min}}$, $p_{r_{\max}}$
Output: output the optimal caching probability $\mathbf{q}^* = [q_1^*, \ldots, q_N^*]$ and the average probability of success transmission $\overline{P}_{\text{suc}}^*$

(1) Initialize $\overline{P}_{\text{suc}} = zeros(0)$
(2) $j = 1$
(3) **for** $p_r = p_{r_{\min}} : p_{r_{\max}}$ **do**
(4) $[\mathbf{x}, fval] = ga\_main(N, \lambda_r, \lambda_e, p_r)$
(5) $\mathbf{q}^*(j,:) = \mathbf{x}(end-3)$
(6) $\overline{\mathbf{P}}_{\text{suc}}^*(j) = -fval$
(7) $j = j + 1$
(8) **end for**
(9) **function** $ga\_main(N, \lambda_r, \lambda_e, p_r)$
(10) ObjectiveFunction=@$ga\_fitness$
(11) $nvars = N + 3$
(12) Initialize LB and UB
(13) ConstraintFunction=@$ga\_constraint$
(14) $[q_i^*, fval] =$ $ga(ObjectiveFunction, nvars, [\,], [\,], [\,], [\,], LB, UB, \ldots, ConstraintFunction, options)$
(15) **return** $[q_i^*, fval]$
(16) **end function**
(17) **function** $ga\_fitness(\mathbf{x})$
(18) $\mathbf{q}_i^* = \mathbf{x}(1 : end-3)$
(19) $p_r = \mathbf{x}(end)$
(20) calculate f_i, P_i^{find}, P_i^{suc}
(21) $\overline{P}_{\text{suc}}^* = \sum_{i=1}^{N} f_i P_i^{\text{find}} P_i^{\text{suc}}$
(22) $y = -\overline{P}_{\text{suc}}^*$
(23) **return** y
(24) **end function**

Algorithm 1: Optimization of probabilistic caching placement.

In Algorithm 1, the function *ga_main* (lines (9)–(16)) is the calling function of GA. The main intension of the function *ga_main* is to define the number of variables (line (11)), initialize lower bound and upper bound (line (12)), and call the fitness function and constraint function of GA to return the optimal q_i^* and the minimum $fval$ (line (14)). The fitness function of GA is presented from lines (17) to (24). The main ideas of the fitness function are to take one input vector $\mathbf{x}$, where $\mathbf{x}$ has as many elements as number of variables, then compute the value of the function, and return that scalar value in its one return argument y. It is worth noting that all variables consist of the caching probability of N files, the intensity of relays λ_r, the intensity of eavesdroppers λ_e, and the transmit power of relays p_r, so the length of $\mathbf{x}$ is equal to $N + 3$, where $\mathbf{x}$ is the vector of all variables. But because there are only N files, we can get that the length of $\mathbf{q}$ should be equal to $length(\mathbf{x}) - 3$. Moreover, because the function of GA is to find the minimum value, we define argument y as the negative of $\overline{P}_{\text{suc}}^*$. Similarly, the GA function assumes the constraint function will take one input $\mathbf{x}$, where $\mathbf{x}$ has as many elements as number of variables in the problem. Furthermore, the constraint function computes the values of all the inequality and equality constraints and designs two vectors c and ceq, respectively, where $c = \text{sum}(\mathbf{x}(1 : end - 3)) - C_R$ and $ceq = [\,]$. The details about the algorithm optimization and the associated analysis can be found in the literature, such as the works [49–52].

5. Numerical and Simulation Results

In this section, the numerical and simulation results are presented to verify the system secure performance in the presence of multiple eavesdroppers and illustrate the effect of key system parameters. In addition, the system performances are compared with the traditional MPC caching placement. Without loss of generality, the secrecy data rate R_s is set to 0.1 bps/Hz, and the noise power is set to one.

As shown in Figure 2, this figure depicts the effect of the number of files N on the average probability of successful transmission, where $p_r = 30$ dB, $C_R = 5$, $\alpha = 2.1$, $\gamma = 0.5$, $R = 100$, $\lambda_r = 4 \times 10^{-3}$, and $\lambda_e = 1 \times 10^{-5}$. From this figure, we can see that the average probability of successful transmission decreases as N increases. And when the number of files N is equal to C_R, the average probability of successful transmission of MPC caching placement is equal to the analytical result of probabilistic caching placement and the analytical lower bound of probabilistic caching placement. However, when N is larger than C_R, the performance of probabilistic caching placement is better than MPC caching placement, and with increasing N, MPC caching placement

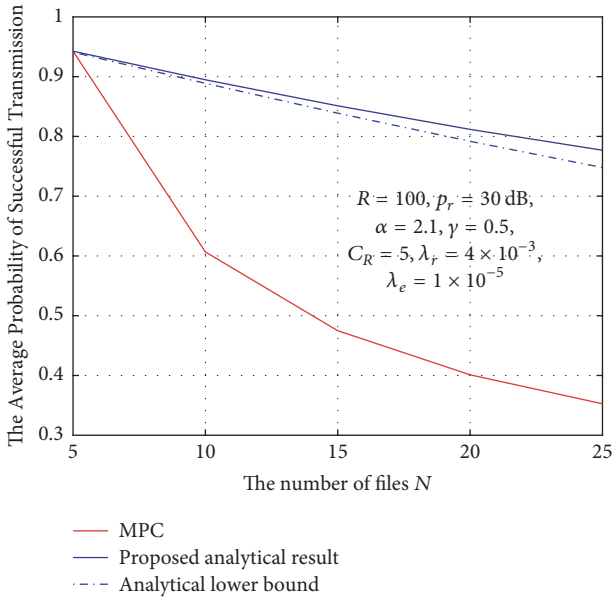


FIGURE 2: Effect of N on the average probability of successful transmission.

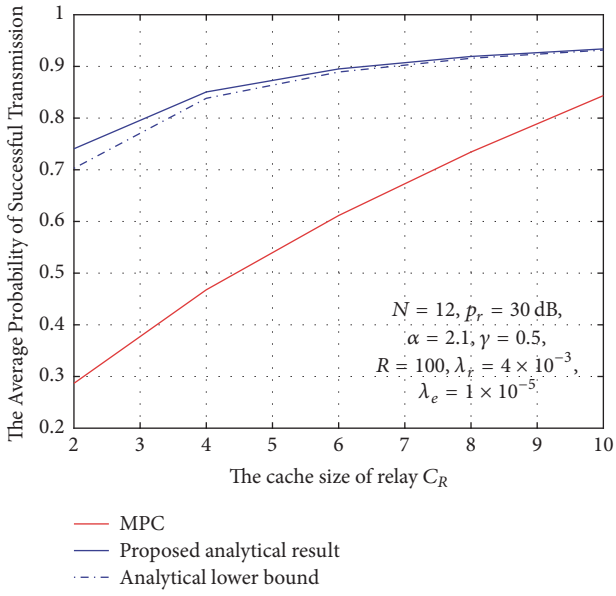


FIGURE 3: Effect of C_R on the average probability of successful transmission.

deteriorates more rapidly than the probabilistic caching placement. The reason is that the MPC caching placement combines all signals to exploit the signal cooperation gain, but the proposed probabilistic caching placement achieves the balance between the signal cooperation gain and the caching diversity gain.

Figure 3 shows the effect of the cache size of relay C_R on the average probability of successful transmission, where $N = 12$, $p_r = 30$ dB, $\gamma = 0.5$, $R = 100$, $\alpha = 2.1$, $\lambda_r = 4 \times 10^{-3}$, and $\lambda_e = 1 \times 10^{-5}$. As observed from the figure, the average probability of successful transmission

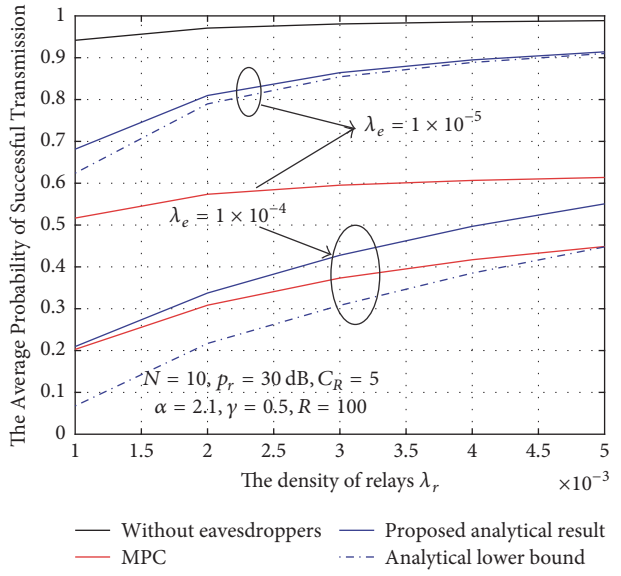


FIGURE 4: Impact of λ_r and λ_e on the average probability of successful transmission.

becomes better as C_R increases, and it is also obvious that the performance of probabilistic caching placement is always higher than MPC caching placement. Moreover, from the picture, we can see that as C_R increases, the analytical result of probabilistic caching placement and the analytical lower bound of probabilistic caching placement are quite closer. And the average probability of successful transmission of probabilistic caching placement and MPC caching placement becomes closer as the value of C_R increases.

Figure 4 shows the effect of the intensity of relays λ_r and the intensity of eavesdroppers λ_e on the average probability of successful transmission, where $N = 10$, $p_r = 30$ dB, $C_R = 5$, $\alpha = 2.1$, $\gamma = 0.5$, and $R = 100$. As observed from the figure, the average probability of successful transmission becomes better as λ_r increases, and the average probability of successful transmission with $\lambda_e = 1 \times 10^{-5}$ is higher than that with $\lambda_e = 1 \times 10^{-4}$. Thus, we can find when the value of λ_e increases, the average probability of successful transmission will decrease. In addition, from the figure, we also can find that the analytical result and analytical lower bound of probabilistic caching placement are quite closer with increasing λ_r. And when $\lambda_e = 1 \times 10^{-4}$, the difference between the analytical result and analytical lower bound is more obvious than $\lambda_e = 1 \times 10^{-5}$. Moreover, when $\lambda_e = 1 \times 10^{-5}$, the analytical result and analytical lower bound of probabilistic caching placement are both higher than MPC caching placement. However when $\lambda_e = 1 \times 10^{-4}$, the analytical lower bound of probabilistic caching placement is lower than MPC. But we also can find the difference between the analytical result and the analytical lower bound of probabilistic caching placement becomes quite closer with increasing λ_r. It is worth noting that the performance without considering security is superior to the performance of considering secure transmission, but in the actual situation, eavesdroppers exist, and we cannot just

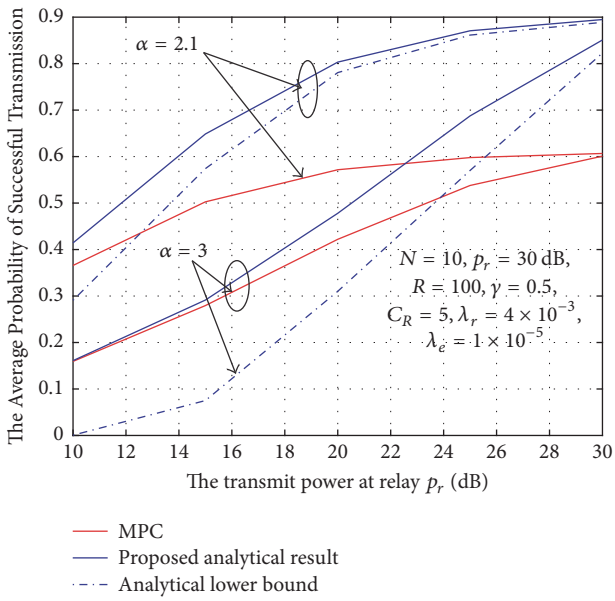


FIGURE 5: Impact of p_r and α on the average probability of successful transmission.

consider the performance of main channel, and we also need to consider the eavesdropper's channel.

Figure 5 shows the effect of the transmit power at relay p_r and the path loss α on the average probability of successful transmission, where $N = 10$, $C_R = 5$, $\gamma = 0.5$, $R = 100$, $\lambda_r = 4 \times 10^{-3}$, and $\lambda_e = 1 \times 10^{-5}$. From this figure, we can find that the average probability of successful transmission increases as p_r increases. Moreover, the analytical result and the analytical lower bound of probabilistic caching placement is quite closer with increasing p_r. In addition, the analytical result of probabilistic caching placement is always higher than MPC caching placement. And for the probabilistic caching placement, with $\alpha = 2.1$, the associated average probability of successful transmission is better than that with $\alpha = 3$, so we can obtain that the average probability of successful transmission deteriorates with larger α. Furthermore, when $\alpha = 3$ and $p_r \leq 12$ dB, the average probability of successful transmission of probabilistic caching placement is almost equal to MPC caching placement. But when $p_r \geq 12$ dB, the average probability of successful transmission of probabilistic caching placement is always higher than MPC caching placement. The reason is that increasing the value of transmit power p_r can exploit the signal cooperation gain and the caching diversity gain, but the MPC caching placement only can utilize the signal cooperation gain, and the probabilistic caching placement can exploit both the signal cooperation gain and the caching diversity gain.

6. Conclusions

In this paper, we designed, analyzed, and optimized the probabilistic caching placement in the presence of multiple eavesdroppers. And the average probability of successful transmission was defined as the main performance metric, which is the probability of finding and then successfully transmitting all the requested files within a radius R. Moreover, the analytical result and the analytical lower bound of average probability of successful transmission were both presented. But due to the nonconvex nature and the complication of average probability of successful transmission, the GA was used to find the optimal solution instead of deriving a closed-form solution. Finally, simulation results were provided to support the studies that the proposed probabilistic caching placement is superior to the MPC caching placement. In addition, the system secure performance can be improved by increasing the value of p_r, C_R, and λ_r but will deteriorate with larger N and λ_e.

Data Availability

The authors state the data availability in this manuscript.

Conflicts of Interest

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

Acknowledgments

This work was supported by the Guangdong Natural Science Funds for Distinguished Young Scholar under Grant 2014A030306027, by the Innovation Team Project of Guangdong Province University under Grant 2016KCXTD017, by the Science and Technology Program of Guangzhou under Grant 201807010103, by the Guangdong Natural Science Funds (Key Project Initiative) under Grant 2017A030308006, and by the Graduate Innovative Research Grant Program of Guangzhou University under Grant 2017GDJC-M17.

References

[1] Z. Chen, J. Lee, T. Q. S. Quek, and M. Kountouris, "Cooperative Caching and Transmission Design in Cluster-Centric Small Cell Networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3401–3415, 2017.

[2] M. Taghizadeh, K. Micinski, S. Biswas, C. Ofria, and E. Torng, "Distributed cooperative caching in social wireless networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 6, pp. 1037–1053, 2013.

[3] W. C. Ao and K. Psounis, "Distributed Caching and Small Cell Cooperation for Fast Content Delivery," in *Proceedings of the the 16th ACM International Symposium*, pp. 127–136, Hangzhou, China, June 2015.

[4] Z. Chen, N. Pappas, and M. Kountouris, "Probabilistic caching in wireless D2D networks: Cache hit optimal versus throughput optimal," *IEEE Communications Letters*, vol. 21, no. 3, pp. 584–587, 2017.

[5] Y. Chen, M. Ding, J. Li, Z. Lin, G. Mao, and L. Hanzo, "Probabilistic small-cell caching: Performance analysis and optimization," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4341–4354, 2017.

[6] J. Song, H. Song, and W. Choi, "Optimal caching placement of caching system with helpers," in *Proceedings of the IEEE*

International Conference on Communications, ICC 2015, pp. 1825–1830, London, UK, June 2015.

[7] J. Rao, H. Feng, C. Yang, Z. Chen, and B. Xia, "Optimal caching placement for D2D assisted wireless caching networks," in *Proceedings of the IEEE International Conference on Communications (ICC '16)*, pp. 1–6, Kuala Lumpur, Malaysia, May 2016.

[8] B. Serbetci and J. Goseling, "On optimal geographical caching in heterogeneous cellular networks," in *Proceedings of the 2017 IEEE Wireless Communications and Networking Conference, WCNC 2017*, San Francisco, Calif, USA, March 2017.

[9] G. Zheng, H. A. Suraweera, and I. Krikidis, "Optimization of hybrid cache placement for collaborative relaying," *IEEE Communications Letters*, vol. 21, no. 2, pp. 442–445, 2017.

[10] A. Sengupta, R. Tandon, and T. C. Clancy, "Fundamental limits of caching with secure delivery," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 355–370, 2015.

[11] N. Zhao, F. Cheng, F. R. Yu et al., "Caching UAV Assisted Secure Transmission in Hyper-Dense Networks Based on Interference Alignment," *IEEE Transactions on Communications*, 2018.

[12] F. Shi, W. Tan, J. Xia, D. Xie, L. Fan, and X. Liu, "Hybrid Cache Placement for Physical-Layer Security in Cooperative Networks," *IEEE Access*, vol. 6, pp. 8098–8108, 2018.

[13] N. Zhao, X. Liu, F. R. Yu, M. Li, and V. C. M. Leung, "Communications, caching, and computing oriented small cell networks with interference alignment," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 29–35, 2016.

[14] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[15] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[16] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[17] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying with Cochannel Interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1494–1505, 2016.

[18] T.-X. Zheng, H.-M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Communications Letters*, vol. 18, no. 8, pp. 1299–1302, 2014.

[19] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying over Correlated Fading Channels," *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 2811–2820, 2017.

[20] X. Lai, W. Zou, D. Xie, and L. Fan, "DF relaying networks in randomly distributed interference environments," *IEEE Access*, vol. 5, pp. 18-909–18-917, 2017.

[21] G. Pan, H. Lei, Y. Deng et al., "On Secrecy Performance of MISO SWIPT Systems with TAS and Imperfect CSI," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 3831–3843, 2016.

[22] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Transactions on Communications*, vol. 64, no. 1, pp. 70–82, 2016.

[23] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Communications*, vol. 14, no. 12, pp. 1–14, 2017.

[24] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy Cooperative Networks with Outdated Relay Selection over Correlated Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7599–7603, 2017.

[25] H. Xu, L. Sun, P. Ren, Q. Du, and Y. Wang, "Cooperative Privacy Preserving Scheme for Downlink Transmission in Multiuser Relay Networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 825–839, 2017.

[26] R. Zhao, Y. Yuan, L. Fan, and Y.-C. He, "Secrecy Performance Analysis of Cognitive Decode-and-Forward Relay Networks in Nakagami-m Fading Channels," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 549–563, 2017.

[27] G. Huang, Q. Zhang, and J. Qin, "Joint Time Switching and Power Allocation for Multicarrier Decode-and-Forward Relay Networks with SWIPT," *IEEE Signal Processing Letters*, vol. 22, no. 12, pp. 2284–2288, 2015.

[28] J. Li, M. Wen, X. Jiang, and W. Duan, "Space-Time Multiple-Mode Orthogonal Frequency Division Multiplexing with Index Modulation," *IEEE Access*, vol. 5, pp. 23212–23222, 2017.

[29] X. Jiang, M. Wen, H. Hai, J. Li, and S. Kim, "Secrecy-Enhancing Scheme for Spatial Modulation," *IEEE Communications Letters*, vol. 22, no. 3, pp. 550–553, 2018.

[30] G. Liu, H. Liu, H. Chen, C. Zhou, and L. Shu, "Position-based adaptive quantization for target location estimation in wireless sensor networks using one-bit data," *Wireless Communications and Mobile Computing*, vol. 16, no. 8, pp. 929–941, 2016.

[31] F. Zhou, L. Fan, N. Wang, G. Luo, J. Tang, and W. Chen, "A Cache-Aided Communication Scheme for Downlink Coordinated Multipoint Transmission," *IEEE Access*, vol. 6, pp. 1416–1427, 2017.

[32] W. Tan, M. Matthaiou, S. Jin, and X. Li, "Spectral Efficiency of DFT-Based Processing Hybrid Architectures in Massive MIMO," *IEEE Wireless Communications Letters*, vol. 6, no. 5, pp. 586–589, 2017.

[33] X. Liu, M. Jia, and X. Tan, "Threshold optimization of cooperative spectrum sensing in cognitive radio networks," *Radio Science*, vol. 48, no. 1, pp. 23–32, 2013.

[34] G. Huang and W. Tu, "Wireless Information and Energy Transfer in Nonregenerative OFDM AF Relay Systems," *Wireless Personal Communications*, vol. 94, no. 4, pp. 3131–3146, 2017.

[35] X.-Q. Jiang, M. Wen, J. Li, and W. Duan, "Distributed Generalized Spatial Modulation Based on Chinese Remainder Theorem," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1501–1504, 2017.

[36] J. Yuan, S. Jin, W. Xu, W. Tan, M. Matthaiou, and K.-K. Wong, "User-Centric Networking for Dense C-RANs: High-SNR Capacity Analysis and Antenna Selection," *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 5067–5080, 2017.

[37] X. Wang, H. Zhang, L. Fan, and Y. Li, "Performance of Distributed Switch-and-Stay Combining for Cognitive Relay Networks with Primary Transceiver," *Wireless Personal Communications*, vol. 97, no. 2, pp. 3031–3042, 2017.

[38] G. Liu, B. Xu, H. B. Chen, C. Zhang, and X. Hu, "Energy-efficient scheduling for distributed estimation inwireless sensor and actuator networks with kriging," *Ad Hoc & Sensor Wireless Networks*, vol. 27, no. 3-4, pp. 197–222, 2015.

[39] G. Huang and W. Tu, "Optimal resource allocation in wireless-powered OFDM relay networks," *Computer Networks*, vol. 104, pp. 94–107, 2016.

[40] W. Tan, S. Jin, C.-K. Wen, and T. Jiang, "Spectral efficiency of multi-user millimeter wave systems under single path with uniform rectangular arrays," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, article no. 181, 2017.

[41] X. Lai, J. Xia, M. Tang, H. Zhang, and J. Zhao, "Cache-aided multiuser cognitive relay networks with outdated channel state information," *IEEE Access*, vol. PP, p. 99, 2018.

[42] J. Li, X. Jiang, Y. Yan, W. Yu, S. Song, and M. H. Lee, "Low Complexity Detection for Quadrature Spatial Modulation Systems," *Wireless Personal Communications*, vol. 95, no. 4, pp. 4171–4183, 2017.

[43] G. Huang and D. Tang, "Wireless Information and Power Transfer in Two-Way OFDM Amplify-and-Forward Relay Networks," *IEEE Communications Letters*, vol. 20, no. 8, pp. 1563–1566, 2016.

[44] G. Liu, J. Yao, Y. Liu, H. Chen, and D. Tang, "Channel-Aware Adaptive Quantization Method for Source Localization in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 214081, 13 pages, 2015.

[45] X. Liu, M. Jia, X. Gu, and X. Tan, "Optimal periodic cooperative spectrum sensing based on weight fusion in cognitive radio networks," *Sensors*, vol. 13, no. 4, pp. 5251–5272, 2013.

[46] W. Tan, D. Xie, J. Xia, W. Tan, L. Fan, and S. Jin, "Spectral and Energy Efficiency of Massive MIMO for Hybrid Architectures Based on Phase Shifters," *IEEE Access*, vol. 6, pp. 11751–11759, 2018.

[47] D. Xie, X. Lai, X. Lei, and L. Fan, "Cognitive Multiuser Energy Harvesting Decode-and-Forward Relaying System with Direct Links," *IEEE Access*, vol. 6, pp. 5596–5606, 2018.

[48] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 7, pp. 1029–1046, 2009.

[49] Y. Liang, H. Wu, G. Huang, J. Yang, and H. Wang, "Thermal performance and service life of vacuum insulation panels with aerogel composite cores," *Energy and Buildings*, vol. 154, pp. 606–617, 2017.

[50] J. Yang, H. Wu, M. Wang, and Y. Liang, "Prediction and optimization of radiative thermal properties of nano TiO2 assembled fibrous insulations," *International Journal of Heat and Mass Transfer*, vol. 117, pp. 729–739, 2018.

[51] J. Yang, H. Wu, M. Wang, S. He, and H. Huang, "Prediction and optimization of radiative thermal properties of ultrafine fibrous insulations," *Applied Thermal Engineering*, vol. 104, pp. 394–402, 2016.

[52] J. Yang, H. Wu, S. He, and M. Wang, "Prediction of thermal conductivity of fiber/aerogel composites for optimal thermal insulation," *Journal of Porous Media*, vol. 18, no. 10, pp. 971–984, 2015.