IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 11, 2021, accepted November 17, 2021, date of publication November 30, 2021,
date of current version December 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3131906

Proactive Eavesdropping via Jamming in NOMA Network

TUNG PHAM HUU[1], **VAN NHAN VO**[2,3], **HUNG TRAN**[4], **TRUONG XUAN QUACH**[5], **AND VIET NGUYEN DINH**[6]

[1]Faculty of Information Technology, National University of Civil Engineering, Hanoi 11616, Vietnam
[2]Faculty of Information Technology, Duy Tan University, Da Nang 550000, Vietnam
[3]Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam
[4]Faculty of Information Technology, Phenikaa University, Hanoi 12116, Vietnam
[5]Faculty of Information Technology, Thai Nguyen University of Information and Communication Technology, Thái Nguyên 24119, Vietnam
[6]Faculty of Information Technology, VNU University of Engineering and Technology, Hanoi 11309, Vietnam

Corresponding author: Hung Tran (hung.tran@phenikaa-uni.edu.vn)

ABSTRACT Recently, non-orthogonal multiple access (NOMA) has been considered as a promising technique in 5G network, and many investigations have addressed on the physical layer security to improve the security performance. In this paper, an alternative problem, where the eavesdropping process is considered as a legal activity, will be analyzed to track suspicious communications. More specifically, we study a wireless surveillance system in which the legitimate monitor is equipped with multi-antenna to overhear the messages between the suspicious receiver and the suspicious transmitter. Suspicious users are grouped into pairs and use the NOMA technique to transmit signals to a suspicious base station. Meanwhile, the legitimate monitor (LM) simultaneously transmits jamming signals, listens to suspicious links, decode-and-forward (DF) the eavesdropped information to the legitimate eavesdropper (LE). Based on the proposed mechanism, we investigate the power allocation policies for jamming signals of the legitimate monitor under deterministic and non-deterministic interference channel. Accordingly, we derive the closed-form expression of the successful eavesdropping probability for the best and the worst user to evaluate the system performance. Monte Carlo simulations are provided to verify our analytical results.

INDEX TERMS Proactive eavesdropping, cooperative jamming, cooperative eavesdropping, wireless surveillance, physical layer security.

I. INTRODUCTION

Non-orthogonal multiple access (NOMA) has been proposed as a promising technique in the fifth generation (5G) networks [1]. This technique is based on the power-domain multiplexing at the transmitter(s) and utilizing successive interference cancellation (SIC) technique at the receiver(s) to serve multiple users in the same resource block (i.e., time/frequency/code) and massive connectivity can be realized efficiently [2]. However, due to the broadcast nature of wireless communication, NOMA is subject to some security problems at which attackers can exploit to extract confidential information [3]. Utilizing this approach of attackers, the physical layer security (PLS) approach named proactive eavesdropping has been adopted and attracted a lot of attention to not only improve the secure communication but also improve the system performance. [4]–[25].

Traditional works in the PLS have often treated eavesdroppers as unauthorized users and as a result, many of them focused on preventing information leaks [26]–[38]. More specifically, Lu. Lv *et al.* proposed a NOMA transmission scheme, which not only reduced the transmission outage probabilities but also decreased the secrecy outage significantly [26]. In [27], given the secrecy outage and transmit power constraints, authors proposed a NOMA scheme that is able to optimize the transmit power and then reduces the risk of eavesdropping. The authors of [28] investigated NOMA systems with untrusted near users, where joint beamforming and power allocation strategy was proposed to achieve a reliable and secure transmission.

Furthermore, the authors of [32] studied beamforming design to enhance PLS of NOMA with the aid of artificial noise. Unlike [32], a multiple-input single-output (MISO)

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Ali.

system was investigated in [33], where a novel artificial noise aided secrecy beamforming was introduced to combat the eavesdroppers. Taking the advantages of relaying networks, works reported in [29]–[31] relied on a dedicated relay to make the communication between the base station (BS) and the paired users to improve ergodic secrecy rates and secrecy outage probability (SOP). Additionally, the secrecy issue of multiple-input multiple-output (MIMO) network with arbitrary number of antennas was studied in [37], where the random binary sequence was employed to achieve a secrecy communication.

In practice, the proactive legal eavesdropping is highly significant to monitor the information exchange between suspicious users such as criminals and terrorists who may use smartphones for illegal activities [5]–[7]. Thus, the eavesdroppers are considered as legitimate monitors for the purpose of wireless surveillance. In other words, the main objective of proactive eavesdropping is to exploit as much information as possible from the suspicious communication link [17], [39].

In [5], the authors proposed a legal eavesdropping system via the jamming approach to maximize the average eavesdropping rate, where the legitimate monitor emits jamming signals with optimized power control to moderate the suspicious communication rate. Subsequently, J. Xu *et al.* investigated a proactive eavesdropping scheme via the cognitive jamming and an optimal power allocation policy was proposed to maximize the eavesdropping non-outage probability and the relative eavesdropping rate in both delay-sensitive and delay-insensitive cases for the suspicious communication [6]. As an extension of [5], [6], works reported in [16] addressed on a multi-antenna full-duplex (FD) monitor and maximized the eavesdropping non-outage probability by optimizing jamming power and transmit/receive beamforming vectors. D. Xu *et al.* considered a downlink suspicious NOMA network with multiple groups of suspicious users and proposed a heuristic iterative algorithm to maximize the number of successfully eavesdropped suspicious users [39]. In [40], under low detection probability condition at the suspicious receiver, the authors proposed an iterative search algorithm to maximize the surveillance performance.

Considering the relaying networks, the works in [8], [14], [15] considered the eavesdropping of the two-hop suspicious communication link. In particular, G. Ma *et al.* studied the wireless surveillance of a two-hop suspicious communication link by a half-duplex legitimate monitor. They concluded that the eavesdropping rate at the legitimate monitor can be significantly improved by jointly optimizing the eavesdropping mode selection as well as the transmit power [15]. X. Jiang *et al.* considered legitimate surveillance in a dual-hop DF relaying system. They proposed two strategies to maximize the eavesdropping rate, the corresponding optimal beamformer, and the power allocation scheme has been derived. The numerical results showed that the system performance is better compared with intuitive benchmark schemes [14]. Meanwhile, authors in [8] proposed extract and approximate optimal jamming scheme for the proactive eavesdropping over an amplify-and-forward (AF) relay network. The results indicated that the optimal jamming scheme outperforms passive monitoring and proactive monitoring via constant-power jamming. H. Wu at *et al.* investigated a proactive eavesdropping scheme with a decode-and-forward relay and optimized the transmit power and location deployment at the relay to maximize the average eavesdropping rate [41].

To investigate relay-aimed proactive eavesdropping systems, J. Moon *et al.* considered a proactive eavesdropping system where a central monitor eavesdrops the information exchanged between a pair of suspicious entities through AF, FD relays and a cooperative jammer. They proposed an effective two-layer optimization method to obtain a globally optimal power allocation at both the relay and the jammer for maximizing the eavesdropping rate. The numerical results indicated that the proposed solution improves the system performance compared to the conventional scheme [11]. Additionally, J. Moon *et al.* investigated a novel proactive eavesdropping method via spoofing relay manner to further improve the information surveillance capability of the legitimate monitor, and three possible spoofing relay strategies were presented to maximize the eavesdropping performance [10].

B. Li *et al.* considered the proactive eavesdropping for multiple suspicious communication links [9], [25]. In [9], B. Li proposed a cooperative eavesdropping scheme, where a primary legitimate monitor and an assistant legitimate monitor cooperatively interfere the suspicious links between an illegal transmitter and receiver to maximize the eavesdropping energy efficiency. The numerical results showed that a cooperative scheme can improve the legitimate eavesdropping performance significantly. Furthermore, B. Li *et al.* presented a novel intervention strategy selection and power allocation solution based on jamming/relay features. They concluded that the proposed approach can effectively improve the eavesdropping rate compared to the conventional eavesdropping approach [25]. However, to the best of the author's knowledge, there are few existing works to address the proactive eavesdropping on the NOMA network which is considered as a potential technique applying for the 5G network.

Thus, we investigate legitimate proactive eavesdropping for a NOMA system where a LM transmits jamming signals to suspicious users to make the eavesdropping channel capacity higher than the data rate of the suspicious users. Taking this opportunity, the LM listens to the message and then forwards the intercepted data from the suspicious users to the LE. Besides, the LE can legitimately eavesdrop through the direct links. The main contributions of this work are summarized as follows:

- The communication protocol for the proactive eavesdropping system in the NOMA network is proposed. Accordingly, power allocation policies for deterministic and non-deterministic interference links of jamming signals of the LM are obtained.

- The closed-form expression of the successful eavesdropping probability for the best and the worst user are derived to evaluate the legitimate eavesdropping performance.
- Numerical results show that the number of user-pair, the number of antennas at the legitimate monitor, and power allocation are important factors to enhance legal eavesdropping performance for the best user.

In this paper, we consider a scenario with a multiple antennas legitimate monitor, multiple antennas suspicious base station and suspicious users employ the NOMA technique to transmit signals to a suspicious base station.

The rest of this paper is organized as follows. In Section II, the system and channel model are introduced. In Section III, the power allocation policies for the jamming signal of the LM under deterministic and non-deterministic interference channel is calculated. Furthermore, the closed-form expressions of the successful eavesdropping probability for the best user and the worst user are derived. In Section IV, numerical results are provided to verify the analytical expressions. Finally, Section V summarizes the paper.

II. SYSTEM MODEL

In this section, we introduce the system model and communication protocol.

A. PROTOCOL DESCRIPTION

We consider an uplink NOMA system as shown in Fig. 1. The system consists one suspicious base station B with N antennas, $2K$ suspicious users denoted by $U = \{U^{(1)}, \ldots, U^{(2K)}\}$, one legitimate monitor E are equipped $M + 1$ antennas, whereas the legitimate eavesdropper D is deployed with a single antenna. The each suspicious user is equipped with a single antenna. We assume that the suspicious users are grouped into pairs randomly $U_l^{(k)}$, $l \in \{1, 2\}$ and $k \in \{1, 2, \ldots, K\}$. The each user-pair $U_l^{(k)}$ employs NOMA technique to transmit uplink signals to B. Without loss of generality, it is assumed that the $U_1^{(k)}$ is the near user and $U_2^{(k)}$ is the far user from the suspicious base station (SBS). It means that $U_2^{(k)}$ was assigned a higher power level than that of $U_1^{(k)}$ [32].

The legitimate monitor E can send the jamming signal to interfere with the SBS while receiving signals from the $U_l^{(k)}$ then E decodes and forwards eavesdropping signals from suspicious links to the legitimate eavesdropper D. In addition, D can overhear signals through the direct link between $U_l^{(k)}$ and D. If the signal over the direct link is weak, then the communication takes place via the legitimate monitor. E works as a jamming and relaying device to improve the legitimate eavesdropped performance.

More specifically, as the user-pair $U_l^{(k)}$ transmit its signal, one antenna among $M + 1$ antennas of E acts as the friendly jammer by generating jamming signals to force $U_l^{(k)}$ to increase its transmit power. Meanwhile, another antenna of E exploits this behavior to overhear the message from $U_l^{(k)}$ over the legitimate eavesdropping link $U_l^{(k)} \rightarrow E$. It is noted that E immediately forwards the decoded message to D once E decodes the eavesdropped message successfully. Moreover, we assume that D is in the coverage range of $U_l^{(k)}$, i.e., D also eavesdrops signals from $U_l^{(k)}$. In the considered context, the suspicious users and B may be devices of criminals or terrorists while E and D may be drones, unmanned aerial vehicle (UAV), or smartphones which are equipped for soldiers in the battle field.

TABLE 1. Summary of notation and abbreviations.

Notation and abbreviation	Definition
B	The base station
E	The legitimate monitor
D	The legitimate eavesdropper
N	The number of antennas installed at the suspicious base station
$M+1$	The number of antennas installed at the legitimate monitor
$2K$	The number of suspicious users
$U_l^{(k)}$	The $k-$th suspicious user-pair, where $l \in$ {1,2} and 1 $\leq k \leq K$
$h_{l,n}^{(k)}$	The channel gain between $U_l^{(k)}$ and the n-th antenna of the SBS, where $1 \leq n \leq N$
$f_{l,m}^{(k)}$	The channel gain between $U_l^{(k)}$ and the m-th antenna of the LM, where $1 \leq m \leq M$
$v_l^{(k)}$	The channel gain between $U_l^{(k)}$ and the LE
g_n	The channel gain between the n-th antenna of the SBS and LM
β_m	The channel gain between the m-th antenna of the LM and LE
$\alpha_1^{(k)}$	The power allocation coefficient in the first phase
$\delta_1^{(k)}$	The power allocation coefficient in the second phase
f_X	The probability density function of X
F_X	The cumulative distribution function of X
NOMA	Non-orthogonal multiple access
DF	Decode-and-forward
5G	Fifth generation
SIC	Successive interference cancellation
PLS	Physical layer security
MISO	Multiple-input single-output
SOP	Secrecy outage probability
MIMO	Multiple-input multiple-output
FD	Full-duplex
AF	Amplify-and-forward
LM	Legitimate monitor
LE	Legitimate eavesdropper
SNR	Signal to noise ratio
SINR	Signal to interference plus noise ratio
BS	Base station
SBS	Suspicious base station

Let $h_{l,n}^{(k)}$, $f_{l,m}^{(k)}$ and $v_l^{(k)}$ denotes the channel gains between $U_l^{(k)}$ and the n-th antenna of B, $U_l^{(k)}$ and the m-th antenna of E and $U_l^{(k)} \rightarrow D$ link, respectively ($n \in \{1, 2, \ldots, N\}$, $m \in \{1, 2, \ldots, M\}$), g_n is the channel gain between the n-th antenna of B and E, β_m denotes the channel gains between the m-th antenna of E and D. Furthermore, we assume the channel state information (CSI) of all links are perfectly known at the LM and LE by the method given in [25], [42]. We also assume that users are operating in the indoor environment and

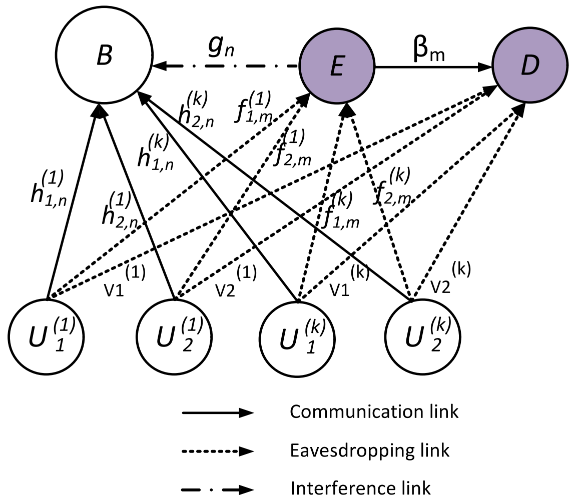

FIGURE 1. System model of proactive eavesdropping in NOMA networks.

there is none-line-of sight among users [43]. Accordingly, all channels are modeled as Rayleigh fading, and the respective channel gains X ($X \in \{h^{(k)}_{l,n}, f^{(k)}_{l,m}, v^{(k)}_l, g_n, \beta_m\}$) are random variables (RV) distributed following exponential distribution with channel mean gain Ω_X. Thus, the probability density function (PDF) and cumulative distribution function (CDF) are formulated, respectively, as follows [44]:

$$f_X(x) = \frac{1}{\Omega_X}\exp\left(-\frac{x}{\Omega_X}\right), \tag{1}$$

$$F_X(x) = 1 - \exp\left(-\frac{x}{\Omega_X}\right). \tag{2}$$

B. SIGNAL MODEL

For communication, the user-pair $U^{(k)}_l$ broadcasts a superimposed signal to B which is a mixture signal of $U^{(k)}_1$ and $U^{(k)}_2$. Meanwhile, the legitimate monitor E broadcasts jamming signal s_J with the transmit power P_J. Then the received signal at the n-th branch antenna of B could be expressed as

$$y^{(B)}_k = \sqrt{\alpha^{(k)}_1 P_s} x^{(k)}_1 h^{(k)}_{1,n} + \sqrt{(1-\alpha^{(k)}_1)P_s} x^{(k)}_2 h^{(k)}_{2,n} + \sqrt{P_J} s_J g_n + \sigma_B, \tag{3}$$

where P_s is the total transmit power of the user-pair $U^{(k)}_l$, $\alpha^{(k)}_1$ denotes the power allocation coefficient corresponding the user $U^{(k)}_1$ in the user-pair $U^{(k)}_l$ and $\sigma_B \sim \mathcal{N}(0, N_0)$ is additive white Gaussian noise (AWGN). It is assumed that $U^{(k)}_1$ has better quality of channel than that one of $U^{(k)}_2$. It means that a higher power level is allocated to $U^{(k)}_2$, while a lower power level will be assigned to $U^{(k)}_1$, i.e, $\alpha^{(k)}_1 < 0.5$.

According to the uplink NOMA principle, B first decodes the signal of the strong user $U^{(k)}_1$ from the received superposed signals by treating the signal of $U^{(k)}_2$ as an interference. After that, the B subtracts the signal of $U^{(k)}_1$ by SIC and then decodes the signal of $U^{(k)}_2$ [45]. As a result, the instantaneous signal-to-interference-plus-noise ratio (SINR) of $U^{(k)}_1$ and $U^{(k)}_2$ at the n-th branch antenna of B subject to the interference induced by E can be respectively formulated, as

$$\gamma^{(k,B)}_{1,n} = \frac{\alpha^{(k)}_1 P_s h^{(k)}_{1,n}}{P_J g_n + (1-\alpha^{(k)}_1)P_s h^{(k)}_{2,n} + N_0}, \tag{4}$$

$$\gamma^{(k,B)}_{2,n} = \frac{(1-\alpha^{(k)}_1)P_s h^{(k)}_{2,n}}{P_J g_n + N_0}, \tag{5}$$

where P_J is the power of jamming signal generated by E.

Since B uses the selective combining technique to process the signal, the SINR of the user-pair $U^{(k)}_l$ at B can be expressed as follows:

$$\gamma^{(k,B)}_1 = \max_{n\in\{1,2,\ldots,N\}}\left\{\gamma^{(k,B)}_{1,n}\right\}, \tag{6}$$

$$\gamma^{(k,B)}_2 = \max_{n\in\{1,2,\ldots,N\}}\left\{\gamma^{(k,B)}_{2,n}\right\}. \tag{7}$$

With (6) and (7), the achievable data rate of $U^{(k)}_l \to B$ suspicious link under the effect of a jamming signal from E can be given respectively as

$$R^{(k,B)}_1 = W\log_2\left(1+\gamma^{(k,B)}_1\right), \tag{8}$$

$$R^{(k,B)}_2 = W\log_2\left(1+\gamma^{(k,B)}_2\right), \tag{9}$$

where W denotes the system bandwidth.

On the other hand, due to the broadcast nature of wireless transmission, E also eavesdrops the signals which transmitted from the user-pair $U^{(k)}_l$. Accordingly, the received signal at the m-th antenna of E is given by

$$y^{(E)}_k = \sqrt{\alpha^{(k)}_1 P_s} x^{(k)}_1 f^{(k)}_{1,m} + \sqrt{(1-\alpha^{(k)}_1)P_s} x^{(k)}_2 f^{(k)}_{2,m} + \sigma_E, \tag{10}$$

where $\sigma_E \sim \mathcal{N}(0, N_0)$ denotes the AWGN at E.

Similarly, we assume that SIC can also be successfully implemented at E, i.e, in the first phase, E first decodes $U^{(k)}_2$'s message $x^{(k)}_2$, then it continues to detect $U^{(k)}_1$'s message $x^{(k)}_1$. As a consequence, the instantaneous SINR of the user-pair $U^{(k)}_l$ at the m-th branch antenna can be expressed as, respectively

$$\gamma^{(k,E)}_{1,m} = \frac{\alpha^{(k)}_1 P_s f^{(k)}_{1,m}}{(1-\alpha^{(k)}_1)P_s f^{(k)}_{2,m} + N_0}, \tag{11}$$

$$\gamma^{(k,E)}_{2,m} = \frac{(1-\alpha^{(k)}_1)P_s f^{(k)}_{2,m}}{N_0}. \tag{12}$$

E also applies the selection combining (SC) technique to enhance the quality of received signal. Accordingly, SINR of the user-pair $U^{(k)}_l$ at E can be expressed, respectively, as follows:

$$\gamma^{(k,E)}_1 = \max_{m\in\{1,2,\ldots,M\}}\left\{\gamma^{(k,E)}_{1,m}\right\}, \tag{13}$$

$$\gamma^{(k,E)}_2 = \max_{m\in\{1,2,\ldots,M\}}\left\{\gamma^{(k,E)}_{2,m}\right\}. \tag{14}$$

In the second phase, E forwards the signal to D over the antenna which has the best channel gain. E operates as jammer to emit the jamming signal, which is known to D while remains unknown to the illegal users. Thus, the jamming signal can be canceled out at D and confuse only the illegal users. The received signal at D can be expressed as

$$y_k^{(D)} = \sqrt{\delta_1^{(k)} P_e} x_1^{(k)} \beta_m^{(k)} + \sqrt{(1-\alpha_1^{(k)}) P_e} x_2^{(k)} \beta_m^{(k)} + \sigma_D, \quad (15)$$

where $P_e \in [0, P_J^{max}]$ is the transmit power of E used to forward the eavesdropping message to D, $\delta_1^{(k)}$ is power allocation coefficient and $\sigma_D \sim \mathcal{N}(0, N_0)$ is AWGN.

D first decodes the signal of user $U_2^{(k)}$ from the received signals by considering the signal of $U_1^{(k)}$ as interference. Accordingly, the instantaneous SINR at D can be written, respectively, as

$$\gamma_{1,m}^{(k,D)} = \frac{\delta_1^{(k)} P_e \beta_m^{(k)}}{N_0}, \quad (16)$$

$$\gamma_{2,m}^{(k,D)} = \frac{(1-\delta_1^{(k)}) P_e \beta_m^{(k)}}{\delta_1^{(k)} P_e \beta_m^{(k)} + N_0}, \quad (17)$$

D also applies the SC technique to improve the quality of received signal. Thus, SINR of the user-pair $U_l^{(k)}$ at D can be expressed, respectively, as follows:

$$\gamma_1^{(k,D)} = \max_{m \in \{1,2,\ldots,M\}} \left\{ \gamma_{1,m}^{(k,D)} \right\}, \quad (18)$$

$$\gamma_2^{(k,D)} = \max_{m \in \{1,2,\ldots,M\}} \left\{ \gamma_{2,m}^{(k,D)} \right\}, \quad (19)$$

Based on (13) and (18), the achievable data rate of $U_1^{(k)}$ at E and D can be expressed, respectively, as follows

$$R_1^{(k,E)} = \frac{1}{2} W \log_2 \left(1 + \gamma_1^{(k,E)}\right), \quad (20)$$

$$R_1^{(k,D)} = \frac{1}{2} W \log_2 \left(1 + \gamma_1^{(k,D)}\right). \quad (21)$$

Next, combining (14) and (19), the achievable rate of $U_2^{(k)}$ at E and D can be formulated, respectively, as follows

$$R_2^{(k,E)} = \frac{1}{2} W \log_2 \left(1 + \gamma_2^{(k,E)}\right), \quad (22)$$

$$R_2^{(k,D)} = \frac{1}{2} W \log_2 \left(1 + \gamma_2^{(k,D)}\right). \quad (23)$$

In direct link, D also can overhear signal from the user-pair $U_l^{(k)}$. Thus, the SINR of $U_l^{(k)} \rightarrow D$ links are expressed, respectively, as follows

$$\gamma_1^{(k,SD)} = \frac{\alpha_1^{(k)} P_s v_1^{(k)}}{(1-\alpha_1^{(k)}) P_s v_2^{(k)} + N_0}, \quad (24)$$

$$\gamma_2^{(k,SD)} = \frac{(1-\alpha_1^{(k)}) P_s v_2^{(k)}}{N_0}. \quad (25)$$

Based on (24) and (25), the achievable data rate of the $U_l^{(k)} \rightarrow D$ links are given, respectively, as follows

$$R_1^{(k,SD)} = W \log_2 \left(1 + \gamma_1^{(k,SD)}\right), \quad (26)$$

$$R_2^{(k,SD)} = W \log_2 \left(1 + \gamma_2^{(k,SD)}\right). \quad (27)$$

With (20), (21), (26), (27), (22) and (23), the end-to-end data rate of $U_l^{(k)}$ at D over the relaying links and direct links is given by

$$R_{l,E2E}^{(k)} = \max \left\{ R_l^{(k,SD)}, \min \left\{ R_l^{(k,E)}, R_l^{(k,D)} \right\} \right\}. \quad (28)$$

III. SYSTEM PERFORMANCE ANALYSIS

In this section, we first derive the power allocation policies for the jamming signal in cases deterministic and non-deterministic channel between LM and SBS is available and is not available. Subsequently, we analyze the successful legitimate eavesdropping probability at D.

A. POWER ALLOCATION POLICY FOR JAMMING SIGNAL

E transmits a proactive jamming signal with power P_J to degrade the achievable data rate of $U_l^{(k)}$ at the suspicious base station, $U_l^{(k)}$ responds by immediately increasing its transmit power P_s to maintain the outage performance of system. Thus, if E causes serious interference to the suspicious base station so that $U_l^{(k)}$ cannot adjust its transmit power to maintain communication rate, $U_l^{(k)}$ will stop communicating and the legitimate eavesdropping process fails.

The transmit power P_s of the user-pair $U_l^{(k)}$ and jamming power P_J of the LM in practice subject to a maximum power constraint as follows:

$$0 \le P_J \le P_J^{max}, \quad (29)$$

$$0 \le P_s \le P_s^{max}. \quad (30)$$

Further, in order not to cause harmful interference to the suspicious base station, E needs to adjust the jamming power to guarantee the decoding outage probability at the suspicious base station which can be expressed in terms of the outage probability constraint as follows:

$$\mathcal{O}_1 = \Pr \left\{ R_1^{(k,B)} \le \gamma_{th} \right\} \le \theta_{th}, \quad (31)$$

$$\mathcal{O}_2 = \Pr \left\{ R_2^{(k,B)} \le \gamma_{th} \right\} \le \theta_{th}, \quad (32)$$

where $\mathcal{O}_1$, $\mathcal{O}_2$ are outage probability of $U_1^{(k)}$ and $U_2^{(k)}$, γ_{th} and θ_{th} are outage target rate and outage probability constraint of B, respectively.

Based on (6) and (7), $\mathcal{O}_1$, $\mathcal{O}_2$ can be expressed, respectively, as

$$\mathcal{O}_1 = \Pr \left\{ \max_{n \in \{1,2,\ldots,N\}} \left\{ \gamma_{1,n}^{(k,B)} \right\} \le \phi_0 \right\},$$

$$= \prod_{n=1}^{N} \Pr \left\{ \frac{\alpha_1^{(k)} P_s h_{1,n}^{(k)}}{P_J g_n + (1-\alpha_1^{(k)}) P_s h_{2,n}^{(k)} + N_0} \le \phi_0 \right\}. \quad (33)$$

$$\mathcal{O}_2 = \Pr \left\{ \max_{n \in \{1,2,\ldots,N\}} \left\{ \frac{(1-\alpha_1^{(k)}) P_s h_{2,n}^{(k)}}{P_J g_n + N_0} \right\} \le \phi_0 \right\},$$

$$= \prod_{n=1}^{N} \Pr \left\{ \frac{(1-\alpha_1^{(k)}) P_s h_{2,n}^{(k)}}{P_J g_n + N_0} < \phi_0 \right\}, \quad (34)$$

where $\phi_0 = 2^{\frac{\gamma_{th}}{W}} - 1$.

Depending on the CSI of the $E \rightarrow B$ interference link, we consider the power allocation for jamming signal in two cases as follows

1) DETERMINISTIC INTERFERENCE LINK FROM THE LE TO THE SBS

In this case, the CSI of the interference link is available at LE. It means that g_n is deterministic.

$$\mathcal{O}_1 = \prod_{n=1}^{N} \int_0^{\infty} F_{h_{1,n}^{(k)}}\left(\frac{\phi_0(P_J g_n + N_0 + (1-\alpha_1^{(k)})P_s x)}{\alpha_1^{(k)} P_s}\right) \times f_{h_{2,n}^{(k)}}(x)dx. \quad (35)$$

Using Equation (1), (2), the $f_{h_{2,n}^{(k)}}$ and $F_{h_{1,n}^{(k)}}$ are given by

$$f_{h_{2,n}^{(k)}}(x) = \frac{1}{\Omega_{h_{2,n}^{(k)}}} \exp\left(-\frac{x}{\Omega_{h_{2,n}^{(k)}}}\right). \quad (36)$$

$$F_{h_{1,n}^{(k)}} = 1 - \exp\left\{\frac{\phi_0(P_J g_n + N_0 + (1-\alpha_1^{(k)})P_s x)}{\alpha_1^{(k)} P_s \Omega_{h_{1,n}^{(k)}}}\right\}. \quad (37)$$

Substituting (36) and (37) into (35), we have

$$\mathcal{O}_1 = \prod_{n=1}^{N}\left[1 - \frac{\alpha_1^{(k)} P_s \Omega_{h_{1,n}^{(k)}} \exp\left(-\frac{(N_0+P_J g_n)\phi_0}{\alpha_1^{(k)} P_s \Omega_{h_{1,n}^{(k)}}}\right)}{(1-\alpha_1^{(k)})P_s\phi_0\Omega_{h_{2,n}^{(k)}} + \alpha_1^{(k)} P_s \Omega_{h_{1,n}^{(k)}}}\right]. \quad (38)$$

We assume that the antennas of suspicious base station close to each other. Thus, all branches of antenna have the same channel mean gain, i.e., $\Omega_{h_{1,n}^{(k)}} = \Omega_{h_1^{(k)}}$ and $\Omega_{h_{2,n}^{(k)}} = \Omega_{h_2^{(k)}}$ [46]. Finally, $\mathcal{O}_1$ is obtained as

$$\mathcal{O}_1 = \left[1 - \frac{\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}} \exp\left(-\frac{(N_0+P_J g_n)\phi_0}{\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}}}\right)}{(1-\alpha_1^{(k)})P_s\phi_0\Omega_{h_2^{(k)}} + \alpha_1^{(k)} P_s \Omega_{h_1^{(k)}}}\right]^N. \quad (39)$$

By substituting (39) into (31) and after some mathematical manipulations, we obtain an expression for the power of the jamming signal as follows:

$$P_J \le P_{J_1}, \quad (40)$$

where

$$P_{J_1} = \left\{\frac{\ln(\tau)\alpha_1 P_s \Omega_{h_1^{(k)}} - N_0\phi_0}{\phi_0 g_n}\right\}^+, \quad (41)$$

$$\tau = \frac{\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}}}{\left(1 - \sqrt[N]{\theta_{th}}\right)\left(\left(1-\alpha_1^{(k)}\right)P_s\phi_0\Omega_{h_2^{(k)}} + \alpha_1 P_s \Omega_{h_1^{(k)}}\right)} \quad (42)$$

and $\{x\}^+ = \max\{x, 0\}$.

Whenever $U_l^{(k)}$ can adjust its transmit power to adapt to the jamming signal and to guarantee its outage performance, E can further increase P_J. However, E must stop increasing transmit power of the jamming signal where $U_l^{(k)}$ reaches the maximum value $P_s = P_s^{max}$. Accordingly, the transmit power of the jamming signal under the outage probability of $U_1^{(k)}$ should satisfy the following constraint:

$$P_J \le \min\left\{P_{J_1}, P_J^{max}\right\}. \quad (43)$$

Next, we calculate the expression for jamming power of E which satisfies $U_2^{(k)}$'s outage probability constraint. By applying exponential distribution, (34) can be derived as

$$\mathcal{O}_2 = \prod_{n=1}^{N}\left[1 - \exp\left(-\frac{\phi_0(P_J g_n + N_0)}{(1-\alpha_1^{(k)})P_s\Omega_{h_{2,n}^{(k)}}}\right)\right], \\ = \left[1 - \exp\left(-\frac{\phi_0(P_J g_n + N_0)}{(1-\alpha_1^{(k)})P_s\Omega_{h_2^{(k)}}}\right)\right]^N. \quad (44)$$

Combining (32) and (44), we obtain an expression for the jamming power as follows:

$$P_J \le P_{J_2}, \quad (45)$$

where

$$P_{J_2} = \left\{\frac{\ln\left(\frac{1}{1-\sqrt[N]{\theta_{th}}}\right)(1-\alpha_1^{(k)})P_s\Omega_{h_2^{(k)}} - \phi_0 N_0}{\phi_0 g_n}\right\}^+ \quad (46)$$

P_J is the power of jamming signal for a given P_s. Although $U_l^{(k)}$ can adapt its transmit power P_s according to the channel condition and interference, it can not increase the power higher than the value P_s^{max}. Further, the right hand side of (45) is a monotonically increasing function with respect to P_s. Thus, the range for the P_J under the outage probability constraint of $U_2^{(k)}$ and peak jamming power constraint of E is obtained as

$$P_J \le \min\left\{P_{J_2}, P_J^{max}\right\}. \quad (47)$$

Combining (29), (43) and (47), the range for the transmit power of the jamming signal in deterministic interference link case is formulated as follows:

$$0 \le P_J \le \min\left\{\min\left\{P_{J_1}, P_{J_2}\right\}, P_J^{max}\right\}. \quad (48)$$

2) NON-DETERMINISTIC INTERFERENCE LINK FROM THE LE TO THE SBS

In this subsection, channel gain g_n is a random variable (RV) distributed following exponential distribution with channel mean gain Ω_g. To archive the analytical expression of $\mathcal{O}_1$ in (33), we have the following lemma.

Lemma 1: Let a, b, and c are positive constants. Further, let X, Y, and Z are independent and exponentially distributed RVs with mean values Ω_X, Ω_Y, and Ω_Z, respectively. Then CDF of T is obtained by (50) *where T is defined as* (49)

$$T = \frac{aX}{bY + cZ + 1} \quad (49)$$

$$F_T(t) = 1 - \frac{\exp\left(\frac{-t}{a\Omega_X}\right)}{\Omega_X\Omega_Y\left(\frac{tb}{a\Omega_X+\frac{1}{\Omega_Y}}\right)\left(\frac{tc}{a\Omega_X+\frac{1}{\Omega_Z}}\right)}. \quad (50)$$

Proof: See Appendix. □

By applying (50), outage probability of $U_1^{(k)}$ can be derived as follows:

$$\mathcal{O}_1 = \prod_{n=1}^{N}\left(1 - \frac{\exp\left(\frac{-\phi_0 N_0}{\alpha_1^{(k)}P_s\Omega_{h_{1,n}^{(k)}}}\right)}{\Delta}\right),$$

$$= \left(1 - \frac{\exp\left(\frac{-\phi_0 N_0}{\alpha_1^{(k)}P_s\Omega_{h_1^{(k)}}}\right)}{\Delta}\right)^N. \quad (51)$$

where $\Delta = \frac{\Omega_{h_1^{(k)}}\Omega_{h_2^{(k)}}\Omega_g^2\phi_0^2 P_J P_s(1-\alpha_1^{(k)})}{\left(\alpha_1^{(k)}P_s\Omega_{h_1^{(k)}}\Omega_g+N_0\right)\left(\alpha_1^{(k)}P_s\Omega_{h_1^{(k)}}\Omega_{h_2^{(k)}}+N_0\right)}$.

By substituting (51) into (31) and after some mathematical manipulations, we obtain an expression for the jamming power of E under the outage probability constraint of $U_1^{(k)}$ as follows:

$$P_J \leq \underbrace{\frac{\exp\left(-\frac{\phi_0 N_0}{\alpha_1^{(k)}P_s\Omega_{h_1^{(k)}}}\right)}{1-\sqrt[N]{\theta_{th}}}\pi_1}_{P_{J_1^*}}, \quad (52)$$

where π_1 is defined as

$$\pi_1 = \frac{(\alpha_1^{(k)}P_s\Omega_{h_1^{(k)}}\Omega_g + N_0)(\alpha_1^{(k)}P_s\Omega_{h_1^{(k)}}\Omega_{h_2^{(k)}} + N_0)}{(1-\alpha_1^{(k)})P_s\Omega_{h_1^{(k)}}\Omega_{h_2^{(k)}}\Omega_g^2\phi_0^2}, \quad (53)$$

To maintain quality of service (QoS) of $U_1^{(k)}$ at SBS, E must control the jamming power to satisfy the following constraint:

$$P_J \leq \min\left\{P_{J_1^*}, P_J^{max}\right\}. \quad (54)$$

Next, we calculate the outage probability of $U_2^{(k)}$. Applying (16) in [47], the OP_2 can be derived as follows:

$$\mathcal{O}_2 = \prod_{n=1}^{N}\left[1 - \frac{(1-\alpha_1^{(k)})P_s\Omega_{h_{2,n}^{(k)}}\exp\left(\frac{-N_0\phi_0}{(1-\alpha_1^{(k)})P_s\Omega_{h_{2,n}^{(k)}}}\right)}{\phi_0 P_J\Omega_g+(1-\alpha_1^{(k)})P_s\Omega_{h_{2,n}^{(k)}}}\right],$$

$$= \left[1 - \frac{(1-\alpha_1^{(k)})P_s\Omega_{h_2^{(k)}}\exp\left(\frac{-N_0\phi_0}{(1-\alpha_1^{(k)})P_s\Omega_{h_2^{(k)}}}\right)}{\phi_0 P_J\Omega_{gn}+(1-\alpha_1^{(k)})P_s\Omega_{h_2^{(k)}}}\right]^N. \quad (55)$$

Combining (29) and (55), we obtain an expression for the jamming power under the outage probability constraint of $U_2^{(k)}$ as follows

$$P_J \leq \underbrace{\frac{(1-\alpha_k)P_s\Omega_{h_2^{(k)}}}{\phi_0\Omega_g}\pi_2}_{P_{J_2^*}}, \quad (56)$$

where π_2 is defined as

$$\pi_2 = \left\{\frac{\exp\left(-\frac{N_0\phi_0}{(1-\alpha_1^{(k)})P_s\Omega_{h_2^{(k)}}}\right)}{1-\sqrt[N]{\theta_{th}}} - 1\right\}^{+}. \quad (57)$$

The right hand side of (56) is a monotonically increasing function with respect to P_s. Thus, the range for the P_J under the outage probability constraint of $U_2^{(k)}$ and peak jamming power constraint of E is formulated as

$$P_J \leq \min\left\{P_{J_2^*}, P_J^{max}\right\}. \quad (58)$$

Combining (29), (54) and (56), the range for the jamming power of E in non-deterministic interference link case is formulated as follows:

$$0 \leq P_J \leq \min\left\{\min\left\{P_{J_1^*}, P_{J_2^*}\right\}, P_J^{max}\right\}. \quad (59)$$

B. SUCCESSFUL LEGITIMATE EAVESDROPPING PROBABILITY ANALYSIS

In this section, we characterize successful legitimate eavesdropping probability at D. The legitimate eavesdropping process is successful, only if the eavesdropping message is decoded successfully at D with the help of E. Here, E acts as a relay and active jamming station to help the eavesdropping process of D.

It is worth noting that $U_1^{(k)}$ has better channel gain than $U_2^{(k)}$, therefore its SINR is better than that one of $U_2^{(k)}$. Accordingly, we consider two cases, namely, the best and the worst user.

1) SUCCESSFUL LEGITIMATE EAVESDROPPING PROBABILITY FOR THE BEST USER

In this subsection, we evaluate the successful legitimate eavesdropping probability for $U_1^{(k)}$ which has the best end-to-end data rate among K user-pairs and the successful legitimate eavesdropping probability for the best user is accordingly expressed as

$$EP_1 = \Pr\left\{\max_{k\in\{1,2,\ldots,K\}}\left\{R_{1,E2E}^{(k)}\right\} \geq r_1\right\}, \quad (60)$$

where $R_{1,E2E}^{(k)}$ is defined in (28). Next, EP_1 can be derived as

$$EP_1 = 1 - \prod_{k=1}^{K}\Pr\left\{\max\left\{R_1^{(k,SD)}, R_1^{min}\right\} \leq r_1\right\},$$

$$= 1 - \prod_{k=1}^{K}P_1P_2, \quad (61)$$

where $R_1^{min} = \min\left\{R_1^{(k,E)}, R_1^{(k,D)}\right\}$. P_1 and P_2 are presented, respectively, as

$$P_1 = \Pr\left\{R_1^{(k,SD)} \le r_1\right\}, \tag{62}$$

$$P_2 = \Pr\left\{R_1^{min} \le r_1\right\}. \tag{63}$$

Next, P_1 is calculated as

$$\begin{aligned} P_1 &= \Pr\left\{\frac{\alpha_1^{(k)}P_s v_1^{(k)}}{(1-\alpha_1^{(k)})P_s v_2^{(k)} + N_0} \le \phi_1\right\}, \\ &= \int_0^\infty \Pr\left\{\frac{\alpha_1^{(k)}P_s v_1^{(k)}}{(1-\alpha_1^{(k)})P_s x + N_0} \le \phi_1\right\} f_{v_2^{(k)}}(x)dx. \end{aligned} \tag{64}$$

where $\phi_1 = 2^{\frac{r_1}{W}} - 1$ and $f_{v_2^{(k)}} = \frac{1}{\Omega_{v_2^{(k)}}}\exp\left(-\frac{x}{\Omega_{v_2^{(k)}}}\right)$. P_1 can be derived as

$$\begin{aligned} P_1 = \frac{1}{\Omega_{v_2^{(k)}}}\int_0^\infty \left(1-\exp\left(-\frac{\phi_1((1-\alpha_1^{(k)})P_s x + N_0)}{\alpha_1^{(k)}P_s\Omega_{v_1^{(k)}}}\right)\right) \\ \times \exp\left(-\frac{x}{\Omega_{v_2^{(k)}}}\right)dx. \end{aligned} \tag{65}$$

After some mathematical manipulations, P_1 is obtained as

$$P_1 = 1 - \frac{\alpha_1^{(k)}\Omega_{v_1^{(k)}}\exp\left(-\frac{\phi_1 N_0}{\alpha_1^{(k)}P_s\Omega_{v_1^{(k)}}}\right)}{\phi_1(1-\alpha_1^{(k)})\Omega_{v_2^{(k)}} + \alpha_1^{(k)}\Omega_{v_1^{(k)}}}. \tag{66}$$

Further, P_2 is calculated as

$$\begin{aligned} P_2 &= \Pr\left\{\min\left\{R_1^{(k,E)}, R_1^{(k,D)}\right\} \le r_1\right\}, \\ &= 1 - (1-P_{21})(1-P_{22}). \end{aligned} \tag{67}$$

where

$$P_{21} = \Pr\left\{R_1^{(k,E)} \le r_1\right\}, \tag{68}$$

$$P_{22} = \Pr\left\{R_1^{(k,D)} \le r_1\right\}. \tag{69}$$

Next, P_{21} is calculated as

$$P_{21} = \Pr\left\{\gamma_1^{(k,E)} \le \phi_2\right\}, \tag{70}$$

where $\phi_2 = 2^{\frac{2r_1}{W}} - 1$. P_{21} is derived as

$$\begin{aligned} P_{21} &= \Pr\left\{\max_{m\in\{1,2,\ldots,M\}}\left\{\gamma_{1,m}^{(k,E)}\right\} \le \phi_2\right\}, \\ &= \prod_{m=1}^{M}\int_0^\infty \Pr\left\{\frac{\alpha_1^{(k)}P_s f_{1,m}^{(k)}}{(1-\alpha_1^{(k)})P_s x + N_0} \le \phi_2\right\} f_{f_{2,m}^{(k)}}(x)dx, \end{aligned} \tag{71}$$

where $f_{f_{2,m}^{(k)}} = \frac{1}{\Omega_{f_{2,m}^{(k)}}}\exp\left(-\frac{x}{\Omega_{f_{2,m}^{(k)}}}\right)$.

We also assume that all branches of antenna of E have the same channel mean gain, i.e., $\Omega_{f_{1,m}^{(k)}} = \Omega_{f_1^{(k)}}$, $\Omega_{f_{2,m}^{(k)}} = \Omega_{f_2^{(k)}}$, $\Omega_{\beta_m^{(k)}} = \Omega_\beta$.

After some mathematical manipulations, P_{21} can be expressed as

$$P_{21} = \left[1 - \frac{\alpha_1^{(k)}\Omega_{f_1^{(k)}}\exp\left(-\frac{\phi_2 N_0}{\alpha_1^{(k)}P_s\Omega_{f_1^{(k)}}}\right)}{\phi_2(1-\alpha_1^{(k)})\Omega_{f_2^{(k)}} + \alpha_1^{(k)}\Omega_{f_1^{(k)}}}\right]^M. \tag{72}$$

Further, we calculate P_{22}. Substituting (21) into (69), P_{22} is derived as

$$\begin{aligned} P_{22} &= \Pr\left\{\gamma_1^{(k,D)} \le \phi_2\right\}, \\ &= \prod_{m=1}^{M}\Pr\left\{\frac{\delta_k P_e \beta_m^{(k)}}{N_0} \le \phi_2\right\}. \end{aligned} \tag{73}$$

Applying exponential distribution, P_{22} can be derived as

$$\begin{aligned} P_{22} &= \prod_{m=1}^{M}\left[\left(1-\exp\left\{-\frac{\phi_2 N_0}{\delta_1^{(k)}P_e\Omega_{\beta_m^{(k)}}}\right\}\right)\right], \\ &= \left[1-\exp\left(-\frac{\phi_2 N_0}{\delta_1^{(k)}P_e\Omega_\beta}\right)\right]^M. \end{aligned} \tag{74}$$

Substituting (72) and (74), we obtain P_2 as

$$\begin{aligned} P_2 = 1 - \left(1-\left[1-\exp\left(-\frac{\phi_2 N_0}{\delta_1^{(k)}P_e\Omega_\beta}\right)\right]^M\right) \\ \times\left(1-\left[1-\frac{\alpha_1^{(k)}\Omega_{f_1^{(k)}}\exp\left(-\frac{\phi_2 N_0}{\alpha_1^{(k)}P_s\Omega_{f_1^{(k)}}}\right)}{\phi_2(1-\alpha_1^{(k)})\Omega_{f_2^{(k)}} + \alpha_1^{(k)}\Omega_{f_1^{(k)}}}\right]^M\right) \end{aligned} \tag{75}$$

Accordingly, EP_1 can formulate the successful eavesdropping probability as follows

$$EP_1 = 1 - \prod_{k=1}^{K} P_1 P_2, \tag{76}$$

where P_1 and P_2 are given by in (66) and (75), respectively.

2) SUCCESSFUL LEGITIMATE EAVESDROPPING PROBABILITY FOR THE WORST USER

In this subsection, we calculate successful legitimate eavesdropping probability for $U_2^{(k)}$ which has the worst end-to-end data rate among K user-pairs. And the successful legitimate eavesdropping probability for the worst user is accordingly expressed as

$$EP_2 = \Pr\left\{\min_{k\in\{1,2,\ldots,K\}}\left\{R_{2,E2E}^{(k)}\right\} \ge r_2\right\}, \tag{77}$$

where $R_{2,E2E}^{(k)}$ is defined in (28).

Further, EP_2 can be derived as

$$\begin{aligned} EP_2 &= \prod_{k=1}^{K}\left(1-\Pr\left\{\max\left\{R_2^{(k,SD)}, R_2^{min}\right\}\le r_2\right)\right\}, \\ &= \prod_{k=1}^{K}(1-F_1F_2), \end{aligned} \tag{78}$$

where $R_2^{min} = \min\left\{R_2^{(k,E)}, R_2^{(k,D)}\right\}$. F_1 and F_2 are presented, respectively, as

$$F_1 = \Pr\left\{R_2^{(k,SD)} \le r_2\right\}, \tag{79}$$

$$F_2 = \Pr\left\{R_2^{min} \le r_2\right\}. \tag{80}$$

Next, F_1 is calculated as

$$F_1 = \Pr\left\{\gamma_2^{(k,SD)} \le \lambda_1\right\}, \tag{81}$$

where $\lambda_1 = 2^{\frac{r_2}{W}} - 1$. Applying exponential distribution, F_1 can be obtained as

$$F_1 = 1-\exp\left(-\frac{\lambda_1 N_0}{(1-\alpha_1^{(k)})P_s\Omega_{v_2^{(k)}}}\right). \tag{82}$$

Next, F_2 is calculated as

$$\begin{aligned} F_2 &= 1-\Pr\left\{\min\left\{R_2^{(k,E)}, R_2^{(k,D)}\right\}\ge r_2\right\}, \\ &= 1-F_{21}F_{22}, \end{aligned} \tag{83}$$

where

$$F_{21} = \Pr\left\{R_2^{(k,E)} \ge r_2\right\}, \tag{84}$$

$$F_{22} = \Pr\left\{R_2^{(k,D)} \ge r_2\right\}. \tag{85}$$

F_{21} is calculated as

$$\begin{aligned} F_{21} &= 1-\Pr\left\{\gamma_2^{(k,E)} \le \lambda_2\right\}, \\ &= 1-\prod_{m=1}^{M}\Pr\left\{f_{2,m}^{(k)} \le \frac{\lambda_2 N_0}{(1-\alpha_1^{(k)})P_s}\right\}, \end{aligned} \tag{86}$$

where $\lambda_2 = 2^{\frac{2r_2}{W}} - 1$.

Applying exponential distribution, F_{21} is derived as

$$\begin{aligned} F_{21} &= 1-\prod_{m=1}^{M}\left[1-\exp\left(\frac{-\lambda_2 N_0}{(1-\alpha_1^{(k)})P_s\Omega_{f_{2,m}^{(k)}}}\right)\right], \\ &= 1-\left[1-\exp\left(\frac{-\lambda_2 N_0}{(1-\alpha_1^{(k)})P_s\Omega_{f_2^{(k)}}}\right)\right]^M. \end{aligned} \tag{87}$$

Further, F_{22} is calculated as

$$\begin{aligned} F_{22} &= 1-\Pr\left\{\gamma_2^{(k,D)} \le \lambda_2\right\}, \\ &= 1-\prod_{m=1}^{M}\Pr\left\{\beta_m^{(k)} \le \frac{\lambda_2 N_0}{\mu P_e}\right\}, \end{aligned}$$

where $\mu = 1-(1+\lambda_2)\delta_1^{(k)}$. Applying exponential distribution, F_{22} is derived as

$$\begin{aligned} F_{22} &= 1-\prod_{m=1}^{M}\left[\left(1-\exp\left\{\frac{-\lambda_2 N_0}{\mu P_e\Omega_{\beta_m^{(k)}}}\right\}\right)\right], \\ &= 1-\left[1-\exp\left(\frac{-\lambda_2 N_0}{\mu P_e\Omega_\beta}\right)\right]^M. \end{aligned} \tag{88}$$

Substituting (87) and (88) into (83), F_2 can be obtained as

$$\begin{aligned} F_2 = 1 &- \left(1-\left[1-\exp\left(\frac{-\lambda_2 N_0}{(1-\alpha_1^{(k)})P_s\Omega_{f_2^{(k)}}}\right)\right]^M\right) \\ &\times\left(1-\left[1-\exp\left(\frac{-\lambda_2 N_0}{\mu P_e\Omega_\beta}\right)\right]^M\right). \end{aligned} \tag{89}$$

Finally, $EP2$ can be obtained as

$$EP_2 = \prod_{k=1}^{K}(1-F_1F_2), \tag{90}$$

where F_1 and F_2 are given in (82) and (89), respectively.

IV. NUMERICAL RESULTS

In this section, we provide numerical examples for the power allocation policies of the jamming signal, and evaluate the successfully legitimate eavesdropping probability at the legitimate eavesdropper of the considered system. We use Monte Carlo simulations by averaging results for independent loops. We consider the system which consists three user-pairs ($K = 3$) with channel mean gains respectively as $\Omega_{h_1}^{(k)} = \{2, 4, 5\}$, $\Omega_{h_2}^{(k)} = \{1, 2, 3\}$, $\Omega_{f_1}^{(k)} = \{1, 0.5, 1.2\}$, $\Omega_{f_2}^{(k)} = \{0.3, 0.1, 0.01\}$, $\Omega_{v_1}^{(k)} = \{0.05, 0.02, 0.09\}$, $\Omega_{v_2}^{(k)} = \{0.002, 0.001, 0.005\}$, $\Omega_\beta = 1$. The other system parameters are as follows [48], [49]:

- System bandwidth: $W = 10^6$ Hz.
- Outage target rates of the LM: $r_1 = r_2 = 10^5$ bps.
- Outage target rates of the SBS: $\gamma_{th} = 10^5$ bps.
- Outage probability constraint: $\theta_{th} = 0.01$.
- Number of antennas of the LM: $M = 5$.
- Number of antennas of the SBS: $N = 5$.
- Transmit signal-to-noise ratio (SNR) of the LM: $\gamma_e = \frac{P_e}{N_0} = 0$ dB.
- Peak transmit SNR of jamming signal, $\gamma_J^{max} = \frac{P_J^{max}}{N_0} = 20$ dB.
- Peak transmit SNR of $U_l^{(k)}$, $\gamma_s^{max} = \frac{P_s^{max}}{N_0} = 20$ dB.
- Power allocation coefficient $\alpha_1^{(k)} = 0.3$, $\delta_1^{(k)} = 0.2$.

Fig. 2 and 3 present the relationship between the transmit SNR of the jamming signal of the legitimate monitor $\gamma_J = P_J/N_0$ and the transmit SNR $\gamma_s = P_s/N_0$ of $U_l^{(k)}$ for deterministic and non-deterministic interference link, respectively. We observe that to force $U_l^{(k)}$ to increase its transmit SNR γ_s, the legitimate monitor must increases the transmit SNR γ_e of jamming signal.

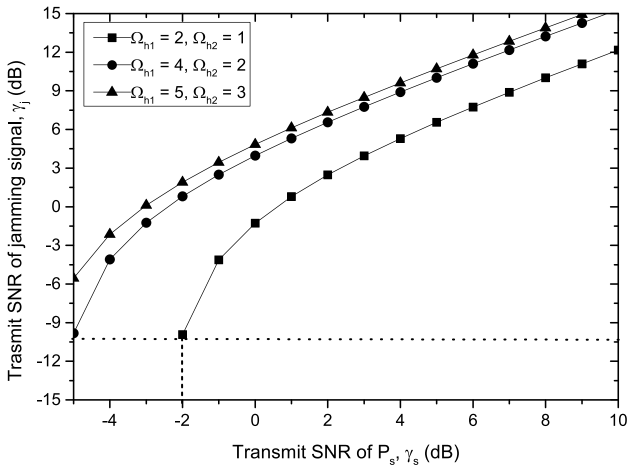

FIGURE 2. The transmit SNR of the jamming signal with deterministic interference channel $E \rightarrow B$, $g_n = 1$.

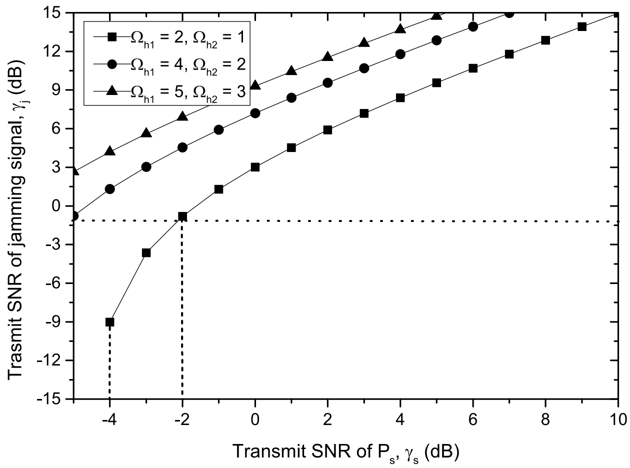

FIGURE 3. The transmit SNR of the jamming signal with non-deterministic interference channel $E \rightarrow B$, $\Omega_{g_n} = 1$.

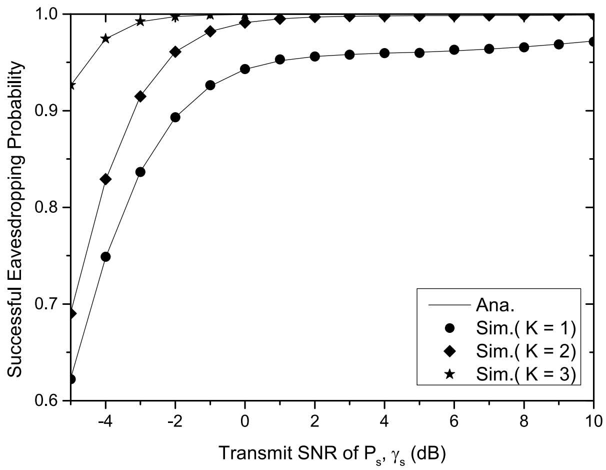

FIGURE 4. Impact of the number of user-pair on the successful legitimate eavesdropping probability of the best user.

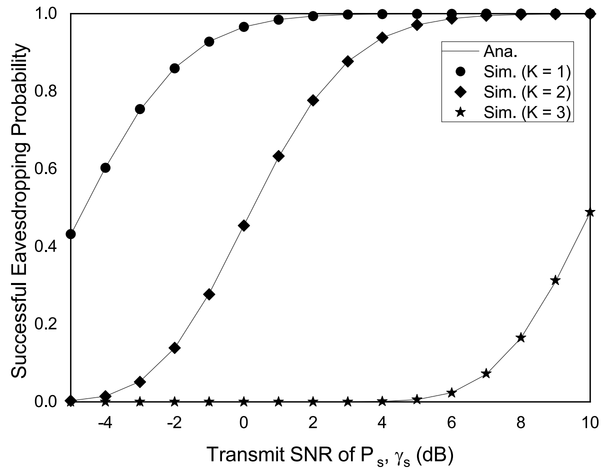

FIGURE 5. Impact of the number of user-pair on the successful legitimate eavesdropping probability of the worst user.

However, for the same region of the $U_l^{(k)}$ transmit SNR [-5, 10] dB, the demand for the transmit SNR of the jamming signal for the non-deterministic interference link is always higher than the one of the deterministic interference link. To make this statement more clear, we observe the case $\Omega_{g_n} = 1$ in both Fig. 2 and 3. Clearly, the transmit SNR of the jamming signal only needs to increase from -10 dB to 12 dB to keep the transmit SNR of the $U_1^{(k)}$ in the range of $[-2, 10]$ dB (see Fig. 2). However, the transmit SNR of the jamming signal must increase from 2 dB to 15 dB to keep the transmit SNR of the $U_1^{(k)}$ in the range of $[-2, 10]$ dB (see Fig. 3). In other words, the LM only needs a low power level for the jamming signal when the LM knows exactly the CSI of the $E \rightarrow B$ interference link.

Furthermore, the result shown in these figures shows that when channel mean gain of $U_l^{(k)} \rightarrow B$ link increases, e.g., $\Omega_{h_1} = \{2, 4, 5\}$, the LM needs more transmit SNR for jamming signal to keep the transmit SNR of $U_l^{(k)}$ at the same level, e.g., $\gamma_s = -2$ (dB). This can be explained by the fact that the user $U_l^{(k)}$ only needs to use a small amount of power to maintain its QoS when $U_l^{(k)} \rightarrow B$ link in a good condition. Thus, LM requires a high power level for the jamming signal to generate sufficient interference to the B.

Figs. 4 shows the impact of the number of user-pair on the successful eavesdropping probability for the best user. It is clear that the successful eavesdropping probability is improved significantly as the number of user-pair increases, i.e,. $K = 1, 2, 3$. As K increases, this probability increase to 1. This means that as the number of user-pair increases, the ability to select the best user is more diverse and efficient. As result, successful eavesdropping probability of system is improved.

Figs. 5 shows the impact of the number of user-pair on the successful eavesdropping probability for the worst user. In contrast to the best user, the successful eavesdropping probability will be reduced quickly as the number of user-pair increases, i.e., $K = 1, 2, 3$. In case $K = 3$, we see that the successful eavesdropping probability is zero when

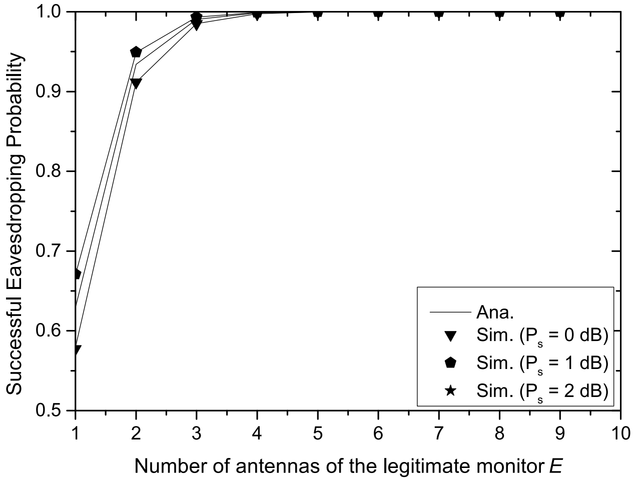

FIGURE 6. **Impact of the number antennas of legitimate eavesdropping on the successful legitimate eavesdropping probability of the best user.**

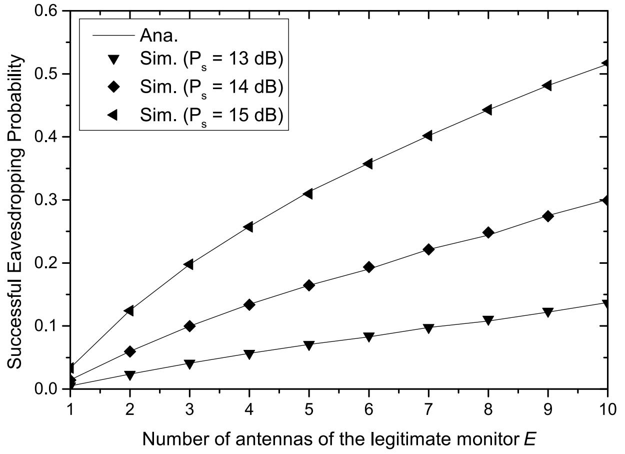

FIGURE 7. **Impact of the number antennas of legitimate eavesdropping on the successful legitimate eavesdropping probability of the worst user.**

the transmit SNR γ_s is smaller than 5 dB. This is because as the number of user-pair increases, the ability to select the worst user is more diverse and efficient. Thus, the successful eavesdropping probability of the system is degraded.

Fig. 6 and 7 show the impact of the number of eavesdropping antennas M at LM on the successful legitimate eavesdropping probability for the best and the worst user. It is observed that the successful legitimate eavesdropping probability increases as the number of eavesdropping antennas increase for both the best and the worst user. This result occurs because the diversity gain at LM increases as M increases. This indicates that increasing the transmit antenna M is an effective yet simple way to improve eavesdropping probability, which is easily achieved in 5G networks with a large antenna array.

Finally, Fig. 8 shows the impact of the power allocation coefficient $\delta_1^{(k)}$ and the transmit power P_s of $U_l^{(k)}$ on the successful legitimate eavesdropping probability for the best user which has the best end-to-end data rate among K users $U_1^{(k)}$. Note that the power allocation coefficient must be between 0 and 0.5. As is shown from this figure, the successful legitimate eavesdropping probability increases significantly as the power allocation coefficient and transmit power increases. This result can be explained by the fact that the legitimate eavesdropper D can more easily capture the signals from the suspicious users as these sources increase their transmit power.

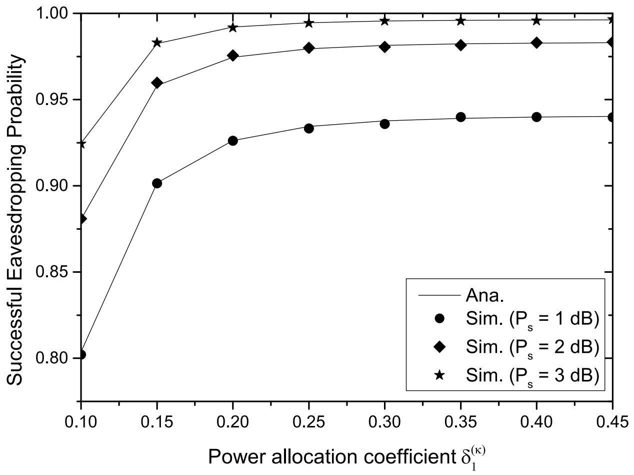

FIGURE 8. **Impact of the power allocation coefficient $\delta_1^{(k)}$ on the successful legitimate eavesdropping of the best user.**

V. CONCLUSION

In this work, we have investigated a proactive eavesdropping scheme in the NOMA networks where the legitimate monitor is proactive to jam the suspicious receivers to improve the eavesdropping performance. The power allocation policies which maintain the outage performance of the suspicious link under deterministic and non-deterministic interference channels were considered. The closed-form expression of the successful eavesdropping probability for the best user and the worst user were derived to evaluate the system performance. The numerical results show that when the interference channel between the LM and SBS is deterministic, the required power level of the jamming signal is smaller than in the case of non-deterministic interference link between LM and SBS. It was shown that the successful eavesdropping probability for best user is higher with increasing the number of user-pair and the number of antennas of the legitimate monitor. Furthermore, the successful eavesdropping probability for the best user was impacted by the power allocation between NOMA users.

APPENDIX

PROOF PROPERTY 1

The CDF of T is defined as follows:

$$\begin{aligned} F_T(t) &= \Pr\left\{\frac{aX}{bY+cZ+1} < t\right\} \\ &= \Pr\left\{X < \frac{t(bY+cZ+1)}{a}\right\} \end{aligned}$$

$$
\begin{aligned}
&= \int_0^\infty \int_0^\infty F_X\left(\frac{t(by+cz+1)}{a}\right) f_Y(y) f_Z(z) dydz \\
&= \int_0^\infty \int_0^\infty \left[1-\exp\left(-\frac{t(by+cz+1)}{a\Omega_X}\right)\right] \\
&\quad \times \frac{1}{\Omega_Y}\exp\left(\frac{-y}{\Omega_Y}\right)\frac{1}{\Omega_Z}\exp\left(-\frac{z}{\Omega_Z}\right)dydz. \\
&= \frac{1}{\Omega_Y}\frac{1}{\Omega_Z}\int_0^\infty \int_0^\infty \left(1-\exp\left(-\frac{t(by+cz+1)}{a\Omega_X}\right)\right) \\
&\quad \times \exp\left(-\frac{y}{\Omega_Y}\right)\exp\left(-\frac{z}{\Omega_Z}\right)dydz. \qquad (91)
\end{aligned}
$$

After some mathematical manipulations, $F_T(t)$ can be derived as

$$F_T(t) = 1 - \frac{\exp\left(\frac{-t}{a\Omega_X}\right)}{\Omega_Y\Omega_Z\left(\frac{tb}{a\Omega_X}+\frac{1}{\Omega_Y}\right)\left(\frac{tc}{a\Omega_X}+\frac{1}{\Omega_Z}\right)}. \tag{92}$$

The proof is completed.

REFERENCES

[1] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE 77th Veh. Technol. Conf. (VTC Spring)*, Kuala Lumpur, Malaysia, Jun. 2013, pp. 1–5.

[2] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2294–2323, 3rd Quart., 2018.

[3] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[4] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 152–159, Aug. 2017.

[5] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80–83, Feb. 2016.

[6] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[7] H. Tran and H.-J. Zepernick, "Proactive attack: A strategy for legitimate eavesdropping," in *Proc. IEEE 6th Int. Conf. Commun. Electron. (ICCE)*, Ha Long, Vietnam, Jul. 2016, pp. 457–461.

[8] D. Hu, Q. Zhang, P. Yang, and J. Qin, "Proactive monitoring via jamming in amplify-and-forward relay networks," *IEEE Signal Process. Lett.*, vol. 24, no. 11, pp. 1714–1718, Nov. 2017.

[9] B. Li, Y. Yao, H. Zhang, Y. Lv, and W. Zhao, "Energy efficiency of proactive eavesdropping for multiple links wireless system," *IEEE Access*, vol. 6, pp. 26081–26090, 2018.

[10] J. Moon, H. Lee, C. Song, S. Kang, and I. Lee, "Relay-assisted proactive eavesdropping with cooperative jamming and spoofing," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6958–6971, Oct. 2018.

[11] J. Moon, H. Lee, C. Song, S. Lee, and I. Lee, "Proactive eavesdropping with full-duplex relay and cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6707–6719, Oct. 2018.

[12] Q. Li, H. Zhang, J. Qiao, and D. Yuan, "Cooperative relay-assisted proactive eavesdropping for wireless information surveillance systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[13] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1449–1461, Dec. 2016.

[14] X. Jiang, H. Lin, C. Zhong, X. Chen, and Z. Zhang, "Proactive eavesdropping in relaying systems," *IEEE Signal Process. Lett.*, vol. 24, no. 6, pp. 917–921, Jun. 2017.

[15] G. Ma, J. Xu, L. Duan, and R. Zhang, "Wireless surveillance of two-hop communications: (Invited paper)," in *Proc. IEEE 18th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Sapporo, Japan, Jul. 2017, pp. 1–5.

[16] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4585–4599, Jul. 2017.

[17] J. Moon, S. H. Lee, H. Lee, and I. Lee, "Proactive eavesdropping with jamming and eavesdropping mode selection," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3726–3738, Jul. 2019.

[18] G. Hu, Y. Cai, and J. Ouyang, "Proactive eavesdropping via jamming for multichannel decode-and-forward relay system," *IEEE Commun. Lett.*, vol. 24, no. 3, pp. 491–495, Mar. 2020.

[19] M. Zhu, J. Mo, N. Xiong, and J. Wang, "Legitimate monitoring via cooperative relay and proactive jamming," *IEEE Access*, vol. 7, pp. 40133–40143, 2019.

[20] Y. Zhang, X. Jiang, C. Zhong, and Z. Zhang, "Performance of proactive eavesdropping in dual-hop relaying systems," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Singapore, Dec. 2017, pp. 1–6.

[21] H. Cai, Q. Zhang, Q. Li, and J. Qin, "Proactive monitoring via jamming for rate maximization over MIMO Rayleigh fading channels," *IEEE Commun. Lett.*, vol. 21, no. 9, pp. 2021–2024, Sep. 2017.

[22] J. Moon, H. Lee, C. Song, and I. Lee, "Multiple amplify-and-forward full-duplex relays for legitimate eavesdropping," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 1–6.

[23] W. Huang, W. Chen, B. Bai, and Z. Han, "Wiretap channel with full-duplex proactive eavesdropper: A game theoretic approach," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7658–7663, Aug. 2018.

[24] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.

[25] B. Li, Y. Yao, H. Chen, Y. Li, and S. Huang, "Wireless information surveillance and intervention over multiple suspicious links," *IEEE Signal Process. Lett.*, vol. 25, no. 8, pp. 1131–1135, Aug. 2018.

[26] L. Lv, Z. Ding, J. Chen, and N. Al-Dhahir, "Design of secure NOMA against full-duplex proactive eavesdropping," *IEEE Wireless Commun. Lett.*, vol. 8, no. 4, pp. 1090–1094, Aug. 2019.

[27] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2196–2206, Oct. 2017.

[28] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, "Secure transmission designs for NOMA systems against internal and external eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2930–2943, 2020.

[29] B. Zheng, M. Wen, C.-X. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426–1440, Jul. 2018.

[30] Y. Feng, S. Yan, C. Liu, Z. Yang, and N. Yang, "Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1670–1683, Jun. 2019.

[31] K. Cao, B. Wang, H. Ding, T. Li, and F. Gong, "Optimal relay selection for secure NOMA systems under untrusted users," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1942–1955, Feb. 2020.

[32] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "Beamforming design and power allocation for secure transmission with NOMA," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2639–2651, May 2019.

[33] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[34] C. Y. Nguyen, H. Tran, T. T. T. Ninh, T. Q. Xuan, and Q. H. Pham, "Security enhancement in NOMA cooperative network with a proactive attack scheme," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, Hanoi, Vietnam, Oct. 2019, pp. 225–230.

[35] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO nonorthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7563–7567, Aug. 2017.

[36] T. P. Huu, V. N. Vo, H. Tran, T. X. Quach, and V. N. Dinh, "Secrecy performance analysis of cooperative NOMA networks with active protection under α - μ fading," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, Hanoi, Vietnam, Oct. 2019, pp. 215–220.

[37] J. Tang, L. Jiao, K. Zeng, H. Wen, and K.-Y. Qin, "Physical layer secure MIMO communications against eavesdroppers with arbitrary number of antennas," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 466–481, 2021.

[38] K. Shim, T. N. Do, and B. An, "Improving physical layer security of NOMA networks by using opportunistic scheduling," in *Proc. 10th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2018, pp. 262–267.

[39] D. Xu, "Proactive eavesdropping of suspicious non-orthogonal multiple access networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13958–13963, Nov. 2020.

[40] Z. Cheng, J. Si, Z. Li, L. Guan, Y. Zhao, D. Wang, J. Cheng, and N. Al-Dhahir, "Covert surveillance via proactive eavesdropping under channel uncertainty," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4024–4037, Jun. 2021.

[41] H. Wu, L. Yan, R. Ma, J. Ou, and J. Cui, "A decode-and-forward relay-aided proactive eavesdropping scheme for wireless surveillance," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Chongqing, China, Aug. 2020, pp. 1104–1109.

[42] X. Wang, J. Wang, L. He, and J. Song, "Outage analysis for downlink NOMA with statistical channel state information," *IEEE Wireless Commun. Lett.*, vol. 7, no. 2, pp. 142–145, Apr. 2018.

[43] T. P. Huu, T. N. Thi-Thanh, C. Nguyen-Yen, H. Tran, V. N. Dinh, and V. N. Vo, "Secrecy outage probability and fairness of packet transmission time in a NOMA system," *IEEE Access*, vol. 8, pp. 79637–79649, 2020.

[44] N. Zhang, J. Wang, G. Kang, and Y. Liu, "Uplink nonorthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 458–461, Mar. 2016.

[45] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, and F. Gong, "On the security enhancement of uplink NOMA systems with jammer selection," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5747–5763, Sep. 2020.

[46] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 1301–1305.

[47] T. P. Huu, T. X. Quach, H. Tran, H.-J. Zepernick, and L. Sibomana, "On proactive attacks for coping with cooperative attacks in relay networks," in *Proc. 23rd Asia–Pacific Conf. Commun. (APCC)*, Perth, WA, Australia, Dec. 2017, pp. 1–6.

[48] T. X. Quach, H. Tran, E. Uhlemann, and M. T. Truc, "Secrecy performance of cooperative cognitive radio networks under joint secrecy outage and primary user interference constraints," *IEEE Access*, vol. 8, pp. 18442–18455, 2020.

[49] V. N. Vo, C. So-In, H. Tran, D.-D. Tran, and T. P. Huu, "Performance analysis of an energy-harvesting IoT system using a UAV friendly jammer and NOMA under cooperative attack," *IEEE Access*, vol. 8, pp. 221986–222000, 2020.

TUNG PHAM HUU received the B.S. degree in information technology from Vietnam National University, Hanoi, Vietnam, in 2002, and the M.S. degree in information technology from Moscow State University, in 2005. He is currently pursuing the Ph.D. degree with the Department of Computer Networks and Communications, Faculty of Information and Technology, Vietnam National University. Since 2007, he has taught and studied at the National University of Civil Engineering, Hanoi. His research interests include physical layer security, NOMA networks, and cognitive radio networks.

VAN NHAN VO received the B.S. degree from Danang University, Vietnam, in 2006, the M.S. degree from Duy Tan University, Vietnam, in 2014, and the Ph.D. degree from Khon Kaen University, Thailand, in 2019, all in computer science. He is currently a Lecturer with Duy Tan University and a Postdoctoral Researcher with the ANT Laboratory, Khon Kaen University. His research interests include information security, physical layer secrecy, radio-frequency energy harvesting, non-orthogonal multiple access, wireless sensor networks, the Internet of Things, unmanned aerial vehicles, and the security of other advanced communication systems.

HUNG TRAN received the B.S. and M.S. degrees in information technology from Vietnam National University, Hanoi, Vietnam, in 2002 and 2006, respectively, and the Ph.D. degree from the Blekinge Institute of Technology, Sweden, in March 2013. In 2014, he was with the Electrical Engineering Department, ETS, Montreal, Canada. From 2015 to 2020, he was a Researcher at Mälardalen University, Sweden. Currently, he is working as a Researcher at the Computer Science Department, Phenikaa University, Hanoi. Besides doing research in the areas of wireless communication, he is also interested in topics of natural language processing, and artificial intelligence which have been applied to develop academic gates platform (https://www.academicgates.com).

TRUONG XUAN QUACH received the bachelor's degree in information technology from Vietnam National University (Hanoi)—VNU University of Engineering and Technology (VNU-UET), Vietnam, in 2002, and the master's degree in computer science from Thai Nguyen University (TNU), Vietnam, in 2007. He is currently pursuing the Ph.D. degree with VNU-UET. Currently, he is also a Lecturer and the Vice-Dean of the Faculty of Information Technology, Thai Nguyen University of Information and Communication Technology (ICTU), Vietnam. His research interests include wireless communication, physical-layer security, and communications theory.

VIET NGUYEN DINH received the B.Sc. degree in radio physics from Hanoi University, in 1976, the M.Sc. degree in science from the Vietnam National University (Hanoi)–University of Science (VNU-HUS), and the Ph.D. degree from the VNU University of Engineering and Technology (VNU-UET), in 2004. He is a Senior Lecturer with the Faculty of Information Technology, VNU-UET. He has been an Associate Professor since 2007. His current research interests include wireless mobile *ad-hoc* networks, wireless sensor networks, QoS guaranteeing for multimedia communication, and network simulation.