Secrecy Performance Analysis of Cooperative NOMA Networks With Active Protection under $\alpha - \mu$ Fading

Tung Pham Huu[1], Van Nhan Vo[2,3], Hung Tran[4], Truong Xuan Quach[5], Viet Nguyen Dinh[6]
[1]National University of Civil Engineering, Vietnam.
[2]International School, Duy Tan University, Vietnam.
[3]Faculty of Science, Khon Kaen University, Thailand.
[4]School of Innovation, Design, and Engineering, Mälardalen University, Sweden.
[5]TNU-University of Information and Communication Technology, Vietnam.
[6]The VNU University of Engineering and Technolog.
E-mail: {tungph@nuce.edu.vn, vonhanvan@dtu.edu.vn, tran.hung@mdh.se, qxtruong@ictu.edu.vn, vietnd@vnu.edu.vn}

***Abstract*—In this paper, we analyze the secrecy performance of a cooperative communication wireless system using non-orthogonal multiple access (NOMA) over $\alpha - \mu$ fading channel. A new cooperative NOMA scheme is proposed to protect the confidential communication that is transmitted from a source to two users by the help of a relay under the monitoring of an eavesdropper (EAV). In particular, the legitimate user generates jamming signals to the EAV while the source transmits the signals to the relay and the source sends jamming signals to the EAV while the relay forwards the signals to the users. In order to evaluate the secrecy performance, the physical layer security (PLS) in term of the secrecy outage probability (SOP) for the active protection scheme (APS) is investigated and compared to that for a benchmark non-protection scheme (NPS). Simulation results show that the APS can effectively enhance the secrecy performance.**

***Index Terms*—Non-orthogonal multiple access, Physical layer security, Secrecy outage probability, Active protection, Cooperative NOMA.**

I. Introduction

Non-orthogonal multiple access (NOMA) is considered as promising technology in fifth generation (5G) networks since it can archives high spectral efficiency [1]. NOMA allows to serve multiple users simultaneously with the same radio resource (e.g., time/frequency). More specifically, multiple users in NOMA can share the same radio resources such as the code-domain or power domain [2]. In code-domain NOMA, different users are assigned different codes and multiplexed over the same time/frequency resources [3], [4]. In contrast, users in power-domain NOMA are assigned different power levels on the basis of channel state information (CSI) for communication. Then users use self interference cancellation (SIC) technique to reduce the interference caused by other users' signal and detect the desired signal from the superimposed received signal [5].

Furthermore, to improve the transmission reliability and extend radio coverage, cooperative NOMA with relay has received much attention in literature [6], [7], [8]. Although cooperative NOMA with relay may improve the transmission reliability, security is one of major challenges due to broadcast nature of wireless communication, i.e., the transmitted signal may be overheard by eavesdroppers (EAVs) over illegal channels. Traditionally, to combat eavesdropping, cryptographic methods are usually applied in upper layer. However, this technique may become vulnerable with development of super computer [6] and physical layer security (PLS) was investigated as an alternative mechanism [9]. This approach is invented by Wyner from an information-theoretical perspective, in which the secrecy capacity is defined as the difference between the capacity of legitimate channel and the capacity of illegitimate channel [9]. Accordingly, many researches have been conducted to guarantee the security through PLS [6].

In addition, to increase secrecy rate and reduce information leakage, some studies focused on strategic design of cooperative NOMA networks with jamming technique are investigated [7], [10], [11]. For example, C. Yuan $et\ al.$ proposed a new cooperative NOMA scheme where the source actively sends jamming signals while the relay is forwarding confidential signals to destination. The result indicated that this proposed NOMA scheme can improve the secrecy rate by about 78.1% [7]. Y. Feng $et\ al.$ focused on the joint of full-duplex and artificial noise techniques at relays and concluded that the SOP performance metric can significantly be improved in cooperative NOMA systems [10]. H. Zhang $et\ al.$ considered a NOMA two-way relay wireless network composed of pre-assigned user pairs. They concluded that all user pairs using jamming signals in the multiple access phase can enhance the secrecy performance [11]. Nevertheless, the above works did not propose the solution to combat the cooperative attack of jammer and EAV for protecting the wireless networks.

Therefore, in this work, we study a cooperative attack in a relay wireless network with NOMA and propose a APS based on a jamming strategy to improve the secrecy performance. In particular, we consider the system in which a source communicates with two legitimate users through a relay, while

978-1-7281-2392-9/19/$31.00 ©2019 IEEE

two attackers (including a jammer and an EAV) try to steal the confidential messages communicated over the relay network. More specifically, the jammer firstly attacks the relay and the users by sending the jamming signal. This leads to the both source and relay must increase their power to satisfy the quality of service (QoS). Unfortunately, the EAV takes this opportunity to improve its overhearing process. In order to overcome this issue, we propose an active noise generating strategy to degrade the attackers and enhance the security communication. Accordingly, the secrecy outage probabilities (SOPs) are introduced for non-protection scheme (NPS) and our proposed strategy, namely active protection scheme (APS). Finally, our obtained numerical results show that proposed solution can enhance the secure communication significantly.

The remaining of this paper is organized as follows: In Section II, the system model, channel assumptions are presented. In Section III, derivations for the secure performance of NPS and APS are presented. Section IV provides simulations to evaluate the secrecy performance. Finally, Section V concludes the paper.

II. System model

Let us consider a cooperative NOMA system which consists of a source S, a relay R, and two legitimate users U_1 and U_2; in which S simultaneously communicates to U_1 and U_2 with the help of R using decode-and-forward (DF) in the presence of two adversaries (i.e., jammer J and EAV E). It is noted that S, U_1, U_2, and E are equipped with a single antenna while relay R has N antennas.

Here, the EAV cooperates with jammer to overhear confidential information. Specially, while the EAV operates as passive mode to monitor the signals, the jammer generates jamming signals to force the source and relay. As a result, the source and relay increase their transmitted powers to guarantee the performance, the EAV can enhance its overhearing ability.

We assume that there is no direct link between the source and the users [12]; hence, the relay is deployed to extend coverage. Note that all links are subject to $\alpha-\mu$ fading distribution. This is general fading distribution which includes the Nakagami-m, Weibull, One -Sided Gaussian, Rayleigh and Negative Exponential distribution are special cases [13]. The respective channel gains X_l are independent and identically distributed (i.i.d). Thus, the probability density function (PDF) of X_l is given by [13]

$$f_{X_l}(x)=\frac{\alpha\mu^{\mu}x^{\alpha\mu-1}}{\Gamma(\mu)\hat{x}^{\alpha\mu}}\exp\left[-\mu\Big(\frac{x}{\hat{x}}\Big)^{\alpha}\right], \tag{1}$$

where α is a non-linearity parameter (arbitrary fading parameter) and $\mu>0$ is related to the number of multipath clusters. Also, μ is known as the inverse of the normalized variance of X^{α} and is calculated as $\mu=\mathbb{E}^2[X^{\alpha}]/\mathbb{V}[X^{\alpha}]$ where $\mathbb{E}[\cdot]$ and $\mathbb{V}[\cdot]$ denote the expectation and variance operators, respectively. Further, $\Gamma(\cdot)$ stands for the gamma function and $\hat{x}$ is the $\alpha-$th root mean value and is defined as $\hat{x}=\sqrt[\alpha]{\mathbb{E}[X^{\alpha}]}$ [14, (8.310.1)]. Moreover, the k-th moment of X is expressed as

$$\mathbb{E}[X^k]=\frac{\hat{x}^k}{\mu^{\frac{k}{\alpha}}}\frac{\Gamma(\mu+\frac{k}{\alpha})}{\Gamma(\mu)}. \tag{2}$$

The CDF of X is also given by

$$F_X(x)=\frac{\Gamma\left[\mu,\mu\Big(\frac{x}{\hat{x}}\Big)^{\alpha}\right]}{\Gamma(\mu)}, \tag{3}$$

where $\Gamma[\cdot,\cdot]$ is the incomplete gamma function [14, (8.350.1)].

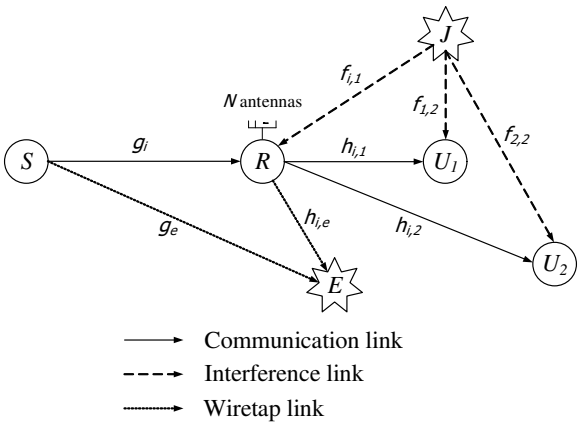

Figure 1. Model of the NOMA network in the presence of cooperative attack of a jammer and an EAV under the NPS.

Next, we introduce the communication protocol of the benchmark scheme NPS and the proposed APS to evaluate the secrecy performance of the considered NOMA system.

A. Non-protection scheme (NPS)

We consider the NPS illustrated in Fig. 1, where neither S nor R has any strategy to secure their communications. Therefore, if J transmits a jamming signal to degrade the system performance of the relay NOMA network, S and R will respond by immediately increasing their transmit power to maintain satisfactory QoS without knowing about existence of EAV.

It is noted that the communication protocol is divided into two phases: S-R communication phase and R-U communication phase. In the first phase, S sends composed signal $\sqrt{\alpha_1 P_s}s_1+\sqrt{\alpha_2 P_s}s_2$ to R, where α_1, α_2 are the power allocation coefficients, and s_1 and s_2 are the signals of U_1 and U_2, respectively. It is assumed that $\alpha_2\geq\alpha_1$ and $\alpha_1+\alpha_2=1$ [15]. The received signal at i-th antenna branch of the R, $1\leq i\leq N$, can be expressed as

$$y_i^r=\sqrt{\alpha_1 P_s}s_1 g_i+\sqrt{\alpha_2 P_s}s_2 g_i+\omega_i^r, \tag{4}$$

where P_s is the transmit power of S, g_i denotes the channel coefficient between R and i-th antenna of R and ω_i^r is additive white Gaussian noise (AWGN) with zero-mean and variance, i.e., $\omega_i^r\sim\mathcal{CN}(0,\sigma_i^2)$. Since the EAV is in the coverage range of the source, the EAV also receives the combined signal from S which is given by

$$y_e^{(1)}=\sqrt{\alpha_1 P_s}s_1 g_e+\sqrt{\alpha_2 P_s}s_2 g_e+\omega_e, \tag{5}$$

where g_e is the channel coefficient from S to the EAV and ω_e denotes the AWGN at the EAV, i.e., $\omega_e\sim\mathcal{CN}(0,\sigma_e^2)$. Here, S allocates a higher power level to the signal of U_2 than that of U_1; thus, at i-th antenna, S first decodes s_2 by treating s_1

978-1-7281-2392-9/19/$31.00 ©2019 IEEE

as an interference, and then obtains s_1 by using SIC [5]. As a result, the signal-to-interference-plus-noise ratios (SINRs) for decoding s_1 and s_2 at antenna branch i-th of the relay R subject to the interference induced by J, respectively, are given by

$$\gamma_{i,r}^{s_1} = \frac{\alpha_1 P_s |g_i|^2}{P_j |f_{i,1}|^2 + \sigma_r^2}, \tag{6}$$

$$\gamma_{i,r}^{s_2} = \frac{\alpha_2 P_s |g_i|^2}{P_j |f_{i,1}|^2 + \alpha_1 P_s |g_i|^2 + \sigma_r^2}, \tag{7}$$

where P_j is the transmit power of J and $f_{i,1}$ is the channel coefficient between J and i-th antenna of the relay.

Adopt to [12], the R uses selective combining (SC) technique to process the received signal. Furthermore, in order to improve the secrecy performance, the relay chooses an antenna such that the SINR of s_2 at R is the highest, i.e,.

$$i^* = \arg \max_{i \in \{1,2,\ldots,N\}} \{\gamma_{i,r}^{s_2}\}. \tag{8}$$

Accordingly, the SINRs for decoding s_1 and s_2 at R can be formulated, respectively, as

$$\gamma_r^{s_1} = \frac{\alpha_1 P_s |g_{i^*}|^2}{P_j |f_{i^*,1}|^2 + \sigma_r^2}, \tag{9}$$

$$\gamma_r^{s_2} = \frac{\alpha_2 P_s |g_{i^*}|^2}{P_j |f_{i^*,1}|^2 + \alpha_1 P_s |g_{i^*}|^2 + \sigma_r^2}. \tag{10}$$

Note that J cooperates with the EAV to attack the relay NOMA network; thus, the efficient interference cancellation techniques can be applied at the EAV to remove the jamming signal from J [16]. Therefore, the signal-to-noise ratio (SNR) and SINR for decoding s_1 and s_2 at the EAV can be respectively expressed as

$$\gamma_{s_1,e}^{(1)} = \frac{\alpha_1 P_s |g_e|^2}{\sigma_e^2}, \tag{11}$$

$$\gamma_{s_2,e}^{(1)} = \frac{\alpha_2 P_s |g_e|^2}{\alpha_1 P_s |g_e|^2 + \sigma_e^2}. \tag{12}$$

In the R-U communication phase, the relay broadcasts a superposed signal to the users. Thus, the received signal at the U_k is formulated as

$$y_k^d = \sqrt{\beta_1 P_r} s_1 h_{i,k} + \sqrt{\beta_2 P_r} s_2 h_{i,k} + \omega_k^d, \tag{13}$$

where $k \in \{1, 2\}$, $h_{i,k}$ is the channel coefficient from i-th antenna of relay to U_k, P_r is the transmission power of relay, and ω_k^d is the AWGN at the U_k, i.e., $\omega_k^d \sim \mathcal{CN}(0, \sigma_d^2)$.

Furthermore, U_2 is staying far away from R which has worse channel condition. Therefore, to improve the secrecy performance, the selected antenna is chosen among N antennas of R such that the channel gain of U_2 is the best, i.e.,

$$m^* = \arg \max_{i \in \{1,2,\ldots,N\}} \{h_{i,2}\}. \tag{14}$$

Accordingly, the SINRs at U_1 and U_2 can be, respectively written as

$$\gamma_d^{s_1} = \frac{\beta_1 P_r |h_{m^*,1}|^2}{P_j |f_{1,2}|^2 + \sigma_d^2}, \tag{15}$$

$$\gamma_d^{s_2} = \frac{\beta_2 P_r |h_{m^*,2}|^2}{\beta_1 P_r |h_{m^*,2}|^2 + P_j |f_{2,2}|^2 + \sigma_d^2}. \tag{16}$$

Because of the broadcast nature, the EAV also receives the combined signal from the relay as

$$y_e^{(2)} = \sqrt{\beta_1 P_r} s_1 h_{i,e} + \sqrt{\beta_2 P_r} s_2 h_{i,e} + \omega_e, \tag{17}$$

where $h_{i,e}$ is channel coefficient from i-th antenna of relay to the EAV. Thus, the SNR and SINR for decoding the signal s_1 and s_2 at the EAV in the second phase can be, respectively written by

$$\gamma_{s_1,e}^{(2)} = \frac{\beta_1 P_r |h_{m^*,e}|^2}{\sigma_e^2}, \tag{18}$$

$$\gamma_{s_2,e}^{(2)} = \frac{\beta_2 P_r |h_{m^*,e}|^2}{\beta_1 P_r |h_{m^*,e}|^2 + \sigma_e^2}. \tag{19}$$

To exploit the confidential message, EAV applies the SC technique to enhance the quality of received signal, this leads to decode the eavesdropped signal more easy. Accordingly, the SNR and SINR received at the EAV can be expressed as follows:

$$\gamma_e^{s_1} = \max \left\{ \gamma_{s_1,e}^{(1)}, \gamma_{s_1,e}^{(2)} \right\}, \tag{20}$$

$$\gamma_e^{s_2} = \max \left\{ \gamma_{s_2,e}^{(1)}, \gamma_{s_2,e}^{(2)} \right\}. \tag{21}$$

B. Active protection scheme (APS)

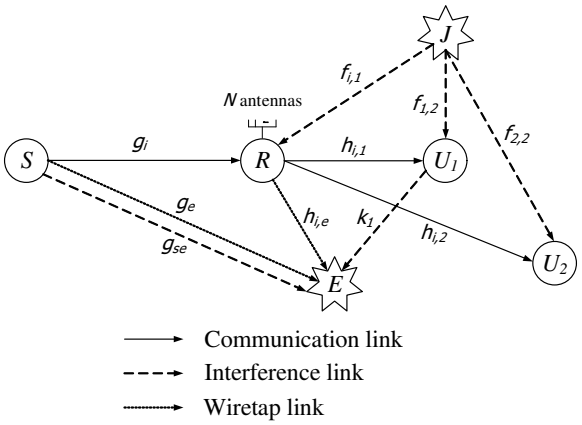

Figure 2. Model of the NOMA network in the presence of cooperative attack of a jammer and an EAV under the APS.

To protect the secrecy communication from S to U_1 and U_2, we propose an active protection approach illustrated in Fig. 2, in which the legitimate users and S generate proactively the jamming signal to force the EAV. More specially, similar to the NPS, the communication protocol is introduced by two phases as follows:

In the S-R communication phase, while S transmits the signals to R, U_1 acts as the first friendly jammer by generating a proactive jamming signals to E with power P_1 to protect this communication. It is noted that R cooperates with U_1; thus, R can cancel the jamming signal from U_1 [16]. Similar to the NPS, R selects the best one among N antennas of R and uses SC technique to process the signal, i.e., the SINRs at i-th antenna of R for decoding s_1 and s_2 are as (9) and (10).

978-1-7281-2392-9/19/$31.00 ©2019 IEEE

On the other hand, the EAV suffers interference from the jamming signal of U_1; hence, the SINRs of EAV for decoding s_1 and s_2 are obtained as

$$\gamma_{s_1,ej}^{(1)} = \frac{\alpha_1 P_s |g_e|^2}{P_1 |k_1|^2 + \sigma_e^2}, \tag{22}$$

$$\gamma_{s_2,ej}^{(1)} = \frac{\alpha_2 P_s |g_e|^2}{\alpha_1 P_s |g_e|^2 + P_1 |k_1|^2 + \sigma_e^2}, \tag{23}$$

where k_1 is channel coefficient of the $U_1 \to E$ link.

In the R-U communication phase, while R forwards the signals to U_1 and U_2 by using DF, S acts as the second friendly jammer by generating a jamming signal with the power P_{se} to degrade the performance of the EAV. Similar to the first phase, U_1 and U_2 cooperate with S; thus, users can cancel the jamming signal from S. Furthermore, R selects the best one among N antennas to improve the secrecy performance, i.e., the SINRs for decoding s_1 and s_2 received at U_1 and U_2 are as in (15) and (16). Accordingly, the SINRs for decoding s_1 and s_2 at EAV in the second phase can be expressed, respectively, as follows:

$$\gamma_{s_1,ej}^{(2)} = \frac{\beta_1 P_r |h_{m^*,e}|^2}{P_{se} |g_{se}|^2 + \sigma_e^2}, \tag{24}$$

$$\gamma_{s_2,ej}^{(2)} = \frac{\beta_2 P_r |h_{m^*,e}|^2}{\beta_1 P_r |h_{m^*,e}|^2 + P_{se} |g_{se}|^2 + \sigma_e^2}, \tag{25}$$

where P_{se} and g_{se} are the jamming signal power of S to E and the channel coefficient of the $S \to E$ interference link in the second phase, respectively.

Finally, the end-to-end SINRs for decoding s_1 and s_2 at EAV can be written, respectively, as follows:

$$\gamma_{ej}^{s_1} = \max\left\{\gamma_{s_1,ej}^{(1)}, \gamma_{s_1,ej}^{(2)}\right\}, \tag{26}$$

$$\gamma_{ej}^{s_2} = \max\left\{\gamma_{s_2,ej}^{(1)}, \gamma_{s_2,ej}^{(2)}\right\}. \tag{27}$$

III. Secrecy outage probability analysis

In this section, we analyze the SOP of the considered system for both the NPS and the APS. To assess the effectiveness of the proposed APS compared to the benchmark NPS, we introduce the respective SOP metric which is defined as the probability that the secrecy capacity is smaller than a given secrecy target rate R [16], i.e.,

$$\mathcal{O}^{sec} = \Pr\{C_S < R\}, \tag{28}$$

where C_S is the secrecy capacity and that is defined as the difference between the legal channel capacity and the wiretap channel capacity.

A. Secrecy outage probability for the NPS

According to [15], the main channel capacity and wiretap channel capacity for decoding s_1 at U_1 and E of the NPS are given, respectively, as follows:

$$C_{NPS}^{1} = \frac{B}{2}\log_2\left(1+\gamma^{s_1}\right), \tag{29}$$

$$C_{NPS}^{1,e} = \frac{B}{2}\log_2\left(1+\gamma_e^{s_1}\right), \tag{30}$$

where B is the bandwidth of the network and $\gamma^{s_1} = \min\{\gamma_r^{s_1}, \gamma_d^{s_1}\}$.

Similar to (29) and (30), the main and wiretap channel capacity for decoding s_2 at U_2 and E of the NPS can be given, respectively, as

$$C_{NPS}^{2} = \frac{B}{2}\log_2\left(1+\gamma^{s_2}\right), \tag{31}$$

$$C_{NPS}^{2,e} = \frac{B}{2}\log_2\left(1+\gamma_e^{s_2}\right). \tag{32}$$

where $\gamma^{s_2} = \min\{\gamma_r^{s_2}, \gamma_d^{s_2}\}$.

Therefore, the secrecy capacities from S to U_1 and U_2 are given, respectively, as follows:

$$C_{NPS}^{1,s} = \left(C_{NPS}^{1} - C_{NPS}^{1,e}\right)^+, \tag{33}$$

$$C_{NPS}^{2,s} = \left(C_{NPS}^{2} - C_{NPS}^{2,e}\right)^+, \tag{34}$$

where $(x)^+ = \max(x, 0)$.

Furthermore, the confidential information is eavesdropped if the event either instantaneous secrecy capacity $C_{NPS}^{1,s}$ or $C_{NPS}^{2,s}$ falls below their own secrecy target rates R_1 and R_2. This can be interpreted into the term of the SOP of the considered system for the NPS as

$$\begin{aligned}\mathcal{O}_{NPS}^{sec} &= \Pr\left\{C_{NPS}^{1,s} < R_1 \ \cup \ C_{NPS}^{2,s} < R_2\right\} \\ &= \Pr\left\{\frac{1+\gamma^{s_1}}{1+\gamma_e^{s_1}} < 2^{\frac{2R_1}{B}} \ \cup \ \frac{1+\gamma^{s_2}}{1+\gamma_e^{s_2}} < 2^{\frac{2R_2}{B}}\right\} \\ &= \Pr\{\gamma^{s_1} < \delta_1 + (\delta_1+1)\gamma_e^{s_1} \\ &\qquad \cup \ \gamma^{s_2} < \delta_2 + (\delta_2+1)\gamma_e^{s_2}\},\end{aligned} \tag{35}$$

where $\delta_1 = 2^{\frac{2R_1}{B}} - 1$ and $\delta_2 = 2^{\frac{2R_2}{B}} - 1$.

B. Secrecy outage probability for the APS

Similar to the NPS, the main and the wiretap channel capacity of U_1 and the EAV for decoding s_1 in the proposed APS are formulated, respectively, as

$$C_{APS}^{1} = \frac{B}{2}\log_2\left(1+\gamma^{s_1}\right), \tag{36}$$

$$C_{APS}^{1,ej} = \frac{B}{2}\log_2\left(1+\gamma_{ej}^{s_1}\right). \tag{37}$$

Similarly, the main and the wiretap channel capacity of U_2 and EAV for decoding s_2 in the proposed APS are obtained, respectively, as follows:

$$C_{APS}^{2} = \frac{B}{2}(\log_2\left(1+\gamma^{s_2}\right), \tag{38}$$

$$C_{APS}^{2,ej} = \frac{B}{2}\log_2\left(1+\gamma_{ej}^{s_2}\right). \tag{39}$$

Accordingly, the secrecy capacities from S to U_1 and U_2 in the APS can be written, respectively, as

$$C_{APS}^{1,s} = \left(C_{APS}^{1} - C_{APS}^{1,ej}\right)^+, \tag{40}$$

$$C_{APS}^{2,s} = \left(C_{APS}^{2} - C_{APS}^{2,ej}\right)^+. \tag{41}$$

978-1-7281-2392-9/19/$31.00 ©2019 IEEE

Finally, similar to (35), the SOP of the considered system for the APS is obtained as

$$\begin{aligned}\mathcal{O}_{APS}^{sec} &= \Pr\left\{C_{APS}^{1,s} < R_1 \ \cup \ C_{APS}^{2,s} < R_2\right\} \\ &= \Pr\left\{\frac{1+\gamma^{s_1}}{1+\gamma_{ej}^{s_1}} < 2^{\frac{2R_1}{B}} \ \cup \ \frac{1+\gamma^{s_2}}{1+\gamma_{ej}^{s_2}} < 2^{\frac{2R_2}{B}}\right\} \\ &= \Pr\left\{\gamma^{s_1} < \delta_1 + (\delta_1+1)\gamma_{ej}^{s_1} \right. \\ &\qquad \left. \cup \ \gamma^{s_2} < \delta_2 + (\delta_2+1)\gamma_{ej}^{s_2}\right\}. \end{aligned} \quad (42)$$

As we know that α-μ fading is one of the most complicated channels, which can describe other channels by adjust alpha and mu parameter. This leads to a fact that the closed-form expressions for (35) and (42) are impossible to obtain for the considered system. However, we will do simulations to examine the effectiveness of the proposed scheme and make comparisons between two two schemes, i.e., NPS and APS.

IV. Numerical results

In this section, we present numerical results to illustrate the impact of system parameters on the secrecy outage probability (SOP) of the non-protection scheme (NPS) and the proposed active protection scheme (APS) by using Monte Carlo simulations. Without loss of generality, we assumed that $\sigma_r^2 = \sigma_d^2 = \sigma_e^2 = N_0$ [7] and defined that $\gamma_s = P_s/N_0, \gamma_{se} = P_{se}/N_0, \gamma_r = P_r/N_0, \gamma_j = P_j/N_0$, and $\gamma_1 = P_1/N_0$ are the transmit SNRs of S, R, J, and U_1, respectively. The system parameters are as follows:

- System bandwidth $B = 5$ MHz
- Outage secrecy target rate $R_1 = R_2 = 1$ kbps
- Number of antennas of the relay $N = 5$

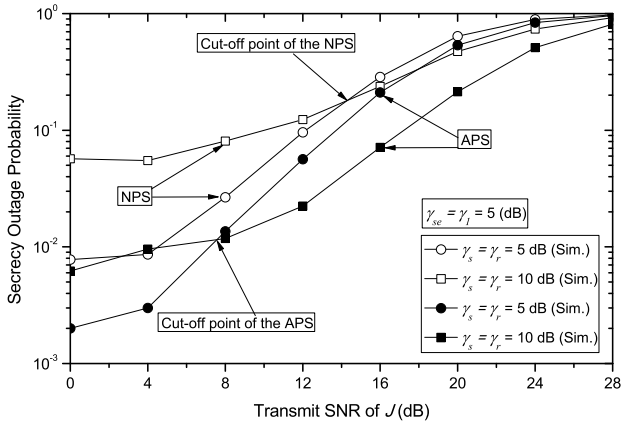

Figure 3. Impact of the transmit SNR at J, S, and R on the SOP for the NPS and APS with $\alpha = 2$, $\mu = 1, \Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$, and $\Omega_{g_e} = \Omega_{g_{s,e}} = \Omega_{h_{i,e}} = \Omega_{f_{i,1}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = 0.1$.

Fig. 3 illustrates the impact of the transmit SNR γ_j on the SOP of both NPS and APS for different transmit SNRs γ_s and γ_r. We can see that the SOP of the APS is significantly lower than that of the NPS for the entire range of the considered transmit SNRs of the jammer. This is because S and U_1 is used as the friendly jammers to degrade the eavesdropping signals at the E in the APS. Furthermore, when the transmit SNR of J decreases, the SOPs for both schemes are improved. This is a fact that the SINRs for decoding the signals s_1 and s_2 at R, U_1, U_2 suffers from the interference caused by the jamming signal of J.

In addition, the SOP of the APS with high γ_s and γ_r, i.e., $\gamma_s = \gamma_r = 10$ (dB), is better than that with low γ_s and γ_r, i.e., $\gamma_s = \gamma_r = 5$ (dB) when γ_j larger than the cut-off point of the APS and vice versa. This trend is applied for the NPS, i.e., when γ_j larger than the cut-off point of the NPS, the SOP with high γ_s and γ_r is outperforms that with low γ_s and γ_r and vice versa. In order to observe more clearly, we plot Fig. 4 to show the effect of γ_j, γ_s, and γ_r on the SOP. We can see that the SOP reaches the optimal point when γ_j, γ_s, and γ_r come to the intermediate points.

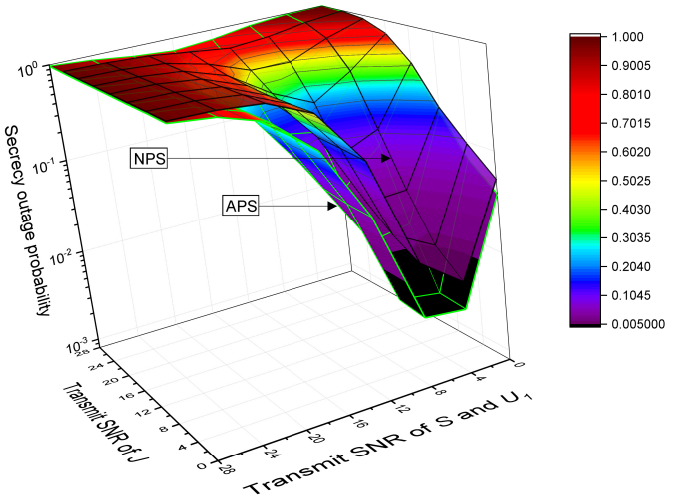

Figure 4. Impact of the transmit SNR at J, S, and R on the SOP for the NPS and APS with $\alpha = 2$, $\mu = 1, \Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$, and $\Omega_{g_e} = \Omega_{g_{s,e}} = \Omega_{h_{i,e}} = \Omega_{f_{i,1}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = 0.1$.

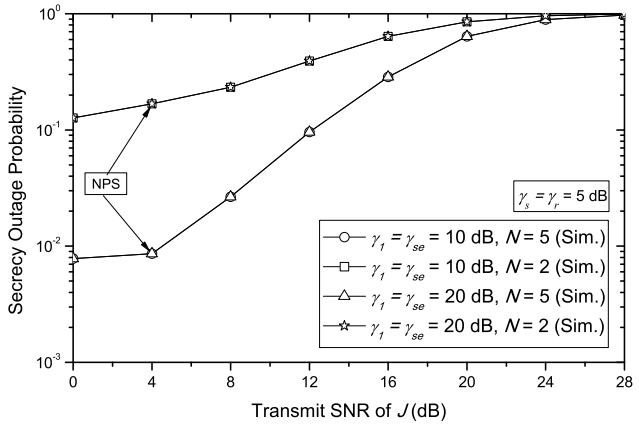

Figure 5. Impact of the number of antennas of R and the transmit SNR at J, S, and U_1 on the SOP for the NPS with $\alpha = 2$, $\mu = 1$, $\Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$, and $\Omega_{g_e} = \Omega_{g_{se}} = \Omega_{h_{i,e}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = \Omega_{f_{i,1}} = 0.1$.

Figs. 5 and 6 show the impact of the number of antennas of the R and the transmit SNR at J, S, and U_1 on the SOP. It clears that the transmit SNRs of the friendly jammer, i.e.,

978-1-7281-2392-9/19/$31.00 ©2019 IEEE

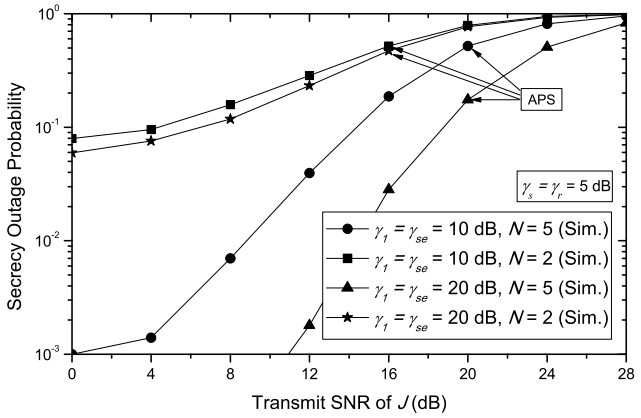

Figure 6. Impact of the number of antennas of R and the transmit SNR at J, S, and U_1 on the SOP for the APS with $\alpha = 2$, $\mu = 1$, $\Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$, and $\Omega_{g_e} = \Omega_{g_{se}} = \Omega_{h_{i,e}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = \Omega_{f_{i,1}} = 0.1$.

S and U_1, increase from $\gamma_{se} = \gamma_1 = 10$ dB to $\gamma_{se} = \gamma_1 = 20$ dB, the SOPs of the APS significantly reduces while that of the NPS is not change. This is a fact that while the NPS does not have any strategy to protect the considered system, the APS uses S and U_1 as two friendly jammers to protect the system by degrading the E. Furthermore, the SOPs of the both schemes are improved as the source's number of antennas increases. This is due to that the higher number of antennas leads to the higher diversity gain at the source.

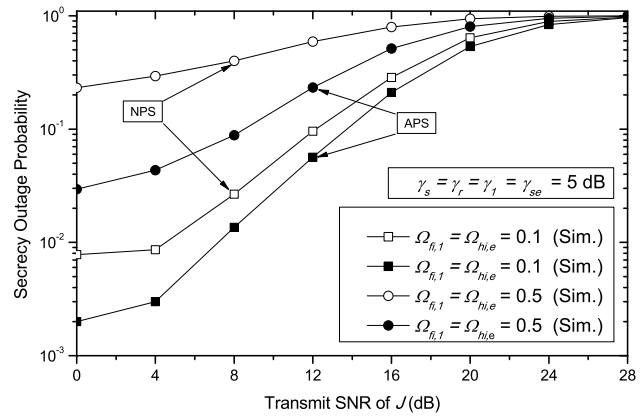

Figure 7. Impact of channel mean gain of the link $J \to R$ and $R \to E$ on the SOP for the NPS and APS with $\alpha = 2, \mu = 1, \Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$, and $\Omega_{g_e} = \Omega_{g_{s,e}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = 0.1$.

Fig. 7 investigates the impact of channel mean gains $\Omega_{f_{i,1}}$ and $\Omega_{h_{i,e}}$ of the $J \to R$ and $R \to E$ links on the secrecy performance. It is observed that the SOP deteriorates fast when the illegitimate links of J and E become stronger. This is obviously because of a fact that the good condition of $J \to R$ link leads to weak R; in contrast, if the condition of $R \to E$ link is better, the EAV will easily capture the confidential information. Again, the secrecy performance is significantly improved with the APS when we compare that with the NPS.

V. Conclusions

In this paper, the secrecy performance of cooperative relay NOMA system was investigated. A new active protection scheme to cope with cooperative jammer-EAV attacks in the cooperative NOMA networks is proposed. Accordingly, the secrecy performance in terms of the SOP was investigated for both non-protection scheme (NPS) and active protection scheme (APS). Simulation results have shown that the SOP of the proposed APS archives a lower than that of the NPS.

ACKNOWLEDGEMENT

This work is partially supported by the SSF framework grant Serendipity.

References

[1] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, "System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)," in *IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Sept 2013, pp. 611–615.

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

[3] Z. Yuan, G. Yu, W. Li, Y. Yuan, X. Wang, and J. Xu, "Multi-user shared access for internet of things," in *IEEE 83rd Vehicular Technology Conference (VTC Spring)*, May 2016, pp. 1–5.

[4] H. Nikopour and H. Baligh, "Sparse code multiple access," in *IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Sept 2013, pp. 332–336.

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

[6] Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, and M. Alouini, "Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay," *IEEE Transactions on Communications*, pp. 1–1, 2019.

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

[8] C. Liu, L. Zhang, M. Xiao, Z. Chen, and S. Li, "Secrecy performance analysis in downlink NOMA systems with cooperative full-duplex relaying," in *IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2018, pp. 1–6.

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

[10] Y. Feng, Z. Yang, and S. Yan, "Non-orthogonal multiple access and artificial-noise aided secure transmission in FD relay networks," in *IEEE Globecom Workshops*, Dec 2017, pp. 1–6.

[11] H. Zhang, N. Yang, K. Long, M. Pan, G. K. Karagiannidis, and V. C. M. Leung, "Secure communications in NOMA system: Subcarrier assignment and power allocation," *IEEE J. on Selected Areas in Commun.*, vol. 36, no. 7, pp. 1441–1452, July 2018.

[12] T. P. Huu, T. X. Quach, H. Tran, H. Zepernick, and L. Sibomana, "On proactive attacks for coping with cooperative attacks in relay networks," in *2017 23rd Asia-Pacific Conference on Communications (APCC)*, Dec 2017, pp. 1–6.

[13] M. D. Yacoub, "The $\alpha - \mu$ distribution: A physical fading model for the stacy distribution," *IEEE Trans. Veh. Technol.*, vol. 56, no. 1, pp. 27–34, Jan. 2007.

[14] I. Gradshteyn and I. Ryzhik, *Table of Integrals, series and products*, 7th ed. Elsevier, 2007.

[15] V. N. Vo, T. G. Nguyen, C. So-In, and H. Tran, "Outage performance analysis of energy harvesting wireless sensor networks for NOMA transmissions," *Mobile Networks and Applications*, pp. 1–19, Dec. 2018.

[16] V. N. Vo, T. G. Nguyen, C. So-In, and D.-B. Ha, "Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer," *IEEE Access*, vol. 5, pp. 25 196–25 206, Oct. 2017.

978-1-7281-2392-9/19/$31.00 ©2019 IEEE