Security-Reliability Analysis of Noma-Based Multi-Hop Relay Networks in Presence of an Active Eavesdropper with Imperfect Eavesdropping CSI

Tran Tin PHU[1,2], *The Hung DANG*[3], *Trung Duy TRAN*[4], *Miroslav VOZNAK*[5]

[1]Wireless Communications Research Group, Ton Duc Thang University,
No. 19 Nguyen Huu Tho Street, Tan Phong Ward, District 7, Ho Chi Minh City, Vietnam
[2]Faculty of Electrical and Electronics Engineering, Ton Duc Thang University,
No. 19 Nguyen Huu Tho Street, Tan Phong Ward, District 7, Ho Chi Minh City, Vietnam
[3]Faculty of Radio-Electronics Engineering, Le Quy Don Technical University,
236 Hoang Quoc Viet Street, Cau Giay District, Hanoi, Vietnam
[4]Department of Telecommunications, Posts and Telecommunications Institute of Technology,
11 Nguyen Dinh Chieu Street, Ho Chi Minh City, Vietnam
[5]Department of Telecommunications, Faculty of Electrical Engineering and Computer Science,
VSB–Technical University of Ostrava, 17. listopadu 15, 708 33 Ostrava, Czech Republic

phutrantin@tdt.edu.vn, danghung8384@gmail.com, trantrungduy@ptithcm.edu.vn, miroslav.voznak@vsb.cz

DOI: 10.15598/aeee.v15i4.2386

Abstract. *In this paper, we evaluate system performances of a multi-hop relay protocol with presence of an active eavesdropper. In the proposed protocol, a source attempts to transmit its data to a destination with assistance of multiple intermediate relays. From the eavesdropping Channel State Information (CSI) estimated, the source and relays adjust their transmit power so that the eavesdropper cannot overhear the transmitted data. Moreover, to enhance throughput for the proposed system, Non-Orthogonal Multiple Access (NOMA) technique with a simple power allocation is also proposed. We derive exact closed-form expressions of the Outage Probability (OP) and throughput for the data transmission over Rayleigh fading channel. In addition, when the CSI estimation is imperfect, Intercept Probability (IP) at the eavesdropper is derived. Finally, Monte Carlo simulations are presented to verify the theoretical derivations.*

Keywords

Intercept probability, multi-hop relay protocol, non-orthogonal multiple access, outage probability, physical-layer security, throughput.

1. Introduction

Recently, Non-Orthogonal Multiple Access (NOMA) technique [1], [2], [3] and [4] has gain much attention as an efficient method to significantly improve the data rate for wireless communication systems. Different from the conventional orthogonal multiple access, a transmitter can simultaneously send multiple data at the same time, code and frequency to one/multiple receivers by allocating different transmit power levels to the transmitted data. At the receivers, a Successive Interference Cancellation (SIC) technique is used to extract the intended data.

Secured communication techniques at the physical layer [5], [6], [7] and [8] have become an efficient method to obtain the data security without using complex cryptographic methods. In the physical-layer security, the physical properties of the wireless channel such as Channel State Information (CSI) and distances of the connection links can be used to protect the transmitted data. To the best of our knowledge, there are several published papers related to physical-layer security issue in NOMA-based relay networks. Particularly, the authors in [9] optimized secrecy sum rate of a NOMA-based downlink system including a transmitter, multiple legitimate users and a passive eavesdropper. Similar to [9], the authors in [10] proposed a secured downlink communication scenario where one multiple antenna base station communicates with multiple single antenna users using NOMA.

Different from the previous published works [9] and [10], this paper considers a multi-hop relay network, in which a source uses NOMA to transmit its data to a destination via multiple intermediate relays, in presence of an active eavesdropper. To avoid the eavesdropper from overhearing the transmitted data, the transmitters including the source and relays attempt to estimate the Channel State Information (CSI) between themselves and the eavesdropper, and then adjust their transmit power appropriately. For performance evaluation, we derive exact closed-form expressions of Outage Probability (OP) and throughput for the proposed scheme over Rayleigh fading channel. Moreover, when the eavesdropping CSI estimation is imperfect, Intercept Probability (IP) at the eavesdropper is also derived. We then perform Monte Carlo simulations to verify our theoretical derivations.

The rest of the paper is organized as follows. The system model and the proposed scheme are described in Sec. 2. In Sec. 3. , the performance evaluation of the protocol is described. The simulation results are presented in Sec. 4. Finally, the paper is concluded in Sec. 5.

2. System Model

Figure 1 shows system model of a NOMA-based multi-hop transmission protocol, where the source (N_0) communicates with the destination (N_K) via the via the multi-hop fashion with the help of K−1 relay nodes, respectively denoted by N_1, N_2,... and N_{K-1}. In the considered network, the Eavesdropper (E) appears and tries to overhear the data transmitted by the source and the relays. Assume that all of the terminals have

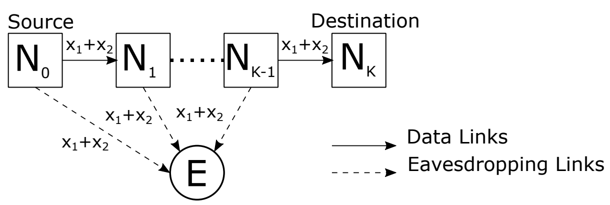

Fig. 1: System model of NOMA-based multi-hop transmission protocol in presence of one eavesdropper.

a single half-duplex radio and a single antenna, and hence a Time-Division Multiple Access (TDMA) is occupied. To avoid the eavesdropper from combining the transmitted data with Maximal Ratio Combining (MRC), the transmitters including source and relays use Randomize-and-Forward (RF) to randomly generate codebook [11] and [12]. We also assume that all of the channels between two arbitrary terminals are Rayleigh fading. Moreover, because the eavesdropper is an active node, the source and relay nodes attempt to estimate Channel State Information (CSI) between themself and the node E.

Considering the communication at the kth hop ($k = 1, 2, ..., K$) where N_{k-1} sends the source data to N_k while E overhears the data. Let h_k and g_k denote the channel coefficients of the $\mathrm{N}_{k-1} \to \mathrm{N}_k$ and $\mathrm{N}_{k-1} \to \mathrm{E}$ links. We also denote g_k^e as the CSI estimated by N_{k-1}. The correlation between g_k and g_k^e can be formulated as in [13] and [14]:

$$g_k^e = \rho g_k + \sqrt{1-\rho^2}\varepsilon, \tag{1}$$

where ρ is channel correlation factor and ε is estimation error.

Moreover, channel gains $\gamma_{\mathrm{D},k} = |h_k|^2$ and $\gamma_{\mathrm{E},k} = |g_k|^2$ are exponential Random Variables (RVs) whose parameters [15] and [16] are $\lambda_{\mathrm{D},k}$ and $\lambda_{\mathrm{E},k}$, respectively. It is worth noting that $\gamma_{\mathrm{E},k}^e = |g_k^e|^2$ also follows an exponential distribution with the parameter $\lambda_{\mathrm{E},k}$. To take path-loss into account, these parameters can be modeled by

$$\lambda_{\mathrm{D},k} = d_k^\beta, \;\; \lambda_{\mathrm{E},k} = l_k^\beta, \tag{2}$$

where d_k and l_k are distances of the $\mathrm{N}_{k-1} \to \mathrm{N}_k$ and $\mathrm{N}_{k-1} \to \mathrm{E}$ links, respectively, and β is path-loss exponent.

Using NOMA, the transmitter N_{k-1} combines two source data, i.e., x_1 and x_2, to create a superimposed data x_c as follows:

$$x_c = \sqrt{\alpha_1 P_{k-1}}x_1 + \sqrt{\alpha_2 P_{k-1}}x_2, \tag{3}$$

where P_{k-1} is transmit power of N_{k-1}, α_1 and α_2 are power allocation coefficients with $\alpha_1 + \alpha_2 = 1$ and $\alpha_1 > \alpha_2 \geq 0$.

Then, u_c is sent to N_k, and the received data at N_k can be expressed as

$$\begin{aligned} z_k &= h_k u_c + n_k, \\ &= \sqrt{\alpha_1 P_{k-1}}h_k u_1 + \sqrt{\alpha_2 P_{k-1}}h_k u_2 + n_k, \end{aligned} \tag{4}$$

where n_k is Gaussian noise at N_k whose mean and variance are 0 and σ_0^2, respectively.

Following the principle of NOMA, by treating u_2 as noise, N_k first decodes u_1 and then removes this data from the received data (z_k). As a result, the instantaneous Signal-to-Interference-plus-Noise Ratio (SINR), with respect to u_1, can be obtained as

$$\Psi_{\mathrm{D},k}^{u_1} = \frac{\alpha_1 P_{k-1}\gamma_{\mathrm{D},k}}{\alpha_2 P_{k-1}\gamma_{\mathrm{D},k} + \sigma_0^2}. \tag{5}$$

After completely removing the interference component $\sqrt{\alpha_1 P_{k-1}}h_k u_1$, the received data z_k can be rewritten by

$$z_k' = \sqrt{\alpha_2 P_{k-1}}h_k u_2 + n_k. \tag{6}$$

From Eq. (6), the instantaneous SINR obtained to decode u_2 is formulated by

$$\Psi_{\mathrm{D},k}^{u_2} = \frac{\alpha_2 P_{k-1}\gamma_{\mathrm{D},k}}{\sigma_0^2}. \quad (7)$$

From Eq. (5) and Eq. (7), the channel capacity, with respect to u_1 and u_2, can be given, respectively by

$$C_{\mathrm{D},k}^{u_1} = \frac{1}{K}\log_2\left(1 + \frac{\alpha_1 P_{k-1}\gamma_{\mathrm{D},k}}{\alpha_2 P_{k-1}\gamma_{\mathrm{D},k} + \sigma_0^2}\right), \quad (8)$$

$$C_{\mathrm{D},k}^{u_2} = \frac{1}{K}\log_2\left(1 + \frac{\alpha_2 P_{k-1}\gamma_{\mathrm{D},k}}{\sigma_0^2}\right), \quad (9)$$

where the factor $\frac{1}{K}$ indicates that the data transmission is split into K orthogonal time slots.

Due to the broadcast nature of wireless channel, the eavesdropper E can receive the data u_c from the node N_{k-1} and decodes u_1 and u_2 with SIC, similarly as the receiver N_k does. Similar to Eq. (8) and Eq. (9), the instantaneous channel capacity received at E, with respect to u_1 and u_2, can be expressed, respectively by

$$C_{\mathrm{E},k}^{u_1} = \frac{1}{K}\log_2\left(1 + \frac{\alpha_1 P_{k-1}\gamma_{\mathrm{E},k}}{\alpha_2 P_{k-1}\gamma_{\mathrm{E},k} + \sigma_0^2}\right), \quad (10)$$

$$C_{\mathrm{E},k}^{u_2} = \frac{1}{K}\log_2\left(1 + \frac{\alpha_2 P_{k-1}\gamma_{\mathrm{E},k}}{\sigma_0^2}\right). \quad (11)$$

Let us consider the probability that N_k can decode both u_1 and u_2 correctly. This event can be formulated by

$$\begin{aligned} J_k &= \Pr\left(C_{\mathrm{D},k}^{u_1} > R_{\mathrm{th}}, C_{\mathrm{D},k}^{u_2} > R_{\mathrm{th}}\right) \\ &= \Pr\left(\begin{array}{l}(\alpha_1 - \alpha_2\tau) P_{k-1}\gamma_{\mathrm{D},k} > \sigma_0^2\tau, \\ \alpha_2 P_{k-1}\gamma_{\mathrm{D},k} > \sigma_0^2\tau\end{array}\right), \end{aligned} \quad (12)$$

where R_{th} is a predetermined target rate, and $\tau = 2^{KR_{\mathrm{th}}} - 1$.

Then, we can give Eq. (11) by the following formula:

$$J_k = \begin{cases} 0, & \text{if } \alpha_1 \le \alpha_2\tau, \\ \Pr\left(\gamma_{\mathrm{D},k} > \max\left(\frac{\xi_1}{P_{k-1}}, \frac{\xi_2}{P_{k-1}}\right)\right), & \text{if } \alpha_1 > \alpha_2\tau, \end{cases} \quad (13)$$

where $\xi_1 = \dfrac{\tau\sigma_0^2}{(\alpha_1 - \alpha_2\tau)}$, $\xi_2 = \dfrac{\tau\sigma_0^2}{\alpha_2}$.

From Eq. (13), we observe that the value α_2 must satisfy the condition by

$$\alpha_1 > \alpha_2\tau \;\Leftrightarrow\; \alpha_2 < \frac{1}{1+\tau}. \quad (14)$$

Next, it is worth noting that if $\Delta_1 \ge \Delta_2$, when N_k decodes u_1 successfully then it also decodes u_2 successfully. Therefore, we propose a simple power allocation as

$$\Delta_1 \ge \Delta_2 \Leftrightarrow \alpha_2 \ge \frac{1}{2+\tau}. \quad (15)$$

Combining Eq. (14) and Eq. (15), we obtain

$$\frac{1}{2+\tau} \le \alpha_2 < \min\left(\frac{1}{1+\tau}, \frac{1}{2}\right). \quad (16)$$

Moreover, from Eq. (16), we can easily observe that to maximize J_k, the optimal values α_1 and α_2 can be given, respectively as

$$\begin{aligned} \alpha_1^* &= \frac{1+\tau}{2+\tau} = \frac{2^{MR_{\mathrm{th}}}}{2^{MR_{\mathrm{th}}}+1}, \\ \alpha_2^* &= \frac{1}{2+\tau} = \frac{1}{2^{MR_{\mathrm{th}}}+1}. \end{aligned} \quad (17)$$

Considering the decoding probability at the eavesdropper; also, once this node can decode u_1 correctly, then it can decode the data u_2 successfully. As mentioned above, the transmitter N_{k-1} attempts to estimate the eavesdropping CSI for adapting its transmit power using the following strategy: $P_{k-1}\gamma_{\mathrm{E},k}^e \le \gamma_{\mathrm{th}}$, where γ_{th} is a predetermined value. Hence, the maximum transmit power of N_{k-1} is obtained by

$$P_{k-1} = \frac{\gamma_{\mathrm{th}}}{\gamma_{\mathrm{E},k}^e}. \quad (18)$$

Substituting Eq. (17) and Eq. (19) into Eq. (5) and Eq. (10), respectively, yields

$$C_{\mathrm{D},k}^{u_1} = \frac{1}{K}\log_2\left(1 + \frac{\alpha_1^*\gamma_{\mathrm{th}}\gamma_{\mathrm{D},k}/\gamma_{\mathrm{E},k}^e}{\alpha_2^*\gamma_{\mathrm{th}}\gamma_{\mathrm{D},k}/\gamma_{\mathrm{E},k}^e + \sigma_0^2}\right), \quad (19)$$

$$C_{\mathrm{E},k}^{u_1} = \frac{1}{K}\log_2\left(1 + \frac{\alpha_1^*\gamma_{\mathrm{th}}\gamma_{\mathrm{E},k}/\gamma_{\mathrm{E},k}^e}{\alpha_2^*\gamma_{\mathrm{th}}\gamma_{\mathrm{E},k}/\gamma_{\mathrm{E},k}^e + \sigma_0^2}\right). \quad (20)$$

Then, the end-to-end channel capacity of the data link can be obtained by

$$C_{\mathrm{D,e2e}}^{u_1} = \min_{k=1,2,\ldots,K}\left(C_{\mathrm{D},k}^{u_1}\right). \quad (21)$$

Moreover, the channel capacity of the eavesdropping links is dominated by the highest link, which means

$$C_{\mathrm{E,e2e}}^{u_1} = \max_{k=1,2,\ldots,K}\left(C_{\mathrm{E},k}^{u_1}\right). \quad (22)$$

From Eq. (21) and Eq. (22), we can formulate the Outage Probability (OP) and the Intercept Probability (IP), respectively as

$$\mathrm{OP} = \Pr\left(C_{\mathrm{D,e2e}}^{u_1} \le R_{\mathrm{th}}\right), \quad (23)$$

$$\mathrm{IP} = \Pr\left(C_{\mathrm{E,e2e}}^{u_1} > R_{\mathrm{th}}\right). \quad (24)$$

Finally, throughput of the $\mathrm{N}_0 \to \mathrm{N}_\mathrm{K}$ connection can be defined by

$$\mathrm{TP} = \frac{2R_{\mathrm{th}}}{K}(1 - \mathrm{OP}), \quad (25)$$

where the factor 2 implies that the destination can receive two data u_1 and u_2 at the same time.

3. Performance Evaluation

3.1. Proposition 1

Outage Probability (OP) of the data link can be expressed by an exact closed-form expression as

$$\mathrm{OP} = 1 - \prod_{k=1}^{K} \frac{\lambda_{\mathrm{E},k}}{\lambda_{\mathrm{E},k} + \theta\lambda_{\mathrm{D},k}}, \tag{26}$$

where

$$\theta = \frac{\tau\sigma_0^2}{\left(\alpha_1^* - \alpha_2^*\tau\right)\gamma_{\mathrm{th}}}. \tag{27}$$

Proof: From Eq. (19), Eq. (21) and Eq. (23), Outage Probability (OP) of the data link is formulated by

$$\begin{aligned} \mathrm{OP} &= 1 - \Pr\left(\min_{k=1,2,\ldots,K}\left(C_{\mathrm{D},k}^{u_1}\right) \geq R_{\mathrm{th}}\right) \\ &= 1 - \prod_{k=1}^{K}\left(1 - \Pr\left(C_{\mathrm{D},k}^{u_1} < R_{\mathrm{th}}\right)\right) \\ &= 1 - \prod_{k=1}^{K}\left(1 - \Pr\left(\frac{\gamma_{\mathrm{D},k}}{\gamma_{\mathrm{E},k}^{e}} < \theta\right)\right). \end{aligned} \tag{28}$$

Then, using Eq. (4), [17] for $\Pr\left(\gamma_{\mathrm{D},k}/\gamma_{\mathrm{E},k}^{e} < \theta\right)$, we can obtain Eq. (26).

3.2. Corollary 1

Without using NOMA, OP can be rewritten by

$$\mathrm{OP}_{\mathrm{wo}} = 1 - \prod_{k=1}^{K} \frac{\lambda_{\mathrm{E},k}\gamma_{\mathrm{th}}}{\lambda_{\mathrm{E},k}\gamma_{\mathrm{th}} + \tau\sigma_0^2\lambda_{\mathrm{D},k}}. \tag{29}$$

Proof: In this case, N_{k-1} only sends u_1 to N_k at the kth time slot. In particular, the fractions of transmit power are set by $\alpha_1 = 1$ and $\alpha_2 = 0$. With the same manner as Proof of Proposition 3.1. We can obtain Eq. (29). **Remark 1:** From Eq. (26), Eq. (28) and Eq. (29), because $\theta \geq \tau\sigma_0^2/\gamma_{\mathrm{th}}$, it is obvious that $\mathrm{OP}_{\mathrm{wo}} \leq \mathrm{OP}$.

3.3. Corollary 2

Throughput of the data link is computed exactly by

$$\mathrm{TP} = \frac{2R_{th}}{K}\left[\prod_{k=1}^{K} \frac{\lambda_{\mathrm{E},k}}{\lambda_{\mathrm{E},k} + \theta\lambda_{\mathrm{D},k}}\right]. \tag{30}$$

Proof: Substituting Eq. (26) into Eq. (25), we obtain Eq. (30).

3.4. Corollary 3

Without using NOMA, throughput of the data link is calculated by

$$\mathrm{TP}_{\mathrm{wo}} = \frac{R_{\mathrm{th}}}{K}\left[\prod_{k=1}^{K} \frac{\lambda_{\mathrm{E},k}\gamma_{\mathrm{th}}}{\lambda_{\mathrm{E},k}\gamma_{\mathrm{th}} + \tau\sigma_0^2\lambda_{\mathrm{D},k}}\right]. \tag{31}$$

Proof: Since the destination only receives one data from source, the system throughput is formulated by

$$\mathrm{TP}_{\mathrm{wo}} = \frac{R_{\mathrm{th}}}{K}\left(1 - \mathrm{OP}_{\mathrm{wo}}\right). \tag{32}$$

Substituting Eq. (30) into Eq. (32), we obtain Eq. (31).

3.5. Proposition 2

An exact closed-form expression of Intercept Probability at the eavesdropper is expressed as

$$\mathrm{IP} = 1 - \left[\frac{1}{2}\left(1 - \frac{1-\theta}{\sqrt{(1+\theta)^2 - 4\rho^2\theta}}\right)\right]^K. \tag{33}$$

Proof: From Eq. (20), Eq. (22) and Eq. (24), IP can be given by

$$\begin{aligned} \mathrm{IP} &= 1 - \Pr\left(\max_{k=1,2,\ldots,K}\left(C_{\mathrm{E},k}^{u_1}\right) \leq R_{th}\right) \\ &= 1 - \prod_{k=1}^{K}\Pr\left(\frac{\gamma_{\mathrm{E},k}}{\gamma_{\mathrm{E},k}^{e}} \leq \theta\right) \\ &= 1 - \prod_{k=1}^{K}\left[1 - \Pr\left(\frac{\gamma_{\mathrm{E},k}}{\gamma_{\mathrm{E},k}^{e}} > \theta\right)\right]. \end{aligned} \tag{34}$$

Using Eq. (7), [14] for $\Pr\left(\gamma_{\mathrm{E},k}/\gamma_{\mathrm{E},k}^{e} > \theta\right)$, we can obtain Eq. (33).

4. Simulation Results

In this section, we present Monte Carlo simulation results to verify the theoretical results and to compare the performances of the protocols discussed in the previous sections. In simulation environment, we consider a two-dimensional plane in which the co-ordinates of the nodes the relay N_k, $k = 0, 1, \ldots, K$, and the eavesdropper are $(k/K,\, 0)$ and $(0.5,\, 1)$, respectively. In all of the simulations, we fix the path-loss exponent (β), the target rate (R_{th}), the variance of noise (σ_0^2) by 3, 0.5 and 1, respectively.

In Fig. 2, we present the outage performance of the proposed protocol as a function of γ_{th}. In this figure, the correlation coefficient ρ is set by 0.99. It can be observed from Fig. 2 that the value OP decreases with the increasing of γ_{th}. Moreover, the outage performance is better with higher number of hops. It is also seen that OP of the proposed system without using NOMA is always lower than that of the NOMA-based system. It is worth noting that the theoretical and simulation results are in good agreement, which validates our theoretical analysis.

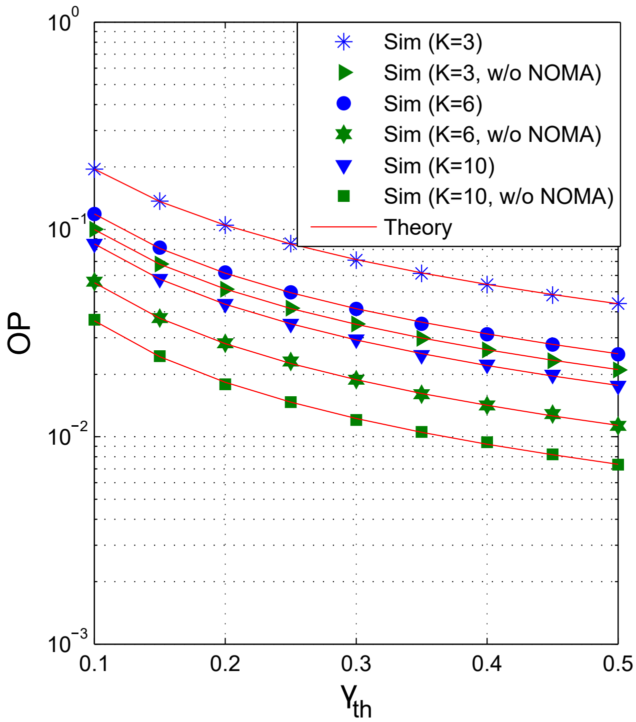

Fig. 2: Outage Probability (OP) as a function of γ_{th} when $\rho = 0.99$.

In Fig. 3, we show the ThroughPut (TP) of the $\text{N}_0 \rightarrow \text{N}_\text{K}$ as a function of γ_{th}. In this figure, the theoretical results are obtained from Corollary, Subsec. 3.3. and Corollary, Subsec. 3.4. , ρ is also set by 0.99. We can be observed that the value TP increases slowly with the increasing of γ_{th}. Besides, the throughput is higher when number of hops decreases and when the number of hops increases in which value TP seems to be saturated with the increasing of γ_{th}. It is also seen that TP of the proposed system without using NOMA is always lower than the NOMA-based system. This again demonstrates the effectiveness of the NOMA-based system as in our proposal.

Figure 4 presents Intercept Probability (IP) as a function of γ_{th} when $\rho = 0.99$. As illustrated in this figure, IP increases with higher value of γ_{th}. It is due to the fact that when γ_{th} is high, the transmit power of N_{k-1} is high, which increases the channel capacity of the eavesdropping links. As expected, this figure shows that when number of hops is lower, value IP is higher.

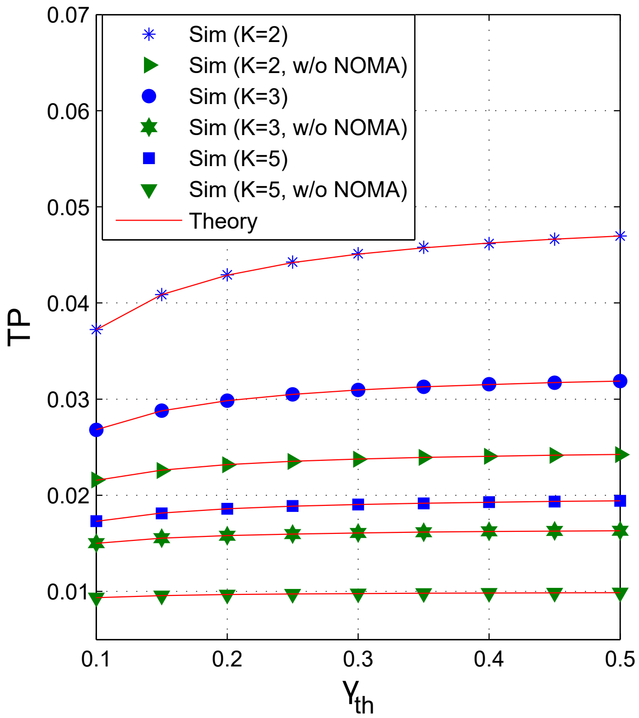

Fig. 3: Throughput of the $\text{N}_0 \rightarrow \text{N}_K$ as a function of γ_{th} when $\rho = 0.99$.

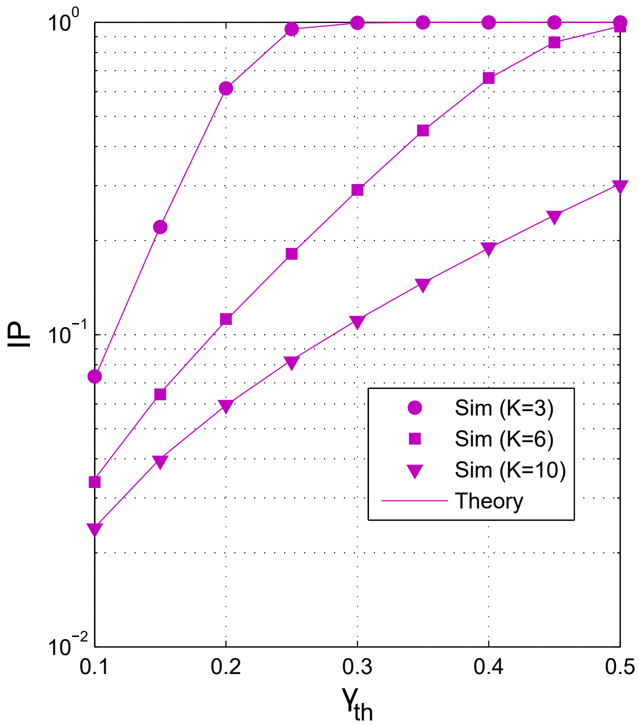

Fig. 4: Intercept Probability (IP) as a function of γ_{th} when $\rho = 0.99$.

Figure 5 shows value IP as a function of γ_{th} when $K = 8$. Similar to Fig. 4, intercept probability at the eavesdropper increases with higher value of γ_{th}. However, we can see that the value IP will be lower with the higher channel correlation factor ρ. Figure 4 and

Fig. 5 validates the simulation and theoretical results are in good agreement.

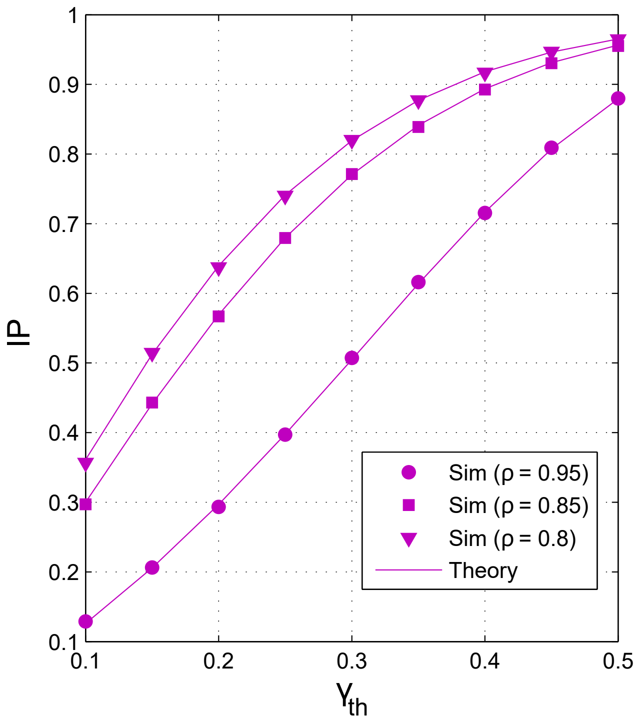

Fig. 5: Intercept Probability (IP) as a function of γ_{th} when $K = 8$.

5. Conclusion

In this paper, we proposed and analyzed system performances of a multi-hop relay protocol with presence of an active eavesdropper. By employing different combining techniques at relays and destination, the diversity order of the proposed protocols equals to the number of hops. In addition, to improve throughput for the multi-hop relay system, we proposed Non-Orthogonal Multiple Access (NOMA) technique with a simple power allocation. We derived the asymptotic closed-form expressions of the outage probability, intercept probability and throughput over Rayleigh fading channel. Finally, Monte Carlo simulations were presented to validate our derivations.

Acknowledgment

The research received a financial support from the SGS grant No. SP2017/174, VSB–Technical University of Ostrava, Czech Republic.

References

[1] DING, Z., Z. YANG, P. FAN and H. V. POOR. On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users. *IEEE Signal Processing Letters*. 2014, vol. 21, iss. 12, pp. 1501–1505. ISSN 1070-9908. DOI: 10.1109/LSP.2014.2343971.

[2] DING, Z., M. PENG and H. V. POOR. Cooperative non-orthogonal multiple access in 5G systems. *IEEE Communications Letters*. 2015, vol. 19, iss. 8, pp. 1462–1465. ISSN 1089-7798. DOI: 10.1109/LCOMM.2015.2441064.

[3] DING, Z., H. DAI and H. V. POOR. Relay Selection for Cooperative NOMA. *IEEE Wireless Communications Letters*. 2016, vol 5, iss. 4, pp. 426–419. ISSN 2162-2337. DOI: 10.1109/LWC.2016.2574709.

[4] LIANG, X., Y. WU, D. W. KWAN, Y. ZUO, S. JIN and H. ZHU. Outage Performance for Cooperative NOMA Transmission with an AF Relay. *IEEE Communications Letters*. 2017, vol. 99, iss. PP, pp. 1–1. ISSN 1089-7798. DOI: 10.1109/LCOMM.2017.2681661.

[5] KRIKIDIS, I., J. THOMPSON and S. MCLAUGHLIN. Relay selection for secure cooperative networks with jamming. *IEEE Transactions on Wireless Communications*. 2009, vol. 8, iss. 10, pp. 5003–5011. ISSN 1536-1276. DOI: 10.1109/TWC.2009.090323.

[6] ZOU, Y., X. WANG, W. SHEN and L. HANZO. Security versus reliability analysis of opportunistic relaying. *IEEE Transactions Vehicular Technology*. 2014, vol. 63, iss. 6, pp. 2653–2661. ISSN 0018-9545. DOI: 10.1109/TVT.2013.2292903.

[7] TRAN, T. D. and N. S. PHAM. Secrecy Performances of Multicast Underlay Cognitive Protocols with Partial Relay Selection and without Eavesdroppers Information. *KSII Transactions on Internet and Information Systems (TIIS)*. 2015, vol. 9, iss. 11, pp. 4623–4643. ISSN 1976-7277. DOI: 10.3837/tiis.2015.11.021.

[8] LIU, Y., L. WANG, T. T. DUY, M. ELKASHLAN and T. Q. DUONG. Relay Selection for Security Enhancement in Cognitive Relay Networks. *IEEE Wireless Communications Letters*. 2015, vol. 4, iss. 1, pp. 46–49. ISSN 2162-2337. DOI: 10.1109/LWC.2014.2365808.

[9] ZHANG, Y., H.-M. WANG, Q. YANG and Z. DING. Secrecy Sum Rate Maximization in Non-Orthogonal Multiple Access. *IEEE Communications Letters*. 2016,

vol. 20, iss. 5, pp. 930–933. ISSN 1089-7798. DOI: 10.1109/LCOMM.2016.2539162.

[10] DING, Z., Z. ZHAO, M. PENG and H. V. POOR. On the Spectral Efficiency and Security Enhancements of NOMA Assisted Multicast-Unicast Streaming. *IEEE Transactions on Communications*. 2017, vol. 65, iss. 7, pp. 3151–3163. ISSN 0090-6778. DOI: 10.1109/TCOMM.2017.2696527.

[11] MO, J., M. TAO and Y. LIU. Relay placement for physical layer security: A secure connection perspective. *IEEE Communications Letters*. 2012, vol. 16, iss. 6, pp. 878–881. ISSN 1089-7798. DOI: 10.1109/LCOMM.2012.042312.120582.

[12] PHU, T. T., T. H. DANG, T. D. TRAN and M. VOZNAK. Analysis of Probability of Non-zero Secrecy Capacity for Multi-hop Networks in Presence of Hardware Impairments over Nakagami-m Fading Channels. *Radio Engineering*. 2016, vol. 25, iss. 4, pp. 774–782. ISSN 1210-2512. DOI: 10.13164/re.2016.0774.

[13] TANG, X., M. ALOUINI and A. GOLDSMITH. Effect of channel estimation error on M-QAM BER performance in rayleigh fading. *IEEE Transactions on Communications*. 1999, vol. 47, iss. 12, pp. 1856–1864. ISSN 0090-6778. DOI: 10.1109/26.809706.

[14] VO, N. Q. B., T. Q. DUONG and C. TELLAMBURA. On the Performance of Cognitive Underlay Multihop Networks with Imperfect Channel State Information. *IEEE Transaction on Communications*. 2013, vol. 61, iss. 12, pp. 4864–4873. ISSN 0090-6778. DOI: 10.1109/TCOMM.2013.110413.130167.

[15] AHN, K. S., S.-W. CHOI and J.-M. AHN. Secrecy Performance of Maximum Ratio Diversity With Channel Estimation Error. *IEEE Signal Processing Letters*. 2015, vol. 22, iss. 11, pp. 2167–2171. ISSN 1070-9908. DOI: 10.1109/LSP.2015.2464716.

[16] NGUYEN, N. T., T. D. TRAN, T. P. TRAN and M. VOZNAK. Performance Evaluation of User Selection Protocols in Random Networks with Energy Harvesting and Hardware Impairments. *Advances in Electrical and Electronic Engineering*. 2016, vol. 14, no. 4, pp. 372–377. ISSN 1336-1376. DOI: 10.15598/aeee.v13i5.1407.

[17] TRAN, T. D. and H. Y. KONG. Performance Analysis of Incremental Amplify-and-Forward Relaying Protocols with Nth Best Partial Relay Selection under Interference Constraint. *Wireless Personal Communications (WPC)*. 2013, vol. 71, iss. 4, pp. 2741–2757. ISSN 0929-6212. DOI: 10.1007/s11277-012-0968-9.

About Authors

Tran Tin PHU was born in Khanh Hoa, Vietnam, in 1979. He received the Bachelor degree (2002) and Master degree (2008) from Ho Chi Minh City University of Science. Currently, he is a lecturer at the Faculty of Electronics Technology (FET), Industrial University of Ho Chi Minh City. Since 2015, he has been participating in Ph.D. program that had been collaborated between Technical University of Ostrava, Czech Republic and Ton Duc Thang University, Ho Chi Minh City. His major research interests are wireless communication in 5G, energy harvesting, performance of cognitive radio and physical layer security.

The Hung DANG was born in Ha Tinh, Vietnam, in 1983. He received the B.Sc. degree in Telecommunication Technological Command from TeleCommunications University (TCU), Nha Trang, Khanh Hoa, in 2006 and M.Sc. degree in Telecommunications Engineering from Posts and Telecommunications Institute of Technology (PTIT), Ho Chi Minh City, Vietnam, in 2014, respectively. In 2012, he joined the Department of Telecommunications Professional of Telecommunications (TCU), as a lecturer. Since 2016, he has been participating in Ph.D. program from Military Technical Academy (MTA), Hanoi, Vietnam. His major research interests are cooperative communications, cognitive radio, and physical layer security.

Trung Duy TRAN was born in Nha Trang city, Vietnam, in 1984. He received the B.Sc. degree in Electronics and Telecommunications Engineering from the French-Vietnamese training Program For Excellent Engineers (PFIEV), Ho Chi Minh City University of Technology, Vietnam in 2007. In 2013, he received the Ph.D. degree in electrical engineering from University of Ulsan, South Korea. In 2013, he joined the Department of Telecommunications, Posts and Telecommunications Institute of Technology (PTIT), as a lecturer. His major research interests are cooperative communications, cognitive radio, and physical layer security.

Miroslav VOZNAK was born in Czech Republic. He received the master degree in Electronics and Telecommunication Technology from the Technical University of Ostrava, Czech Republic, in 1995. In 2002, he received the Ph.D. degree in Telecommunication Engineering from Technical University of Ostrava, Czech Republic. In 2009, he appointed an Associate professor in Electronics and Communication Engineering from Technical University of Ostrava. He is member of the Scientific Board of Faculty of Electrical Engineering and Computer Science, VSB–Technical University of Ostrava, several editorial committees of journals, several scientific committees of conferences.