ANALYSES OF TRANSMIT ANTENNA SELECTION TO ENHANCE SECURITY PERFORMANCE IN COOPERATIVE RADIO COMMUNICATION NETWORKS UNDER WIRETAP CHANNEL

Le Tien Si, Pham Ngoc Thoa, Thieu Doan Quang Huy, Pham Ngoc Son*
Ho Chi Minh City University of Technology and Education, Vietnam

Received 27/03/2019, Peer reviewed 08/04/2019, Accepted for publication 23/04/2019.

ABSTRACT

In this paper, we investigate the physical layer security technique of a cooperative communication network with a source node having multiple transmitting antennas, in which these antennas provide the most optimal antenna to increase security performance to a destination node via a relay node in the presence of an eavesdropper node. Here, we propose and analyze a transmission antenna selection (TAS) solution to enhance security performance in the eavesdropping channel, the cooperative communication model between the source node including multiple transmitting antennas and a destination node through a relay node and the influence of the eavesdropping node. The secrecy performance is exactly evaluated based on the secrecy outage probability (SOP) of the main channel compared to the eavesdropping channel in the Rayleigh fading channels. Monte-Carlo simulation method is applied to verify simulations and theoretical analysis results in the proposed model. The results show that when using such multiple transmit antennas significantly enhanced the system's security performance.

Keywords: *Physical layer security; transmit antenna selection (TAS); security capacity; secrecy outage probability; Rayleigh.*

1. INTRODUCTION

Cooperative communication is an effective method to improve network performance in a radio transmission environment between two nodes via an intermediate node, called a relay node [1, 2]. The purpose of this method is aimed to improve channel capacity and increase diversity. In this model, we have two protocols for handling signals at the relay node [3, 4]. Firstly, the relay node will decode the received signal from the source node and forward it to the destination node. This is the decode-and-forward (DF) protocol. Note that the decoded signal at the relay node may not be correct. Therefore, if a signal is decoded incorrectly at the relay node, it is concerned to the destination node, the decoding at the destination node is meaningless [5].

Another one, for the amplify-and-forward (AF) protocol, the relay node will amplify the received signal and forward it to the destination node. Each relay node in this method receives the jammed version of the signal transmitted by its source node, then amplifies the received signal and forwards it to the destination node. The relay node after amplifying and transmitting this noise version to the destination node. The destination node will combine the information sent by the relay node and it will make the final decision on the transmitted signal [2].

In general, in these two protocols, the amplify-and-forward (AF) protocol will avoid complex encoding but it is susceptible to interference because when amplifying it can amplify both signals and noise. In cooperative communication, selecting the relay node has many methods such as selecting the local relay node and selecting the opportunity relay node. In particular, the local relay node selecting technique based on the signal-to-noise ratio (SNR) on the

transmission link from the source node to the relay node or from the relay node to the destination node. Meanwhile, the technique of selecting an opportunity relay node will consider the selection based on balancing the SNR ratio between the two transmissions from the relay node to the source and destination node [6-8].

Due to the transmitting characterization of radio networks, the transmitted signals can be overheard by an eavesdropping device so our security and privacy are the biggest concerns for today's wireless technologies.

Therefore, physical layer security technology had been studied and implemented to increase the security of the obtained data signal at the destination, node when there is influence of the eavesdropping node. When the channel quality is transmitted between the source and the destination node is greater than the channel quality between the source and the eavesdropper node, the destination node will receive a security signal and the eavesdropping node may receive noise information from the source [1, 5, 9]. The secrecy capacity (SC) is now determined based on the total security data on the source node compared to the destination. Therefore, when increasing this ratio will increase the security capacity of the transmission channel [4]. In this paper, we propose a cooperative communication model between the source and the destination node via a relay node and the influence of eavesdropping node.

The system performance is evaluated based on the secrecy outage probability between the source node and the destination node. In the above proposed protocols, we consider based on the best SNR ratio from the relay node to the destination node. Besides, the consideration is based on the probability of signals decoding successfully from the source node to the destination node under the influence of the eavesdropping node. We select a best transmit antenna b among the M transmit antennas of the source node S, a relay node R, a destination node D and an eavesdropping node E to enhance the security performance in the cooperative communication network [10] through physical layer security technology [4, 11-13]. The results show that when using multiple transmit antennas enhances the system's security performance significantly [9, 14-15]. In addition, a multiple radio frequency antenna transmitter helps to reduce costs, complexity, size and power consumption [16].

The paper is organized as follows. Section 2 describes a system model of a two-stage relaying mode over Rayleigh fading channels. Exact secrecy outage probability analyses are performed in Section 3. Section 4 presents the simulation results and respective evaluations. Conclusions are summarized in Section 5.

2. SYSTEM MODEL

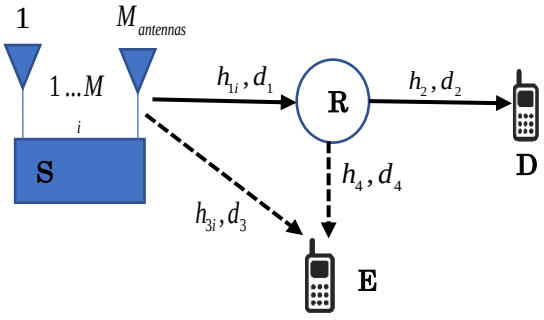

***Fig.1** System model*

Figure 1 shows the proposaled system model. The system consisting of the source node S transmits signal information to the destination node D with M -antennas via the relay node R. We assume that there is no straight line between the source node and the destination node and the eavesdropper node E can get transmitted information from the source node to the destination node. We propose that there is a best transmit selected antenna b in M -transmit antennas with a capacity of enhancing the best security performance of the system and assuming that the relay node R, the destination node D, the eavesdropping node E has a single antenna, transmit power is P, noise power N_0 .

In Figure 1, (h_{1i}, d_1), (h_2, d_2), (h_{3i}, d_3), (h_4, d_4) denote the Rayleigh fading channel coefficients and the normalized distances between the transmission links S-R, R-D, S-E and R-E, respectively. Therefore, the Rayleigh channel gains $g_{1i} = |h_{1i}|^2$, $g_2 = |h_2|^2$, $g_{3i} = |h_{3i}|^2$, and $g_4 = |h_4|^2$, are random variables and belong exponential distributions [4]. Probability density function (PDF) and cumulative distribution function (CDF) of random variable g_z are presented as, respectively, $f_{g_z}(t) = \lambda_z e^{-\lambda_z t}$ and $F_{g_z}(t) = 1 - e^{-\lambda_z t}$, where $z \in \{1i, 2, 3i, 4\}$, $\lambda_z = d_z^{-\beta}$, and β is path loss coefficient [4]. We note that $\lambda_{1i} = \lambda_1 = d_1^{-\beta}$ and $\lambda_{3i} = \lambda_3 = d_3^{-\beta}$.

The operation principle of this model is divided into two times slots. In the first time slot, the source node S transmits information to the relay node R and the eavesdropper node E whereas the relay node R decodes and forwards this information to the destination node D and the eavesdropping node E in the second time slot.

According to the proposed system model, the signal transmission from S to R, R to D is a random signal corresponding to the variables h_{1i} and h_2. In this case, we assume that all radio communication channels are flat fading channels.

In the first time slot, the source node S transmits a radio signal x and the relay node R will receive that signal, P is the transmit power at the node S; n_R is the noise and y_R is the received signal at R. Then the signal received at R are represented from the antenna i as following formula [5]:

$$y_R^i = \sqrt{P} x h_{1i} + n_R \quad (1)$$

The Signal-to-Noise Ratio (SNR) at the relay R to safely decode the signal x_s transmitted by the antenna i is obtained as:

$$SNR_{SR}^i = \frac{P}{N_0} |h_{1i}|^2 = \gamma g_{1i} \quad (2)$$

where $\gamma = P/N_0$

Similarly, in the second time slot, the relay R will decode the received signal and forward it to the destination D. The noise and the received signal at the destination D is denoted respectively as n_D, y_D and are presented as in the formula (3):

$$y_D = \sqrt{P} x h_2 + n_D \quad (3)$$

The SNR at the destination node D to safely receive the signal x_R is obtained as:

$$SNR_{RD} = \gamma g_2 \quad (4)$$

At node E, there are signals from two sources of two different time slots. The one is received from the antenna i of the source S and the other is from the relay R. The received signal at E from the antenna i of the source S can be deduced as:

$$y_{E_{SE}}^i = \sqrt{P} x h_{3i} + n_E \quad (5)$$

The received signal at the eavesdropper E from the relay R can be deduced as:

$$y_{E_{RE}} = \sqrt{P} x h_4 + n_E \quad (6)$$

Similarly, the SNRs at the eavesdropper E from the antenna i of the source S and the node R are obtained, respectively, as

$$SNR_{SE}^i = \frac{P}{N_0} |h_{3i}|^2 = \gamma g_{3i} \quad (7)$$

$$SNR_{RE} = \frac{P}{N_0} |h_4|^2 = \gamma g_4 \quad (8)$$

3. PERFORMANCE ANALYSIS

In this section, we analyze the secrecy outage probability of the proposed system. We assume that a node decodes the received signals safely and successfully if the achievable security capacity (SC) is greater than or equal the achieved threshold security rate R_T as in [5, 15]. The achievable rates from transmitting at the antenna i of links S-R,

R-D, S-E and R-E are denoted respectively as R_{SR}^i, R_{RD}, R_{SE}^i, R_{RE} and are presented as in the formulas (9).

In the first time slot, we have R_{SR}^i, R_{SE}^i and we also have R_{RD}, R_{RE} in the second time slot, respectively as:

$$R_X^i = \frac{1}{2}\log_2\left(1+SNR_X^i\right) \quad (9)$$

where a coefficient $1/2$ is due to the system operating in two times slots, $X \in \{SR, SE, RD, RE\}$. The superscript i in (9) is deleted when $X \in \{RD, RE\}$

In order to enhance the security of the system or to reduce the eavesdropping capacity, the best antenna from the source node S to the relay R is proposed as

$$b = \arg\max_{i=1,2,...M} g_{1i} \text{ or } g_{1b} = \max_{i=1,2,...M} g_{1i} \quad (10)$$

In (10), the CDF and PDF of g_{1b} are obtained, respectively, as

$$\begin{aligned} F_{g_{1b}}(x) &= \Pr[g_{1b} < x] = \Pr\left[\max_{i=1,2,...M} g_{1i} < x\right] \\ &= \prod_{i=1}^{M} \Pr[g_{1i} < x] = \prod_{i=1}^{M} F_{g_{1i}}(x) \\ &= \left(1-e^{-\lambda_1 x}\right)^M = \sum_{p=0}^{M} (-1)^p \times C_M^p \times e^{-\lambda_1 px} \end{aligned} \quad (11)$$

$$\begin{aligned} f_{g_{1b}}(x) &= \frac{\partial F_{g_{1b}}(x)}{\partial x} = \frac{\partial\left(1-e^{-\lambda_1 x}\right)^M}{\partial x} \\ &= \lambda_1 \sum_{p=0}^{M} (-1)^{p+1} \times p \times C_M^p \times e^{-\lambda_1 px} \end{aligned} \quad (12)$$

where $C_N^n = N!/n!(N-n)!$.

Then, the achievable security capacity SC_{SR} and SC_{RD} of the transmissions from S to R, and R to D are presented by, respectively as

$$SC_{SR} = \max(R_{SR}^b - R_{SE}^b, 0) \quad (13)$$

$$SC_{RD} = \max(R_{RD} - R_{RE}, 0) \quad (14)$$

The secrecy outage probability of the source node S occurs in the following two cases: the first case, secrecy error from the best antenna b of the source node S to the relay node R; and the second case, secrecy error from the relay node R to the destination node D when the relay node R has successfully and safely decoded the signal of the source S in the first time slot. Therefore, the secrecy outage probability P^{sop} is represented by a mathematical formula as follows:

$$\begin{aligned} P^{SOP} &= \Pr[\min(SC_{SR}, SC_{RD}) < R_T] \\ &= \Pr[\mathrm{SC}_{SR} < R_T] + \Pr[\mathrm{SC}_{SR} \ge R_T, \mathrm{SC}_{RD} < R_T] \end{aligned} \quad (15)$$

Since the probability of the achievable security capacity (SC) from the best antenna b of the source node S to the relay node R and the probability of the achievable security capacity from the relay node R to the second destination node D is two independent events, so the secrecy outage probability is calculated as follows from the mathematical formula

$$\begin{aligned} P^{SOP} &= \Pr[\mathrm{SC}_{SR} < R_T] + \Pr[\mathrm{SC}_{SR} \ge R_T] \times \Pr[\mathrm{SC}_{RD} < R_T] \\ &= \Pr[\mathrm{SC}_{SR} < R_T] + \{(1-\Pr[\mathrm{SC}_{SR} < R_T])\} \times \Pr[\mathrm{SC}_{RD} < R_T] \end{aligned} \quad (16)$$

where:

$$\Pr[SC_{SR} < R_T] = \Pr\left[R_{SR}^b - R_{SE}^b < R_T\right] \quad (17)$$

$$\Pr[SC_{RD} < R_T] = \Pr[R_{RD} - R_{RE} < R_T] \quad (18)$$

Substituting R_{SR}^b and R_{SE}^b in (9) into (17), we have an expression as

$$\begin{aligned} \Pr[\mathrm{SC}_{SR} < R_T] &= \Pr\left[R_{SR}^b - R_{SE}^b < R_T\right] \\ &= \Pr\left[\frac{1}{2}\log_2\left(\frac{1+SNR_{SR}^b}{1+SNR_{SE}^b}\right) < R_T\right] \\ &= \Pr\left[\frac{1+SNR_{SR}^b}{1+SNR_{SE}^b} < 2^{2R_T}\right] \end{aligned} \quad (19)$$

By using the formulas SNR_{SR}^b and SNR_{SE}^b in (2) and (7), respectively, the probability $\Pr[\mathrm{SC}_{SR} < R_T]$ is expressed as

$$\Pr[\mathrm{SC}_{SR} < R_T] = \Pr\left[\frac{1+\gamma g_{1b}}{1+\gamma g_{3b}} < 2^{2R_T}\right]$$
$$= \Pr\left[1+\gamma g_{1b} < 2^{2R_T}\left(1+\gamma g_{3b}\right)\right] \quad (20)$$
$$= \Pr\left[g_{1b} < \underbrace{\frac{2^{2R_T}-1}{\gamma}}_{a} + g_{3b}\right] = \int_0^{+\infty} f_{g_{3b}}(x) \times F_{g_{1b}}(a+x)dx$$

Substituting the PDF and the CDF of the random variables g_{3b} and g_{1b}, respectively, into the formula (20), we have a result as

$$\Pr\left[SC_{SR} < R_T\right] = \int_0^{+\infty} \lambda_3 e^{-\lambda_3 x} \times \sum_{p=0}^{M} (-1)^p C_M^p \times e^{-\lambda_1 p(a+x)} dx$$
$$= \lambda_3 \sum_{p=0}^{M} (-1)^p C_M^p \times e^{-\lambda_1 pa} \times \int_0^{+\infty} e^{-x(\lambda_1 p+\lambda_3)} dx \quad (21)$$
$$= \lambda_3 \sum_{p=0}^{M} C_M^p \frac{(-1)^p e^{-\lambda_1 pa}}{\lambda_3 + p\lambda_1}$$

Similarly, the probability $\Pr[\mathrm{SC}_{RD} < R_T]$ is solved as

$$\Pr\left[SC_{RD} < R_T\right] = \Pr\left[R_{RD} - R_{RE} < R_T\right] = 1 - \frac{\lambda_4 \times e^{-a\lambda_2}}{\lambda_4 + p\lambda_2} \quad (22)$$

Substituting (21) and (22) into (16), the secrecy outage probability P^{SOP} is obtained in a closed-form expression as (23)

$$P^{SOP} = 1 - \frac{\lambda_4 \times e^{-a\lambda_2}}{\lambda_4 + p\lambda_2} + \frac{\lambda_3 \times \lambda_4 \times e^{-a\lambda_2}}{\lambda_4 + p\lambda_2} \sum_{P=0}^{M} C_M^p \frac{(-1)^p e^{-\lambda_1 pa}}{\lambda_3 + p\lambda_1} \quad (23)$$

4. SIMULATION RESULTS

In this section, we perform Monte-Carlo simulations to verify the analytical results presented in Section III. We present representative numerical results to demonstrate the achievable security capability improvement of the proposed TAS scheme. The theory results are based on the analyzed mathematical formulas and using Monte-Carlo simulation method to verify them. The simulation environment is a two-dimensional coordinate system. The source node S is set at the origin $(0,0)$, the relay node R is coordinated at (x_R, y_R), the destination node D is coordinated at $(x_D, y_D) = (1,0)$ and the eavesdropping node E is at (x_E, y_E).

Figure 2 presents the secrecy outage probabilities versus the number of transmit antennas M, $M = \{1,...,10\}$ when the threshold rate is to constant as $R_T = 0.5$ (bit/s/Hz), $x_R = 0.5$, $y_R = 0$, $x_E = 0.25$, $y_R = -1$. From Fig. 2, we can see the effect of the number of TAS to the secrecy outage probability plotted according to the change of TAS from $M = 1$ to $M = 10$. When we increase the number of transmit antennas from $M = 1$ to $M = 10$, the secrecy outage probability decreases. This proves to transmit antenna selection make secrecy performance better. In addition, the simulation results match with the analysis results. This proves the correctness in theoretical analysis results.

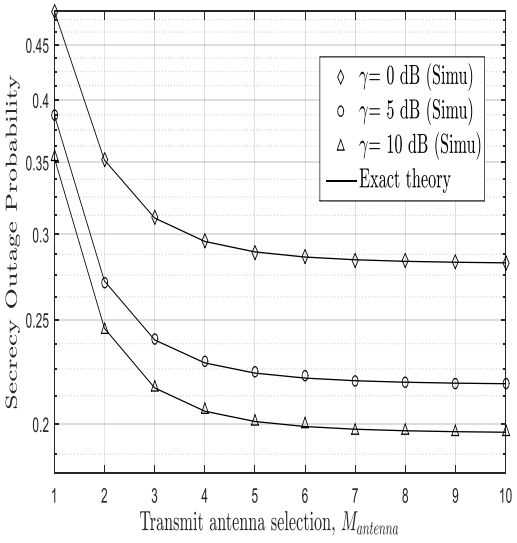

***Fig. 2** Secrecy outage probability versus the number of TAS when $R_T = 0.5$ bits/s/Hz, $x_R = 0.5$, $y_R = 0$, $x_E = 0.25$ and $y_E = 0$*
(Markers denote simulated results).

Figure 3 presents the secrecy outage probability versus γ when the threshold rate R is to constant as $R_T = 0.5$ (bit/s/Hz),

$x_R = 0.5$, $y_R = 0$, $x_E = 0.25$ and $y_E = -1$. From Fig.3 when γ increases, the secrecy outage probability decreases. That is because when we increase the transmit power, the capacity of both the expected channel and the eavesdropping channel also increase. It's more difficult to eavesdrop by node E. In addition, it is also seen from Fig.3 that the performance of the system shows the slightly worse performance when TAS of M is smaller.

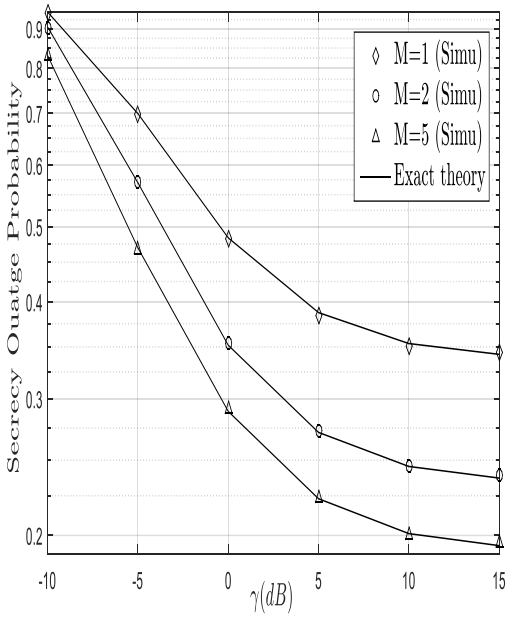

Fig. 3 *Secrecy outage probability versus* γ *when the the threshold rate* $R_T = 0.5\,bit/s/Hz$, $x_R = 0.5$, $y_R = 0$, $x_E = 0.25$ *and* $y_E = -1$ *(Markers denote simulated results).*

Figure 4 presents the secrecy outage probability versus the coordinate of the relay node R on the x -axis (x_R) when $M = \{3,5\}$; the relay node is moved on x -axis from $x_R = 0.1$ to $x_R = 0.9$ whereas the coordinate of the relay node R on y -axis (y_R) is fixed at $y_R = 0$. The coordinate of the eavesdropping node E is $x_E = 0.5$, $y_E = -1$; $\gamma = 5\,dB$ and the threshold rate R is to constant as $R_T = 0.5$ (bit/s/Hz). From Fig. 4, we can observe the secrecy outage probability varying strongly according to the different locations of the node R. The secrecy outage probability achieves the best performance at about $x_R = 0.65$.

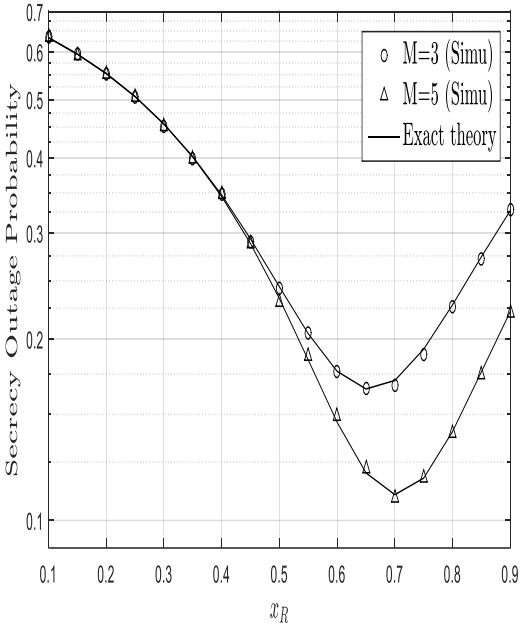

Fig. 4 *Secrecy outage probability as a function of* x_R *when* $M = \{3,5\}$; $x_R = 0.1$ *to* $x_R = 0.9$ *whereas the coordinate of the relay node R on* y*-axis* (y_R) *is fixed at* $y_R = 0$, *the threshold rate* $R_T = 0.5\,bit/s/Hz$, $x_E = 0.25$, $y_E = -1$ *(Markers denote simulated results).*

Figure 5 presents the secrecy outage probability versus the coordinate of the node E on the y –axis (y_E) when $M = \{1,3\}$; the coordinate x_E is set to a constant as $x_E = 0.65$ whereas y_E is moved on y -axis from $y_E = -3$ to $y_E = 3$. The coordinate of the relay node R is $x_R = 0.5$, $y_R = 0$; $\gamma = 5\,dB$ and the threshold rate R is to constant as $R_T = 0.5$(bit/s/Hz). As shown in Fig.5, the secrecy outage probabilities decrease when the eavesdropping node moves farther the source and relay node.

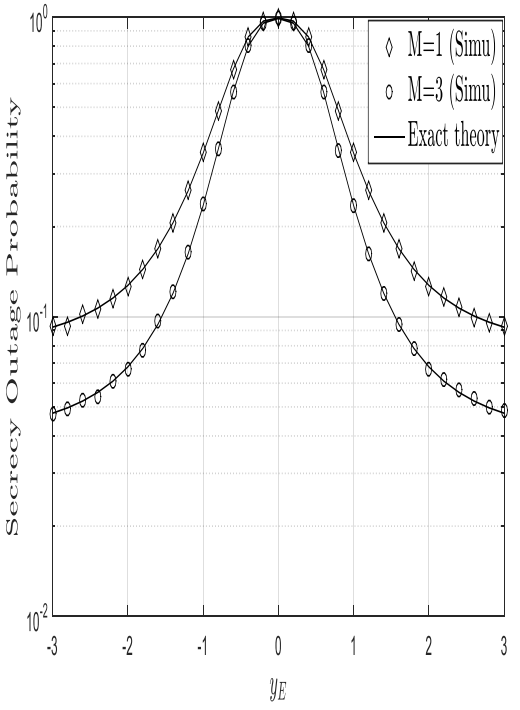

Fig. 5 *Secrecy outage probability as a function of y_E when $M = \{1,3\}$; whereas the coordinate of the node E on x-axis (x_E) is fixed at $x_E = 0.65$, the threshold rate $R_T = 0.5 bit/s/Hz$, $x_R = 0.5$, $y_R = 0$ (Markers denote simulated results).*

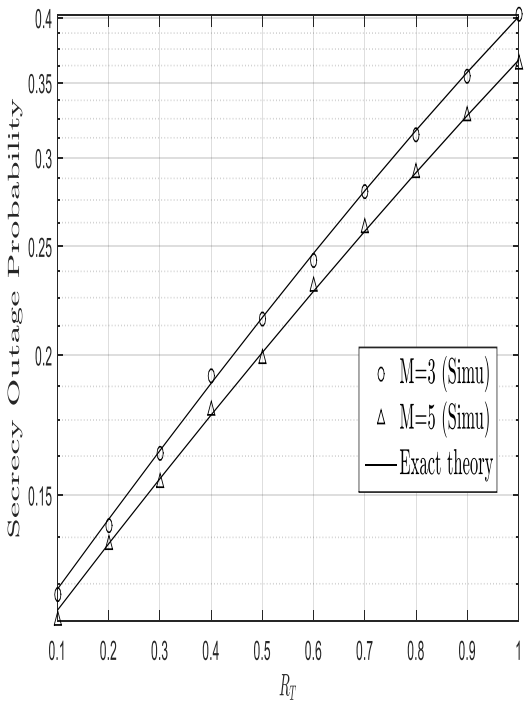

Fig. 6 *Secrecy outage probability versus the threshold rate R_T when when $\gamma = 10 dB$; the coordinate of the R node is $x_R = 0.5$, $y_R = 0$; the coordinate of the E node is $x_E = 0.25$, $y_E = -1$ and the number of TAS is to constant as $M = \{3,5\}$ (Markers denote simulated results).*

Figure 6 shows the secrecy outage probability versus the threshold rate R_T when $\gamma = 10 dB$; the coordinate of the node R is $x_R = 0.5$, $y_R = 0$; the coordinate of the E node is $x_E = 0.25$, $y_E = -1$ and the number of TAS is to constant as $M = \{3,5\}$. From Fig.6, the secrecy outage probability increases when R_T increases. This is because, with an increasing R_T, a higher transmit power is used at the source node S. Meanwhile, as the transmit power of node S increases, more interference is encountered at the eavesdropper in tapping the S-R and R-D transmissions and thus the secrecy performance of the proposaled system model is enhanced.

5. CONCLUSION

In this paper, we investigated and analyzed the impacts of TAS on secrecy performance of a practical wireless dual-hop relay system in the presence of an eavesdropper. In this scheme, there are two hops the same Rayleigh fading, the first hop from the source to the relay and the second hop from the relay to the destination. The relay helped to forward data signals from the source to the destination based on an achievable secrecy capability. The secrecy performance was exactly evaluated by the secrecy outage probability of the achievable secrecy capability. We derived the exact and asymptotic closed-form expressions for the secrecy outage probability and verified them

by the Monte Carlo simulations. The results have shown that the proposed TAS scheme is adopted, increasing the number of the antennas at the source node S or base station can significantly improve the SOP of the system model. Additionally, the proposed TAS scheme takes more advantages as the number of antennas at the source node increases. However, the system performance of the model is declined when the SNR increases. We also pointed out that the secrecy performance of the proposed scheme becomes more vulnerable when the eavesdropper located closer to the source node. Finally, the theoretical results match with the simulation results.

ACKNOWLEDGEMENTS

This research is funded by The Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2019.13.

REFERENCES

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679-695, April 2018.

[2] X. Tao, X. Xu and Q. Cui, "An overview of cooperative communications," *IEEE Communications Magazine*, vol. 50, no. 6, pp. 65-71, June 2012.

[3] P. N. Son and H. Y. Kong, "An approach of Relay ordering to improve OFDM-based cooperation," *IEICE Transactions on Communications*, vol. E98-B, no. 5, pp. 870-877, May 2015.

[4] Weifeng Su, Ahmed K. sadek, K. J. Ray Liu, "Cooperative Communication Protocols in wireless networks: Performance Analys and Optimum Power Allocation", *Wireless Personal Communications*, vo. 44, no. 2, pp. 181-217, Jan. 2008.

[5] P. N. Son and H. Y. Kong, "Cooperative Communication with energy harvesting relays under Physical Layer Security," *IET Communications*, vol. 9, no. 17, pp. 2131-2139, Nov. 2015.

[6] M. H. D. Khan and M. S. Elmusrati, "Performance analysis of power allocation and relay location in a cooperative relay network," *2015 17th International Conference on Advanced Communication Technology (ICACT)*, Seoul, South Korea, 2015, pp. 444-449.

[7] P. Li, S. Guo, W. Zhuang and B. Ye, "On Efficient Resource Allocation for Cognitive and Cooperative Communications," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 2, pp. 264-273, February 2014.

[8] P. S. Bithas, A. A. Rontogiannis and G. K. Karagiannidis, "An Improved Threshold-Based Channel Selection Scheme for Wireless Communication Systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1531-1546, Feb. 2016.

[9] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober and I. B. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144-154, January 2013.

[10] M. Yang, D. Guo, Y. Huang, T. Q. Duong and B. Zhang, "Physical Layer Security With Threshold-Based Multiuser Scheduling in Multi-Antenna Wireless Networks," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 5189-5202, Dec. 2016.

[11] H. Lei, J. Zhang, K-H Park, P. Xu, Z. Zhang, G. Pan, M-S Alouini, "Secrecy Outage of Max–Min TAS Scheme in MIMO-NOMA Systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 6981-6990, Aug. 2018.

[12] K. Shim, H. Oh, T. N. Do and B. An, "A Physical Layer Security-Based Transmit Antenna Selection Scheme for NOMA Systems," *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, Prague, Czech Republic, 2018, pp. 597-602.
[13] S. Asaad, A. Bereyhi, A. M. Rabiei, R. R. Müller and R. F. Schaefer, "Optimal Transmit Antenna Selection for Massive MIMO Wiretap Channels," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 817-828, April 2018.
[14] F. A. Khan, K. Tourki, M. Alouini and K. A. Qaraqe, "Outage and SER performance of spectrum sharing system with TAS/MRC," *2013 IEEE International Conference on Communications Workshops (ICC)*, Budapest, Hungary, 2013, pp. 381-385.
[15] H. Alves, R. D. Souza, M. Debbah and M. Bennis, "Performance of Transmit Antenna Selection Physical Layer Security Schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372-375, June 2012.
[16] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875-1888, March 2010.

Corresponding author:
Pham Ngoc Son
Ho Chi Minh City University of Technology and Education
Email: sonpndtvt@hcmute.edu.vn