IMPROVING SECRECY COOPERATION TRANSMISSIONS USING POWER ALLOCATION STRATEGY

CẢI THIỆN TRUYỀN HỢP TÁC AN TOÀN SỬ DỤNG CHIẾN LƯỢC CHỈ ĐỊNH CÔNG SUẤT

Pham Ngoc Son
Ho Chi Minh City university of Technology and Education

Received 30/5/2016, Peer reviewed 10/10/2016, Accepted for publication 28/10/2016

ABSTRACT

In wireless communication, the secrecy of data transmission is an important objective, and especially when eavesdropper nodes are near source nodes. In this case, eavesdropper nodes can wiretap easily any information from the source nodes. In this paper, an approach method to improve secrecy cooperation transmissions using combined signals is investigated in which data and jamming signals are combined at a source node based on power allocation strategy. The secrecy system performances are evaluated using asymptotic secrecy outage probabilities of end-to-end achievable secrecy rates over flat and block Rayleigh fading channels. Monte-Carlo simulation results are presented to verify the theoretical analyses. The main contributions of the proposed protocol are as follows. First, the jamming signals at the source node are secret against a relay and an eavesdropper node. Second, an amplify-and-forward method is applied so the relay cannot know the secrecy signal along with the jamming signals. Third, by transmitting the jamming signals from the source node, the proposed protocol prevents wiretapping by nearby eavesdropper. Finally, the asymptotic analysis is valid with the simulation result evaluating the secrecy performance of the proposed protocol.

Keywords: *Physical layer security; cooperative communication; jamming; power allocation strategy; amplify-and-forward.*

TÓM TẮT

Trong truyền thông không dây, việc bảo mật truyền dữ liệu là mục tiêu quan trọng, và đặc biệt khi các nút nghe lén ở gần các nút nguồn. Trong trường hợp này, các nút nghe lén có thể dễ dàng lấy trộm bất kỳ thông tin từ các nút nguồn. Trong bài báo này, một phương pháp tiếp cận để cải thiện việc truyền hợp tác an toàn sử dụng chiến lược chỉ định công suất. Hiệu năng hệ thống an toàn được đáng giá dùng xác xuất dừng an toàn gần đúng của tốc độ an toàn có thể đạt được từ nguồn đến đích trong môi trường fading Rayleigh phẳng và theo khối. Các kết quả mô phỏng Monte-Carlo được trình bày để kiểm tra các phân tích lý thuyết. Các đóng góp chính của giao thức được đề xuất như sau. Đầu tiên, các tín hiệu nhiễu nhân tạo ở nút nguồn không được biết ở nút chuyển tiếp và nút nghe lén. Thứ hai, phương pháp khuếch đại và chuyển tiếp được sử dụng, vì thế, nút chuyển tiếp không biết được tín hiệu an toàn và nhiễu nhân tạo của nút nguồn. Thứ ba, bằng cách phát tín hiệu nhiễu nhân tạo của nút nguồn, giao thức được đề xuất ngăn chặn việc nghe trộm của nút nghe lén ở gần nguồn. Cuối cùng, phân tích gần đúng có giá trị khi so sánh với kết quả mô phỏng trong đánh giá hiệu năng của giao thức được đề xuất.

Từ khóa: *Bảo mật lớp vật lý; truyền thông hợp tác; nhiễu nhân tạo; chiến lược chỉ định công suất; khuếch đại chuyển tiếp.*

1. INTRODUCTION

Because of broadcasting of signals in the wireless environment, secrecy transmission is an important objective [1-3]. In the secrecy transmission, eavesdroppers illegally try to wiretap the transmitted data of other communication links. In [1], A.D. Wyner discovered that if the quality of the main channel is higher than that of the wiretap channel then the transmit signal is secure. Secrecy performance is characterized with an achievable secrecy rate (ASR) metric that expresses the difference between the achievable data rate of the main channel and that of the wiretap channel [2]. To overcome the fading environment as well as to enhance secrecy performance, cooperative communication has been considered in physical layer security [3-5]. Relays in a decode-and-forward scheme can decode and retransmit received signals from source nodes or can amplify received signals plus noise and forward them to destination nodes in an amplify-and-forward scheme [6-7]. Optimal relay selections have been considered to maximize the end-to-end secrecy paths [4], and exploitations of jamming signals has been studied in which the source nodes lease friendly wireless nodes to operate as jammers [3-4]. Jammers create artificial interference to reduce the quality of the eavesdropping channel, and thus the secrecy performance is enhanced. The jamming signals can be known at the source, destination and relay nodes; hence, the desired communications cannot be affected by the interference signals. However, in above solutions, the physical layer security has serious disadvantages when eavesdropper nodes are near the source nodes. In this case, the eavesdropper nodes can easily wiretap any information from the source nodes, and the selected best relay uses the received data for individual purposes.

In this paper, the author propose a method to improve the secrecy cooperation transmissions using power allocation strategy in which a source node combines its secrecy signal with its jamming signal using the power allocation strategy as in [8-9] before broadcasting to relay, destination and even eavesdropper nodes. In addition, in the proposed protocol, the maximal ratio combining (MRC) method is applied at the destination and the eavesdropper to increase the quality of their desired signals. The secrecy system performance of the proposed protocol is evaluated using the secrecy outage probability of the end-to-end ASR. The theoretical expression of the proposed protocol is given in the asymptotic form of the secrecy outage probability. The main contributions of the proposed protocol are as follows. First, the jamming signals at the source node are secret against the relay and eavesdropper nodes. Second, I apply an amplify-and-forward scheme so the relay cannot know both the secrecy signal and the jamming signals. Third, the eavesdropper node has difficulty wire tapping the secrecy signal when it is near the source node because of the direct jamming signal from the source node. Fourth, the relay will compensate for the loss of power used for transmitting the jamming signals expressed in the power allocation strategy; hence, the secrecy performance of the proposed protocol will improve on existing methods. Finally, the asymptotic expression of the proposed protocol is worthy.

This paper is organized as follows: Section 2 describes the jamming amplify-and-forward scheme; Section 3 analyzes and calculates the secrecy outage probability of the proposed protocol; Section 4 presents and discusses the simulation results; and Section 5 summarizes my conclusions.

2. SYSTEM MODEL

Fig.1 presents a jamming amplify-and-forward scheme under physical layer security, including a source node S, a destination node D, a relay node R and an eavesdropper node E. In Figure 1, the source node S transmits a secrecy signal to the destination node D through the intermediate relay node R. I propose some assumptions as following: 1) the eavesdropper node E tries to overhear the secrecy signal of a source-destination link; 2) each node has a single antenna and operates in half-duplex mode; 3) all nodes suffer the zero-mean additive white Gaussian noise (AWGN) with the same variance N_0; 4) the nodes S and D can accurately estimate the location of eavesdropper node E (This assumption is based on the practice that eavesdropper E is an active node, as in [2], and usually replies to the set-up messages of the S and D nodes to be served in the future, as described in [10]).

In Figure 1, (h_0, d_0), (h_1, d_1), (h_2, d_2), (h_3, d_3), and (h_4, d_4) denote the Rayleigh fading channel coefficients and the distances of the links *S-D*, *S-R*, *R-D*, *S-E*and *R-E*, respectively. I assume that all channels suffer flat-block Rayleigh fading in which the channel coefficients are constant in a packet interval and change from packet to packet. Hence, the channel gains $\omega_i = |h_i|^2$ have exponential distributions with parameters $\lambda_i = d_i^{\beta}$, respectively, where β is a path-loss exponent, $i \in \{0,1,2,3,4\}$.

In this paper, a jamming amplify-and-forward scheme under physical layer security is proposed, in which the source node S owns a secrecy signal x and a jamming signal j. The secret transmission of the secrecy signal x is the main target; the transmission of the jamming signal j supports the main target by creating artificial interference to decrease the quality of the channel to eavesdropper node E. The seed for generating the jamming signal j is not shared with the relay and eavesdropper nodes and can be changed frequently. The destination can know the jamming signal j based on the secrecy parameters at the higher layers.

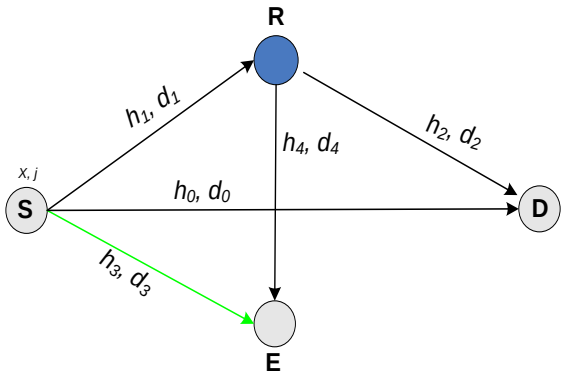

***Fig.1** Jamming amplify-and-forward scheme.*

In my proposed protocol, the eavesdropper node E can be near the source node S, thus the source node S transmits a combination signal that includes the secrecy signal x and the jamming signal j in the first timeslot. In this case, the relay node R only amplifies the received signals from the source S; as a result, the relay R cannot distinguish the secrecy signal x from the jamming signal j. The combined signal of the source node S can be obtained using the power allocation strategy [8-9] as

$$x_s = \sqrt{\alpha P}\,x + \sqrt{(1-\alpha)P}\,j \qquad (1)$$

where $E\{x\} = E\{j\} = 0$ and $E\{|x|^2\} = E\{|j|^2\} = 1$.

The operation principle of the proposed protocol is based on a time-division channel model and split into two timeslots as follows.

1) In the first timeslot, the source node *S* broadcasts the combined signal x_s in (1) to the relay R, the destination node D, and the eavesdropper node E. The combined signal x_s in (1) will create an artificial interference for the eavesdropper E without affecting the destination node D.

2) In the second timeslot,the relay R will amplify the received signals and forward them to the destination node D and the eavesdropper node E.

In the first time slot, the received signals at the relay R, the destination node D, and the eavesdropper node E are given, respectively, as

$$\begin{aligned} y_R &= h_1 x_s + n_R \\ &= \sqrt{(1-\alpha)P}\,x h_1 + \sqrt{\alpha P}\,j h_1 + n_R \end{aligned} \quad (2)$$

$$\begin{aligned} y_D &\overset{(3.1)}{=} h_0 x_s + n_{D,1} \\ &\overset{(3.2)}{=} \sqrt{(1-\alpha)P}\,x h_0 + \sqrt{\alpha P}\,j h_0 + n_{D,1} \\ &\overset{(3.3)}{=} \sqrt{(1-\alpha)P}\,x h_0 + n_{D,1} \end{aligned} \quad (3)$$

$$\begin{aligned} y_E &= h_3 x_s + n_{E,1} \\ &= \sqrt{(1-\alpha)P}\,x h_3 + \sqrt{\alpha P}\,j h_3 + n_{E,1} \end{aligned} \quad (4)$$

where P is the total transmit power of the source node *S*; (αP) and $\left((1-\alpha)P\right)$ are power parts allocated to the jamming signal j and the desired secrecy signal $x$of the source node S, respectively, $0 \le \alpha \le 1$; n_R, $n_{D,1}$ and $n_{E,1}$ are the zero-mean AWGN at nodes R, D, and E at the first timeslot, respectively.

In Formula (3), (3.3) is given by omitting the component $\sqrt{\alpha P}\,j h_0$ because the destination node D knows the jamming signal j.

In the second timeslot, the relay R will amplify the received signal y_R with a gain G [5, Eq. (3)] as

$$\begin{aligned} G &= \left(\sqrt{(1-\alpha)P|h_1|^2 + \alpha P|h_1|^2 + N_0}\right)^{-1} \\ &= \left(\sqrt{P|h_1|^2 + N_0}\right)^{-1} \end{aligned} \quad (5)$$

The received signals at the destination node D and the eavesdropper node E are given, respectively, as

$$\begin{aligned} y_{D,2} &\overset{(6.1)}{=} \sqrt{P} G y_R h_2 + n_{D,2} \\ &\overset{(6.2)}{=} \frac{\sqrt{P}\left\{\sqrt{(1-\alpha)P}\,x h_1 + \sqrt{\alpha P}\,j h_1 + n_R\right\} h_2}{\sqrt{P|h_1|^2 + N_0}} + n_{D,2} \\ &\overset{(6.3)}{=} \frac{P\sqrt{(1-\alpha)}\,x h_1 h_2 + \sqrt{P} n_R h_2}{\sqrt{P|h_1|^2 + N_0}} + n_{D,2} \end{aligned} \quad (6)$$

$$\begin{aligned} y_{E,2} &= \sqrt{P} G y_R h_4 + n_{E,2} \\ &= \frac{\sqrt{P}\left\{\sqrt{(1-\alpha)P}\,x h_1 + \sqrt{\alpha P}\,j h_1 + n_R\right\} h_4}{\sqrt{P|h_1|^2 + N_0}} + n_{E,2} \end{aligned} \quad (7)$$

Where in, $n_{D,2}$ and $n_{E,2}$ are the zero-mean AWGN at nodes D and E at the second timeslot, respectively.

In Formula (6), (6.3) is given by omitting the component $\sqrt{P}\sqrt{\alpha P}\,j h_1$ because the destination node D knows the jamming signal j.

3. SECRECY OUTAGE PROBABILITY ANALYSIS

In this section, I analyze the secrecy outage probability of the proposed protocol to evaluate the transmission security. I note that the eavesdropper node E does not know the jamming signals j; therefore the components $\sqrt{\alpha P}\,j h_3$ in (4), and $P\sqrt{\alpha}\,j h_1 h_4 \big/ \sqrt{P|h_1|^2 + N_0}$ in (7) are artificial

interferences created by the source node S to prevent the eavesdropper node E from overhearing the secrecy packet *x*.

In the first timeslot, the received SNRs at the destination node D, denoted as $\gamma_{D,1}$, is given from (3) as

$$\gamma_{D,1} = (1-\alpha) P|h_0|^2 / N_0 = (1-\alpha)\gamma_0 \quad (8)$$

where $\gamma_0 = \underbrace{(P/N_0)}_{\overline{\gamma}} \times |h_0|^2$ and $\overline{\gamma}$ is defined as a transmit SNR.

Similarly, the received SNR at the eavesdropper node E, denoted as $\gamma_{E,1}$, is obtained from (4) as

$$\gamma_{E,1} = \frac{(1-\alpha) P|h_3|^2}{\alpha P|h_3|^2 + N_0} = \frac{(1-\alpha)\gamma_3}{\alpha\gamma_3 + 1} \quad (9)$$

where $\gamma_3 = P|h_3|^2 / N_0 = \overline{\gamma} \times |h_3|^2$.

In the second timeslot, $\gamma_{D,2}$ and $\gamma_{E,2}$ are denoted as the received SNR sat the destination node D and the eavesdropper node E, respectively, and are given from (6) and (7) as

$$\gamma_{D,2} = \frac{P^2(1-\alpha)|h_1|^2|h_2|^2 / \left(P|h_1|^2 + N_0\right)}{PN_0|h_2|^2 / \left(P|h_1|^2 + N_0\right) + N_0} \quad (10)$$
$$= (1-\alpha)\gamma_1\gamma_2 / (\gamma_1 + \gamma_2 + 1)$$

$$\gamma_{E,2} = \frac{\dfrac{P^2(1-\alpha)|h_1|^2|h_4|^2}{P|h_1|^2 + N_0}}{\dfrac{P\left(\alpha P|h_1|^2 + N_0\right)|h_4|^2}{P|h_1|^2 + N_0} + N_0} \quad (11)$$
$$= (1-\alpha)\gamma_1\gamma_4 / (\alpha\gamma_1\gamma_4 + \gamma_1 + \gamma_4 + 1)$$

where $\gamma_m = P|h_m|^2 / N_0 = \overline{\gamma} \times |h_m|^2, m \in \{1, 2, 4\}$.

In this paper, the MRC method [2, Eq. (14)] is applied at both the destination node D and the eavesdropper node E to increase the decoding capacity and the wiretapping operation. The end-to-end SNRs at the destination node D and the eavesdropper node E are given as

$$\gamma_k = \gamma_{k,1} + \gamma_{k,2},\ k \in \{D, E\} \quad (12)$$

Based on the Formulas (8), (10), (9) and (11) with (12), I obtain

$$\gamma_D = (1-\alpha)\gamma_0 + \frac{(1-\alpha)\gamma_1\gamma_2}{\gamma_1 + \gamma_2 + 1} \quad (13)$$

$$\gamma_E = \frac{(1-\alpha)\gamma_3}{\alpha\gamma_3 + 1} + \frac{(1-\alpha)\gamma_1\gamma_4}{\alpha\gamma_1\gamma_4 + \gamma_1 + \gamma_4 + 1} \quad (14)$$

From the received SNRs (13-14), the achievable data rates of the desired link *S-D* and the eavesdropped link *S-E* to decode the secrecy signal *x* are expressed, respectively, denoted as R_D and R_E, as

$$R_k = (1/2) \times \log_2(1 + \gamma_k),\ k \in \{D, E\} \quad (15)$$

where the factor (1/2) means that secrecy signals are transmitted in two timeslots.

I note that the destination node D will receive the secrecy signal *x* while the eavesdropper node E will wiretap this signal. Hence, the end-to-end ASR of the source-destination link is given [2, Eq. (10) and 4, Eq. (8)] as

$$ASR = \left[R_D - R_E\right]^+ = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right)\right]^+$$
$$= \left[\frac{1}{2}\log_2\left(\frac{1 + (1-\alpha)\gamma_0 + \dfrac{(1-\alpha)\gamma_1\gamma_2}{\gamma_1 + \gamma_2 + 1}}{1 + \dfrac{(1-\alpha)\gamma_3}{\alpha\gamma_3 + 1} + \dfrac{(1-\alpha)\gamma_1\gamma_4}{\alpha\gamma_1\gamma_4 + \gamma_1 + \gamma_4 + 1}}\right)\right]^+ \quad (16)$$

where $\left[x\right]^+$ is defined as $\max\{x, 0\}$.

The secrecy outage probability of the proposed protocol is defined as the probability that the end-to-end ASR is less than the target secrecy rate R_t. Hence, the secrecy outage probability is expressed as

$$P^{sop} = \Pr\left[ASR < R_t\right] = \Pr\left[\left[\frac{1}{2}\log_2\left(\left(1+(1-\alpha)\gamma_0+\frac{(1-\alpha)\gamma_1\gamma_2}{\gamma_1+\gamma_2+1}\right)\Big/ \left(1+\frac{(1-\alpha)\gamma_3}{\alpha\gamma_3+1}+\frac{(1-\alpha)\gamma_1\gamma_4}{\alpha\gamma_1\gamma_4+\gamma_1+\gamma_4+1}\right)\right)\right]^+ < R_t\right] \quad (17)$$

From (17), I observe that the expression of the secrecy outage probability P^{sop} is complex and depends on random variables (RVs) $\gamma_0, \gamma_1, \gamma_2, \gamma_3$ and γ_4 . Hence, a closed-form expression of the secrecy outage probability P^{sop} is not feasible.

Formula (17) can be equivalently rewritten as

$$P^{sop} = \Pr\left\{(1-\alpha)\gamma_0+\frac{(1-\alpha)\gamma_1\gamma_2}{\gamma_1+\gamma_2+1} < \underbrace{2^{2R_t}-1}_{\theta} + (\theta+1)(1-\alpha)\left\{\frac{\gamma_3}{\alpha\gamma_3+1}+\frac{\gamma_1\gamma_4}{\alpha\gamma_1\gamma_4+\gamma_1+\gamma_4+1}\right\}\right\} \quad (18)$$

When $SNR\,\bar{\gamma}$ is large ($\bar{\gamma}\to\infty$), then P^{sop} is approximately expressed as

$$P^{sop} \approx \Pr\left\{\begin{matrix}(1-\alpha)\gamma_0+(1-\alpha)\times\dfrac{\gamma_1\gamma_2}{\gamma_1+\gamma_2+1} < \\ \theta+(\theta+1)(1-\alpha)\left\{\dfrac{\gamma_3}{\alpha\gamma_3}+\dfrac{\gamma_1\gamma_4}{\alpha\gamma_1\gamma_4}\right\}\end{matrix}\right\} = \Pr\left\{\begin{matrix}\gamma_0+\underbrace{\gamma_1\gamma_2/(\gamma_1+\gamma_2+1)}_{X} < \\ \underbrace{\theta/(1-\alpha)+2(\theta+1)/\alpha}_{\xi}\end{matrix}\right\} \quad (19)$$

Because the channel gains $\omega_i = |h_i|^2$ are exponential RVs with parameters $\lambda_i = d_i^{\beta}$, then $\gamma_i = \bar{\gamma}\times\omega_i$ are also exponential RVs with parameters $\lambda_i/\bar{\gamma}$, respectively, $i\in\{0,1,2,3,4\}$.

From the definition of X in (20), X is a MacDonald RV [11, Eq. (1)], $X \sim MD\left(\lambda_1/\bar{\gamma}, \lambda_2/\bar{\gamma}\right)$, and has a cumulative distribution function (CDF) and a probability density function (PDF) from [11, Eq. (2-3)] as

$$F_X(x) = 1-2e^{-(\lambda_1+\lambda_2)x/\bar{\gamma}}\sqrt{\lambda_1\lambda_2 x(x+1)\Big/\left(\bar{\gamma}\right)^2} \times K_1\left(2\sqrt{\lambda_1\lambda_2 x(x+1)\Big/\left(\bar{\gamma}\right)^2}\right) \quad (20)$$

$$f_X(x) = 2e^{-(\lambda_1+\lambda_2)x/\bar{\gamma}}\times \left[\left(\frac{\lambda_1\lambda_2(2x+1)}{\left(\bar{\gamma}\right)^2}\right)\times K_0\left(2\sqrt{\frac{\lambda_1\lambda_2(2x+1)}{\left(\bar{\gamma}\right)^2}}\right) + \frac{(\lambda_1+\lambda_2)}{\bar{\gamma}}\times\sqrt{\frac{\lambda_1\lambda_2 x(x+1)}{\left(\bar{\gamma}\right)^2}}\times K_1\left(2\sqrt{\frac{\lambda_1\lambda_2 x(x+1)}{\left(\bar{\gamma}\right)^2}}\right)\right] \quad (21)$$

where $x \geq 0$, and $K_\nu(x)$ is the ν^{th}-order modified Bessel function of the second kind [11, Eq. (8.432.6)].

Formula (20) is given as

$$P^{sop} \approx \Pr\left\{\gamma_0 + X < \xi\right\} = \int_0^{\xi} f_{\gamma_0}(x)\times F_X(\xi-x)\,dx = \int_0^{\xi}\frac{\lambda_0 e^{-\lambda_0 x/\bar{\gamma}}}{\bar{\gamma}}\left\{1-2e^{-(\lambda_1+\lambda_2)(\xi-x)/\bar{\gamma}} \times\sqrt{\lambda_1\lambda_2(\xi-x)(\xi-x+1)\Big/\left(\bar{\gamma}\right)^2} \times K_1\left(2\sqrt{\lambda_1\lambda_2(\xi-x)(\xi-x+1)}/\bar{\gamma}\right)\right\}dx \quad (22)$$

After some manipulations of (22), I obtain the single-integral form expression of P^{sop} as

$$P^{sop} \approx 1-\lambda_0 e^{-\lambda_0\xi/\bar{\gamma}}/\bar{\gamma} - 2\lambda_0 e^{-(\lambda_1+\lambda_2)\times\xi/\bar{\gamma}}\sqrt{\lambda_1\lambda_2}\Big/\left(\bar{\gamma}\right)^2 \times\int_0^{\xi} e^{-(\lambda_0-\lambda_1-\lambda_2)x/\bar{\gamma}}\times\sqrt{(\xi-x)(\xi-x+1)} \times K_1\left(2\sqrt{\lambda_1\lambda_2(\xi-x)(\xi-x+1)}/\bar{\gamma}\right)dx \quad (23)$$

where $K_\nu(x)$ is the ν^{th}-order modified Bessel function of the second kind [12, Eq. (8.432.6)], $\xi = \theta/(1-\alpha)+2(\theta+1)/\alpha$.

4. SIMULATION RESULTS AND DISCUSSIONS

This section discusses the analysis and simulation results of the proposed cooperation transmission. The analysis results are drawn from the asymptotic expressions derived above, and the simulation results are based on Monte-Carlo experiments. In a two-dimensional plane, the coordinates of the source S, the destination D, the eavesdropper E, and the relay R are set as S(0,0), D(1,0), R(x_r, y_r), and E(x_e, y_e), where $0 < x_r, x_e < 1$.

Thus,

$d_1 = \sqrt{x_r^2 + y_r^2}$, $d_2 = \sqrt{(1-x_r)^2 + y_r^2}$, $d_3 = \sqrt{x_e^2 + y_e^2}$, and $d_4 = \sqrt{(x_r - x_e)^2 + (y_r - y_e)^2}$.

I assume that the target secrecy rate and the path-loss exponent are constant (R_t=1 (bit/s/Hz), $\beta = 3$), and the SNR on the x-axis is defined as $SNR = \bar{\gamma} = P/N_0$.

Figure 2 presents the secrecy outage probabilities of the proposed protocol at the destination node D as a function of the SNR (dB) when the eavesdropper node is near the source node, E(0.1,0), and R (0.5, 0.1). As a result, the distance parameters are obtained $d_1 = d_2 = 0.51$, $d_3 = 0.1$, and $d_4 = 0.41$. As shown in Figure 2, the secrecy performance of the proposed protocol outperforms a secrecy transmission without jamming ($\alpha = 0$). These results occur because when the eavesdropper node is near the source node, the jamming signal from the source node will create artificial interference to efficiently decrease the quality of the source-eavesdropper link. The extra power required for transmitting the secrecy signal will be provided by the relay with the amplify-and-forward method. In addition, the MRC method is applied at the destination node to increase the quality of the desired end-to-end source-destination link (12). In addition, the secrecy outage probability of the proposed protocol decreases when α increases from 01 to 0.5, and increases when α decreases from 0.9 to 0.5 because the source node adjusts the power of the jamming signal, a condition that should be satisfied both creating the artificial interference and transmitting the secrecy signal. Figure 2 shows that the asymptotic expression of (23) is valid with the simulation results evaluating the secrecy performance of the proposed protocol.

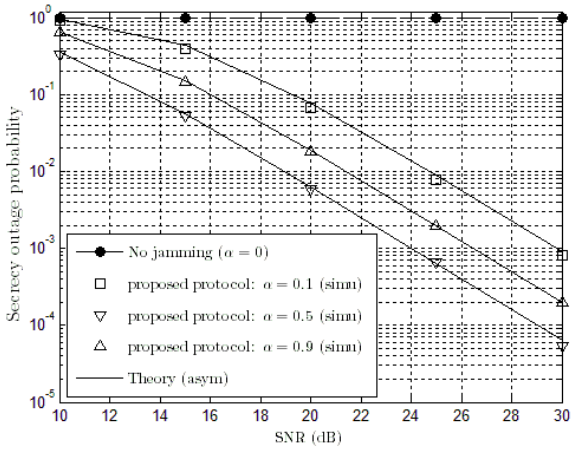

Fig.2 *Thesecrecy outage probability of the proposed protocol at the destination node D as a function of the SNR (dB) when R (0.5, 0.1), E (0.1, 0) (correspond to $d_1 = d_2 = 0.51$, $d_3 = 0.1$, $d_4 = 0.41$).*

Figure 3 presents the secrecy outage probabilities of the proposed protocol at the destination node D as a function of the location of the relay x_r when $y_r = 0$, *SNR = 25* (dB), E (0.5, 0.5), and $\alpha = 0.1$. As shown in Figure 3, the secrecy outage probability of the proposed protocol is smallest when the relay is at the midpoint between the source node and the destination node ($x_r = 0.5$).

5. CONCLUSIONS

In this paper, I proposed the jamming method was proposed to improve the secrecy cooperation transmissions in which the source node transmits a combined signal of the secrecy signal and the jamming signal using the power allocation strategy. I analyzed and evaluated t The secrecy performance was analyzed and evaluated based on the secrecy outage probability of the achievable secrecy rate. The secrecy outage probabilities are obtained using asymptotic expressions. The results show the following advantages. First, the proposed protocol well solved the location problem of an eavesdropper node near the source node. Second, the proposed protocol outperforms the secrecy transmission without jamming. Third, the secrecy outage probabilities of the proposed protocol is probabilities of the proposed protocol are smallest when the relay is at the midpoint between the source and destination nodes. In addition, the asymptotic expressions of the secrecy outage probabilities of the proposed protocol are valid in evaluating the secrecy performance.

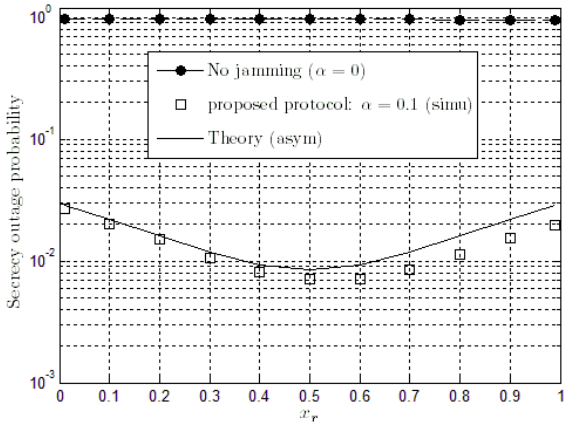

Fig.3 *These crecy outage probability of the proposed protocol at the destination node D as a function of the location of the relay x_r on the x-axis when y_r=0, SNR=25 (dB), E (0.5, 0.5) (corresponding to d_3= d_4=0.71), and* $\alpha = 0.1$.

REFERENCES

[1] A.D. Wyner, The wire-tap channel, *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, 1975.

[2] Lun Dong, Zhu 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, 2010.

[3] Zhiguo Ding, Mai Xu, Jianhua Lu and Fei Liu, Improving Wireless Security for Bidirectional Communication Scenarios, *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2842-2848, 2012.

[4] Jingchao Chen, Lingyang Song, Zhu Han and Bingli Jiao, Joint Relay and Jammer Selection for Secure Decode-and-Forward Two-Way Relay Communications, *Global Telecommunications Conference (GLOBECOM 2011)*, Houston, Texas, USA, Dec. 2011, pp. 1-5.

[5] T.T. Kim and H.V. Poor, Secure relaying: can publicly transferred keys increase degrees of freedom?,*47th Annual Allerton Conference on Communication, Control, and Computing*, 2009 *(Allerton 2009)*, Monticello, Illinois, USA, Oct. 2009, pp. 1076 – 1081.

[6] Y.M. Khattabi and M.M. Matalgah, Performance Analysis of Multiple-Relay AF Cooperative Systems Over Rayleigh Time-Selective Fading Channels With Imperfect Channel Estimation, *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 427 – 434, 2016.

[7] Z. He, X. Zhang, Y. Bi, W. Jiang and Y. Rong, Optimal Source and Relay Design for Multiuser MIMO AF Relay Communication Systems with Direct Links and Imperfect Channel Information, *IEEE Transactions on Wireless Communications*, DOI: 10.1109/TWC.2015.2497683, 2015.

[8] Minghua Xia and S. Aissa,Cooperative AF Relaying in Spectrum-Sharing Systems: Outage Probability Analysis under Co-Channel Interferences and Relay Selection, *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3252–3262, 2012.

[9] S.S Ikki, and M.H. Ahmed, Performance Analysis of Adaptive Decode-and-Forward Cooperative Diversity Networks with Best-Relay Selection, *IEEE Transaction on communications*, vol. 58, no. 1, pp. 68-72, 2010.

[10] K. Junsu, A. Ikhlef and R. Schober, Combined relay selection and cooperative beamforming for physical layer security, *Journal of Communications and Networks*, vol. 14, no. 4, pp. 364-373, 2012.

[11] B. Barua, H.Q. Ngo and Hyundong Shin, On the SEP of Cooperative Diversity with Opportunistic Relaying,*IEEE Communications letters*,vol. 12, no. 10, pp. 727-729, 2008.

[12] I.S. Gradshteyn, I.M. Ryzhik, A. Jeffrey and D. Zwillinger, *Table of Integral, Seriesand Products*, Academic press, 7th edn.2007.

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