Achieving zero secrecy outage in amplify-and-forward relaying systems

Huynh Huy Cuong[1], Nguyen Manh Hung[2], Nguyen Thi Ngoc Thuy[3, 4], Ta Quang Hien[3, 4*]

[1]Institute of Information Technology, Academy of Military Science and Technology, 17 Hoang Sam, Nghia Do, Cau Giay, Hanoi, Vietnam;
[2]Institute of Electronics, Academy of Military Science and Technology, 17 Hoang Sam, Nghia Do, Cau Giay, Hanoi, Vietnam;
[3]International University, Vietnam National University HCMC, Linh Trung, Thu Duc City, Ho Chi Minh City, Vietnam;
[4]Vietnam National University HCMC, Linh Trung, Thu Duc City, Ho Chi Minh City, Vietnam.
[*]Corresponding author: tqhien@hcmiu.edu.vn
Received 28 Dec. 2023; Revised 10 Mar. 2024; Accepted 14 Mar. 2024; Published 1 Apr. 2024.
DOI: https://doi.org/10.54939/1859-1043.j.mst.CAPITI.2024.89-96

ABSTRACT

A proposed artificial noise (AN) injection strategy is considered in amplify-and-forward (AF) relaying systems. The limit of secrecy rate, hence the resulting zero-outage secrecy throughput, is determined subject to guarantee zero secrecy outage toward any powerful eavesdropper. The results show that the proposed simple strategy can achieve zero secrecy outage, which cannot be achieved in literature, and that it is easy to apply in wireless networks. The results also show an important finding: increasing throughput against increasing transmit power in secrecy.

Keywords: Artificial noise injection; Secrecy outage probability; Zero-outage secrecy capacity.

1. INTRODUCTION

Wireless services have become an integral part of modern life, serving a wide range of essential purposes for both individuals and businesses. The allure of wireless networks lies in their convenience, cost-efficiency, and effectiveness, leading to a significant surge in their usage. However, it is crucial to acknowledge the inherent vulnerability of these networks to unauthorized access and potential tampering. Such breaches in security can have severe consequences, including the exposure of valuable information and unforeseen negative outcomes. Hence, the importance of incorporating robust security measures into the design of wireless systems cannot be emphasized enough. While traditional cryptosystems have been conventionally utilized to enhance security, they may not always be suitable for certain architectural setups. As a compelling alternative, recent advancements in information theory have shed light on the potential of leveraging the physical layer to effectively address security concerns [1, 2].

The basic idea to guarantee secret transmission is to have the main channels better than the wiretap channel. To do this, one potential solution is the AN injection strategy. By introducing confusion to eavesdroppers, this technique aims to mitigate their ability to intercept sensitive information. Noteworthy, the AN lies on the null space of the main channel and will only affect eavesdroppers but the legitimate receivers [3]. The idea of AN has been extended to multiple-antenna [4], jamming full-duplex receiver [5] and full-duplex relay selection [6]. However, if eavesdroppers possess superior communication channels, particularly when eavesdroppers have an infinite number of antennas or are located close to the transmitter for extremely high wiretap channels, the secrecy cannot be guaranteed any more.

For some circumstances that require the secrecy outage probability zero, such as credit number transmission, the design of secret transmission becomes difficult as the secrecy outage probability is naturally non-zero. Recently, [7] has proposed a novel scheme of AN injection to achieve secret transmission while guaranteeing zero secrecy outage probability. Therefore, this paper extends the work in [7] for amplify-and-forward relaying and proposes a novel transmission strategy in the

sense of minimizing the time slot of transmitting only AN. Then, this paper characterizes the zero-outage secret transmission and secrecy throughput.

2. MODEL DESCRIPTION

Figure 1 illustrates secure communication in relaying systems, where the transmitter (Alice) securely delivers messages to the receiver (Bob) toward the eavesdropper (Eve) with the aid of decode-and-forward Relay. Assume that all nodes are equipped with a single antenna. The secure transmission consists of three phases: Alice only transmits the AN in the first phase, then Alice sends both the secure message and AN to other channels in the second phase, and Relay decodes and forwards the message to Bob and Eve in the third phase. This scheme aims to send a secure message to the recipient without leaking information to Eve through the time slot we help the recipient remove AN in received signals while the eavesdropper cannot remove it. To do this, we assume that the pilot signal is transmitted by Relay to other channels, then Alice fed back. Then, Relay and Bob will have CSI knowledge of the channels between them and Alice, while the CSI between Alice and Eve will not be known to Eve.

Assume that $h_{ij}^{(n)}$ is the channel between nodes i and j at n-th phase for $i,j \in \{A,B,E,R\}$, which represent Alice, Bob, Eve, and Relay, respectively, and $h_{ij}^{(n)} \sim CN(0,\sigma_{ij}^2)$, where σ_{ij}^2 denotes the channel variance. Furthermore, n_i is assumed as the background noise at each node with $i \in \{B,E,R\}$ and follows a Gaussian distribution with zero mean and variance of σ_n^2.

A. Three-phase transmission

1) Only AN transmission: In the first phase, Alice only transmits the AN as:

$$x_A^{(1)} = \frac{h_{AB}^{(1)*}}{\left|h_{AB}^{(1)}\right|^2}\sqrt{P_1}\,\omega \tag{1}$$

for $\left|h_{AB}^{(1)}\right|^2 \geq \tau_1$,where $P_1 = P\sigma_{AB}^2/E_1(\tau_1/\sigma_{AB}^2)$ with P denoted as the average transmit power of the transmitter (Alice), $E_1(x) = \int_x^\infty e^{-t}dt/t$ denoted as the exponential integral [8], and ω is AN signal and has a complex Gaussian distribution, i.e. $\omega \sim CN(0,1)$. The received signal at node i is given by:

$$r_i^{(1)} = \frac{h_{Ai}^{(1)}h_{AB}^{(1)*}}{\left|h_{AB}^{(1)}\right|^2}\sqrt{P_1}\,\omega + n_i^{(1)} \tag{2}$$

where $i \in \{B, R, E\}$.

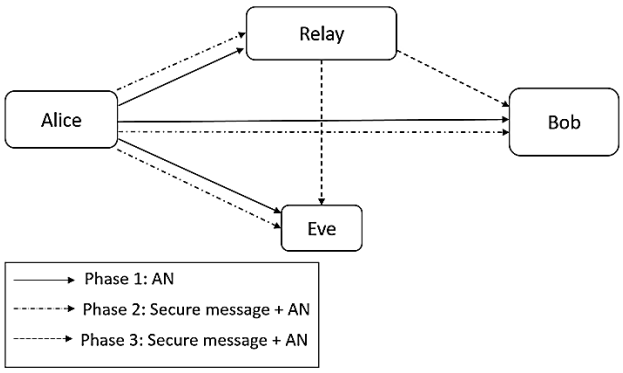

Figure 1. *System model.*

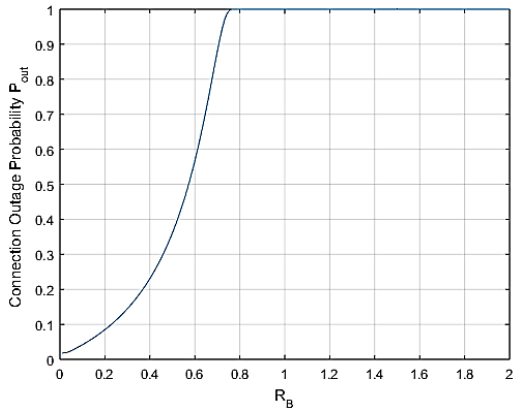

Figure 2. *Connection outage probability P_{out} versus R_B; $\beta = 0.4$ and $P/\sigma_n^2 = 20$ dB.*

2) Two-phase amplify-and-forward transmission: After Alice sends the AN in the first phase, Alice continues to amplify and forward the AN with its secure message to Bob in the second phase. Alice's transmitted signal is:

$$x_A^{(2)} = \frac{h_{AR}^{(2)*}}{\left|h_{AR}^{(2)}\right|^2}\left(\sqrt{\beta P_2}s + \sqrt{(1-\beta)P_2}\,\omega\right) \tag{3}$$

for $\left|h_{AR}^{(2)}\right|^2 \geq \tau_2$, where $P_2 = P\sigma_{AR}^2/E_1(\tau_2/\sigma_{AR}^2)$, s is normalized secure information signals ($s \sim CN(0,1)$), β is the portion of the power used for the signal-bearing information with $0 < \beta < 1$.

Then, Relay amplifies and forwards its received signal

$$r_R^{(2)} = \sqrt{\beta P_2}s + \sqrt{(1-\beta)P_2}\,\omega + n_R^{(2)} \tag{4}$$

and forward $\sqrt{P_R}r_R^{(2)}/\left|r_R^{(2)}\right|$ to Bob. Hence, the received signals at Bob and Eve in the third phase are obtained by:

$$r_i^{(3)} = h_{Ri}^{(3)}\sqrt{P_R}\frac{r_R^{(2)}}{\left|r_R^{(2)}\right|} + n_i^{(3)} = h_{Ri}^{(3)}\sqrt{P_R}\frac{\sqrt{\beta P_2}s + \sqrt{(1-\beta)P_2}\,\omega + n_R^{(2)}}{\sqrt{P_2+\sigma_n^2}} + n_i^{(3)} \tag{5}$$

for $i \in \{B,E\}$.

B. Outage Probability

In this section, we shall elucidate the concept of connection outage probability, an integral measure of the probability of Bob encountering difficulties in decoding the security message. From the three phases, Bob receives:

$$\begin{aligned} r_B^{(1)} &= \sqrt{P_1}\,\omega + n_B^{(1)} \\ r_B^{(2)} &= \frac{h_{AB}^{(2)}h_{AR}^{(2)*}}{\left|h_{AR}^{(2)}\right|^2}\left(\sqrt{\beta P_2}s + \sqrt{(1-\beta)P_2}\,\omega\right) + n_B^{(2)} \\ r_B^{(3)} &= h_{RB}^{(3)}\sqrt{P_R}\frac{\sqrt{\beta P_2}s + \sqrt{(1-\beta)P_2}\,\omega + n_R^{(2)}}{\sqrt{P_2+\sigma_n^2}} + n_B^{(3)} \end{aligned} \tag{6}$$

Then, Bob can eliminate AN in $r_B^{(2)}$ and $r_B^{(3)}$ from $r_B^{(1)}$ by

$$\begin{aligned} r_B^{(2)'} &= r_B^{(2)} - \frac{h_{AB}^{(2)}h_{AR}^{(2)*}}{\left|h_{AR}^{(2)}\right|^2}\sqrt{\frac{(1-\beta)P_2}{P_1}}\,r_B^{(1)} \\ &= \frac{h_{AB}^{(2)}h_{AR}^{(2)*}}{\left|h_{AR}^{(2)}\right|^2}\sqrt{\beta P_2}s + n_B^{(2)} - \frac{h_{AB}^{(2)}h_{AR}^{(2)*}}{\left|h_{AR}^{(2)}\right|^2}\sqrt{\frac{(1-\beta)P_2}{P_1}}\,n_B^{(1)} \end{aligned} \tag{7}$$

and

$$\begin{aligned} r_B^{(3)'} &= r_B^{(3)} - h_{RB}^{(3)}\sqrt{\frac{P_R}{P_1}}\sqrt{\frac{(1-\beta)P_2}{P_2+\sigma_n^2}}\,r_B^{(1)} \\ &= h_{RB}^{(3)}\sqrt{\frac{\beta P_2 P_R}{P_2+\sigma_n^2}}s + h_{RB}^{(3)}\sqrt{\frac{P_R}{P_2+\sigma_n^2}}\,n_R^{(2)} + n_B^{(3)} - h_{RB}^{(3)}\sqrt{\frac{P_R}{P_1}}\sqrt{\frac{(1-\beta)P_2}{P_2+\sigma_n^2}}\,n_B^{(1)} \end{aligned} \tag{8}$$

Hence, the capacity at Bob is obtained via the technique of the receiver's maximum ratio combining of $r_B^{(2)'}$ and $r_B^{(3)'}$

$$C_B = \frac{1}{3} log_2 \left(1 + \frac{\left| \frac{h_{AB}^{(2)} h_{AR}^{(2)*}}{\left| h_{AR}^{(2)} \right|^2} \right|^2 \frac{\beta P_2}{\sigma_n^2}}{1 + \left| \frac{h_{AB}^{(2)} h_{AR}^{(2)*}}{\left| h_{AR}^{(2)} \right|^2} \right|^2 \frac{(1-\beta)P_2}{P_1}} + \frac{\left| h_{RB}^{(3)} \right|^2 \frac{\beta P_2 P_R}{(P_2 + \sigma_n^2)\sigma_n^2}}{1 + \left| h_{RB}^{(3)} \right|^2 \frac{P_R}{P_2 + \sigma_n^2} + \left| h_{RB}^{(3)} \right|^2 \frac{(1-\beta)P_2 P_R}{(P_2 + \sigma_n^2)P_1}} \right) \quad (9)$$

Let:

$$W = \frac{\left| h_{RB}^{(3)} \right|^2 \frac{\beta P_2 P_R}{(P_2 + \sigma_n^2)\sigma_n^2}}{1 + \left| h_{RB}^{(3)} \right|^2 \frac{P_R}{P_2 + \sigma_n^2} + \left| h_{RB}^{(3)} \right|^2 \frac{(1-\beta)P_2 P_R}{(P_2 + \sigma_n^2)P_1}} \quad (10)$$

where its probability density function (PDF) is derived in Appendix A as:

$$p_W(\omega) = exp\left(- \frac{\omega / \sigma_{RB}^2}{\frac{\beta P_2 P_R}{(P_2 + \sigma_n^2)\sigma_n^2} - \omega\left(\frac{P_R(1 + (1-\beta)P_2/P_1)}{P_2 + \sigma_n^2} \right)} \right) \frac{\frac{\beta P_2 P_R / \sigma_{RB}^2}{(P_2 + \sigma_n^2)\sigma_n^2}}{\left(\frac{\beta P_2 P_R}{(P_2 + \sigma_n^2)\sigma_n^2} - \omega\left(\frac{P_R(1 + (1-\beta)P_2/P_1)}{P_2 + \sigma_n^2} \right) \right)^2} \quad (11)$$

for $\omega < \frac{\beta P_2 / \sigma_n^2}{1 + (1-\beta)P_2/P_1}$. Therefore, Bob's outage probability is obtained by:

$$P_{out} = \Pr(C_B < R_B) = \Pr\left(\frac{\left| \frac{h_{AB}^{(2)} h_{AR}^{(2)*}}{\left| h_{AR}^{(2)} \right|^2} \right|^2 \beta P_2 / \sigma_n^2}{1 + \left| \frac{h_{AB}^{(2)} h_{AR}^{(2)*}}{\left| h_{AR}^{(2)} \right|^2} \right|^2 (1-\beta)P_2/P_1} < (2^{3R_B} - 1 - W) \right)$$

$$= 1 - \int_0^{\frac{\frac{\beta P_2}{\sigma_n^2}}{1 + \frac{(1-\beta)P_2}{P_1}}} p_W(\omega) \frac{exp\left(- \frac{\tau}{\sigma_{AR}^2} \left(1 + \frac{(2^{3R_B} - 1 - \omega)\sigma_{AR}^2 / \sigma_{AB}^2}{\left(\frac{(1-\beta)P_2}{P_1} - \frac{\beta P_2}{\sigma_n^2}(2^{3R_B} - 1 - \omega) \right)^+} \right) \right)}{1 + \frac{(2^{3R_B} - 1 - \omega)\sigma_{AR}^2 / \sigma_{AB}^2}{\left(\frac{(1-\beta)P_2}{P_1} - \frac{\beta P_2}{\sigma_n^2}(2^{3R_B} - 1 - \omega) \right)^+}} d\omega \quad (12)$$

where (12) is derived in Appendix A. The connection outage probability P_{out} versus R_B is illustrated in figure 2, which shows the outage probability increases when R_B increases.

3. ZERO-OUTAGE SECRET TRANSMISSION

Zero-outage secret transmission is the transmission of a message undetected, which relies on the quantity of data needed, which is determined by the favorable disparity between the fixed transmission rate (R_B) and the confidential transmission rate (R_S).

A. Zero Secrecy Outage Probability

In this subsection, we shall ascertain the probability of a breach of confidentiality, which is defined as the likelihood of Eve successfully intercepting and decoding a secure message. By considering the transmission of such a message as a prerequisite, denoted as R_B and R_S, representing the transmit rate and the secrecy rate, respectively, we can determine the essential rate differential $R_B - R_S$ required for transmitting the message without the risk of eavesdropping. The received signal from three phases for Eve:

$$r_E^{(1)} = \frac{h_{AE}^{(1)} h_{AB}^{(1)*}}{\left|h_{AB}^{(1)}\right|^2}\sqrt{P_1}\,\omega + n_E^{(1)}$$

$$r_E^{(2)} = \frac{h_{AE}^{(2)} h_{AR}^{(2)*}}{\left|h_{AR}^{(2)}\right|^2}\left(\sqrt{\beta P_2}s + \sqrt{(1-\beta)P_2}\,\omega\right) + n_E^{(2)} \tag{13}$$

$$r_E^{(3)} = h_{RE}^{(3)}\sqrt{P_R}\frac{\sqrt{\beta P_2}s + \sqrt{(1-\beta)P_2}\,\omega + n_R^{(2)}}{\sqrt{P_2+\sigma_n^2}} + n_E^{(3)}$$

Since Eve does not know $h_{AE}^{(1)}$, Eve cannot remove AN by using $r_E^{(1)}$, hence decoding the secure message via $r_E^{(2)}$ and $r_E^{(3)}$. Then, the capacity of decoding s at Eve is given by:

$$C_E = \frac{1}{3}\log_2\left(1 + \gamma_E^{(2)} + \gamma_E^{(3)}\right) \tag{14}$$

where

$$\gamma_E^{(2)} = \frac{\left|\frac{h_{AE}^{(2)} h_{AR}^{(2)*}}{\left|h_{AR}^{(2)}\right|^2}\right|^2 \beta P_2}{\left|\frac{h_{AE}^{(2)} h_{AR}^{(2)*}}{\left|h_{AR}^{(2)}\right|^2}\right|^2 (1-\beta)P_2 + \sigma_n^2} \tag{15}$$

$$\gamma_E^{(3)} = \frac{\left|h_{RE}^{(3)}\right|^2 \beta P_2 P_R}{\left|h_{RE}^{(3)}\right|^2 (\sigma_n^2 + (1-\beta)P_2 P_R) + \sigma_n^2(P_2+\sigma_n^2)}$$

As a result, the secrecy outage probability is given by [9]

$$P_{so} = Pr(C_E > R_B - R_S) = Pr\left(\gamma_E^{(2)} + \gamma_E^{(3)} > 2^{3(R_B - R_S)} - 1\right) \tag{16}$$

For $P_{so} \to 0$ or, equivalently, $\gamma_E^{(2)} + \gamma_E^{(3)} \le 2^{3(R_B-R_S)} - 1$ with probability 1 for any value of $h_{AE}^{(2)}$ and $h_{RE}^{(3)}$. Since $\gamma_E^{(2)} \le \beta/(1-\beta)$ and $\gamma_E^{(3)} \le \beta P_2 P_R/(\sigma_n^2 + \beta P_2 P_R)$, the zero secrecy outage probability ($P_{so} \to 0$) can be guaranteed by having

$$\frac{\beta}{1-\beta} + \frac{\beta P_2 P_R}{\sigma_n^2 + \beta P_2 P_R} \le 2^{3(R_B - R_S)} - 1 \tag{17}$$

or, equivalently,

$$R_S \le \left[R_B - \frac{1}{3}log_2\left(1 + \frac{\beta}{1-\beta} + \frac{\beta P_2 P_R}{\sigma_n^2 + \beta P_2 P_R}\right)\right]^+ \tag{18}$$

Note that the constraint of secrecy rate in (18) is to guarantee the zero-secrecy outage probability regardless of the location of Eve.

B. Secrecy Throughput

The zero-outage secrecy throughput denotes η is defined as the amount of secure information that achieves the utmost level of confidentiality while ensuring zero instances of information leakage when $P_{so} \rightarrow 0$. Then, the zero-outage secrecy throughput is defined by:

$$\eta = \max_{R_B} \left[R_B - \frac{1}{3} log_2 \left(1 + \frac{\beta}{1-\beta} + \frac{\beta P_2 P_R}{\sigma_n^2 + \beta P_2 P_R} \right) \right]^+ \times (1 - P_{out}) \times Pr\left(\left| h_{AB}^{(1)} \right|^2 \geq \tau_1 \right) \times Pr\left(\left| h_{AR}^{(2)} \right|^2 \geq \tau_2 \right) \quad (19)$$

where $Pr\left(\left| h_{AB}^{(1)} \right|^2 \geq \tau_1 \right)$ and $Pr\left(\left| h_{AR}^{(2)} \right|^2 \geq \tau_2 \right)$ are the transmission probability.

4. NUMERICAL RESULTS

In this section, we will show the numerical results of zero-secrecy throughout. For simplicity, the parameters are set up as follows: $\sigma_{ij}^2 = 1$ for $i, j \in \{B,R,E\}$, $\sigma_n^2 = 1$ and $\tau_1 = \tau_2 = \tau$. Then, $P_1 = P_2 = P/E_1(\tau)$.

Figure 3 illustrates the zero-outage secrecy throughput η versus the power allocated to secure message β. An optimum power allocation exists to maximize the zero-outage secrecy throughput. Also, it is interesting that the secrecy throughput increases with increasing transmit power, as illustrated in figure 4, with the zero-outage secrecy throughput η versus the transmit signal-to-noise ratio (SNR) P/σ_n^2 when the optimum power allocation is applied.

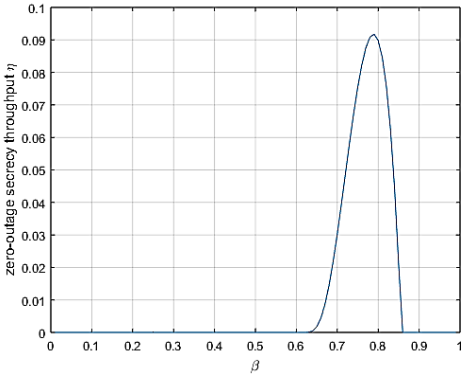

Figure 3. *Zero-outage secrecy throughput η versus β.*

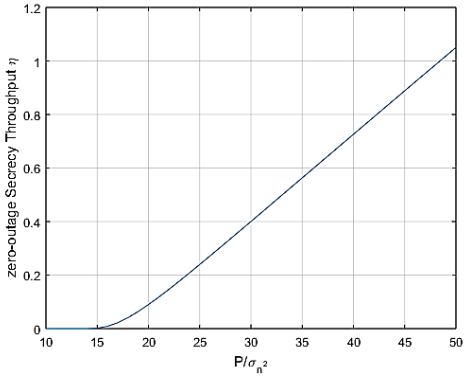

Figure 4. *η versus P/σ_n^2 when the optimum power allocation is applied.*

5. CONCLUSIONS

The paper proposed a simple strategy of secure transmissions in amplify-and-forward relaying systems to achieve zero-outage secrecy. A novel transmission strategy in amplifying-and-forwarding systems with the use of only one extra time slot for AN to guarantee zero-outage secrecy. The zero-outage secrecy throughput is then determined and characterized according to system parameters. The results showed that an optimum power allocation exists to maximize the secrecy throughput and that the throughput increases with increasing transmit power, which has not been achieved in the literature. This indicates the practical use of the proposed transmission strategy in security. For future work, extension to short packet transmission will be considered, and an information-theoretical study of zero-outage secrecy will be concerned when the secrecy coding is relaxed or not used.

APPENDIX A

In this Appendix, we will find the cumulative density function (CDF) of:

$$Z = \frac{aX/Y}{1 + bX/Y} \tag{20}$$

for $a, b > 0$, where X has exponential distribution with mean σ^2_X and Y not less than τ has exponential distribution with mean σ^2_Y. We will also find the probability density function (PDF):

$$W = \frac{aX}{1 + bX} \tag{21}$$

The CDF of Z is derived as

$$\begin{aligned} \Pr(Z < z) &= \Pr\left(X < Y\frac{z}{(a - bz)^+}\right) \\ &= 1 - \int_{\tau}^{\infty} \exp\left(-\frac{y}{\sigma_X^2}\frac{z}{(a - bz)^+}\right)\frac{\exp(-y/\sigma_Y^2)}{\sigma_Y^2}dy \\ &= 1 - \frac{\exp\left(-\frac{\tau}{\sigma_Y^2}\left(\frac{z\sigma_Y^2/\sigma_X^2}{(a - bz)^+}\right)\right)}{1 + \frac{z\sigma_Y^2/\sigma_X^2}{(a - bz)^+}} \end{aligned} \tag{22}$$

Also, since:

$$\Pr(W < \omega) = \Pr\left(X < \frac{\omega}{(a - b\omega)^+}\right) = 1 - \exp\left(-\frac{\omega/\sigma_X^2}{(a - b\omega)^+}\right) \tag{23}$$

The PDF of W for $\omega < a/b$ is given by:

$$p_W(\omega) = \frac{d\Pr(W < \omega)}{d\omega} = \frac{1/\sigma_X^2}{(a - b\omega)^2}\exp\left(-\frac{\omega/\sigma_X^2}{(a - b\omega)}\right) \tag{24}$$

REFERENCES

[1]. Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, *"Physical layer security in wireless networks: a tutorial,"* IEEE Wireless Communications, vol. 18, no. 2, pp. 66–74, (2011).

[2]. M. Bloch and J. Barros, *"Physical-Layer Security: From Information Theory to Security Engineering"*. Cambridge University Press, (2011).

[3]. S. Goel and R. Negi, *"Guaranteeing secrecy using artificial noise,"* IEEE transactions on wireless communications, Vol. 7, No. 6, pp. 2180–2189, (2008).

[4]. M. Ahmed and L. Bai, *"Secrecy capacity of artificial noise aided secure communication in mimorician channels,"* IEEE Access, Vol. 6, pp. 7921–7929, (2018).

[5]. G. Zheng, I. Krikidis, J. Li and A. P. Petropulu, *"Improving physical layer secrecy using full-duplex jamming receivers,"* IEEE Transactions on Signal Processing, Vol. 61, No. 20, pp. 4962–4974, (2013).

[6]. Z. Cao, X. Ji, J. Wang, S. Zhang, Y. Ji, Y. Li, and J. Wang, *"Security-reliability trade-off analysis of an-aided relay selection for full-duplex relay networks,"* IEEE Transactions on Vehicular Technology, Vol. 70, No. 3, pp. 2362–2377, (2021).

[7]. H. Q. Ta, L. Cao, and H. Oh, *"Novel noise injection scheme to guarantee zero secrecy outage under imperfect csi,"* Entropy, Vol. 25, No. 12, p. 1594, (2023).

[8]. I. S. Gradshteyn and I. M. Ryzhik, *"Table of integrals, series, and products"*. Elsevier/Academic Press, Amsterdam, seventh ed., (2007). Translated from the Russian, Translation edited and with a preface by Alan Jeffrey and Daniel Zwillinger, With one CD-ROM (Windows, Macintosh and UNIX).

[9]. X. Zhou, M. R. McKay and B. Maham *"Rethinking the secrecy outage formulation: A secure transmission design perspective,"* IEEE Communications Letters, Vol. 15, No. 3, pp. 302–304, (2011).

TÓM TẮT

Truyền thông trong mạng khuếch đại và chuyển tiếp với xác suất dừng bảo mật bằng không

Giải pháp mới chèn nhiễu nhân tạo (AN) được đề xuất trong hệ thống khuếch đại và chuyển tiếp (AF). Với giải pháp này, giới hạn tốc độ truyền tin bảo mật cũng như thông lượng được xác định để đảm bảo xác suất dừng bảo mật bằng không với bất kỳ nút nghe trộm nào. Kết quả cho thấy giải pháp truyền đơn giản và đạt được xác suất dừng bảo mật bằng không mà các giải pháp cũ không thực hiện được. Kết quả còn cho thấy với giải pháp này có thể tăng thông lượng bằng cách tăng công suất phát vượt qua giới hạn của các giải pháp bảo mật cũ.

Từ khoá: Chèn nhiễu nhân tạo; Xác suất dừng bảo mật.