TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 24, No. 2, April 2026, pp. 420~430
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v24i2.27314

Secure two-way relaying with successive interference cancellation and fountain codes: performance analysis

Nguyen Thi Hau[1,2], Tran Trung Duy[3]
[1]Department of Electronics and Telecommunication Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Ho Chi Minh City, Vietnam
[2]Faculty of Engineering and Technology, Saigon University, Ho Chi Minh City, Vietnam
[3]Faculty of Telecommunications 2, Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam

Article Info

Article history:

Received Apr 12, 2025
Revised Dec 1, 2025
Accepted Dec 8, 2025

Keywords:

Digital network coding
Fountain codes
Interference cancellation
Physical layer security
Two-way relaying

ABSTRACT

This paper proposes a secure two-way relaying (TWR) scheme using fountain codes (FCs), successive interference cancellation (SIC), and digital network coding (DNC). Using FCs, two sources exchange their data by first encoding the data into a series of packets (called encoded packets). These encoded packets are then exchanged between the sources via the help of a common relay, and they are also overheard by an eavesdropper. The packet exchange is carried out over two time slots: i) in the first time slot, both sources send their encoded packets to the rela y; and ii) the relay applies SIC to decode two received packets, and then broadcasts the exclusive OR (XORed) packet to both sources in the second time slot. The sources and the eavesdropper try to collect a sufficient number of encoded packets to successfully recover the original data. This paper derives and validates exact closed-form expressions for system throughput (TP), system outage probability (SOP), and system intercept probability (SIP) over Rayleigh fading channels. Furthermore, our findings reveal a reliability-security trade-off as well as the impact of system parameters on the network performance.

Corresponding Author:

Nguyen Thi Hau
Faculty of Engineering and Technology, Saigon University
273 An Duong Vuong Street, Cho Quan Ward, Ho Chi Minh City, Vietnam
Email: hau.nt@sgu.edu.vn

1. INTRODUCTION

Recently, two-way relaying (TWR) [1]-[4] has emerged as an effective technique for enhancing both data throughput and coverage in next-generation wireless communication systems. In TWR scheme, one or many intermediate relays assist the exchange of data between two source nodes [5]-[10]. In the conventional TWR scheme, 04 phases are used to exchange 02 packets between two sources. The researches [5], [6] combined digital network coding (DNC) and decoding and forward (DF) relaying to reduce 1 phase, resulting in data exchange occurring in 03 phases. In these schemes, two source nodes send their packets to the relay in the first two phases, the relay performs exclusive OR (XOR) operation on two encoded packets in the third phase, and broadcasts the XORed packet to both sources. Unlike the schemes proposed in [5]-[10] the TWR scheme in this work uses only two phases. Indeed, the relay nodes in [7]-[10] employ successive interference cancellation (SIC) to decode the received packets at the first phase, and forward the packets to two sources in the second phase. Huynh *et al*. [7], relay selection techniques were employed to enhance performance for the TWR schemes, while Dao and Son [10] proposed the TWR schemes using energy harvesting (EH). Additionally, the authors in [11], [12] explored reconfigurable intelligent surfaces (RIS)

working as a common relay to improve the spectral efficiency of two-way communication. However, the previous works [5]-[12] did not consider fountain codes (FCs) and physical-layer security (PLS).

Due to the broadcast of wireless channels, ensuring secure communication has become a critical challenge in the TWR networks. To achieve secure communication, PLS which exploits the natural characteristics of wireless channels such as fading, interference, and noise can be effectively applied to the TWR networks [13]-[15]. Cai *et al.* [13], proposed a randomize and forward (RanF) technique, where two source and relay nodes transmit different codewords to limit the overhearing ability of the eavesdropper. Liu *et al.* [14] introduced a secure amplify-and-forward (AF) TWR scheme-aided simultaneous wireless information and power transfer (SWIPT) technique where multi-antenna source and relay nodes operate in the full-duplex mode. Luo *et al*. [15], the PLS TWR models using intelligent reflecting surfaces (IRS) were proposed and analyzed.

Recently, the integration of error correction codes (ECC) and PLS to simultaneously enhance security and performance has emerged as a promising solution in wireless communication [16]. Following these approaches, FCs, known for their rateless property, offer significant advantages such as adaptability to dynamic channel conditions, simplified coding and decoding protocols, and robustness against packet loss, making them attract more attention in recent studies [17], [18]. To reconstruct the original data, receivers have to sufficiently collect encoded packets [19], [20]. According to [21], [22], achieving data security requires that legitimate users or destinations collect a sufficient number of encoded packets before eavesdroppers. Nguyen [23] analyzed the reliability-security trade-off (RST) in the secure TWR networks between two clusters of nodes using DNC. Unlike the authors in [23], [24] proposed TWR CR schemes that incorporate FCs, RIS, and wireless EH, where RIS can replace a relay node to facilitate data exchange between two source nodes.

To the best of our knowledge, the work in [25] is the study most closely related to our work. While [25] investigated a SIC-DNC-based TWR network employing FCs, its analysis was limited to the outage performance and therefore focused exclusively on the reliability of the system. However, modern wireless networks require not only high reliability but also robustness against eavesdropping threats [16]. Unlike [25], this paper extends the research by integrating a passive eavesdropper into the system model and conducting a comprehensive joint evaluation of reliability and security performance. In the proposed scheme, two source nodes exchange encoded packets via a DF relay in two time slots, while an eavesdropper attempts to intercept. During the first time slot, both sources transmit encoded packets to the relay, which employs SIC to decode the received packets. Then, the relay performs XOR on these packets and broadcasts the XORed packet to both sources in the second time slot. If two source nodes collect a sufficient number of encoded packets, they can reconstruct the desired data. Also, if the eavesdropper can correctly recover the original data, the data of the two sources is intercepted. We derive closed-form expressions for SOP and SIP, evaluate the reliability–security trade-off, and demonstrate how system parameters such as relay position, power allocation factor, and the maximum number of transmission times influence overall system performance. This comprehensive analysis offers deeper insights into the advantages that FCs introduce to the secure SIC-DNC-based TWR network that has not been explored in [25]. The remainder of the paper is organized as follows: section 2 presents the system model and scheme operation; section 3 analyzes performance; section 4 provides simulation and theoretical results; and section 5 concludes with a summary and future directions.

2. SECURE TWR WITH SIC AND FCs

2.1. System model

In the proposed scheme presented in Figure 1, since there exists no direct communication between two source nodes S_1 and S_2 due to the far distance, S_1 and S_2 have to exchange their data with the assistance of the relay (R) In the network, the eavesdropper (E) attempts to overhear the data sent from S_1 and S_2. All of the nodes are equipped with a single antenna and operate in a half-duplex mode. Let us denote $x_1(x_2)$ as the data sent from $S_1(S_2)$, and $p_1(p_2)$ as encoded packets of $S_1(S_2)$, respectively. Before transmission data takes place, $S_1(S_2)$ divides $x_1(x_2)$ into small packets, then perform XOR operation on these packets to continuously generate Fountain packets $p_1(p_2)$. The exchange of encoded packets in the proposed scheme occurs in two time slots. At the first time slot, both S_1 and S_2 simultaneously send p_1 and p_2 to R. Then, R uses SIC technique to decode p_1 and p_2. If both p_1 and p_2 are decoded correctly, R performs the XOR operation over p_1 and p_2 to make $p_\oplus$, where $p_\oplus = p_1 \oplus p_2$. In the second time slot, R broadcasts $p_\oplus$ to S_1 and S_2. If R only decodes p_1 (or p_2) successfully, it only transmits p_1 (or p_2) to S_2 (or S_1) in the second time slot.

Let $H_{\min}$ denote the number of encoded packets that S_1, S_2, and E need to obtain for reconstructing the data x_1 and x_2. Let $H_{\max}$ denote the maximum number of transmissions of S_1 and S_2, where $H_{\max} \geq H_{\min}$ [23]-[25]. We also denote d_{XY} and β as the distance between X and Y, and path-loss exponential, respectively,

where $X, Y \in \{S_1, S_2, R, E\}$. Let denote σ_0^2 as variance of Gaussian noises at all receivers. Finally, P_{S_1}, P_{S_2}, and P_R are denoted as transmit power of S_1, S_2, and R, respectively.

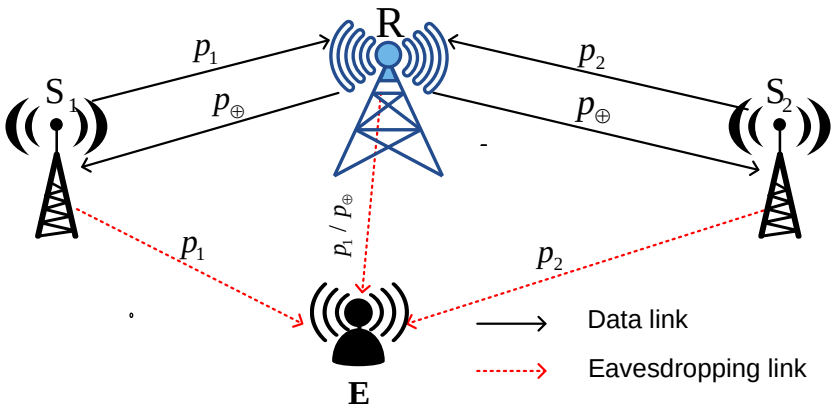

Figure 1. The proposed secure TWR scheme using FCs and SIC

Assume that all channels are block Rayleigh fading, where channel coefficients remain constant during one time slot, and change independently after each time slot. Let h_{XY} and $g_{XY} = |h_{XY}|^2$ denote channel coefficient and channel gain of between X and Y, respectively. As in studies [23]-[25], g_{XY} has cumulative distribution function (CDF) and probability density function (PDF), respectively as:

$$F_{g_{XY}}(x) = 1 - exp(-\lambda_{XY} x), f_{g_{XY}}(x) = \lambda_{XY}\, exp(-\lambda_{XY} x) \quad (1)$$

where $g_{XY} = (d_{XY})^{\beta}$ [23]-[25].

In practical scenarios, implementing such secure TWR schemes may face challenges related to hardware limitations, latency, and energy efficiency, which can affect real-time system performance. Moreover, the proposed secure TWR scheme can be extended to future 6G and IoT networks, where EH and hardware impairments (HIs) become important factors for practical deployment. However, in this study, we focus on analyzing the secure TWR scheme using SIC and FCs under ideal SIC conditions and without considering energy constraints or HIs at the nodes. These aspects are left for future research to evaluate their impact on the system's secrecy and reliability performance.

2.2. Transmit power formulation and transmission of encoded packets

For a fair comparison between our scheme (named SIC-2TS) and the conventional DNC scheme (named DNC-3TS), we assume that the total transmit power in two schemes is the same, i.e.,

$$P_{S_1} + P_{S_2} = 2P, P_R = P \quad (2)$$

Note that the transmit power of S_1, S_2 and R in the DNC-3TS scheme is $P_{S_1} = P_{S_1} = P_R = P$. Moreover, we propose a simple power allocation method for (2) as follows:

$$P_{S_1} = 2\alpha P, P_{S_1} = 2(1-\alpha)P \quad (3)$$

where α is a pre-designed power allocation factor and $0 < \alpha < 1$.

– Remark 1: without loss of generality, we can assume S_1 is nearer R than S_2, i.e., $d_{S_1R} < d_{S_2R}$. Hence, we can assume that the $S_1 \to R$ channel is better than the $S_2 \to R$, and hence, R uses SIC to decode p_1 first, treating the signal from S_2 as interference. After cancelling p_1, R decodes p_2.

In the first time slot, S_1 and S_2 at the same time transmit their packets to R. The signal-to-interference-plus-noise ratio (SNR) obtained at R for decoding p_1 and p_2, can be expressed, respectively as (see [26]):

$$\gamma_{S_1\to \mathrm{R},p_1}^{\text{SIC-2TS}} = \frac{P_{S_1} g_{S_1 R}}{P_{S_2} g_{S_2 R} + \sigma_0^2} = \frac{2\alpha \Delta g_{S_1 R}}{2(1-\alpha)\Delta g_{S_2 R} + 1}, \gamma_{S_2\to \mathrm{R},p_2}^{\text{SIC-2TS}} = \frac{P_{S_2} g_{S_2 R}}{\sigma_0^2} = 2(1-\alpha)\Delta g_{S_2 R}. \quad (4)$$

where $\Delta = \frac{P}{\sigma_0^2}$. Then, the corresponding channel capacity obtained at R can be given, respectively as:

$$C_{S_1\to \mathrm{R},p_1}^{\text{SIC-2TS}} = \frac{1}{2} log_2\left(1 + \gamma_{S_1\to \mathrm{R},p_1}^{\text{SIC-2TS}}\right), C_{S_2\to \mathrm{R},p_2}^{\text{SIC-2TS}} = \frac{1}{2} log_2\left(1 + \gamma_{S_2\to \mathrm{R},p_2}^{\text{SIC-2TS}}\right) \quad (5)$$

where the factor $1/2$ implies that the packet exchange is carried out over two time slots.

Similar to R, E also employs SIC to detect p_1 and p_2 in the first time slot. Hence, the instantaneous channel capacity obtained at E to decode p_1 and p_2 can be expressed, respectively, as:

$$C_{S_1\to \mathrm{E},p_1}^{\text{SIC-2TS}} = \frac{1}{2} log_2\left(1 + \frac{2\alpha \Delta g_{S_1 E}}{2(1-\alpha)\Delta g_{S_2 E} + 1}\right), C_{S_2\to \mathrm{E},p_2}^{\text{SIC-2TS}} = \frac{1}{2} log_2\left(1 + 2(1-\alpha)\Delta g_{S_2 E}\right). \quad (6)$$

– Remark 2: we also assume that $d_{S_1 E} < d_{S_2 E}$, and similar to R, E will decode p_1 first. Note that if $d_{S_1 E} \geq d_{S_2 E}$, the IP/SIP performance at E is worse than those with $d_{S_1 E} < d_{S_2 E}$. Next, assume that the packet $p_i (i = 1,2)$ can be correctly decoded by $A (A \in \{\mathrm{R},\mathrm{E}\})$ if $C_A^{p_i} \geq C_{\text{th}}$, where C_{th} is an outage threshold. If $C_A^{p_i} < C_{\text{th}}$, the decoding of p_i at A fails. Hence, there are three possible cases regarding the decoding status at R as follows:

Case 1: if R can correctly decode both p_1 and p_2, and it then broadcasts $p_\oplus$ to both S_1 and S_2 in the second time slot. Therefore, the capacity of the $R \to B$ links ($B \in \{S_1, S_2, E\}$) can be formulated as:

$$C_{R\to \mathrm{B},p_\oplus}^{\text{SIC-2TS}} = \frac{1}{2} log_2(1 + \Delta g_{\mathrm{RB}}) \quad (7)$$

Case 2: if R can only decode p_1 correctly, it will transmit p_1 to S_2 in the second time slot. In this case, the channel capacity of the $R \to C$ links ($C \in \{S_2, E\}$) links can be given as:

$$C_{R\to \mathrm{C},p_1}^{\text{SIC-2TS}} = \frac{1}{2} log_2(1 + \Delta g_{\mathrm{RC}}) \quad (8)$$

Case 3: in this case, R cannot decode both p_1 and p_2, and there is no transmission at the second phase.

Next, we consider the DNC-3TS scheme, where each packet exchange is performed via three time slots: i) S_1 transmits p_1 to R at the first time slot; ii) S_2 transmits p_2 to R at the second time slot; iii) R broadcasts $p_\oplus$ to S_1 and S_2 at the third time slot. It is also worth noting that if R only decodes p_1 or p_2 correctly, it will send $p_1 (p_2)$ to $S_2 (S_1)$ at the third time slot. Therefore, we can formulate the channel capacity obtained at the node Y, due to the transmission of the packet p_* of the node X, as follows:

$$C_{X\to Y,p_*}^{\text{DNC-3TS}} = \frac{1}{3} log_2(1 + \Delta g_{\mathrm{XY}}). \quad (9)$$

where $p_* \in \{p_1, p_2, p_\oplus\}$.

3. PERFORMANCE EVALUATION

This section derives exact closed-form expressions of system throughput (TP), SOP and SIP for the SIC-2TS and DNC-3TS schemes. Now, we will calculate the probability that the node B in SIC-2TS and DNC-3TS can correctly receive one encoded packet p_i.

3.1. Decoding probability of one encoded packet

In SIC-2TS, the probability that one packet p_1 is successfully reached to S_2 can be formulated as:

$$\begin{aligned}\psi_{\mathrm{S}_2,p_1}^{\text{SIC-2TS}} &= \Pr\left(C_{\mathrm{S}_1\to \mathrm{R},p_1}^{\text{SIC-2TS}} \geq C_{\text{th}}\right)\Pr\left(C_{\mathrm{R}\to \mathrm{S}_2,p_{**}}^{\text{SIC-2TS}} \geq C_{\text{th}}\right) = \Pr\left(g_{\mathrm{S}_1\mathrm{R}} \geq \rho_1 g_{\mathrm{S}_2\mathrm{R}} + \rho_0\right)\Pr\left(g_{\mathrm{RS}_2} \geq \rho_2\right) \\ &= \left[\int_0^{+\infty}\left(1 - F_{g_{\mathrm{S}_2\mathrm{R}}}(\rho_1 x + \rho_0)\right) f_{g_{\mathrm{S}_2\mathrm{R}}}(x)\,dx\right]\left(1 - F_{\mathrm{RS}_2}(\rho_2)\right) = \frac{\lambda_{\mathrm{S}_2\mathrm{R}}}{\lambda_{\mathrm{S}_2\mathrm{R}} + \lambda_{\mathrm{S}_1\mathrm{R}}\rho_1}\exp\left(-\lambda_{\mathrm{S}_1\mathrm{R}}\rho_0 - \lambda_{\mathrm{S}_2\mathrm{R}}\rho_2\right).\end{aligned} \quad (10)$$

where $p_{**} \in \{p_1, p_\oplus\}$, $\gamma_{\text{th}} = 2^{2C_{\text{th}}} - 1$, $\rho_0 = \frac{\gamma_{\text{th}}}{2\alpha\Delta}$, $\rho_1 = \frac{(1-\alpha)\gamma_{\text{th}}}{\alpha}$ and $\rho_2 = \frac{\gamma_{\text{th}}}{\Delta}$.

Considering the source S_1, the probability that it correctly receives one packet p_2 can be given as:

$$\begin{aligned}\psi_{S_1,p_2}^{\text{SIC-2TS}} &= Pr\left(C_{S_1\to \text{R},p_1}^{\text{SIC-2TS}} \geq C_{\text{th}}, C_{S_2\to \text{R},p_2}^{\text{SIC-2TS}} \geq C_{\text{th}}\right) Pr\left(C_{R\to S_1,p_\oplus}^{\text{SIC-2TS}} \geq C_{\text{th}}\right) \\ &= Pr\left(g_{S_1R} \geq \rho_0 + \rho_1 g_{S_2R}, g_{S_2R} \geq \rho_3\right) Pr\left(g_{\text{RS}_1} \geq \rho_2\right) \\ &= \left[\int_{\rho_3}^{+\infty} f_{g_{S_2R}}(x)\left(1 - F_{g_{S_1R}}(\rho_0 + \rho_1 x)\right) dx\right]\left(1 - F_{g_{\text{RS}_1}}(\rho_2)\right)\end{aligned} \tag{11}$$

where $\rho_3 = \frac{\gamma_{\text{th}}}{2(1-\alpha)\Delta}$. We note here that to correctly decode p_2, R must correctly decode p_1 first.

Then, substituting (1) into (11), after some manipulations, we have:

$$\psi_{S_1,p_2}^{\text{SIC-2TS}} = \frac{\lambda_{S_2R}}{\lambda_{S_2R}+\lambda_{S_1R}\rho_1} exp\left(-\lambda_{S_1R}(\rho_0 + \rho_2)\right) exp\left(-\left(\lambda_{S_2R} + \lambda_{S_1R}\rho_1\right)\rho_3\right) \tag{12}$$

Next, the probability that E intercepts one packet p_1 in SIC-2TS can be formulated as:

$$\begin{aligned}\zeta_{E,p_1}^{\text{SIC-2TS}} &= Pr\left(C_{S_1\to \text{E},p_1}^{\text{SIC-2TS}} \geq C_{\text{th}}\right) + Pr\left(C_{S_1\to \text{E},p_1}^{\text{SIC-2TS}} < C_{\text{th}}\right) Pr\left(C_{S_1\to \text{R},p_1}^{\text{SIC-2TS}} \geq C_{\text{th}}, C_{S_2\to \text{R},p_2}^{\text{SIC-2TS}} < C_{\text{th}}\right) Pr\left(C_{R\to \text{E},p_1}^{\text{SIC-2TS}} \geq C_{\text{th}}\right) \\ &= \underbrace{Pr\left(g_{S_1E} \geq \rho_1 g_{S_2E} + \rho_0\right)}_{I_1} + \underbrace{Pr\left(g_{S_1E} < \rho_1 g_{S_2E} + \rho_0\right) Pr\left(g_{S_1R} \geq \rho_0 + \rho_1 g_{S_2R}, g_{S_2R} < \rho_3\right) Pr\left(g_{\text{RE}} \geq \rho_2\right)}_{I_2}\end{aligned} \tag{13}$$

In (13), I_1 is the probability that E can correctly decode p_1 received from S_1 at the first time slot, and I_2 is the probability that E can correctly decode p_1 from R at the second time slot. Similar to (10) and (11), we have the following results:

$$I_1 = \frac{\lambda_{S_2E}}{\lambda_{S_2E}+\lambda_{S_1E}\rho_1} exp\left(-\lambda_{S_1E}\rho_0\right), Pr\left(g_{\text{RE}} \geq \rho_2\right) = exp\left(-\lambda_{\text{RE}}\rho_2\right) \tag{14}$$

$$Pr\left(g_{S_1R} \geq \rho_0 + \rho_1 g_{S_2R}, g_{S_2R} < \rho_3\right) = \frac{\lambda_{S_2R}\, exp\left(-\lambda_{S_1R}\rho_0\right)}{\lambda_{S_2R}+\lambda_{S_1R}\rho_1}\left(1 - exp\left(-\left(\lambda_{S_1R}\rho_1 + \lambda_{S_2R}\right)\rho_3\right)\right) \tag{15}$$

Substituting (14) and (15) into (13), we obtain an exact closed-form expression of $\zeta_{E,p_1}^{\text{SIC-2TS}}$ as:

$$\begin{aligned}\zeta_{\text{E},p_1}^{\text{SIC-2TS}} &= \frac{\lambda_{\text{S}_2\text{E}} \exp\left(-\lambda_{\text{S}_1\text{E}}\rho_0\right)}{\lambda_{\text{S}_2\text{E}} + \lambda_{\text{S}_1\text{E}}\rho_1} \\ &\quad + \left(1 - \frac{\lambda_{\text{S}_2\text{E}} \exp\left(-\lambda_{\text{S}_1\text{E}}\rho_0\right)}{\lambda_{\text{S}_2\text{E}} + \lambda_{\text{S}_1\text{E}}\rho_1}\right)\left[\frac{\lambda_{\text{S}_2\text{R}} \exp\left(-\lambda_{\text{S}_1\text{R}}\rho_0 - \lambda_{\text{RE}}\rho_2\right)}{\lambda_{\text{S}_2\text{R}} + \lambda_{\text{S}_1\text{R}}\rho_1}\left(1 - \exp\left(-\left(\lambda_{\text{S}_1\text{R}}\rho_1 + \lambda_{\text{S}_2\text{R}}\right)\rho_3\right)\right)\right].\end{aligned} \tag{16}$$

Also, the probability that E intercepts one packet p_2 in SIC-2TS can be formulated as:

$$\begin{aligned}\zeta_{\text{E},p_2}^{\text{SIC-2TS}} &= \Pr\left(C_{\text{S}_1\to\text{E},p_1}^{\text{SIC-2TS}} \geq C_{\text{th}}, C_{\text{S}_2\to\text{E},p_2}^{\text{SIC-2TS}} \geq C_{\text{th}}\right) \\ &\quad + \Pr\left(C_{\text{S}_1\to\text{E},p_1}^{\text{SIC-2TS}} \geq C_{\text{th}}, C_{\text{S}_2\to\text{E},p_2}^{\text{SIC-2TS}} < C_{\text{th}}\right)\Pr\left(C_{\text{S}_1\to\text{R},p_1}^{\text{SIC-2TS}} \geq C_{\text{th}}, C_{\text{S}_2\to\text{R},p_2}^{\text{SIC-2TS}} \geq C_{\text{th}}\right)\Pr\left(C_{\text{R}\to\text{E},p_\oplus}^{\text{SIC-2TS}} \geq C_{\text{th}}\right) \\ &= \underbrace{\Pr\left(g_{\text{S}_1\text{E}} \geq \rho_0 + \rho_1 g_{\text{S}_2\text{E}}, g_{\text{S}_2\text{E}} \geq \rho_3\right)}_{I_3} \\ &\quad + \underbrace{\Pr\left(g_{\text{S}_1\text{E}} \geq \rho_0 + \rho_1 g_{\text{S}_2\text{E}}, g_{\text{S}_2\text{E}} < \rho_3\right)\Pr\left(g_{\text{S}_1\text{R}} \geq \rho_0 + \rho_1 g_{\text{S}_2\text{R}}, g_{\text{S}_2\text{R}} \geq \rho_3\right)\Pr\left(g_{\text{RE}} \geq \rho_2\right)}_{I_4}.\end{aligned} \tag{17}$$

In (17), I_3 is the probability that E can correctly decode p_2 received from S_2 at the first time slot, and I_4 is the probability that E can correctly decode p_1 and $p_\oplus$ from S_1 and R at the first and second time slot, respectively, and then E can obtain p_2 by performing the XOR operation between p_1 and $p_\oplus$.

Using the results in (10), (11), (14) and (15) to calculate the probabilities in (17), we finally obtain:

$$\zeta_{E,p_2}^{\text{SIC-2TS}} = \frac{\lambda_{S_2E}\, exp\left(-\lambda_{S_1E}\rho_0-(\lambda_{S_2E}+\lambda_{S_1E}\rho_1)\rho_3\right)}{\lambda_{S_2E}+\lambda_{S_1E}\rho_1} + \frac{\lambda_{S_2E}\lambda_{S_2R}\, exp\left(-(\lambda_{S_1E}+\lambda_{S_1R})\rho_0-(\lambda_{S_2R}+\lambda_{S_1R}\rho_1)\rho_3-\lambda_{\text{RE}}\rho_2\right)}{(\lambda_{S_2E}+\lambda_{S_1E}\rho_1)(\lambda_{S_2R}+\lambda_{S_1R}\rho_1)}\left(1-exp\left(-\left(\lambda_{S_2E}+\lambda_{S_1E}\rho_1\right)\rho_3\right)\right) \quad (18)$$

Considering the DNC-3TS scheme, the probability that one packet $p_1(p_2)$ is correctly decoded by the source $S_2(S_1)$ can be computed exactly as:

$$\psi_{S_2,p_1}^{\text{DNC-3TS}} = Pr\left(C_{S_1\to\text{R},p_1}^{\text{DNC-3TS}} \geq C_{\text{th}}\right) Pr\left(C_{R\to S_2,p_1}^{\text{DNC-3TS}} \geq C_{\text{th}}\right) = exp\left(-\left(\lambda_{S_1R}+\lambda_{S_2R}\right)\rho_4\right), \psi_{S_1,p_2}^{\text{DNC-3TS}} = Pr\left(C_{S_1\to\text{R},p_2}^{\text{DNC-3TS}} \geq C_{\text{th}}\right) Pr\left(C_{R\to S_1,p_2}^{\text{DNC-3TS}} \geq C_{\text{th}}\right) = exp\left(-\left(\lambda_{S_2R}+\lambda_{S_1R}\right)\rho_4\right) \quad (19)$$

where $\rho_4 = \frac{2^{3C_{\text{th}}}-1}{\Delta}$.

Finally, the probability that E intercepts one packet $p_1(p_2)$ in DNC-3TS is computed as:

$$\zeta_{E,p_1}^{\text{DNC-3TS}} = Pr\left(C_{S_1\to\text{E},p_1}^{\text{DNC-3TS}} \geq C_{\text{th}}\right) + Pr\left(C_{S_1\to\text{E},p_1}^{\text{DNC-3TS}} < C_{\text{th}}\right) Pr\left(C_{S_1\to\text{R},p_1}^{\text{DNC-3TS}} \geq C_{\text{th}}\right) Pr\left(C_{S_2\to\text{R},p_2}^{\text{DNC-3TS}} < C_{\text{th}}\right) Pr\left(C_{R\to\text{E},p_1}^{\text{DNC-3TS}} \geq C_{\text{th}}\right) + Pr\left(C_{S_1\to E,p_1}^{DNC\text{-}3TS} < C_{th}\right) Pr\left(C_{S_1\to R,p_1}^{DNC\text{-}3TS} \geq C_{th}\right) Pr\left(C_{S_2\to R,p_2}^{DNC\text{-}3TS} \geq C_{th}\right) Pr\left(C_{S_2\to E,p_2}^{DNC\text{-}3TS} \geq C_{th}\right) Pr\left(C_{R\to\text{E},p_\oplus}^{\text{DNC-3TS}} \geq C_{\text{th}}\right) = exp\left(-\lambda_{S_1E}\rho_4\right) + \left(1-exp\left(-\lambda_{S_1E}\rho_4\right)\right) exp\left(-\left(\lambda_{S_1R}+\lambda_{\text{RE}}\right)\rho_4\right)\left(1-exp\left(-\lambda_{S_2R}\rho_4\right)+exp\left(-\left(\lambda_{S_2R}+\lambda_{S_2E}\right)\rho_4\right)\right) \quad (20)$$

$$\zeta_{E,p_2}^{DNC\text{-}3TS} = Pr\left(C_{S_2\to E,p_2}^{DNC\text{-}3TS} \geq C_{th}\right) + Pr\left(C_{S_2\to E,p_2}^{DNC\text{-}3TS} < C_{th}\right) Pr\left(C_{S_2\to R,p_2}^{DNC\text{-}3TS} \geq C_{th}\right) Pr\left(C_{S_1\to R,p_1}^{DNC\text{-}3TS} < C_{th}\right) Pr\left(C_{R\to E,p_2}^{DNC\text{-}3TS} \geq C_{th}\right) + Pr\left(C_{S_2\to E,p_2}^{DNC\text{-}3TS} < C_{th}\right) Pr\left(C_{S_1\to R,p_1}^{DNC\text{-}3TS} \geq C_{th}\right) Pr\left(C_{S_2\to R,p_2}^{DNC\text{-}3TS} \geq C_{th}\right) Pr\left(C_{S_1\to E,p_1}^{DNC\text{-}3TS} \geq C_{th}\right) Pr\left(C_{R\to E,p_\oplus}^{DNC\text{-}3TS} \geq C_{th}\right) = exp\left(-\lambda_{S_2E}\rho_4\right) + \left(1-exp\left(-\lambda_{S_2E}\rho_4\right)\right) exp\left(-\left(\lambda_{S_2R}+\lambda_{RE}\right)\rho_4\right)\begin{pmatrix}1-exp\left(-\lambda_{S_1R}\rho_4\right)\\ +exp\left(-\left(\lambda_{S_1R}+\lambda_{S_1E}\right)\rho_4\right)\end{pmatrix} \quad (21)$$

3.2. OP (SOP) and IP (SIP) performance of SIC-2TS and DNC-3TS

At first, OP at the source $S_i(i=1,2)$ is defined as the probability that S_i cannot gather enough H_{min} packets $p_j(j=1,2, j\neq i)$ after the transmission ends, while IP at E (with respect to x_i) is the probability that E can collect at least H_{min} packets p_i. Therefore, OP at $S_i(i=1,2)$ in the proposed SIC-2TS scheme can be obtained as:

$$\text{OP}_{S_i}^{\text{SIC-2TS}} = \sum_{n=0}^{H_{min}\Sigma\left(\psi_{S_i,p_j}^{\text{SIC-2TS}}\right)^n\left(1-\psi_{S_i,p_j}^{\text{SIC-2TS}}\right)^{H_{max}}}\binom{H_{max}}{n} \quad (22)$$

where $\binom{H_{max}}{n}$ is the binomial coefficient, i.e., $\binom{H_{max}}{n}\frac{(H_{max}())}{n!(H_{max}()).}$

Then, IP at E in SIC-2TS, with respect to the data x_i, can be expressed as:

$$\text{IP}_{E,x_i}^{\text{SIC-2TS}} = \sum_{n=H_{min}}^{H_{max}\Sigma\left(\zeta_{E,p_i}^{\text{SIC-2TS}}\right)^n\left(1-\zeta_{E,p_i}^{\text{SIC-2TS}}\right)^{H_{max}}}\binom{H_{max}}{n} \quad (23)$$

For the DNC-3TS scheme, OP at S_i and IP with respect to x_i can be computed, respectively as:

$$\begin{aligned}\text{OP}_{\text{S}_i}^{\text{DNC-3TS}} &= \sum_{n=0}^{H_{\min}-1}\binom{H_{\max}}{n}\left(\psi_{\text{S}_i,p_j}^{\text{DNC-3TS}}\right)^n\left(1-\psi_{\text{S}_i,p_j}^{\text{DNC-3TS}}\right)^{H_{\max}-n},\\ \text{IP}_{\text{E},x_i}^{\text{DNC-3TS}} &= \sum_{n=H_{\min}}^{H_{\max}}\binom{H_{\max}}{n}\left(\zeta_{\text{E},p_i}^{\text{DNC-3TS}}\right)^n\left(1-\zeta_{\text{E},p_i}^{\text{DNC-3TS}}\right)^{H_{\max}-n}.\end{aligned} \quad (24)$$

Next, SOP of the T scheme is defined as the probability that one of two sources in the T scheme is in outage, and SIP of the T scheme is defined as the probability that the data x_1 or x_2 is intercepted, where $T \in$ {SIC-2TS,DNC-3TS}. Therefore, we can express SOP and SIP in the T scheme, respectively as:

$$\text{SOP}^T = 1-\left(1-\text{OP}_{S_1}^T\right)\left(1-\text{OP}_{S_2}^T\right), \text{SIP}^T = 1-\left(1-\text{IP}_{E,x_1}^T\right)\left(1-\text{IP}_{E,x_2}^T\right). \quad (25)$$

3.3. Throughput of SIC-2TS and DNC-3TS

This subsection evaluates the TP of the SIC-2TS and DNC-3TS schemes at the target rate C_{th}. Indeed, TP of SIC-2TS and DNC-3TS can be expressed, respectively as:

$$\text{TP}^{\text{SIC-2TS}} = \frac{C_{\text{th}}}{2}\left(1 - \text{OP}_{S_1}^{\text{SIC-2TS}}\right) + \frac{C_{\text{th}}}{2}\left(1 - \text{OP}_{S_2}^{\text{SIC-2TS}}\right), \text{TP}^{\text{DNC-3TS}} = \frac{C_{\text{th}}}{3}\left(1 - \text{OP}_{S_1}^{\text{DNC-3TS}}\right) + \frac{C_{\text{th}}}{3}\left(1 - \text{OP}_{S_2}^{\text{DNC-3TS}}\right). \quad (26)$$

4. RESULTS AND DISCUSSION

This section presents both simulation and theoretical results of TP, SOP and SIP for SIC-2TS and DNC-3TS. In the simulations, we place all nodes at the following positions: $\text{S}_1(0,0)$, $S_2(1,0)$, $E(x_E, y_E) = E(0.2,-1)$, and $R(x_R, 0)$, where $0 < x_R < 0.5$. Next, for the illustration only, we fix the values of several system parameters by $\beta = 3$, $\sigma_0^2 = 1$, $C_{\text{th}} = 1$, and H_{min}.

Figure 2 shows the TP of the considered schemes as a function of the transmit SNR Δ (dB) with $H_{\text{max}} = 7, x_R = 0.35$, and $\alpha = \{0.6, 0.8\}$. As seen from Figure 2, TP of SIC-2TS scheme is higher than that of DNC-3TS, and TP of both schemes increase when Δ (dB) increases. Moreover, TP of SIC-2TS is higher with $\alpha = 0.8$.

Figure 3 compares TP of SIC-2TS and DNC-3TS as α changes, and with $H_{\text{max}} = 7$, $x_R = \{0.15, 0.3\}, \Delta = 10(\text{dB})$, and $E(0.2,-1)$. As observed from Figure 3, the TP performance of DNC-3TS is not affected by the value of α, while our scheme can obtain the highest throughput at $\alpha = 0.4$ (as $x_R = 0.15$), and at $\alpha = 0.7$ (as $x_R = 0.3$). It is seen from Figure 3 that if the value of α is not designed appropriately, TP of SIC-2TS may be lower than that of DNC-3TS. From Figures 2 and 3, it is worth noting that the simulation results validate the theoretical ones.

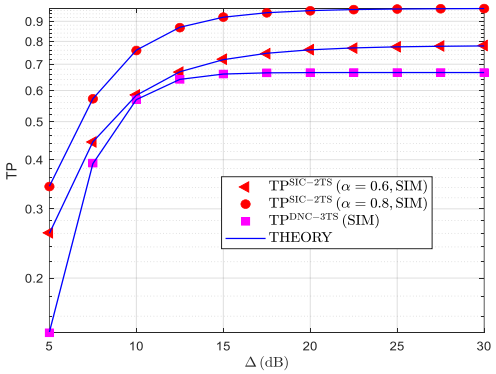

Figure 2. TP versus Δ (dB) with $\text{H}_{max} = 7$, $\text{x}_\text{R} = 0.35$, and $\alpha = \{0.6, 0.8\}$

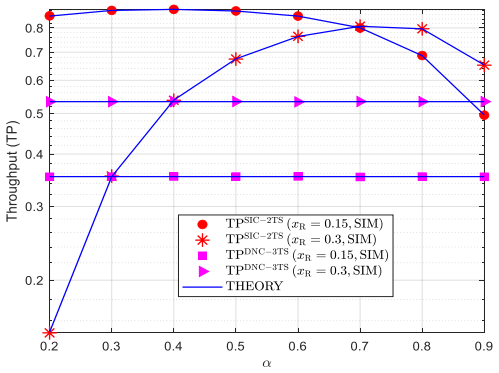

Figure 3. TP versus α with $H_{max} = 7$, $x_\text{R} = \{0.15, 0.3\}$, and $\Delta = 10(\text{dB})$

Figure 4 illustrates the TP performance as a function of x_R when $H_{max}\Delta = 10(\text{dB})$, and $\alpha = \{0.6, 0.7, 0.8\}$. It can be seen from Figure 4 that as $\alpha = 0.6, \alpha = 0.7$, and $\alpha = 0.8$, SIC-2TS can achieve the highest throughput at $x_R = 0.2$, $x_R = 0.25$ and $x_R = 0.3$, respectively. In contrast, TP of DNC-3TS increases with the increase of x_R. Finally, we can see that when the relay is placed near S_1 (x_R is low), the throughput of SIC-2TS is much higher than that of DNC-3TS.

In Figure 5, we compare the SOP and SIP of two considered schemes as Δ changes and with $\text{H}_{max} = 7$, $x_R = 0.15, \alpha = \{0.6, 0.8\}$, and $E(0.2,-1)$. We see that as Δ increases, SOP of SIC-2TS and DNC-3TS decreases, but SIP of SIC-2TS and DNC-3TS increases. We also see that the SOP of SIC-2TS is lower than SOP of DNC-3TS at low and medium SNR values. In addition, SIP of DNC-3TS is almost higher than SIP of SIC-2TS. It is also seen that SIP of SIC-2TS with $\alpha = 0.8$ is higher than that with $\alpha = 0.6$, while SOP of SIC-2TS with $\alpha = 0.8$ is only lower than that with $\alpha = 0.6$ as $\Delta \geq 25$ dB.

Figures 6 and 7 present the SOP and SIP performance versus α and H_{max}, respectively. From Figure 6, the DNC-3TS scheme obtains better SOP performance, as compared with the SIC-2TS scheme. However, the SIP performance of SIC-2TS is much better than that of DNC-3TS. In low α range, increasing α can improve

SOP performance, whereas it degrades the SIP performance of SIC-2TS scheme. This is due to the fact that the power allocated for two sources becomes more balanced, enabling effective SIC technique at relay with these α values, and improving decoding performance for both the relay and eavesdropper. As a result, SOP decreases while SIP increases.

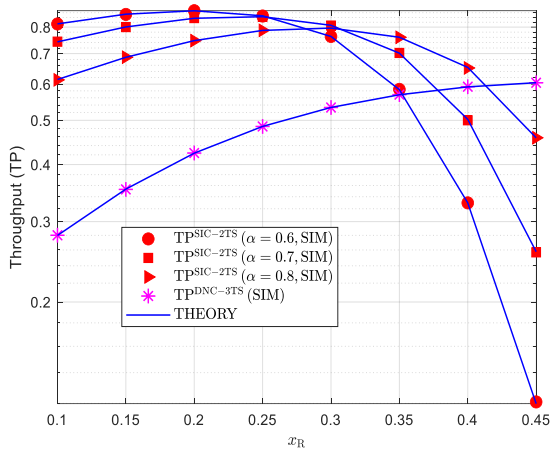

Figure 4. TP versus x_{R} with $H_{max} = 7$, $\Delta = 10$(dB), and $\alpha = \{0.6,0.7,0.8\}$

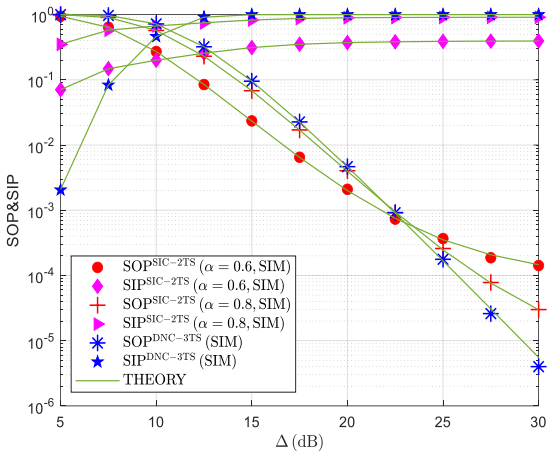

Figure 5. SOP and SIP versus Δ (dB) with $H_{max} = 7$, $x_R = 0.15$, and $\alpha = \{0.6,0.8\}$

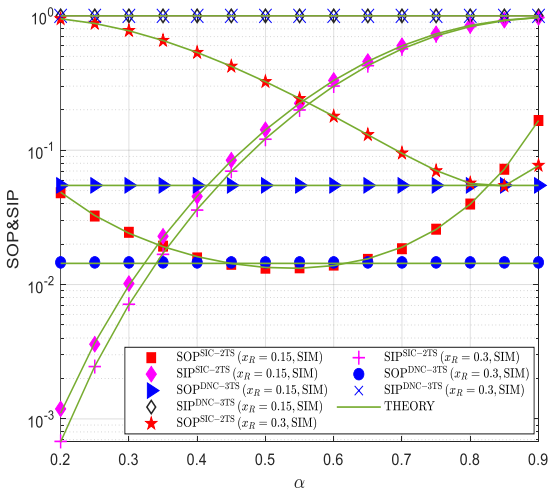

Figure 6. SOP and SIP versus α with $H_{max} = 7$, $x_{\mathrm{R}} = \{0.15,0.3\}$, and $\Delta = 16$(dB)

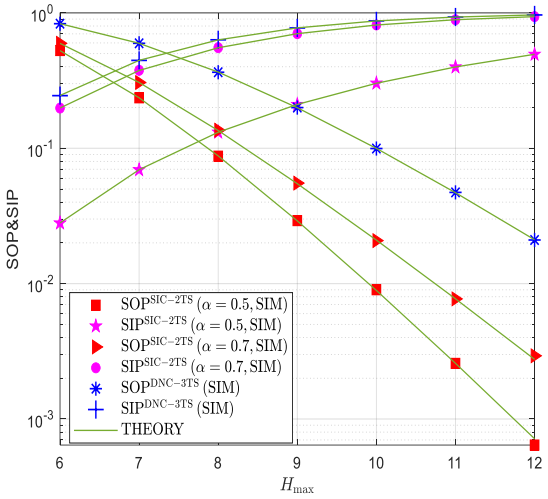

Figure 7. SOP and SIP versus H_{max} with $\alpha = \{0.5,0.7\}$, $\Delta = 10$ (dB), and $x_R = 0.2$

Like Hau *et al*. [25] Figure 6 also shows that there exist optimal power allocation factors corresponding to the relay's positions, where the SOP performance of our scheme is best. However, unlike [25], the optimal (x_R, α)value in SIC-2TS scheme appears in the low α range rather than at high α due to differences in the adopted power allocation method.

Figure 7 shows that the SIC-2TS scheme consistently outperforms the DNC-3TS scheme in terms of both the SOP and SIP performance. Next, when H_{max} increases, SOP in both schemes decreases, but SIP increases. This is due to the fact that all receivers in two considered schemes have more opportunities to collect a sufficient number of encoded packets for the data recovery.

The results in Figure 8 indicate that the position of the relay significantly impacts both the SOP and SIP performance of the SIC-2TS and DNC-3TS schemes. When x_R is low (i.e., x_R is less than 0.27), the SOP performance of SIC-2TS is better than that of DNC-3TS. Moreover, SIC-2TS can achieve better SIP performance than DNC-3TS for all x_R values.

Figure 9 shows the trade-off between SIP and SOP of the SIC-2TS and DNC-3TS schemes. At first, Figure 9 shows that achieving a lower SOP value leads to higher SIP values for both schemes, indicating SOP-SIP trade-off. We can see that SIC-2TS obtains much better SOP-SIP trade-off performance, i.e., at the same SOP values, the SIP value of SIC-2TS is much lower than that of DNC-3TS. Moreover, the SOP-SIP trade-off performance of SIC-2TS is better as H_{max} decreases, while that of DNC-3TS is better with higher H_{max}.

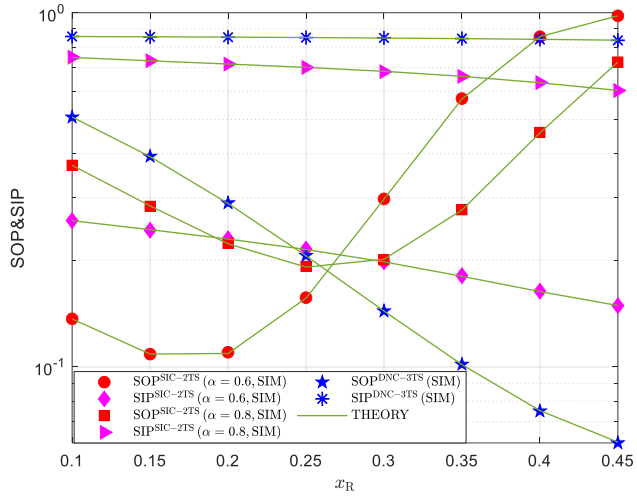

Figure 8. SOP and SIP versus x_R with $H_{max} = 7$, $\Delta = 12(\text{dB})$, and $\alpha = \{0.6,0.8\}$

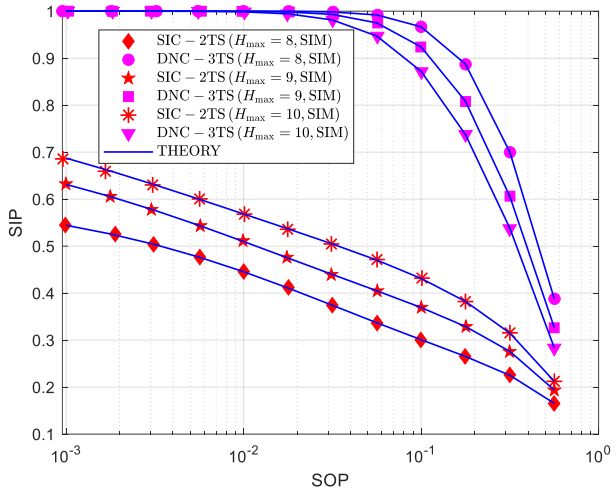

Figure 9. SIP-SOP trade-off when $\alpha = 0.6$, $x_R = 0.2$, with different H_{max} values

5. CONCLUSION

This paper proposed and evaluated the SOP and SIP performance of the secure TWR scheme employing FCs, SIC, and DNC through theoretical analysis and Monte-Carlo simulations. The study also examined the impact of key system parameters, including the relay's position, the power allocation factor, and the maximum number of transmission times, on throughput, SOP, and SIP. The obtained results showed that optimal power allocation to the two sources enhances performance, with higher power allocation factors improving SOP. In addition, when any user is closer to the relay, we can also achieve better SOP performance. Notably, the results demonstrate that the best SOP and SIP performance can be achieved by optimizing the relay's position, the power allocation factor, and the maximum number of transmission times. For the SOP-SIP trade-off, the findings revealed an inherent trade-off between SOP and SIP depending on

these parameters in both schemes, and SIC-2TS scheme can obtain better SOP-SIP trade-off performance with lower H_{max} values. Future research will further extend the proposed secure TWR scheme by incorporating EH and HIs effects to evaluate its applicability in emerging 6G and IoT communication scenarios.

FUNDING INFORMATION

This work is a part of the research project CS.2025.B1.024 funded by Saigon University.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Nguyen Thi Hau	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Tran Trung Duy	✓		✓	✓			✓			✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Derived data supporting the findings of this study are available from the corresponding author.

REFERENCES

[1] H. Cao, L. Fu, and H. Dai, "Throughput analysis of the two-way relay system with network coding and energy harvesting," in *2017 IEEE International Conference on Communications (ICC)*, IEEE, May 2017, pp. 1–6, doi: 10.1109/ICC.2017.7997272.
[2] Y. Liu, C. Yan, H. Yang, X. Bai, and L. Cong, "Optimal power splitting in wireless powered communication network with two-way relay," in *2017 IEEE 17th International Conference on Communication Technology (ICCT)*, IEEE, Oct. 2017, pp. 545–548, doi: 10.1109/ICCT.2017.8359695.
[3] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. M. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1714–1725, Oct. 2016, doi: 10.1109/TII.2015.2489610.
[4] J. Wang, G. Wang, B. Li, H. Yang, Y. Hu, and A. Schmeink, "Massive MIMO two-way relaying systems with SWIPT in IoT networks," *IEEE Internet of Things Journal*, vol. 8, no. 20, pp. 15126–15139, Oct. 2021, doi: 10.1109/JIOT.2020.3032446.
[5] P. N. Son and H. Y. Kong, "Improvement of the two-way decode-and-forward scheme by energy harvesting and digital network coding relay," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 3, Mar. 2017, doi: 10.1002/ett.2960.
[6] P. N. Son and H. Y. Kong, "Exact outage probability of two-way decode-and-forward scheme with opportunistic relay selection under physical layer security," *Wireless Personal Communications*, vol. 77, no. 4, pp. 2889–2917, Aug. 2014, doi: 10.1007/s11277-014-1674-6.
[7] T. P. Huynh, P. N. Son, and M. Voznak, "Exact outage probability of two-way decode-and-forward NOMA scheme with opportunistic relay selection," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 12, pp. 5862–5887, Dec. 2019, doi: 10.3837/tiis.2019.12.005.
[8] X. Wang, M. Jia, I. W.-H. Ho, Q. Guo, and F. C. M. Lau, "Exploiting Full-Duplex Two-Way Relay Cooperative Non-Orthogonal Multiple Access," *IEEE Transactions on Communications*, vol. 67, no. 4, pp. 2716–2729, Apr. 2019, doi: 10.1109/tcomm.2018.2890264.
[9] X. Yue, Y. Liu, S. Kang, A. Nallanathan, and Y. Chen, "Modeling and Analysis of Two-Way Relay Non-Orthogonal Multiple Access Systems," *IEEE Transactions on Communications*, vol. 66, no. 9, pp. 3784–3796, Sep. 2018, doi: 10.1109/tcomm.2018.2816063.
[10] T.-T. T. Dao and P. N. Son, "Performance evaluation of two-way relaying network using nonlinear energy-harvesting and SIC techniques," in *Green Energy and Technology*, 2024, pp. 625–633, doi: 10.1007/978-981-97-1868-9_62.
[11] S. Atapattu, R. Fan, P. Dharmawansa, G. Wang, and J. Evans, "Two–way communications via reconfigurable intelligent surface," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, May 2020, pp. 1–6, doi: 10.1109/WCNC45663.2020.9120479.
[12] Z. Liu *et al.*, "Performance analysis of reconfigurable intelligent surface assisted two-Way NOMA networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 12, pp. 13091–13104, Dec. 2022, doi: 10.1109/TVT.2022.3201371.
[13] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When Does Relay Transmission Give a More Secure Connection in Wireless

Ad Hoc Networks?," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 624–632, Apr. 2014, doi: 10.1109/tifs.2013.2297835.
[14] F. Liu, Y. Liu, Y. Liu, and J. Yu, "Secure beamforming in full-duplex two-way relay networks with SWIPT for multimedia transmission," *IEEE Access*, vol. 8, pp. 26851–26862, 2020, doi: 10.1109/ACCESS.2020.2970612.
[15] J. Luo, F. Wang, and S. Wang, "Secure two-way transmission via autonomous reconfigurable intelligent surface," *IEEE Wireless Communications Letters*, vol. 12, no. 2, pp. 262–266, Feb. 2023, doi: 10.1109/LWC.2022.3223345.
[16] M. Mitev, A. Chorti, H. V. Poor, and G. P. Fettweis, "What physical layer security can do for 6G security," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 375–388, 2023, doi: 10.1109/OJVT.2023.3245071.
[17] S. M. Mirrezaei, K. Faez, and S. Yousefi, "Towards fountain codes," *Wireless Personal Communications*, vol. 77, no. 2, pp. 1533–1562, Jul. 2014, doi: 10.1007/s11277-013-1597-7.
[18] S. Chanayai and A. Apavatjrut, "Fountain codes and their applications: comparison and implementation for wireless applications," *Wireless Personal Communications*, vol. 121, no. 3, pp. 1979–1994, Dec. 2021, doi: 10.1007/s11277-021-08749-w.
[19] L. Sun and H. Xu, "Fountain-coding-based secure communications exploiting outage prediction and limited feedback," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 740–753, Jan. 2019, doi: 10.1109/TVT.2018.2885869.
[20] M. Abughalwa and M. O. Hasna, "A secrecy study of UAV based networks with fountain codes and FD jamming," *IEEE Communications Letters*, vol. 25, no. 6, pp. 1796–1800, Jun. 2021, doi: 10.1109/LCOMM.2021.3056389.
[21] S. Jain and R. Bose, "Secure cooperative transmission in rateless-coded environment using TAS and artificial noise," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 12416–12421, Dec. 2019, doi: 10.1109/TVT.2019.2947065.
[22] S. Jain and R. Bose, "NOMA combined with RC for reliable and secure transmission in a delay-constrained system," *IEEE Wireless Communications Letters*, vol. 10, no. 12, pp. 2639–2643, Dec. 2021, doi: 10.1109/LWC.2021.3110264.
[23] T.-H. Nguyen, "Analysis of outage probability and intercept probability trade-off for secure two-way relaying schemes between two clusters of nodes using fountain codes," *Journal of Science and Technique*, vol. 13, no. 02, Dec. 2024, doi: 10.56651/lqdtu.jst.v13.n02.927.ict.
[24] H. T. Nguyen, N.-T. Hau, N. Van Toan, V. T. Ty, and T. T. Duy, "Fountain coding based two-way relaying cognitive radio networks employing reconfigurable intelligent surface and energy harvesting," *Telecom*, vol. 6, no. 1, p. 1, Dec. 2024, doi: 10.3390/telecom6010001.
[25] N. T. Hau, N. L. Anh, L. C. Khan, and N. T. Hieu, "Outage performance of rateless codes based two-way relay scheme using successive interference cancellation," in *2024 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, IEEE, Nov. 2024, pp. 1–4, doi: 10.1109/ICCE-Asia63397.2024.10773631.
[26] A.-T. Le, T.-H. Vu, N. H. Tu, T. N. Nguyen, L.-T. Tu, and M. Voznak, "Active-reconfigurable-repeater-assisted NOMA networks in internet of things: reliability, security, and covertness," *IEEE Internet of Things Journal*, vol. 12, no. 7, pp. 8759–8772, Apr. 2025, doi: 10.1109/JIOT.2024.3503278.

BIOGRAPHIES OF AUTHORS

Nguyen Thi Hau received the B.E. degree in Electronics and Telecommunication Engineering from the University of Danang–University of Science and Technology (DUT) (Vietnam) in 2007 and the M.S. degree in Electronics Engineering from Ho Chi Minh City University of Technology (Vietnam) in 2011. She is currently working as a lecturer at Saigon University (SGU) and pursuing the Ph.D. degree in the Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH). Her research interests include cooperative communications, cognitive radio, energy harvesting, physical-layer security in wireless communications, and fountain codes. She can be contacted at email: hau.nt@sgu.edu.vn.

Tran Trung Duy received the Ph.D. degree in Electrical Engineering from the University of Ulsan, South Korea in 2013. In 2013, he joined Posts and Telecommunications Institute of Technology, Ho Chi Minh City Campus (PTIT-HCM). From 2022, he has been an Associate Professor of Wireless Communications at PTIT-HCM. From 2017, he has been an Associate Editor for EAI Endorsed Transactions on Industrial Networks and Intelligent Systems Journal. From 2023, he has been an Associate Editor for the Advances in Electrical and Electronic Engineering Journal. His major research interests are cooperative communications, cooperative multi-hop, cognitive radio, physical-layer security, energy harvesting, hardware impairments, and fountain codes. He can be contacted at email: trantrungduy@ptithcm.edu.vn.