EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems Research Article EAI.EU

Network-Coding-based Jamming With Triple Transmission Time Slots: A Method To Secure Transmission In An Extreme Case of Source-Wiretapping and Unshared Jamming Signal

Truc Thanh Tran *

[1]Institute of Research and Development, Duy Tan University, Danang, Vietnam

Abstract

This article resolves an extreme case in physical layer security: an eavesdropper, located near to a source, can spy on the jamming-seed if it is just cryptographically shared. The direct link between the source and destination is even unavailable. The system is proposed to operate in triple transmission phases (timeslots). In the first phase, jamming signal is proposed to carry a random binary network-coding-based jamming (NCJ) message, transmitted by an active jammer. As NCJ cannot be just cryptographically protected, we propose a solution of using physical layer security to secure this message. As a result, a network-coding method can be employed in which NCJ acts as a key to protect the source message from this extreme case of wiretapping. The spatial diversities in both jamming and legitimate transmission is fully exploited to overcome this challenge with high performance. Analysis and simulation of the outage performance and comparison with current methods are provided to validate the performance of the proposed method.

Received on 04 June 2021; accepted on 21 June 2021; published on 23 June 2021

Keywords: Jamming, physical-layer secrecy rate, relay.

doi:10.4108/eai.23-6-2021.170242

1. Introduction

Cryptographic security is a popular methodology for avoiding the detection of desire messages by unauthorized users [1]. However, in wireless communication, unauthorized nodes can create a great deal of potentially cryptographic attacks on the network once they are located in the same coverage.

Therefore, there has recently been considerable interest in physical-layer security (PLS), which explores the characteristics of wireless channels to improve wireless transmission security [2–25]. In wireless adhoc network scenarios, it is natural that methods of PLS are based on cooperative communication since most of the network devices have single antennas [3–5, 9, 23, 26–28]. Several works have even considered the security in the case that devices are powered by wireless environment [22]. There are two popular kinds of cooperative approaches for mitigating or suppressing the impact of the eavesdropping, as presented in the next two paragraphs.

First, cooperation from relays was introduced to avoid (or to mitigate) the wiretapping region (or its impact) [3, 4, 13–22]. In these works, the direct-link from the source to the eavesdropper is usually not closed to the source. The relays are deployed in the appropriate positions where the impact of wiretapping is mild or ignorable. For example, having the relay closed to the source is preferred in order to reduce the transmitting power of the source, and thus the eavesdropper is out of the coverage. Since many relays are able to securely receive the source transmission in the first phase, they can create a distributed beamformer in the second phase. This allows them to null the desired transmitting signal at the eavesdropper, or more generally, to maximize the secrecy rate at the legitimate receivers [13, 22, 29]. As a result, the eavesdropper nodes are not able

*Corresponding author. Email: tranthanhtruc1982@gmail.com to reach the transmission message. These types of approaches are referred to as beamforming cooperation (BFC) in this article. However, BFC requires all of the relays to know the other instantaneous channel state information (CSI). Updating the CSI usually consumes a large amount of time, thus requiring a great deal of radio resources and increased hardware complexity. It is much simpler if only a single relay is selected for cooperation, *e.g.*, the relay selection with a decode-and-forward, as presented in [4, 20, 30–35]. In that case, exploitation of the spatial diversity can help the system to mitigate the impact of the eavesdropping in the region surrounding the destination [4]. This method is known as the typical decode-and-forward (TDF) in this article. In both BFC and TDF, jamming techniques are not employed. On the other hand, several studies propose that some relays, *e.g.*, those that do not perform the forwarding task, are eligible to become active jammers [3]. Though jamming can degrade the decoding performance of the eavesdropper, it creates some harmful interference to the legitimate receiver [3, 36]. The higher spatial diversity, as a result of the multiple jammers, is the key to overcoming this situation. For example, Krikidis *et al.* attempted to select the best jammer and relay for the most jamming and transmitting efficiency [3]. Basically, a single active jammer is selected from multiple nodes to improve the performance of PLS. This method refers to the single-jammer cooperative jamming (SJJ) approach in this article [3, 37–39].

Second, if the deployment of the relays can neither avoid nor mitigate the impact of the wiretapping, *e.g.*, the case where the eavesdropper is too close to the source, all or part of these relays become jammers to assist the direct-link transmission, rather than serving as normal relays [28]. The study by Y. Liu *et al.* even allows the source and destination to be the jammers for enabling a cooperative transmission [5]. These were done by employing a distributed beamforming-based cooperative jamming (D-BF-CJ), in which multiple jammers employ the same jamming signal to enable the beamformer. Each jammer uses an appropriate weight founded by maximizing the secrecy rate or nulling the jamming signal at the receivers (the ones that decode the information message of the source) [5, 13, 28]. The main difference between D-BF-CJ and the BFC is that D-BF-CJ uses the beamformer for the jamming signal, whereas the BFC uses the beamformer for the desired transmitting signal.

Similar to the BFC, the D-BF-CJ method also requires knowing the CSI of all of the jammers. In addition, all jammers must have the same jamming signal so that the beamformer is applicable [5, 13, 28]. Every jammer contains a jamming generator to create the random jamming signal. To allow for generating the same jamming signal, all jammers must have the same seed. This seed thus is shared over the legitimate nodes and must be unknown by the eavesdropper. Consequently, the seed is vulnerable to be attacked by eavesdropper on the basis of a long-term observation on the jamming signals. Therefore, the only way to secure the seed regardless of any decryption methods used at the eavesdropper is again the PLS. Assuming that the seed can be secured using PLS, question whether jamming in D-BF-CJ can resolve the problems when the eavesdropper locates very close to source for wiretapping still remains.

This article considers an extreme case of eavesdropping in the wireless ad-hoc network: a single eavesdropper locates nearby the source to wiretap information; the seed can be even wiretapped if its transmission is only protected by cryptographic scheme. Further, the direct channel between source and destination is assumed to be unavailable. These assumptions lead to that both BFC and TDF quite limited. In the case of SJJ, the jamming signal degrading the signal-to-noise ratio (SNR) of the eavesdropper is much stronger than usual. As a result, it also increases harmful interference at the desired receiver. Therefore, it is not expected to deal with this situation.

In the D-BF-CJ scheme, it is always required the seed to be shared to jammers. PLS is considered as the alternative method to protect seed. It will be used as a reference to compared with the proposed method, as lately mentioned in Section 4.4 and 5.

In this article, we use PLS to protect a random binary jamming message generated by a jammer from being wiretapping by the eavesdropper. Then, an application of network-coding to create a secure data message based on this jamming message is proposed to cope with the reality that the eavesdropper locates close to the source for wiretapping [40, 41]. The binary jamming technique was also applied in other previous works of mine and colleges. However, its applications were with simple system models and thus still contain limitations. The transmission protocol in [41] just consists of two timeslots. One was for the jamming task and the remain was responsible for the direct transmission from source to destination. Spatial diversity exploitation was only supported to the jamming task. Its advantages in legitimate transmissions were still abandoned. Overcoming this drawback is hence the target of this study.

The data transmission intervals are proposed to be divided into three timeslots. The first timeslot is for the transmission of the jamming signal rather than a normal broadcast. In particular, the jamming signal is proposed to carry an amount of random binary messages, instead of being a pure random signal as usual. It is known as the network-coding-based jamming (NCJ) message in this article. This allows the source to create a network-coding-based message

(NCM) based on exclusive-ORing (XORing) its binary information and the NCJ message. The NCM is then cooperatively transmitted over the next two timeslots. The NCM is free from being eavesdropped once the NCJ message is secured in the first phase. Therefore, the important issue is to physically secure the NCJ message. The degree of wiretapping NCJ is much less than that of wiretapping a transmission from the source because the NCJ message is transmitted from the jammer. There was no spatial diversity exploitation in either jamming task or legitimate transmissions. This challenge will be resolved in this article in which a fully spatial diversity protocol is proposed with detail descriptions and analysis.

We organize the remainder of the article as follows. The next section is the System Model section. Our system is composed of multiple relays and multiple jammers. We then present the proposed hybrid method of PLS in which NCJ and the triple-phase transmission are emphasized. We also analyze the theoretical outage performance of the proposed system in this section. For comparison purposes, we introduce the outage performance expressions of several conventional methods in section 4. Especially, in 4.4, we discuss the use of the PLS method for sharing the seed to make the D-BF-CJ available. Simulation results and discussions are provided in section 5. We finally conclude our work in section 6.

2. System Model

The system used in this article is shown in Fig. 1 and consists of source S, destination D, an eavesdropper E, a set of M relays $\mathcal{P}_{\mathrm{R}} = \{\mathrm{R}_1, \ldots, \mathrm{R}_M\}$ and a set of N jammers $\mathcal{P}_{\mathrm{J}} = \{\mathrm{J}_1, \ldots, \mathrm{J}_N\}$. Notations $h_{\mathrm{R}_k\mathrm{S}}$, $h_{\mathrm{R}_k\mathrm{D}}$ and $h_{\mathrm{R}_k\mathrm{E}}$, where $1 \leq k \leq M$, denote the channel-state-information (CSI) that corresponds to the links R$_k$–S, R$_k$–D and R$_k$–E, respectively. h_{SD} and h_{SE} denote the CSI accordingly for the links $\mathrm{S}-\mathrm{D}$ and $\mathrm{S}-\mathrm{E}$. $h_{\mathrm{J}_k\mathrm{S}}$, $h_{\mathrm{J}_k\mathrm{D}}$ and $h_{\mathrm{J}_k\mathrm{E}}$ denote the CSI of the links J$_k$–S, J$_k$–D, and J$_k$–E, respectively. A specific CSI h_{ij} of the link between nodes i and j, where $i, j \in \{\mathrm{S}, \mathrm{D}, \mathrm{E}\} \cup \mathcal{P}_{\mathrm{R}} \cup \mathcal{P}_{\mathrm{J}}$, is known by both of them. Including pilot signals in the control messages, *e.g.*, the request-to-send and clear-to-send messages, allows the two nodes of a specific link to estimate their common CSI. In this article, we assume the errors in estimating the CSI are ignorable. The eavesdropper CSI, $h_{i,\mathrm{E}}$, where $i \neq \mathrm{E}$, is known by node i, as assumed in several previous studies [5, 28]. The assumption is valid when an eavesdropper also belongs to the same network. For example, a network consisting of multiple levels of services usually divides itself into a hierarchical structure. Users with higher priority are then protected from the listening by those with lower priority. It is obvious that the lower users become the eavesdroppers if they attempt to decode the unauthorized information. In that case, certain knowledge related to the eavesdropper, *e.g.*, position, CSI, etc., is still known and monitored by the network.

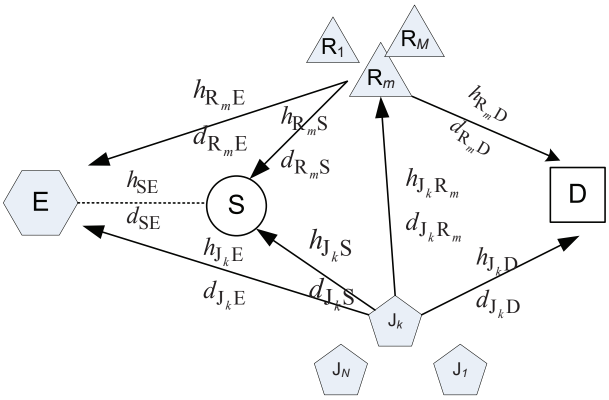
R$_1$
R$_M$
R$_m$
$h_{\mathrm{R}_m\mathrm{E}}$
$d_{\mathrm{R}_m\mathrm{E}}$
$h_{\mathrm{R}_m\mathrm{S}}$
$d_{\mathrm{R}_m\mathrm{S}}$
$h_{\mathrm{R}_m\mathrm{D}}$
$d_{\mathrm{R}_m\mathrm{D}}$
E
h_{SE}
d_{SE}
S
D
$h_{\mathrm{J}_k\mathrm{R}_m}$
$d_{\mathrm{J}_k\mathrm{R}_m}$
$h_{\mathrm{J}_k\mathrm{E}}$
$d_{\mathrm{J}_k\mathrm{E}}$
$h_{\mathrm{J}_k\mathrm{S}}$
$d_{\mathrm{J}_k\mathrm{S}}$
$h_{\mathrm{J}_k\mathrm{D}}$
$d_{\mathrm{J}_k\mathrm{D}}$
J$_k$
J$_N$
J$_1$

Figure 1. System Model

Channels between the links are independently distributed, experiencing the slow and flat Rayleigh fading. The average powers of h_{ij}, where $i, j \in \left\{\{\mathrm{S}, \mathrm{D}, \mathrm{E}\} \cup \mathcal{P}_{\mathrm{R}} \cup \mathcal{P}_{\mathrm{J}}\right\}$, are denoted by Ω_{ij}, respectively. In this article, all modeled average CSI are dependent upon the distances of their links and the common path loss exponent, ϑ. The distance d_{ij} represents the distance of the link between nodes i and j. The value Ω_{ij} is modeled by its distance such that $\Omega_{ij} = d_{ij}^{-\vartheta}$. We also define the instantaneous channel power of CSI h_{ij} as follows: $\gamma_{ij} \triangleq \left|h_{ij}\right|^2$. Further, it should be noted that all of the nodes are based on a single antenna in half-duplex mode.

3. Hybrid Physical-Layer Security Method: Network-coding-based Jamming and the Three Phase-based Transmission

The transmission interval is divided into three timeslots. We propose a method of using a binary jamming, instead of using a purely noisy jamming signal. $\mathcal{M}_s$ denotes the binary message that S would like to transmit to D. It is then represented by a complex signal, s, where $\mathrm{E}\{s\} = 0$ and $\mathrm{E}\{|s|^2\} = 1$. Each jammer J$_k$ generates a random binary message, known as the NCJ message $\mathcal{M}_k$, from its own seed; this message is then represented by a NCJ signal u_k, where $E\{u_k\} = 0$ and $E\{|u_k|^2\} = 1$. The proposed jamming signal is completely different from those presented in the previous studies. The jamming signal is a random signal and it carries a random binary message. The the seed for generating $\mathcal{M}_k$ is not either shared over unchanged over time. So it will be secured even when eavesdropper uses the long-term observation to discover the jamming signals.

Here, the lengths in bits of $\mathcal{M}_k$ and $\mathcal{M}_s$ are set to be the same, and as a result, the source shares this knowledge, *e.g.*, by setting certain control bits in its request-to-send message. The first timeslot is for transmitting a jamming signal, denoted as u_k, and the next two timeslots are for the decode-and-forward of the signal carrying the information signal of the source.

The next subsection describes the transmissions with three phases when a specific jammer J_k, $1 \le k \le N$, is assumed to be the active jammer, and a specific relay R_m, $1 \le m \le M$, is assumed to be the active relay.

3.1. Transmission in the first phase

In the first phase, J_k transmits u_k, allowing nodes S, D and E to receive the signal as shown below:

$$y_{j,1} = \sqrt{P_1} h_{\mathrm{J}_k j} u_k + n_{j,1} \tag{1}$$

where $j \in \{\mathrm{S}, \mathrm{D}, \mathrm{E}\}$, P_1 is the transmitting power and $n_{j,1}$ is the complex white noise, $n_{j,1} \sim \mathcal{CN}(0,1)$, in the first phase. The target transmission rate is denoted as R_t. $\mathcal{R}_{\mathrm{S},\mathrm{J}_k}$ and $\mathcal{R}_{\mathrm{D},\mathrm{J}_k}$ denote the secrecy rates of the transmission from J_k to nodes S and D, respectively. The terms $C_{\mathrm{S},\mathrm{J}_k}$, $C_{\mathrm{D},\mathrm{J}_k}$ and $C_{\mathrm{E},\mathrm{J}_k}$ are the achievable rates of the transmissions from J_k to S, D and E, respectively. These achievable rates are expressed as follows:

$$C_{\mathrm{S},\mathrm{J}_k} = \frac{1}{3}\log_2\left(1 + P_1 \gamma_{\mathrm{J}_k\mathrm{S}}\right) \tag{2}$$

$$C_{\mathrm{D},\mathrm{J}_k} = \frac{1}{3}\log_2\left(1 + P_1 \gamma_{\mathrm{J}_k\mathrm{D}}\right) \tag{3}$$

$$C_{\mathrm{E},\mathrm{J}_k} = \frac{1}{3}\log_2\left(1 + P_1 \gamma_{\mathrm{J}_k\mathrm{E}}\right) \tag{4}$$

The pre-log factor is 1/3 because the total number of transmission phases is three. The secrecy rates are then calculated as follows:

$$\begin{aligned}\mathcal{R}_{\mathrm{S},\mathrm{J}_k} &= \left[C_{\mathrm{S},\mathrm{J}_k} - C_{\mathrm{E},\mathrm{J}_k}\right]^+ \\ &= \frac{1}{3}\left[\log_2\left(\frac{1 + P_1\gamma_{\mathrm{J}_k\mathrm{S}}}{1 + P_1\gamma_{\mathrm{J}_k\mathrm{E}}}\right)\right]^+ \\ &\approx \frac{1}{3}\log_2\left(\frac{\gamma_{\mathrm{J}_k\mathrm{S}}}{\gamma_{\mathrm{J}_k\mathrm{E}}}\right), \quad \text{for } P_1 \gg 1\end{aligned} \tag{5}$$

$$\begin{aligned}\mathcal{R}_{\mathrm{D},\mathrm{J}_k} &= \left[C_{\mathrm{D},\mathrm{J}_k} - C_{\mathrm{E},\mathrm{J}_k}\right]^+ \\ &= \frac{1}{3}\left[\log_2\left(\frac{1 + P_1\gamma_{\mathrm{J}_k\mathrm{D}}}{1 + P_1\gamma_{\mathrm{J}_k\mathrm{E}}}\right)\right]^+ \\ &\approx \frac{1}{3}\log_2\left(\frac{\gamma_{\mathrm{J}_k\mathrm{D}}}{\gamma_{\mathrm{J}_k\mathrm{E}}}\right), \quad \text{for } P_1 \gg 1\end{aligned} \tag{6}$$

where $[x]^+ = \max\{x, 0\}$.

3.2. Transmission in the second and third phases

Due to the fact that the two messages, $\mathcal{M}_k$ and $\mathcal{M}_s$, have the same length in bits, their transmissions have the same target transmission rate R_t. In other words, when condition $\mathcal{T}_1(\mathrm{J}_k)$ occurs, where $\mathcal{T}_1(\mathrm{J}_k) = \left(\mathcal{R}_{\mathrm{S},\mathrm{J}_k} > R_t\right) \cap \left(\mathcal{R}_{\mathrm{D},\mathrm{J}_k} > R_t\right)$, the message $\mathcal{M}_k$ is securely transmitted to S and D; thus, node E cannot eavesdrop this message.

Let us consider the case where condition $\mathcal{T}_1(\mathrm{J}_k)$ is satisfied in this subsection. In that case, node S then creates a message, known as $\mathcal{M}_\oplus$, from $\mathcal{M}_s$ and $\mathcal{M}_k$, using the network-coding technique as follows: $\mathcal{M}_\oplus = \mathcal{M}_s \oplus \mathcal{M}_k$. The created message is also known as the NCM; which is then represented by a complex signal, v_k, where $E\{v_k\} = 0$ and $E\left\{|v_k|^2\right\} = 1$. The notation $\oplus$ denotes the XOR operator. The source S then transmits the signal v_k in the second phase, allowing the relay group to receive the signal as follows:

$$y_{\mathrm{R}_l,2} = \sqrt{P_2} h_{\mathrm{R}_l\mathrm{S}} v_k + n_{\mathrm{R}_l,2} \tag{7}$$

R_l, where $1 \le l \le M$, is a specific relay, P_2 is the transmitting power and $n_{\mathrm{R}_l,2}$ is the noise at node R_l in the second phase, $n_{\mathrm{R}_l,2} \sim \mathcal{CN}(0,1)$. By transmitting the message $\mathcal{M}_\oplus$, node E cannot eavesdrop on message $\mathcal{M}_s$, which is contained in $\mathcal{M}_\oplus$ as a result of the network coding, because it does not have message $\mathcal{M}_k$ due to that $\mathcal{T}_1(\mathrm{J}_k)$ was already assumed to be satisfied. Therefore, transmission of the message $\mathcal{M}_s$ in the form of $\mathcal{M}_\oplus$ is always secured once the condition $\mathcal{T}_1(\mathrm{J}_k)$ occurs. The capacity of the received signal at the relay R_l, denoted as $C_{\mathrm{R}_l,\mathrm{S}}$, is expressed as follows:

$$C_{\mathrm{R}_l,\mathrm{S}} = \frac{1}{3}\log_2\left(1 + P_2\gamma_{\mathrm{R}_l\mathrm{S}}\right) \tag{8}$$

We define $\mathcal{L}_1$ as the group of relays that successfully decode the message $\mathcal{M}_\oplus$, $\mathcal{L}_1 = \left\{\mathrm{R}_l \,\middle|\, C_{\mathrm{R}_l,\mathrm{S}} > R_t, 1 \le l \le M\right\}$. It should be noted that the system does not need to secure message $\mathcal{M}_\oplus$ because node E cannot decode message $\mathcal{M}_s$ contained in this message.

If $\mathcal{L}_1$ is not an empty set, one of the nodes in $\mathcal{L}_1$, *e.g.*, R_m, is selected as the active relay to forward the signal v_k to the destination.

Let us consider the case that R_m exists in $\mathcal{L}_1$ and serves as the active relay. Consequently, node D receives a signal in the third phase as follows:

$$y_{\mathrm{D},\mathrm{R}_m} = \sqrt{P_3} h_{\mathrm{R}_m\mathrm{D}}\, v_k + n_{\mathrm{D},3} \tag{9}$$

where $n_{\mathrm{D},3}$ is the complex white noise, $n_{\mathrm{D},3} \sim \mathcal{CN}(0,1)$, and P_3 is the transmitting power. If the destination successfully decodes $\mathcal{M}_\oplus$, it is able to derive the source message as follows: $\mathcal{M}_s = \mathcal{M}_\oplus \oplus \mathcal{M}_k$. It should be noted that the destination already safely and successfully decodes the NCJ message $\mathcal{M}_k$ in the first phase as we are considering that $\mathcal{T}_1\left(\mathrm{J}_k\right)$ is satisfied. $C_{\mathrm{D,R}_m}$ denotes the capacity at node D, and is expressed as follows:

$$C_{\mathrm{D,R}_m} = \frac{1}{3}\log_2\left(1 + P_3\gamma_{\mathrm{R}_m\mathrm{D}}\right) \tag{10}$$

Therefore, the condition for message $\mathcal{M}_s$ to be securely and successfully transmitted, according to the active jammer J_k and the active relay R_m, is expressed by the condition, $\mathcal{T}_2\left(\mathrm{R}_m\right)$, as follows:

$$\mathcal{T}_2\left(\mathrm{R}_m\right) = \left(C_{\mathrm{R}_m,\mathrm{S}} > R_t\right) \cap \left(C_{\mathrm{D},R_m} > R_t\right) \tag{11}$$

Let us consider the case when $\mathcal{L}_1$ is an empty set. As a result, there is no relay that successfully decodes message $\mathcal{M}_\oplus$. Therefore, all of the relays are then simply kept silent in the third phase and the system is in outage.

The NCJ message operates in a similar way to a secure key to decode the true information message of the source. It raises an argument whether the eavesdropper can detect this key based on the observation on NCMs. The answer is “yes, it can.” if the NCMs are observed in a long term and all of these messages must have the same NCJ message. The answer is “no, it cannot.” in our proposed method because NCJ message is secured by PLS and can be freely, independently and frequently changed by each jammer so that all NCMs do not have the same NCJ message in a long term[1].

3.3. Jammer and Relay Selection

Jammer Selection. The setup time occurs prior to each transmission time and is necessary for updating the knowledge of the instantaneous CSI of the links. A pilot signal is contained in each typical control message, *e.g.*, request-to-send (RTS) or clear-to-receive (CTR) messages, etc., to allow nodes to estimate their CSI from the node transmitting the control message. Please refer to Table 1 for descriptions on selection of the activejammer and relay.

In the setup time, the source first wants to update the eavesdropper CSI. The source transmits a request-to-update (RTU) message to request node E to update its CSI [2]. Node E then includes a pilot signal in its reply message, the acknowledgement message, which is

Table 1. Diagram of the description of the jammer, mode and relay selection.

	Action		Comments
1	S transmits RTU		
2	E transmits ACK_1		ACK_1 contains the pilot signal.
3	S transmits RTS_1		RTS_1 contains pilot signal, the CSI value h_{SE}.
4	S waits for a reply from D with interval τ		D will not reply because RTS_1 does not reach D
5	The head cluster node R_1 transmits RTS_2.		RTS_2 contains the pilot signal, h_{SE}, to take over the task of RTS_1.
6	D transmits CTR_1		CTR_1 contains the pilot signal. CTR_1 starts the relay selection process.
7	Jammer selection within interval Δ_J		The active jammer is selected by (12).
8	J_a transmits either the JCC or JR message. If JCC is transmitted, the system continues its action in the next step. If JR is transmitted, the system will skip step 9 and goes to step 10		The JCC message is transmitted if $\mathcal{T}_1\left(\mathrm{J}_a\right)$ is satisfied. Otherwise, JR is transmitted. JCC contains the pilot signal. JR indicates that no jammer is selected and the system is in outage.
9	Relay selection within the interval Δ_R.		For JCC, selected by (13).
		R_a transmits CTR_2 within the duration Δ_R if it is successfully selected.	CTR_2 contains the pilot signal.
10	If JR was already launched or the relay selection time Δ_R expires without CTR_2, data transmission is discarded	If CTR_2 is transmitted the system starts the data information transmission in three timeslots.	The transmission of the message CTR_2 indicates that the active relay is successfully selected and the system is not in outage. Therefore, the system starts its data transmission if the relay selection ends and CTR_2 was launched.

[1] A concern might be raised when the NCJ message is a pseudo-random bit-string because its generation consequently requires a seed which can be recovered based on a long-term observation on NCMs. However, in the proposed method, the no requirement to share seed with other nodes allows each jammer to even freely and frequently vary its own seed over time, when the NCJ message is a pseudo-random bit-string. In general, the NCJ message can be freely, independently and frequently changed by each jammer over time.

[2] We previously assumed that node E is also in the same network, but with lower priority, and it becomes the eavesdropper when attempting to access the unauthorized data. Therefore, the source already knows that node E is one of its neighbors.

known as ACK_1, to allow S and others to estimate its CSI [3].

Next, the source sends an RTS message, known as RTS_1, to request a transmission to destination D. Based on the pilot signal contained in this control message, node E, the relays and the jammers can estimate their CSI from the source. It should be noted that the eavesdropping CSI, h_{SE}, is also contained in RTS_1. This will be necessary for the relay selection in Mode 2. D cannot send any feedback because RTS_1 does not reach it due to the unavailability of the direct link. Therefore, after waiting an amount of time, *e.g.*, τ, without feedback from D, the head node of the relay group, *e.g.*, R_1, takes over the task to inform D of the request from S. Here, the discussion on the interval of τ is skipped because it is not the focus of this article. It then continues to create and transmit another RTS message, RTS_2, to let D know the intention of the transmission from the source. Overhearing RTS_2, D feedbacks a CTR message, known as CTR_1. The pilot signal contained in CTR_1 allows all remaining nodes, except S, to estimate the destination CSI.

The relay and jammer groups now have sufficient knowledge about the CSI from S, D and E, and they perform the selections of the active jammer and active relay before acknowledging the feedback of the destination. First, all jammers start to select the active jammer. A sufficient period of time, Δ_{J}, is allocated for this selection. We denote J_a as the active jammer, and it is selected based on equations (5) and (6), as follows:

$$\begin{aligned} \text{J}_a &= \text{argmax}_{\text{J}_k \in \mathcal{P}_\text{J}} \left\{ \min\left\{ \mathcal{R}_{\text{S},\text{J}_k}, \mathcal{R}_{\text{D},\text{J}_k} \right\} \right\} \\ &\approx \text{argmax}_{\text{J}_k \in \mathcal{P}_\text{J}} \left\{ \min\left\{ \frac{\gamma_{\text{J}_k\text{S}}}{\gamma_{\text{J}_k\text{E}}}, \frac{\gamma_{\text{J}_k\text{D}}}{\gamma_{\text{J}_k\text{E}}} \right\} \right\}, \quad \text{for } P_1 \gg 1 \,. \end{aligned} \tag{12}$$

Having knowledge of the CSI from the source, destination and eavesdropper, each jammer J_k can calculate its secrecy rates $\mathcal{R}_{\text{S},\text{J}_k}$ and $\mathcal{R}_{\text{D},\text{J}_k}$. Techniques, such as the use of countdown timers, to implement the best selection can be found in many previous works. Here, we simply assumed that J_a can be selected according to the above selection rule, within the duration Δ_{J}. The condition $\mathcal{T}_1(\text{J}_a)$ is thus determined by comparing $\mathcal{R}_{\text{S},\text{J}_a}$ and $\mathcal{R}_{\text{D},\text{J}_a}$ with the target transmission rate R_t.

In the case where condition $\mathcal{T}_1(\text{J}_a)$ is satisfied, J_a transmits a message, known as the jamming cooperation confirmation (JCC) message, allowing others to know it. If $\mathcal{T}_1(\text{J}_a)$ fails, J_a transmits a message, known as the jamming rejection (JR) message, to refuse its cooperation, allowing the system to know that the system is in outage and thus, the system is silent in the data transmission time.

Relay Selection. The pilot signal is included in the JCC message, allowing S, D and E to estimate the CSI from J_a. Overhearing JCC, the relays know that they have to start to select the active relay, denoted R_a.

The relays R_l, $1 \le l \le M$, can calculate their capacities, $C_{\text{R}_l,\text{S}}$, and only those satisfying the condition, $C_{\text{R}_l,\text{S}} > R_t$, automatically set themselves to be in group $\mathcal{L}_1$. A sufficient duration, e.g., Δ_{R}, is allocated for this selection. If group $\mathcal{L}_1$ is not an empty set, the relays then select the active relay, denoted as R_a, as follows:

$$\begin{aligned} \text{R}_a &= \text{argmax}_{\text{R}_m \in \mathcal{L}_1} \left\{ C_{\text{D},\text{R}_m} \right\} \\ &= \text{argmax}_{\text{R}_m \in \mathcal{L}_1} \left\{ \gamma_{\text{R}_m\text{D}} \right\} . \end{aligned} \tag{13}$$

R_a is empty only when $\mathcal{L}_1$ is an empty set. We assume that the selection rule can be performed within the duration Δ_{R}. If $\mathcal{L}_1$ is not an empty set, R_a is always selected before the selection time Δ_{R} expires, because this interval is assumed to be sufficient for the selection. R_a then immediately creates and transmits a CTR message, known as CTR_2. Thus, CTR_2 is always transmitted before the selection time Δ_{R} expires. This message actually takes over the job of CTR_1, which cannot reach node S. CTR_2 also contains the pilot signal, allowing the others to estimate the CSI from R_a. Overhearing CTR_2, the system starts the transmission time in which J_a and R_a are the active jammer and relay, respectively. The empty result of the relay selection is indicated by the fact that the selection period, Δ_{R}, runs out without the message CTR_2. When either JR or the relay selection time δ_R running out without CTR_2 occurs, the system simply does not allow for any data transmission. Therefore, the system will be in silence in the respective data transmission time if this occurs.

The descriptions of the active jammer and relay selections are summarized in the diagram shown in Table **??**.

3.4. Outage Performance Analysis

The successful transmission occurs when the following conditions are satisfied: $\mathcal{T}_1(\text{J}_a)$ is true and $\mathcal{T}_2(\text{R}_a)$ is true, where J_a is selected from (12) and R_a is selected from (13).

Probability for a successful transmission. The distributions of $h_{\text{J}_a\text{S}}$ and $h_{\text{J}_a\text{E}}$ are necessary when computing the secrecy rates in the transmission for the binary jamming message. They are independent from the CSI, which are essential for calculating the achievable rates, $C_{\text{R}_a,\text{S}}$ and C_{D,R_a}, at the relay and D. Thus, the probability for

[3] Here, not updating the CSI causes node E to be punished with a certain penalty, *e.g.*, no allowance for either transmitting or receiving its authorized data. As a result, E always obliges the request-to-update from S.

successful transmission, denoted as $P_{\text{suc},1}$, is computed as follows:

$$\begin{aligned} P_{\text{suc},1} &= \Pr\left\{\mathcal{T}_1\left(\mathrm{J}_a\right) \cap \mathcal{T}_2\left(\mathrm{R}_a\right)\right\} \\ &= \Pr\left\{\mathcal{T}_1\left(\mathrm{J}_a\right)\right\} \Pr\left\{\mathcal{T}_2\left(\mathrm{R}_a\right)\right\} \\ &= \underbrace{\Pr\left\{\left(\mathcal{R}_{\mathrm{S},\mathrm{J}_a} > R_t\right) \cap \left(\mathcal{R}_{\mathrm{D},\mathrm{J}_a} > R_t\right)\right\}}_{T_1} \\ &\quad \times \underbrace{\Pr\left\{\left(C_{\mathrm{R}_a,\mathrm{S}} > R_t\right) \cap \left(C_{\mathrm{D},R_a} > R_t\right)\right\}}_{T_2}. \end{aligned} \tag{14}$$

The probability T_1 is rewritten as follows:

$$\begin{aligned} T_1 &\approx \Pr\left\{ \begin{array}{c} \left(\frac{1}{3}\log_2\left(\frac{\gamma_{\mathrm{J}_a\mathrm{S}}}{\gamma_{\mathrm{J}_a\mathrm{E}}}\right) > R_t\right) \\ \cap\left(\frac{1}{3}\log_2\left(\frac{\gamma_{\mathrm{J}_a\mathrm{D}}}{\gamma_{\mathrm{J}_a\mathrm{E}}}\right) > R_t\right) \end{array} \right\}, \quad \text{for } P_1 \gg 1 \\ &= \Pr\left\{\min\left\{\frac{\gamma_{\mathrm{J}_a\mathrm{S}}}{\gamma_{\mathrm{J}_a\mathrm{E}}}, \frac{\gamma_{\mathrm{J}_a\mathrm{D}}}{\gamma_{\mathrm{J}_a\mathrm{E}}}\right\} > 2^{3R_t}\right\} \\ &= 1 - \Pr\left\{\min\left\{\frac{\gamma_{\mathrm{J}_a\mathrm{S}}}{\gamma_{\mathrm{J}_a\mathrm{E}}}, \frac{\gamma_{\mathrm{J}_a\mathrm{D}}}{\gamma_{\mathrm{J}_a\mathrm{E}}}\right\} < 2^{3R_t}\right\} \\ &= 1 - \Pr\left\{\max_{1\le k\le N}\left\{\min\left\{\frac{\gamma_{\mathrm{J}_k\mathrm{S}}}{\gamma_{\mathrm{J}_k\mathrm{E}}}, \frac{\gamma_{\mathrm{J}_k\mathrm{D}}}{\gamma_{\mathrm{J}_k\mathrm{E}}}\right\}\right\} < 2^{3R_t}\right\} \\ &= 1 - \Pr\left\{\bigcap_{k=1}^{N}\left(\min\left\{\frac{\gamma_{\mathrm{J}_k\mathrm{S}}}{\gamma_{\mathrm{J}_k\mathrm{E}}}, \frac{\gamma_{\mathrm{J}_k\mathrm{D}}}{\gamma_{\mathrm{J}_k\mathrm{E}}}\right\} < 2^{3R_t}\right)\right\} \\ &= 1 - \prod_{k=1}^{N}\Pr\left\{\min\left\{\frac{\gamma_{\mathrm{J}_k\mathrm{S}}}{\gamma_{\mathrm{J}_k\mathrm{E}}}, \frac{\gamma_{\mathrm{J}_k\mathrm{D}}}{\gamma_{\mathrm{J}_k\mathrm{E}}}\right\} < 2^{3R_t}\right\} \\ &= 1 - \prod_{k=1}^{N}\left(1 - \underbrace{\Pr\left\{\min\left\{\frac{\gamma_{\mathrm{J}_k\mathrm{S}}}{\gamma_{\mathrm{J}_k\mathrm{E}}}, \frac{\gamma_{\mathrm{J}_k\mathrm{D}}}{\gamma_{\mathrm{J}_k\mathrm{E}}}\right\} > 2^{3R_t}\right\}}_{I_{1,k}}\right). \end{aligned} \tag{15}$$

We define that $\rho_1 = 2^{3R_t}$. The term $I_{1,k}$ can be computed as follows:

$$\begin{aligned} I_{1,k} &= \mathrm{E}_{\gamma_{\mathrm{J}_k\mathrm{E}}}\left\{\Pr\left\{\min\left\{\frac{\gamma_{\mathrm{J}_k\mathrm{S}}}{x}, \frac{\gamma_{\mathrm{J}_k\mathrm{D}}}{x}\right\} > \rho_1 \left|\gamma_{\mathrm{J}_k\mathrm{E}} = x\right.\right\}\right\} \\ &= \mathrm{E}_{\gamma_{\mathrm{J}_k\mathrm{E}}}\left\{ \begin{array}{c} \Pr\left\{\gamma_{\mathrm{J}_k\mathrm{S}} > x\rho_1 \left|\gamma_{\mathrm{J}_k\mathrm{E}} = x\right.\right\} \\ \times\Pr\left\{\gamma_{\mathrm{J}_k\mathrm{D}} > x\rho_1 \left|\gamma_{\mathrm{J}_k\mathrm{E}} = x\right.\right\} \end{array} \right\} \\ &= \int_0^\infty \exp\left(-\frac{x\rho_1}{\Omega_{\mathrm{J}_k\mathrm{S}}}\right)\exp\left(-\frac{x\rho_1}{\Omega_{\mathrm{J}_k\mathrm{D}}}\right)\frac{1}{\Omega_{\mathrm{J}_k\mathrm{E}}}\exp\left(-\frac{x}{\Omega_{\mathrm{J}_k\mathrm{E}}}\right)dx \\ &= \int_0^\infty \frac{1}{\Omega_{\mathrm{J}_k\mathrm{E}}}\exp\left(-\left(\frac{\rho_1}{\Omega_{\mathrm{J}_k\mathrm{S}}} + \frac{\rho_1}{\Omega_{\mathrm{J}_k\mathrm{D}}} + \frac{1}{\Omega_{\mathrm{J}_k\mathrm{E}}}\right)x\right)dx \\ &= \frac{1}{\Omega_{\mathrm{J}_k\mathrm{E}}}\left(\frac{\rho_1}{\Omega_{\mathrm{J}_k\mathrm{S}}} + \frac{\rho_1}{\Omega_{\mathrm{J}_k\mathrm{D}}} + \frac{1}{\Omega_{\mathrm{J}_k\mathrm{E}}}\right)^{-1} \end{aligned} \tag{16}$$

Substituting (16) into (15), we obtain the value of the probability T_1 as follows:

$$\begin{aligned} T_1 &\approx 1 - \prod_{k=1}^{N}\left(1 - \frac{1}{\Omega_{\mathrm{J}_k\mathrm{E}}}\left(\frac{\rho_1}{\Omega_{\mathrm{J}_k\mathrm{S}}} + \frac{\rho_1}{\Omega_{\mathrm{J}_k\mathrm{D}}} + \frac{1}{\Omega_{\mathrm{J}_k\mathrm{E}}}\right)^{-1}\right), \\ &\text{for } P_1 \gg 1\,. \end{aligned} \tag{17}$$

ρ_2 denotes the value of $2^{3R_t} - 1$. The probability T_2 is rewritten as follows:

$$T_2 = \Pr\left\{\left(\gamma_{\mathrm{R}_a\mathrm{S}} > \frac{\rho_2}{P_2}\right) \cap \left(\gamma_{\mathrm{R}_a\mathrm{D}} > \frac{\rho_2}{P_3}\right)\right\} \tag{18}$$

$\mathcal{C}_n^M$ represents the n-combination of the set with M elements, $\mathcal{C}_n^M = \frac{M!}{n!(M-n)!}$. The set $\{L_1, \ldots, L_d, \ldots, L_n\}$ defines a n-element set in which each element, L_d, where $1 \le d \le n$, is selected from M relays, $L_d \in \mathcal{P}_\mathrm{R}$. It is explicit that we can create $\mathcal{C}_n^M$ different n-element sets from M relays. Each of them, *e.g.*, the i-th set, is denoted as $L_{1,i}^n$, $1 \le i \le \mathcal{C}_n^M$. Mathematically, $L_{1,i}^n \triangleq \{L_1, \ldots, L_n\}$ and $1 \le i \le \mathcal{C}_n^M$. Similarly, there are possibly $\mathcal{C}_n^M$ different groups of $\mathcal{L}_1$ with $|\mathcal{L}_1| = n$. These groups form a space of the relay groups, denoted as $\Lambda_1(n)$, that have the same size of n. Mathematically, $\Lambda_1(n) \triangleq \{\mathcal{L}_1 \,\|\mathcal{L}_1| = n\}$. Using $L_{1,i}^n$, where $1 \le i \le \mathcal{C}_n^M$, to represent a specific group of $\mathcal{L}_1$, $\Lambda_1(n)$ is simpler when expressed as follows: $\Lambda_1(n) = \left\{L_{1,1}^n, \ldots, L_{1,i}^n, \ldots, L_{1,\mathcal{C}_n^M}^n\right\}$. As a result, equation (18) is equivalently expressed as follows:

$$\begin{aligned} T_2 &= \sum_{n=1}^{M}\sum_{i=1}^{\mathcal{C}_n^M}\underbrace{\Pr\left\{\mathcal{L}_1 = L_{1,i}^n, |\mathcal{L}_1| = n\right\}}_{I_{2,n,i}} \\ &\quad \times \underbrace{\Pr\left\{\max_{L_d \in L_{1,i}^n}\left\{\gamma_{L_d\mathrm{D}} > \frac{\rho_2}{P_3}\right\}\left|\mathcal{L}_1 = L_{1,i}^n, |\mathcal{L}_1| = n\right.\right\}}_{I_{3,n,i}} \end{aligned} \tag{19}$$

Because $h_{\mathrm{R}_l\mathrm{S}}$, $\mathrm{R}_l \in \mathcal{P}_\mathrm{R}$, is independently distributed, $I_{2,n}$ is computed as follows:

$$\begin{aligned} I_{2,n,i} &= \prod_{\substack{d\,=\,1 \\ L_d\,\in\,L_{1,i}^n}}^{n}\Pr\left\{\gamma_{L_d\mathrm{S}} > \frac{\rho_2}{P_2}\right\}\prod_{\mathrm{R}_l \in \left\{\mathcal{P}_\mathrm{R} \backslash L_{1,i}^n\right\}}\Pr\left\{\gamma_{\mathrm{R}_l\mathrm{S}} < \frac{\rho_2}{P_2}\right\} \\ &= \prod_{\substack{d\,=\,1 \\ L_d\,\in\,L_{1,i}^n}}^{n}\exp\left(-\frac{\rho_2}{P_2\Omega_{L_d\mathrm{S}}}\right)\prod_{\mathrm{R}_l \in \left\{\mathcal{P}_\mathrm{R} \backslash L_{1,i}^n\right\}}\left(1 - \exp\left(-\frac{\rho_2}{P_2\Omega_{\mathrm{R}_l\mathrm{S}}}\right)\right) \end{aligned} \tag{20}$$

The CSI $h_{L_d\mathrm{D}}$ are independent of those forming the set $\mathcal{L}_1$. Therefore, the term $I_{3,n,i}$ is calculated as follows:

$$\begin{aligned}
I_{3,n} &= \Pr\left\{\max_{L_d\in L_{1,i}^n}\left\{\gamma_{L_d\mathrm{D}} > \frac{\rho_2}{P_3}\right\}\right\} \\
&= 1-\Pr\left\{\max_{L_d\in L_{1,i}^n}\left\{\gamma_{L_d\mathrm{D}} < \frac{\rho_2}{P_3}\right\}\right\} \\
&= 1-\prod_{\substack{d\,=\,1\\ L_d\,\in\, L_{1,i}^n}}^{n} \Pr\left\{\gamma_{L_d\mathrm{D}} < \frac{\rho_2}{P_3}\right\} \\
&= 1-\prod_{\substack{d\,=\,1\\ L_d\,\in\, L_{1,i}^n}}^{n} \left(1-\exp\left(-\frac{\rho_2}{P_3\Omega_{L_d\mathrm{D}}}\right)\right).
\end{aligned} \tag{21}$$

By substituting (20) and (21) into (19), the term T_2 is calculated. From (14), (17) and (19), the value of $P_{\mathrm{suc},1}$ is expressed as follows:

$$\begin{aligned}
&P_{\mathrm{suc},1} \\
&\approx \left(1-\prod_{k=1}^{N}\left(1-\frac{1}{\Omega_{\mathrm{J}_k\mathrm{E}}}\left(\begin{matrix}\frac{\rho_1}{\Omega_{\mathrm{J}_k\mathrm{S}}}+\frac{\rho_1}{\Omega_{\mathrm{J}_k\mathrm{D}}}\\ +\frac{1}{\Omega_{\mathrm{J}_k\mathrm{E}}}\end{matrix}\right)^{-1}\right)\right) \\
&\times\sum_{n=1}^{M}\sum_{i=1}^{n}\left(\begin{matrix}\prod_{d=1,L_d\in L_{1,i}^n}^{n}\exp\left(-\frac{\rho_2}{P_2\Omega_{L_d\mathrm{S}}}\right)\\ \prod_{\mathrm{R}_l\in\left\{\mathcal{P}_\mathrm{R}\backslash L_{1,i}^n\right\}}\left(1-\exp\left(-\frac{\rho_2}{P_2\Omega_{\mathrm{R}_l\mathrm{S}}}\right)\right)\\ \left(1-\prod_{d=1,L_d\in L_{1,i}^n}^{n}\left(1-\exp\left(-\frac{\rho_2}{P_3\Omega_{L_d\mathrm{D}}}\right)\right)\right)\end{matrix}\right)
\end{aligned} \tag{22}$$

Outage probability. Therefore, the outage probability, denoted as P_{out}, is determined as follows:

$$P_{out} = 1 - P_{\mathrm{suc},1}. \tag{23}$$

4. The Outage Probability in Several Current Cooperative Jamming Methods

In this section, we introduce the expression of the outage probabilities of TDF, BFC, SJJ, D-BF-CJ which were previously studied in [3–5, 13, 28]. These methods are then compared to the proposed method to validate the advantages of the new scheme.

4.1. The outage performance in TDF

The TDF method does not use the jamming technique. Therefore, all jammers are designed to be relays, making the total relay to be $(M+N)$ relays, R_l and J_k for $1 \le l \le M$ and $1 \le k \le N$.

Transmission in the first timeslot. In the first time slot, S simply transmits its signal, s, which carries its binary message $\mathcal{M}_s$, to the relay groups. Consequently, the relays and eavesdropper receive the signal as follows:

$$y_{j,1} = \sqrt{P_4}h_{j\mathrm{S}}\; s + n_{j,1} \tag{24}$$

where $n_{j,1}$ is the complex white noise of node j, where $j \in \{\mathrm{E},\mathrm{R}_1,\ldots,\mathrm{R}_M,\ldots,\mathrm{J}_1,\ldots,\mathrm{J}_N\}$ in the first timeslot, $n_{j,1} \sim \mathcal{CN}(0,1)$. P_4 is the transmitting power of the source. The time slot in this case is 3/2 longer than that in the proposed method. Therefore, P_4 is set to be $\frac{2}{3}P_2$ to ensure the same energy consumption at S, as in the previous mode. $\hat{C}_{j,\mathrm{S}}$ denotes the capacities at node j, and it is expressed as follows:

$$\hat{C}_{j,\mathrm{S}} = \frac{1}{2}\log_2\left(1+\frac{2}{3}P_2\gamma_{j\mathrm{S}}\right) \tag{25}$$

$\widehat{\mathcal{R}}_{j,\mathrm{S}}$ denotes the secrecy rate of the relay j, where j is R_l or J_k, which is expressed as follows:

$$\begin{aligned}
\widehat{\mathcal{R}}_{j,\mathrm{S}} &= \left[\hat{C}_{j,\mathrm{S}} - \hat{C}_{\mathrm{E},\mathrm{S}}\right]^+ \\
&= \left[\frac{1}{2}\log_2\left(\frac{1+\frac{2}{3}P_2\gamma_{j\mathrm{S}}}{1+\frac{2}{3}P_2\gamma_{\mathrm{SE}}}\right)\right]^+ \\
&\approx \left[\frac{1}{2}\log_2\left(\frac{\gamma_{j\mathrm{S}}}{\gamma_{\mathrm{SE}}}\right)\right]^+, \quad \text{for } P_2 \gg 1
\end{aligned} \tag{26}$$

The relays, which successfully decode message $\mathcal{M}_s$ while E fails to eavesdrop it, form a group known as $\mathcal{L}_2$, where $\mathcal{L}_2 = \left\{\mathrm{R}_l, J_k \left|\widehat{\mathcal{R}}_{\mathrm{R}_l,\mathrm{S}} > R_t, \widehat{\mathcal{R}}_{\mathrm{J}_k,\mathrm{S}} > R_t,\ 1 \le l \le M, 1 \le k \le N\right.\right\}$.

Transmission in the second timeslot. A certain node, *e.g.*, R, where $R \in \mathcal{L}_2$, is selected to be the active relay, forwarding this message to the destination. Thus, nodes D and E receive the signals, respectively, as follows:

$$y_{\mathrm{D},2} = \sqrt{P_5}h_{\mathrm{RD}}\; s + n_{\mathrm{D},2} \tag{27}$$

$$y_{\mathrm{E},2} = \sqrt{P_5}h_{\mathrm{RE}}\; s + n_{\mathrm{E},2} \tag{28}$$

$n_{\mathrm{E},2}$ is the complex white noise of E in this phase, $n_{\mathrm{E},2} \sim \mathcal{CN}(0,1)$. The transmitting power P_5 is set to be equal to $\frac{2}{3}(P_1+P_3)$ to satisfy the same total energy as used by jammer J_k and relay R_m in the proposed method. The total energy consumed by the jammer and relay in the proposed method is $(P_1+P_3)/3$, as compared to the energy used by the relay in the current mode, $\frac{P_5}{2}$. This explains the presence of the factor 2/3, as shown here.

At node E, it attempts to employ the maximum ratio combiner (MRC) to maximize the SNR of the signal s, because it receives the same signal in two time slots. $\hat{C}_{\mathrm{E},2}$ denotes the capacity at E, with respect to the use of MRC, and is written as follows:

$$\hat{C}_{\mathrm{E},2} = \frac{1}{2}\log_2\left(1+\frac{2}{3}P_2\gamma_{\mathrm{SE}}+\frac{2}{3}(P_1+P_3)\gamma_{\mathrm{RE}}\right) \tag{29}$$

However, node D cannot employ MRC in the same way as E because its direct link to S is unavailable. $\hat{C}_{\mathrm{D},2}$ denotes the capacity at D in this phase, and is expressed as follows:

$$\hat{C}_{\mathrm{D},2} = \frac{1}{2}\log_2\left(1 + \frac{2}{3}\left(P_1 + P_3\right)\gamma_{R\mathrm{D}}\right) \tag{30}$$

$\widehat{\mathcal{R}}_{\mathrm{D},R}$ denotes the secrecy rate at D, expressed as follows:

$$\begin{aligned}\widehat{\mathcal{R}}_{\mathrm{D},R} &= \left[\hat{C}_{\mathrm{D},2} - \hat{C}_{\mathrm{E},2}\right]^+ \\ &= \left[\frac{1}{2}\log_2\left(\frac{1 + \frac{2}{3}\left(P_1 + P_3\right)\gamma_{R\mathrm{D}}}{1 + \frac{2}{3}P_2\gamma_{\mathrm{SE}} + \frac{2}{3}\left(P_1 + P_3\right)\gamma_{R\mathrm{E}}}\right)\right]^+ \\ &\approx \frac{1}{2}\log_2\left(\frac{\gamma_{R\mathrm{D}}}{\frac{P_2}{P_1+P_3}\gamma_{\mathrm{SE}} + \gamma_{R\mathrm{E}}}\right), \quad \text{for } P_1, P_2, P_3 \gg 1\end{aligned} \tag{31}$$

The condition for which node D safely and successfully decodes message $\mathcal{M}_s$, corresponding to the active relay R, is known as $\mathcal{T}_3\left(R\right)$, shown as follows:

$$\mathcal{T}_3\left(R\right) = \left\{\left(\mathcal{L}_2 \neq \emptyset\right) \cap \left(\mathrm{R}_m \in \mathcal{L}_2\right) \cap \left(\widehat{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m} > R_t\right)\right\} \tag{32}$$

Active relay selection. The active relay is selected based on the following expression:

$$\mathrm{R}_a = \mathrm{argmax}_{R\in\mathcal{L}_2}\left\{\widehat{\mathcal{R}}_{\mathrm{D},R}\right\} \tag{33}$$

Outage probability of TDF. Therefore, the outage probability of TDF, denoted as P^I_{out}, is expressed as follows:

$$P^I_{out} = \Pr\left\{\begin{array}{l}\bigcap_{l=1}^{M} \overline{\left(\widehat{\mathcal{R}}_{\mathrm{R}_l,\mathrm{S}} > R_t\right) \cap \left(\widehat{\mathcal{R}}_{\mathrm{D},\mathrm{R}_l} > R_t\right)} \\ \bigcap_{k=1}^{N} \overline{\left(\widehat{\mathcal{R}}_{\mathrm{J}_k,\mathrm{S}} > R_t\right) \cap \left(\widehat{\mathcal{R}}_{\mathrm{D},\mathrm{J}_k} > R_t\right)}\end{array}\right\} \tag{34}$$

where $\widehat{\mathcal{R}}_{R,\mathrm{S}} > R_t$ is required for a relay R to safely and successfully decodes the source message in the first timeslot. The condition $\widehat{\mathcal{R}}_{D,R} > R_t$ is required to allow D to safely and successfully decodes the source message in the second slot, corresponding to when R is selected as the active relay.

4.2. The outage performance in SJJ

In SJJ, in addition to the transmission of the source, the active jammer attempts to jam the eavesdropper. Let us consider the secrecy rate when a certain relay, *e.g.*, R_m, is selected to be the active relay and a certain jammer, *e.g.*, J_k, is selected to be the active jammer. In the two phases, J_k transmits the jamming signals with the power of P_6. The value of P_6 must be $\frac{P_1}{6}$, requiring the total jamming energy used for both timeslots to be $P_1/3$, as in the proposed method. In the cooperative phase, R_m forwards the signal with the power of $\frac{2}{3}P_3$, to make their energy equal to $\frac{P_3}{3}$, as the proposed method. Consequently, the energy values for transmission from the source, relay and jammer are the same as in the proposed method. The secrecy rate at R_m in the end of the first phase, denoted as $\dot{\mathcal{R}}_{\mathrm{R}_m,\mathrm{S},\mathrm{J}_k}$, is as follows:

$$\dot{\mathcal{R}}_{\mathrm{R}_m,\mathrm{S},\mathrm{J}_k} = \left[\frac{1}{2}\log_2\left(\frac{1 + \frac{\frac{2}{3}P_2\gamma_{\mathrm{R}_m\mathrm{S}}}{1+\frac{P_1}{6}\gamma_{\mathrm{J}_k\mathrm{R}_m}}}{1 + \frac{\frac{2}{3}P_2\gamma_{\mathrm{SE}}}{1+\frac{P_1}{6}\gamma_{\mathrm{J}_k\mathrm{E}}}}\right)\right]^+ \tag{35}$$

The secrecy rate in the second phase, denoted as $\dot{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m,\mathrm{J}_k}$, is expressed as follows:

$$\dot{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m,\mathrm{J}_k} = \left[\frac{1}{2}\log_2\left(\frac{1 + \frac{\frac{2}{3}P_3\gamma_{\mathrm{R}_m\mathrm{D}}}{1+\frac{P_1}{6}\gamma_{\mathrm{J}_k\mathrm{D}}}}{1 + \frac{\frac{2}{3}P_2\gamma_{\mathrm{SE}}}{1+\frac{P_1}{6}\gamma_{\mathrm{J}_k\mathrm{E}}} + \frac{\frac{2}{3}P_3\gamma_{\mathrm{R}_m\mathrm{E}}}{1+\frac{P_1}{6}\gamma_{\mathrm{J}_k\mathrm{E}}}}\right)\right]^+ \tag{36}$$

The transmission in this method is in outage when there is no pair of $(\mathrm{J}_k, \mathrm{R}_m)$, for $1 \leq k \leq N$ and $1 \leq m \leq M$, satisfying the condition $\left(\dot{\mathcal{R}}_{\mathrm{R}_m,\mathrm{S},\mathrm{J}_k} > R_t\right) \cap \left(\dot{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m,\mathrm{J}_k} > R_t\right)$. The outage probability, denoted as P^{II}_{out}, is expressed as follows:

$$P^{II}_{out} = \Pr\left\{\bigcap_{k=1}^{N}\bigcap_{m=1}^{M}\overline{\left(\dot{\mathcal{R}}_{\mathrm{R}_m,\mathrm{S},\mathrm{J}_k} > R_t\right) \cap \left(\dot{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m,\mathrm{J}_k} > R_t\right)}\right\} \tag{37}$$

4.3. Outage performance with the BFC method

In this scenario, only the source transmits the signal in the first timeslot, as in the TDF method. All relays R_l and J_k act as the relay, similar to the case presented in section 4.1. The nodes that securely and successfully decode the source message in the first phase form the relay group $\mathcal{L}_3$. Consider the case that $|\mathcal{L}_3| = n \geq 1$, all of the relays in $\mathcal{L}_3$ form a beamformer which is $w = (w_1, \ldots, w_n)^T$, $\|w\| = 1$, to maximize the secrecy rate [20]. For a specific group of $\mathcal{L}_3 = \{L_1, \ldots, L_d, \ldots, L_n\}$, where L_d are selected from the relays and jammers, $1 \leq d \leq n$, $L_d \in \mathcal{P}_\mathrm{R} \cup \mathcal{P}_\mathrm{J}$. We denote $h_{\mathcal{L}_3,i}$ as the CSI vector from nodes in $\mathcal{L}_3$ to node i, where $i \in \{\mathrm{D}, \mathrm{E}\}$. Mathematically, $h_{\mathcal{L}_3,i} = \left(h_{L_1 i}, \ldots, h_{L_d i}, \ldots, h_{L_n i}\right)^H$. It should be noted that x^H is the conjugate transpose of vector x. Each node L_d then transmits the signal s with power $\frac{2}{3}\left(P_1 + P_3\right)$ and weight w_d in the second phase. This power value results in the same energy, the amount that is used for both jamming and relaying in the proposed method. Therefore, node D and E receive the signals as follows:

$$y_{\mathrm{D},2} = \sqrt{\frac{2}{3}\left(P_1 + P_3\right)}h^H_{\mathcal{L}_3,\mathrm{S}}w\ s + n_{\mathrm{D},2} \tag{38}$$

$$y_{\mathrm{E},2} = \sqrt{\frac{2}{3}\left(P_1 + P_3\right)}h^H_{\mathcal{L}_3,\mathrm{E}}w\ s + n_{\mathrm{E},2}\,. \tag{39}$$

Node E employs MRC for the two signals received in two timeslots. As a result, the secrecy rate at D is

$$\ddot{\mathcal{R}}_D = \begin{cases} \frac{1}{2}\log_2\left(\frac{1+\frac{2}{3}(P_1+P_3)w^H h_{\mathcal{L}_3,\mathrm{D}} h^H_{\mathcal{L}_3,\mathrm{D}} w}{1+\frac{2}{3}P_2\gamma_{\mathrm{SE}}+\frac{2}{3}(P_1+P_3)w^H h_{\mathcal{L}_3,\mathrm{E}} h^H_{\mathcal{L}_3,\mathrm{E}} w}\right), |\mathcal{L}_3| \neq 0 \\ 0, |\mathcal{L}_3| = 0 \end{cases} \tag{40}$$

The weight vector w conditioned on $|\mathcal{L}_3| = n \neq 0$ is based on

$$\max_{w} \ddot{\mathcal{R}}_D \qquad \text{s.t. } \|w\| = 1 \tag{41}$$

The beamformer was resolved by J. Li *et al.* (see section III.A in [28]). The outage probability, denoted as P^{III}_{out}, is as follows:

$$P^{III}_{out} = 1 - \sum_{n=0}^{M} \Pr\left\{(|\mathcal{L}_3| = n)\, n\left(\ddot{\mathcal{R}}_D > R_t\right)\right\} \tag{42}$$

4.4. The application of PLS to secure the sharing seed: lower-bound of outage probability of D-BF-CJ in the extreme case

In this section, the D-BF-CJ method is assumed to use PLS to protect the shared seed. To avoid any confusion, we term the NCJ message $\mathcal{M}_k$, for $k \in \{1, \ldots, N\}$, as the common seed (CS) to generate the same jamming signals at jammers in the scope of this subsection [4]. Application of the PLS into protecting the seed and data transmissions still requires the three timeslots as same as in the proposed method.

Transmission in the first timeslot. Suppose that J_k transmits u_k which presents the message $\mathcal{M}_k$. Node j, where $j \in \{J_1, \ldots, J_N\} \backslash J_k$, receives the signal as follows:

$$y_{j,1} = \sqrt{\dot{P}_1} h_{\mathrm{J}_k j} u_k + n_{j,1} \tag{43}$$

where $\dot{P}_1$ is the transmitting signal power. The capacities at node j is thus: $C_{j,\mathrm{J}_k} = \frac{1}{3}\log_2\left(1 + P_1\gamma_{\mathrm{J}_k j}\right)$. Therefore, the secrecy rate at node j, where $j \neq \mathrm{E}$, is as follows:

$$\begin{aligned} \mathcal{R}_{j,\mathrm{J}_k} &= \left[C_{j,\mathrm{J}_k} - C_{\mathrm{E},\mathrm{J}_k}\right]^+ \\ &= \frac{1}{3}\left[\log_2\left(\frac{1 + P_1\gamma_{\mathrm{J}_k j}}{1 + P_1\gamma_{\mathrm{J}_k \mathrm{E}}}\right)\right]^+ \\ &\approx \frac{1}{3}\log_2\left(\frac{\gamma_{\mathrm{J}_k j}}{\gamma_{\mathrm{J}_k \mathrm{E}}}\right), \quad \text{for } P_1 \gg 1\,. \end{aligned} \tag{44}$$

In general, it is not necessary that all jammers are required to decode the CS message $\mathcal{M}_k$. Therefore, we denote $\mathcal{Q}_{J_k}$ as the subset of jammers which obtains the CS message from the broadcast of J_k, and it is expressed by $\mathcal{Q}_{J_k} = \{Q_1, \ldots, Q_i, \ldots, Q_n\}$, where $\left|\mathcal{Q}_{J_k}\right| = n$. Therefore, $n \leq N$. The condition allows all jammers in $\mathcal{Q}_{J_k}$ to securely and successfully decode the CS message is as follows:

$$\min_{j\, \in \mathcal{Q}_{J_k},\ j \neq J_k} \left\{\mathcal{R}_{j,\mathrm{J}_k}\right\} > R_{cs} \tag{45}$$

The D-BF-CJ requires at least two jammers to perform the beamforming. Therefore, the system is immediately in outage if there is no set of $\mathcal{Q}_{J_k}$, for $n \geq 2$ and for all $k \in \{1, \ldots, N\}$, satisfying the condition (45). Equivalently, the system is immediately in outage when

$$\max_{j\, \in \mathcal{Q}_{J_k}, j \neq J_k, \left|\mathcal{Q}_{J_k}\right| = N} \left\{\mathcal{R}_{j,\mathrm{J}_k}\right\} < R_{cs}, \quad \forall 1 \leq k \leq N \tag{46}$$

Transmission in the second timeslot. Assuming that we already successfully find a set of $\mathcal{Q}_{J_k}$, where $2 \leq \left|\mathcal{Q}_{J_k}\right| \leq N$, all jammers then join into the D-BF-CJ. Let us consider the case when R_m is selected the active relay. The received signal at R_m, where $1 \leq m \leq M$, and E in the second phase as follows:

$$y_{\mathrm{R}_m,2} = \sqrt{P_2} h_{\mathrm{R}_m\mathrm{S}}\, s + \sqrt{\dot{P}_2} h^H_{\mathcal{Q}_{J_k},\mathrm{R}_m} w_{\mathcal{Q}_{J_k},1} x + n_{\mathrm{R}_k,2} \tag{47}$$

$$y_{\mathrm{E},2} = \sqrt{P_2} h_{\mathrm{SE}}\, s + \sqrt{\dot{P}_2} h^H_{\mathcal{Q}_{J_k},\mathrm{E}} w_{\mathcal{Q}_{J_k},1} x + n_{E,2} \tag{48}$$

where a specific $\mathcal{Q}_{J_k}$ group is expressed by $\mathcal{Q}_{J_k} = \{Q_1, \ldots, Q_i, \ldots, Q_n\}$, where $\left|\mathcal{Q}_{J_k}\right| = n$, and Q_i is selected from the jammer group. $\dot{P}_2$ is the transmitting power of the jamming signal x. Further, x is the jamming signal which is a random Gaussian signal with zero mean and unit variance, and it does not contain any information. $h_{\mathcal{Q}_{J_k},j}$ is the instantaneous CSI of the group $\mathcal{Q}_{J_k}$ to node j, $h_{\mathcal{Q}_{J_k},j} = \left(h_{Q_1 j}, \ldots, h_{Q_i j}, \ldots, h_{Q_n j}\right)^H$. Further, $w_{\mathcal{Q}_{J_k},l}$ is the weight vector, where $w_{\mathcal{Q}_{J_k},l} = (w_{l1}, \ldots, w_{ln})^T$ and $l \in \mathbb{N}$. The notation $n_{j,i}$ is defined as the Gaussian noise with zero mean and unit variance at node j in the i-th phase. The secrecy rate at R_m is expressed as follows:

$$\widetilde{\mathcal{R}}_{\mathrm{R}_m} = \begin{cases} \frac{1}{3}\log_2\left(\frac{1+\frac{P_2\gamma_{\mathrm{SR}_m}}{1+\dot{P}_2 w^H_{\mathcal{Q}_{J_k},1} h_{\mathcal{Q}_{J_k},\mathrm{R}_m} h^H_{\mathcal{Q}_{J_k},\mathrm{R}_m} w_{\mathcal{Q},1}}}{1+\frac{P_2\gamma_{\mathrm{SE}}}{1+\dot{P}_2 w^H_{\mathcal{Q}_{J_k},1} h_{\mathcal{Q}_{J_k},\mathrm{E}} h^H_{\mathcal{Q}_{J_k},\mathrm{E}} w_{\mathcal{Q}_{J_k},1}}}\right), \left|\mathcal{Q}_{J_k}\right| \geq 2 \\ 0, \left|\mathcal{Q}_{J_k}\right| < 2 \end{cases} \tag{49}$$

The weight vector $w_{\mathcal{Q}_{J_k},1}$ is then calculated to optimize the secrecy rate at R_m and maintaining no interference

[4] The CS message is not necessary to be the same length in bits as the binary information message of the source, and thus, R_{cs} is defined as the target transmission rate corresponding to transmitting the CS message. R_{cs} can have a different value from R_t.

at R_m as follows:

$$\max_{w_{\mathcal{Q}_{J_k},1}} \widetilde{\mathcal{R}}_{\mathrm{R}_m,\mathcal{Q}_{J_k}}, \quad \text{s.t.} \left\| w_{\mathcal{Q}_{J_k},1} \right\| = 1 \text{ and } h^H_{\mathcal{Q}_{J_k},\mathrm{R}_m} w_{\mathcal{Q}_{J_k},1} = 0 \tag{50}$$

In that case, $\widetilde{\mathcal{R}}_{\mathrm{R}_m}$ is rewritten as follows:

$$\widetilde{\mathcal{R}}_{\mathrm{R}_m,\mathcal{Q}_{J_k}} = \begin{cases} \frac{1}{3}\log_2\left(\dfrac{1+P_2\gamma_{\mathrm{SR}_m}}{1+\frac{P_2\gamma_{\mathrm{SE}}}{1+\dot{P}_2 w^H_{\mathcal{Q}_{J_k},1} h_{\mathcal{Q}_{J_k},\mathrm{E}} h^H_{\mathcal{Q}_{J_k},\mathrm{E}} w_{\mathcal{Q}_{J_k},1}}}\right), & \left|\mathcal{Q}_{J_k}\right| \geq 2 \\ 0, \left|\mathcal{Q}_{J_k}\right| < 2 \end{cases} \tag{51}$$

As a result, the problem (50) is reformed as follows [13]:

$$\max_{w_{\mathcal{Q}_{J_k},1}} w^H_{\mathcal{Q}_{J_k},1} h_{\mathcal{Q}_{J_k},\mathrm{E}} h^H_{\mathcal{Q}_{J_k},\mathrm{E}} w_{\mathcal{Q}_{J_k},1}, \quad \text{s.t.} \left\| w_{\mathcal{Q}_{J_k},1} \right\| = 1 \text{ and } h^H_{\mathcal{Q}_{J_k},\mathrm{R}_m} w_{\mathcal{Q}_{J_k},1} = 0 \tag{52}$$

R_m successfully and securely decodes the source message if the following condition is satisfied:

$$\widetilde{\mathcal{R}}_{\mathrm{R}_m} \geq R_t \tag{53}$$

Transmission in the third timeslot. Let us consider the case when R_m successfully and securely decodes the source message. In this case, R_m will forward the source message to D and the jammers in $\mathcal{Q}_{J_k}$ performs their jamming task in the third phase. Node j, where $j \in \{\mathrm{D}, \mathrm{E}\}$, receives the signal as follows:

$$y_{j,3} = \sqrt{P_3} h_{\mathrm{R}_m\mathrm{D}}\, s + \sqrt{\dot{P}_3} h^H_{\mathcal{Q}_{J_k},\mathrm{D}} w_{\mathcal{Q}_{J_k},2}\, y + n_{j,D} \tag{54}$$

where $\dot{P}_3$ is the transmitting power of the jamming signal y. Further, y is the jamming signal which is a random Gaussian signal with zero mean and unit variance. It is not as same as the signal x because the CS allows jammers in $\mathcal{Q}_{J_k}$ to generate the same random signal.

The secrecy rate at D is defined and expressed as follows[5]:

$$\widetilde{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m,\mathcal{Q}_{J_k}} = \begin{cases} \frac{1}{3}\log_2\left(\dfrac{1+P_3\gamma_{\mathrm{R}_m\mathrm{D}}}{\left(1+\frac{P_2\gamma_{\mathrm{SE}}}{1+\dot{P}_2 w^H_{\mathcal{Q}_{J_k},1} h_{\mathcal{Q}_{J_k},\mathrm{E}} h^H_{\mathcal{Q}_{J_k},\mathrm{E}} w_{\mathcal{Q}_{J_k},1}} + \frac{P_3\gamma_{\mathrm{R}_m\mathrm{E}}}{1+\dot{P}_3 w^H_{\mathcal{Q}_{J_k},2} h_{\mathcal{Q}_{J_k},\mathrm{E}} h^H_{\mathcal{Q}_{J_k},\mathrm{E}} w_{\mathcal{Q}_{J_k},2}}\right)}\right), & \left|\mathcal{Q}_{J_k}\right| \geq 2 \\ 0, \left|\mathcal{Q}_{J_k}\right| < 2 \end{cases} \tag{55}$$

according to the maximization [13]:

$$\max_{w_{\mathcal{Q}_{J_k},2}} w^H_{\mathcal{Q}_{J_k},2} h_{\mathcal{Q}_{J_k},\mathrm{E}} h^H_{\mathcal{Q}_{J_k},\mathrm{E}} w_{\mathcal{Q}_{J_k},2}, \quad \text{s.t.} \left\| w_{\mathcal{Q}_{J_k},2} \right\| = 1 \text{ and } h^H_{\mathcal{Q}_{J_k},\mathrm{D}} w_{\mathcal{Q}_{J_k},2} = 0\,. \tag{56}$$

Note that $w_{\mathcal{Q}_{J_k},1}$ is already determined in the second timeslot. Both maximization problems in (52) and (56) were already resolved in [13]. The total power consumed at the jammers in $\mathcal{Q}$ is $\dot{P}_1 + \dot{P}_2 + \dot{P}_3$, this value must be the same as the power used in the active jammer in the proposed method. Therefore, $\dot{P}_1 + \dot{P}_2 + \dot{P}_3 = P_1$. In this article, for the simplification, we equally uses the same power as follows: $\dot{P}_1 = \dot{P}_2 = \dot{P}_3 = P_1/3$.

Lower-bound of Outage Probability. The condition that allows a specific J_k jammer (as the active jammer), a specific $\mathcal{Q}_{J_k}$ set of jammers and relay R_m (as the active relay) to provide a successful and secure transmission for the source message is expressed as follows:

$$\mathcal{T}_4\left(\mathcal{Q}_{J_k}, \mathrm{R}_m\right) \triangleq \left(\min_{j\in\mathcal{Q}_{J_k}, j\neq J_k} \left\{\mathcal{R}_{j,\mathrm{J}_k}\right\} > R_{cs}\right) \cap \left(\widetilde{\mathcal{R}}_{\mathrm{R}_m,\mathcal{Q}_{J_k}} > R_t\right) \cap \left(\widetilde{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m,\mathcal{Q}_{J_k}} > R_t\right) \tag{57}$$

It is clear that

$$\Pr\left\{\mathcal{T}_4\left(\mathcal{Q}_{J_k}, \mathrm{R}_m\right)\right\} \leq \Pr\left\{\underbrace{\left(\widetilde{\mathcal{R}}_{\mathrm{R}_m,\mathcal{Q}_{J_k}} > R_t\right) \cap \left(\widetilde{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m,\mathcal{Q}_{J_k}} > R_t\right)}_{\mathcal{T}_5\left(\mathcal{Q}_{J_k},\mathrm{R}_m\right)}\right\} \tag{58}$$

[5] The eavesdropper can use the MRC while D is impossible. It is because the direct link from S to D is unavailable.

It is easy to find that $\mathcal{Q}_{J_k} \subset \mathcal{P}_J$. Further, the value of $\max_{w_{\mathcal{Q}_{J_k},1}} w^H_{\mathcal{Q}_{J_k},1} h_{\mathcal{Q}_{J_k},\mathrm{E}} h^H_{\mathcal{Q}_{J_k},\mathrm{E}} w_{\mathcal{Q}_{J_k},1}$ corresponding to the maximization problem (52) is less than the value of $\max_{w_{\mathcal{P}_J,1}} w^H_{\mathcal{P}_J,1} h_{\mathcal{P}_J,\mathrm{E}} h^H_{\mathcal{P}_J,\mathrm{E}} w_{\mathcal{P}_J,1}$ with the constraints $\left\| w_{\mathcal{P}_J,1} \right\| = 1$ and $h^H_{\mathcal{P}_J,\mathrm{R}_m} w_{\mathcal{P}_J,1} = 0$, because of $\mathcal{Q}_{J_k} \subset \mathcal{P}_J$ [6]. As a result, $\widetilde{\mathcal{R}}_{\mathrm{R}_m,\mathcal{Q}_{J_k}} \le \widetilde{\mathcal{R}}_{\mathrm{R}_m,\mathcal{P}_J}$. Similarly, we also have $\widetilde{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m,\mathcal{Q}_{J_k}} < \widetilde{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m,\mathcal{P}_J}$. As a result,

$$\begin{aligned} &\Pr\left\{\mathcal{T}_4\left(\mathcal{Q}_{J_k}, \mathrm{R}_m\right)\right\} \\ &\quad \le \Pr\left\{\mathcal{T}_5\left(\mathcal{Q}_{J_k}, \mathrm{R}_m\right)\ \right\} \\ &\quad \le \Pr\left\{\underbrace{\left(\widetilde{\mathcal{R}}_{\mathrm{R}_m,\mathcal{P}_J} > R_t\right) \cap \left(\widetilde{\mathcal{R}}_{\mathrm{D},\mathrm{R}_m,\mathcal{P}_J} > R_t\right)}_{\mathcal{T}_6(\mathcal{P}_J, R_m)}\right\}. \end{aligned} \tag{59}$$

The condition $\mathcal{T}_6\left(\mathcal{P}_J, R_m\right)$ indicates the case that all jammers always obtain the CS message and they join into the jamming tasks in the second and third timeslots.

The system is in outage when we cannot find any specific J_k jammer, a specific $\mathcal{Q}_{J_k}$ set of jammers and relay R_m to satisfy the condition $\mathcal{T}_4\left(\mathcal{Q}_{J_k}, \mathrm{R}_m\right)$. As a result, the outage probability is expressed as follows:

$$P^{IV}_{out} = \Pr\left(\bigcap_{k=1}^{N} \bigcap_{n=2}^{N} \bigcap_{i=1}^{C^N_n} \bigcap_{m=1}^{M} \left(\overline{\mathcal{T}_4\left(\mathcal{Q}_{J_k}, \mathrm{R}_m\right)}\right)\right) \tag{60}$$

where n is the size of the specific $\mathcal{Q}_{J_k}$ set.

It is clear that the condition $\mathcal{T}_4\left(\mathcal{Q}_{J_k}, \mathrm{R}_m\right)$ is stricter than $\mathcal{T}_5\left(\mathcal{Q}_{J_k}, \mathrm{R}_m\right)$ (see (57) and (58)). Further, $\mathcal{T}_5\left(\mathcal{Q}_{J_k}, \mathrm{R}_m\right)$ is stricter than $\mathcal{T}_6\left(\mathcal{P}_J, R_m\right)$ (see (58) and (59)). As a result, the lower-bound of the outage probability is expressed as follows:

$$\begin{aligned} P^{IV}_{out} &\ge P^{IV,low}_{out} \\ &= \Pr\left(\bigcap_{k=1}^{N} \bigcap_{n=2}^{N} \bigcap_{i=1}^{C^N_n} \bigcap_{m=1}^{M} \left(\overline{\mathcal{T}_6\left(\mathcal{P}_J, R_m\right)}\right)\right) \\ &= \Pr\left(\bigcap_{m=1}^{M} \left(\overline{\mathcal{T}_6\left(\mathcal{P}_J, R_m\right)}\right)\right) \end{aligned} \tag{61}$$

Here, it should be noted that $\mathcal{T}_6\left(\mathcal{P}_J, R_m\right)$ expresses that looser case that all jammers always obtain the CS message. Therefore, the lower bound outage probability $P^{IV,low}_{out}$ is no longer dependent of the active jammer selection, size and combination of specific set $\mathcal{Q}_{J_k}$.

In this article, we simulate the lower-bound outage performance $P^{IV,low}_{out}$ of the D-BF-CJ to compare with that of the proposed method.

5. Simulations and Discussions

Nodes S, D and E are located at coordinates $(0, 0)$, $(1, 0)$ and $(x_\mathrm{E}, y_\mathrm{E})$, respectively. M relays R_l, for $1 \le l \le M$, are uniformly distributed in a circle centered at the point C_R with radius r_R. Similarly, jammers J_k are uniformly distributed in the region bounded by the circle with central point C_J and radius r_J. These locations are depicted in Fig. 2. In this simulation, we set C_R to be the same as C_J, and $r_\mathrm{R} = r_\mathrm{J}$, because the relays and jammers are typically in the same region in practice. $\mathrm{C}_\mathrm{R} \equiv \mathrm{C}_\mathrm{J}\,(0.5, 0)$ and $r_\mathrm{R} = r_\mathrm{J} = 0.25$. The transmitting powers are set as follows: $P_1 = 10$, $P_2 = 10$ and $P_3 = 10$. It should be noted that noise powers are normalized at the unit. The path loss is $\vartheta = 4$. The target transmission rate is set at $R_t = 0.25$ (bits/s/Hz). For each scenario regarding the random positions of relays and jammers, we measure the outage performance which is presented in term of outage probability (OPR). The average outage performance (AOP) is then calculated based on a sufficient number of the OPRs with respect to that various scenarios of positions of relays and jammers are surveyed. Thus, average outage probability (AOPR) is considered as metric to present the AOP in this article[7].

The AOPR as a function of the number of relays, M, is depicted in Fig. 3. The number of jammers is fixed at $N = 6$. Two positions of E are surveyed; they are $\mathrm{E}\,(0, 0.1)$ and $\mathrm{E}\,(0, 0.2)$, resulting in the distance d_SE equal to 0.1 and 0.2, respectively. Observing the figure, we can see that the analysis and simulation are matched with each other in the proposed method. In TDF, SJJ and BFC, the figure validates that the proposed method obtains considerable improvement in the AOP, as compared to the current methods of TDF, SJJ and BFC.

[6] We can observe this rule by comparing two simple cases. *i*) $A = max_{\omega_1,\omega_2}\left\{\omega_1 a_1 + \omega_2 a_2\right\}$ s.t. $\omega_1 b_1 + \omega_2 b_2 = 0$ and $\sqrt{|\omega_1|^2 + |\omega_2|^2} = 1$. *ii*) $B = max_{\omega_1,\omega_2,\omega_3}\left\{\omega_1 a_1 + \omega_2 a_2 + \omega_3 a_3\right\}$ s.t. $\omega_1 b_1 + \omega_2 b_2 + \omega_3 b_3 = 0$ and $\sqrt{|\omega_1|^2 + |\omega_2|^2 + |\omega_3|^2} = 1$. It is easy to find that by setting $\omega_3 = 0$, the problem *ii*) becomes as same as the problem *i*). Therefore, $B \ge A$.

[7] The term of "theo-prop" indicates the theoretical AOPR of the proposed method, in which every OPR corresponding to a specific scenario of the positions of relays and jammers is calculated based on (23). The term of "sim-prop" is referred to as the simulated AOPR of the proposed method. For the methods of TDF, SJJ and BFC, their OPRs of a specific scenario of locations of relays and jammers are obtained by simulation, which is on the basis of expressions (34), (37) and (42), respectively. Their AOPR is obtained on the basis of the sufficient number of their OPR values with respect to that various scenarios of locations of relays and jammers are observed. For D-BF-CJ, we simulate its lower-bound of OPR (see (61)) and then calculate the respective simulated lower-bound of AOPR.

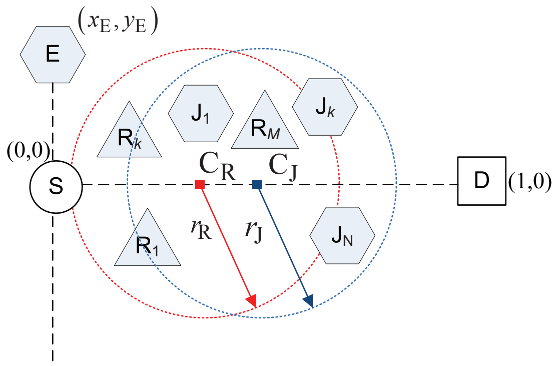

Figure 2. Locations of nodes in the system

In the proposed method, the increase in the number of relays does not create much improvement because of this reasons. The outage performance depends highly on the transmission of the NCJ message from the active jammer, rather than depending on the decode-and-forward of the NCM message. In other words, when M increases to a large number, T_2 appoaches 1. As a result, $P_{\text{suc},1} \rightarrow T_1$, and $P_{\text{suc},1}$ no longer heavily depends on M. We can see that the AOPRs of TDF, SJJ and BFC are very high because of the high SNR at E.

Now, let us discuss the lower-bound of the D-BF-CJ in Fig. 3. For a eavesdropper position which is not very strictly close to the source such as $E(0, 0.2)$ in the figure, D-BF-CJ can offer the outperformance as compared to the proposed method, as seen in the range of $M > 6$, because the distance between the source and the eavesdropper is not sufficiently close, and thus, the received jamming signal is considerably stronger than the source signal. However, if the eavesdropper locates very close to source, AOP of D-BF-CJ is rapidly degraded (meaning that AOPR rapidly increases) as seen in the case of $E(0, 0.1)$ in the figure. Here, the proposed method considerably outperforms D-BF-CJ.

The next survey attempts to investigate the importance of the use of multiple jammers in the proposed method, as shown in Fig. 4. We fix the number of relays at $M = 5$ while changing the number of jammers. We can see that the increase in N results in a considerable change in the AOP. The AOPR decreases as N increases. Meanwhile, the AOPRs of the TDF, SJJ and BFC methods are nearly the same and at a high value as N increases. The D-BF-CJ can outperform the proposed method only when source and the eavesdropper is not sufficiently close to each other, as seen in the case of $E\,(0, 0.2)$. The lower-bound AOPR of D-BF-CJ is below that of the proposed method in this case. However, Fig. 4 confirms again that the proposed methods is superior to all of the remaining if E locates very close to S, as seen in the case of $E\,(0, 0.1)$. We also observe several properties as follows. The greater number of jammers is used, the greater benefit is created by the jammers in the proposed method (also in the D-BF-CJ). Thus, this figure validates the effective exploitation of the spatial diversity with multiple jammers in the proposed method.

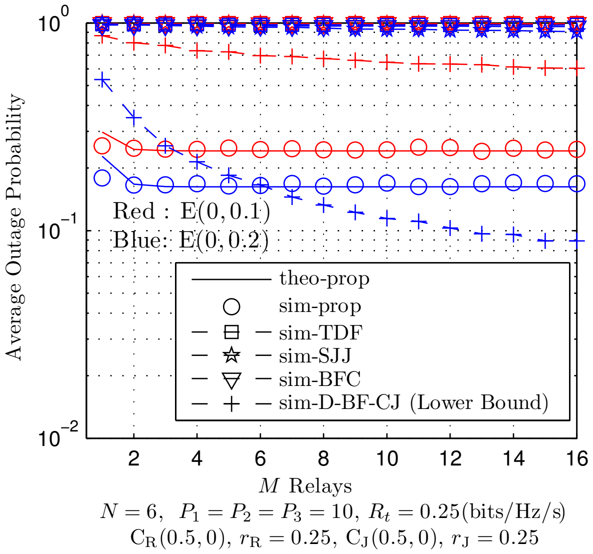

Figure 3. Outage probability in relation to changes in the number of relays with $N = 6$.

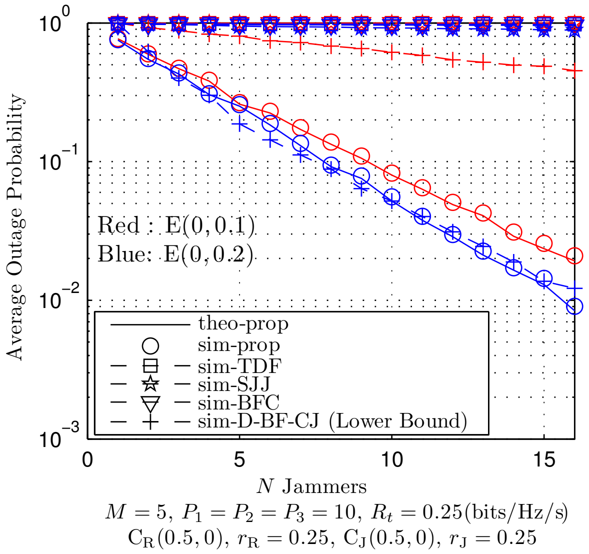

Figure 4. Outage performance in relation to the changes in the number of jammers with a fixed number of relays $M = 5$.

Fig. 5 evaluates the AOPR as a function of the target transmission rate. We set $N = 3$ and $M = 6$. Although the pre-log factor in the secrecy rates in the proposed method is 1/3, the AOP of the proposed method is still better than the TDF, SJJ and BFC methods when R_t changes. Because the distance between S and E

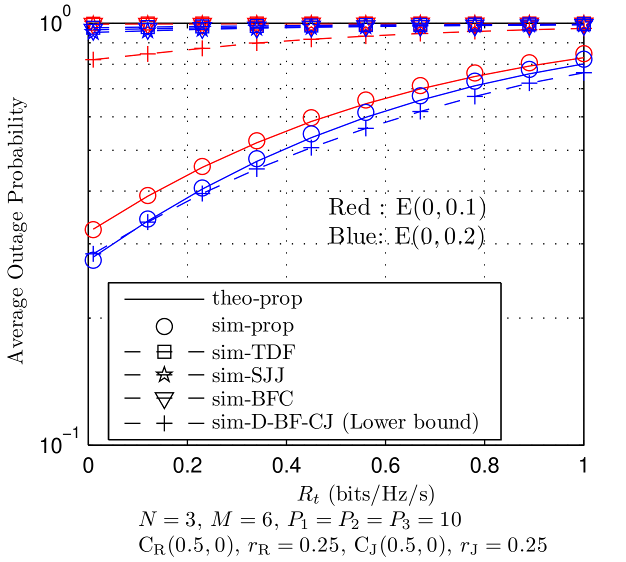

Figure 5. Outage performance in relation to the changes in the target transmission rate R_t. $M = 6$, $N = 3$.

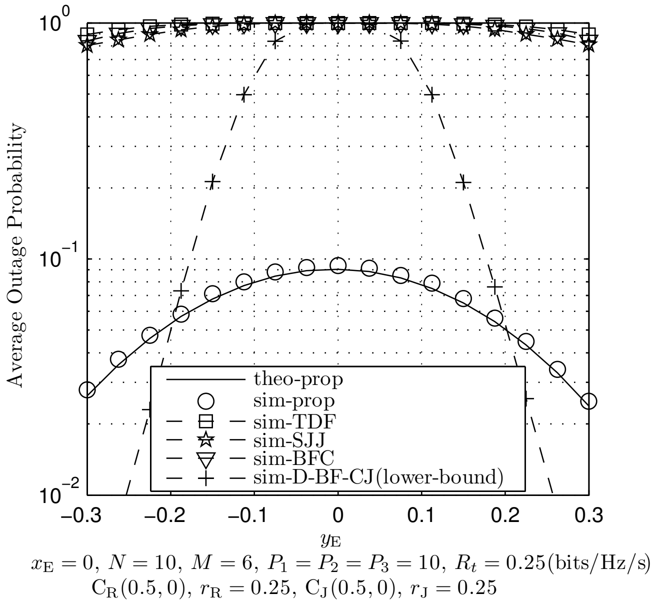

Figure 6. Outage performance in relation to the changes in the possition of the eavesdropper. $M = 6$, $N = 10$.

is not sufficiently close, we can see that the lower-bound of AOPR corresponding to D-BF-CJ is less than the AOPR of the proposed method, as seen in the case of $E(0, 0.2)$. The proposed method has a considerable outperformance of AOPR as compared with that of D-BF-CJ when E is very close to S, because the effect of jamming is not sufficiently stronger than the wiretapping channel, as seen in the case of $E(0, 0.1)$. This means that the advantages created by the binary jamming method not only compensate for the degradation resulting from the use of three phases, but it also creates more opportunities for a successful transmission in such the extreme case as already mentioned.

Characteristics of the AOPR when the distance from S to E, d_{SE}, changes are depicted in Fig. 6. Here, we change d_{SE} by moving the eavesdropper along the y-axis; thus $d_{\mathrm{SE}} = |y_{\mathrm{E}}|$. In the region extremely near to the source, $-0.2 \leq y \leq 0.2$, the system is completely in outage for all of the previous PLS methods. Meanwhile, the proposed method still enables opportunities for successful transmission. When d_{SE} increases, the wiretapping channel is degraded, thus all of the AOPRs decrease and D-BF-CJ can outperform the proposed method as shown in the region $|y_E| \geq 0.2$. However, the proposed method is still superior to the other remaining methods.

6. Conclusions

This article has considered a solution to an extremely strict scenario in wireless PLS, in which the eavesdropper is near to the source to wiretap the source-transmission and the use of cryptographically method to secure the shared seed is vulnerable to being attacked. The direct link of legitimate transmission is even unavailable. We proposed a new method to cope with this case. The binary jamming with triple transmission phases is proposed to provide the physical layer security, protecting the legitimate nodes from wiretapping. TDF, BFC, SJJ and D-BF-CJ are in detail mentioned and compared to the proposed scheme. It shows that these previous schemes are extremely limited while the new one well outperforms in this extreme circumstance. The outage performance in a scenario of multiple jammers and relays are theoretically analyzed and carefully examined by simulation . It presents that simulation and theoretical graphs are well matched.

References

[1] da Silva, E., dos Santos, A.L., Albini, L.C.P. and Lima, M.N. (2008) Identity-based key management in mobile ad hoc networks: techniques and applications. *IEEE Wireless Communications* **15**(5): 46–52. doi:10.1109/MWC.2008.4653131.

[2] Huang, J. and Swindlehurst, A.L. (2011) Cooperative jamming for secure communications in mimo relay networks. *IEEE Transactions on Signal Processing* **59**(10): 4871–4884. doi:10.1109/TSP.2011.2161295.

[3] Krikidis, I., Thompson, J.S. and McLaughlin, S. (2009) Relay selection for secure cooperative networks with

jamming. *IEEE Transactions on Wireless Communications* **8**(10): 5003–5011. doi:10.1109/TWC.2009.090323.

[4] Xiaojun Sun, Wei Xu, M.J. and Zhao, C. (2013) Opportunistic selection for decode-and-forward cooperative networks with secure probabilistic constraints. *Wireless Personal Communications* **70**. doi:https://doi.org/10.1007/s11277-012-0771-7.

[5] Liu, Y., Li, J. and Petropulu, A.P. (2013) Destination assisted cooperative jamming for wireless physical-layer security. *IEEE Transactions on Information Forensics and Security* **8**(4): 682–694. doi:10.1109/TIFS.2013.2248730.

[6] Bloch, M., Barros, J., Rodrigues, M.R.D. and McLaughlin, S.W. (2008) Wireless information-theoretic security. *IEEE Transactions on Information Theory* **54**(6): 2515–2534. doi:10.1109/TIT.2008.921908.

[7] Liu, R., Maric, I., Spasojevic, P. and Yates, R.D. (2008) Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Transactions on Information Theory* **54**(6): 2493–2507. doi:10.1109/TIT.2008.921879.

[8] Barros, J. and D. Rodrigues, M.R. (2006) Secrecy capacity of wireless channels. In *2006 IEEE International Symposium on Information Theory*: 356–360. doi:10.1109/ISIT.2006.261613.

[9] Ding, Z., Leung, K.K., Goeckel, D.L. and Towsley, D. (2011) Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting. *IEEE Transactions on Wireless Communications* **10**(6): 1725–1729. doi:10.1109/TWC.2011.040511.101694.

[10] Parada, P. and Blahut, R. (2005) Secrecy capacity of simo and slow fading channels. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*: 2152–2155. doi:10.1109/ISIT.2005.1523727.

[11] Khisti, A. and Wornell, G.W. (2010) Secure transmission with multiple antennaspart ii: The mimome wiretap channel. *IEEE Transactions on Information Theory* **56**(11): 5515–5532. doi:10.1109/TIT.2010.2068852.

[12] Shafiee, S. and Ulukus, S. (2007) Achievable rates in gaussian miso channels with secrecy constraints. In *2007 IEEE International Symposium on Information Theory*: 2466–2470. doi:10.1109/ISIT.2007.4557589.

[13] Dong, L., Han, Z., Petropulu, A.P. and Poor, H.V. (2010) Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing* **58**(3): 1875–1888. doi:10.1109/TSP.2009.2038412.

[14] Ding, F., Wang, H., Zhang, S. and Dai, M. (2016) Multiuser untrusted relay networks with joint cooperative jamming and opportunistic scheduling under perfect and outdated csi. *Electronics Letters* **52**(23): 1925–1927. doi:https://doi.org/10.1049/el.2016.3079, URL `https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/el.2016.3079`.

[15] Lin, Z., Cai, Y., Yang, W. and Wang, L. (2016) Robust secure switching transmission in multi-antenna relaying systems: cooperative jamming or decode-and-forward beamforming. *IET Communications* **10**(13): 1673–1681. doi:https://doi.org/10.1049/iet-com.2016.0051, URL `https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-com.2016.0051`.

[16] Dang, C., Jiménez-Rodríguez, L., Tran, N.H., Shetty, S. and Sastry, S. (2017) On secrecy rate and optimal power allocation of the full-duplex amplify-and-forward relay wire-tap channel. *IEEE Transactions on Vehicular Technology* **66**(5): 3887–3899. doi:10.1109/TVT.2016.2600658.

[17] Ju, H., Kim, D., Poor, H.V. and Hong, D. (2012) Bi-directional beamforming and its capacity scaling in pairwise two-way communications. *IEEE Transactions on Wireless Communications* **11**(1): 346–357. doi:10.1109/TWC.2011.111611.110970.

[18] Kim, D., Park, S., Ju, H. and Hong, D. (2014) Transmission capacity of full-duplex-based two-way ad hoc networks with arq protocol. *IEEE Transactions on Vehicular Technology* **63**(7): 3167–3183. doi:10.1109/TVT.2014.2302013.

[19] Zheng, G., Krikidis, I., Li, J., Petropulu, A.P. and Ottersten, B. (2013) Improving physical layer secrecy using full-duplex jamming receivers. *IEEE Transactions on Signal Processing* **61**(20): 4962–4974. doi:10.1109/TSP.2013.2269049.

[20] Fan, L., Lei, X., Yang, N., Duong, T.Q. and Karagiannidis, G.K. (2017) Secrecy cooperative networks with outdated relay selection over correlated fading channels. *IEEE Transactions on Vehicular Technology* **66**(8): 7599–7603. doi:10.1109/TVT.2017.2669240.

[21] Shim, K., Do, N.T. and An, B. (2017) Performance analysis of physical layer security of opportunistic scheduling in multiuser multirelay cooperative networks. *Sensors* **17**(2). doi:10.3390/s17020377, URL `https://www.mdpi.com/1424-8220/17/2/377`.

[22] Huang, Y., Wang, J., Zhong, C., Duong, T.Q. and Karagiannidis, G.K. (2016) Secure transmission in cooperative relaying networks with multiple antennas. *IEEE Transactions on Wireless Communications* **15**(10): 6843–6856. doi:10.1109/TWC.2016.2591940.

[23] Jiang, X., Zhong, C., Chen, X., Duong, T.Q., Tsiftsis, T.A. and Zhang, Z. (2016) Secrecy performance of wirelessly powered wiretap channels. *IEEE Transactions on Communications* **64**(9): 3858–3871. doi:10.1109/TCOMM.2016.2592529.

[24] Yan, P., Yang, J., Liu, M., Sun, J. and Gui, G. (2020) Secrecy outage analysis of transmit antenna selection assisted with wireless power beacon. *IEEE Transactions on Vehicular Technology* **69**(7): 7473–7482. doi:10.1109/TVT.2020.2992766.

[25] Kavaiya, S., Patel, D.K., Ding, Z., Guan, Y.L. and Sun, S. (2021) Physical layer security in cognitive vehicular networks. *IEEE Transactions on Communications* **69**(4): 2557–2569. doi:10.1109/TCOMM.2020.3038904.

[26] Yuksel, M. and Erkip, E. (2007) Secure communication with a relay helping the wire-tapper. In *2007 IEEE Information Theory Workshop*: 595–600. doi:10.1109/ITW.2007.4313141.

[27] Aggarwal, V., Sankar, L., Calderbank, A.R. and Poor, H.V. (2009) Secrecy capacity of a class of orthogonal relay eavesdropper channels. In *2009 Information Theory and Applications Workshop*: 295–300. doi:10.1109/ITA.2009.5044960.

[28] Li, J., Petropulu, A.P. and Weber, S. (2011) On cooperative relaying schemes for wireless physical layer security. *IEEE Transactions on Signal Processing* **59**(10): 4985–4997. doi:10.1109/TSP.2011.2159598.

[29] Wang, X., Wang, K. and Zhang, X.D. (2013) Secure relay beamforming with imperfect channel side information. *IEEE Transactions on Vehicular Technology* **62**(5): 2140–2155. doi:10.1109/TVT.2012.2230657.

[30] Jameel, F., Wyne, S. and Ding, Z. (2018) Secure communications in three-step two-way energy harvesting df relaying. *IEEE Communications Letters* **22**(2): 308–311. doi:10.1109/LCOMM.2017.2772244.

[31] Zou, Y., Wang, X. and Shen, W. (2013) Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack. In *2013 IEEE International Conference on Communications (ICC)*: 2183–2187. doi:10.1109/ICC.2013.6654851.

[32] Huang, J. and Swindlehurst, A.L. (2013) Wireless physical layer security enhancement with buffer-aided relaying. In *2013 Asilomar Conference on Signals, Systems and Computers*: 1560–1564. doi:10.1109/ACSSC.2013.6810559.

[33] Haroun, M.F. and Aaron Gulliver, T. (2015) Secret key generation using chaotic signals over frequency selective fading channels. *IEEE Transactions on Information Forensics and Security* **10**(8): 1764–1775. doi:10.1109/TIFS.2015.2428211.

[34] Hui, H., Swindlehurst, A.L., Li, G. and Liang, J. (2015) Secure relay and jammer selection for physical layer security. *IEEE Signal Processing Letters* **22**(8): 1147–1151. doi:10.1109/LSP.2014.2387860.

[35] Ghose, S., Kundu, C. and Bose, R. (2016) Secrecy performance of dual-hop decode-and-forward relay system with diversity combining at the eavesdropper. *IET Communications* **10**(8): 904–914. doi:https://doi.org/10.1049/iet-com.2015.1060, URL https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-com.2015.1060.

[36] Kolokotronis, N., Fytrakis, K., Katsiotis, A. and Kalouptsidis, N. (2015) A cooperative jamming protocol for physical layer security in wireless networks. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*: 5803–5807. doi:10.1109/ICASSP.2015.7179084.

[37] Tran, T.T. and Kong, H.Y. (2014) Csi-secured orthogonal jamming method for wireless physical layer security. *IEEE Communications Letters* **18**(5): 841–844. doi:10.1109/LCOMM.2014.040214.140109.

[38] Zhao, R., Huang, Y., Wang, W. and Lau, V.K.N. (2016) Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming. *IEEE Transactions on Wireless Communications* **15**(4): 2537–2551. doi:10.1109/TWC.2015.2504526.

[39] Shang, Z., Zhang, T., Liu, Y., Cai, Y. and Yang, W. (2019) Secrecy performance analysis of cognitive radio networks with full-duplex relaying. In *2019 IEEE/CIC International Conference on Communications in China (ICCC)*: 700–705. doi:10.1109/ICCChina.2019.8855966.

[40] Tran, T.T. and Kong, H.Y. (2014) An application of network-coding technique into cooperative jamming. In *2014 27th Biennial Symposium on Communications (QBSC)*: 218–222. doi:10.1109/QBSC.2014.6841217.

[41] Tran, T.T. and Kong, H.Y. (2015) A method enabling exploitation of spatial diversity and physical layer security in an extreme case of source-wiretapping without a jamming beamformer. *Journal of Communications and Networks* **17**(5): 482–490. doi:10.1109/JCN.2015.000086.