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

Intercept Probability Analysis of Cooperative Cognitive Networks Using Fountain Codes and Cooperative Jamming

Tran Trung Duy[1,*], Le Chu Khan[1], Nguyen Thanh Binh [1], Nguyen Luong Nhat[1]

[1]Posts and Telecommunications Institute of Technology, HoChiMinh City, Vietnam

Abstract

This paper evaluates intercept probability (IP) of a cooperative cognitive radio network. Using Fountain codes, a secondary source continuously generates encoded packets, and sends them to secondary destination and relay nodes that attempt to receive a sufficient number of the encoded packets for recovering the source data. If the relay can sufficiently collect the packets before the destination, it replaces the source to transmit the encoded packets to the destination. Also in the secondary network, a passive eavesdropper attempts to illegally receive the packets sent by the source and relay nodes, and if it can accumulate enough encoded packets, the source data is intercepted. To enhance secrecy performance, in terms of IP, a cooperative jammer is used to transmit noises on the eavesdropper. We also propose a simple transmit power allocation method for the secondary transmitters such as source, relay and jammer so that outage performance of a primary network is not harmful. We derive an exact closed-form expression of IP over Rayleigh fading channel, and verify it by performing Monte-Carlo simulations.

Received on 23 December 2020; accepted on 22 January 2021; published on 26 January 2021

Keywords: Fountain Codes, underlay cognitive radio networks, physical-layer security, cooperative jamming, intercept probability

doi:10.4108/eai.26-1-2021.168229

1. Introduction

Recently, physical-layer security (PLS) [1–3] has been proposed to provide security for wireless communication systems. To improve secrecy performance of the PLS models, joint transmit and receive diversity methods [4–6] in MIMO (Multiple Input Multiple Output) networks were proposed and analyzed. In [4, 5], a source selects one of its transmit antennas to maximize instantaneous signal-to-noise ratio (SNR) obtained at a destination that employs section combining (SC) or maximal ratio combining (MRC) for decoding source signals. Also in [4, 5], a multi-antenna eavesdropper can use MRC or SC technique to combine overheard signals. In [6], the authors evaluated impact of channel correlation on the secrecy performance of the MIMO wiretap networks using transmit antenna selection (TAS) at the transmitter, and MRC at the legitimate receiver and eavesdropper nodes. In case that the wireless devices have only a single antenna (due to limitation of size, energy and storage), cooperative communication approaches [7–9] can be employed to create a virtual MIMO system. Reference [10] studied optimal relay placement problem to maximize the secrecy performance for SISO (Single Input Single Output) dual-hop decode-and-forward (DF) relaying networks. In addition, the authors in [10] proposed a randomize-and-forward (RF) strategy to prevent the eavesdropper from combining the signals received from source and relay nodes with MRC. Reference [11] proposed various relay selection methods for secrecy performance enhancement at the second transmission phase (cooperative phase) under effect of co-channel interference (CCI). In [12], secrecy outage probability of secure amplify-and-forward (AF) relaying schemes with relay selection in the CCI environments were analyzed. Reference [13] studied the secrecy performance of wirelessly powered wiretap channels, where the transmitter could

*Corresponding author. Email: trantrungduy@ptithcm.edu.vn

harvest energy from wireless signals of a dedicated power beacon, and use the harvested energy to transmit its data. The authors of [14] evaluated secrecy outage probability for a cooperative Non-Orthogonal Multiple Access (NOMA) for both DF and AF relaying networks. Different with [10]-[14], performance of the secure transmission schemes proposed in [15, 16] is measured via outage probability (OP) of data links and intercept probability (IP) of eavesdropping links. As proved in [15, 16], there exists a trade-off between security (IP) and reliability (OP) in the PLS systems.

The secrecy performance can be enhanced by decreasing quality of the eavesdropping channels by using cooperative jamming (CJ) [17–23]. In CJ, jammer nodes are employed to transmit artificial noises on the eavesdroppers. Conventionally, the cooperative jammer and the legitimate destination are near together so that they can securely exchange information about the noises generated by the jammers [18]. As a result, the legitimate destinations can remove the interference components from their received signals while the eavesdroppers cannot. As shown in [19–23], the CJ-based PLS models obtain better secrecy performance as compared with the corresponding ones without using CJ. In [19], the authors studied the security-reliability tradeoff of CJ-based PLS wireless networks with presence of multiple user pairs and multiple eavesdroppers. Reference [20] proposed a secure transmission scheme for down-link Internet of Things (IoT) networks, using cooperative jamming to against multiple eavesdroppers. In [21], the CJ technique is employed to enhance the secrecy performance for the multi-user NOMA systems. Different with [19–21], the jammer nodes in [22, 23] have to harvest wireless energy from ambient sources for performing the CJ operation. Moreover, depending on the harvested energy, various jammer selection methods were proposed in [22, 23] to improve the end-to-end secrecy performance for dual-hop and multi-hop DF relaying networks.

References [24–30] studied the PLS models in underlay cognitive radio networks (UCRNs), where transmitters in a secondary network must reduce their transmit power so that performance of a primary network is not harmful. Reference [24] considered a secure cognitive transmission with a multi-antenna secondary transmitter, a multi-antenna secondary receiver and a multi-antenna passive eavesdropper. In [25] , various joint relay and jammer selection approaches were proposed to enhance the secrecy performance for the secondary network. Different with [24, 25], reference [26] evaluated outage probability (OP) of UCRNs under joint constraints of maximal interference threshold, CCI from the primary network and IP obtained by the eavesdropper. The authors in [27] proposed various relay selection approaches to improve the IP-OP trade-off for UCRNs. Reference [28] introduced a PLS spectrum sharing model consisting of multiple secondary source-destination pairs. Moreover, in [28], when one of the secondary sources is selected to transmit data to its destination, one of the remaining ones is opportunistically employed to play role as the cooperative jammer. The authors of [29] proposed the PLS scheme in dual-hop cognitive radio networks with multiple eavesdroppers who attempt to overhear data of a secondary source at the second hop. In [30], the authors analyzed the secrecy performance of UCRNs under joint constraints of secrecy outage and primary user interference.

Recently, Fountain codes (FCs) [31, 32] have gained much attention due to simple implementation and adaptation with channel conditions. Using FCs, a source can generate a limitless number of the encoded packets (or Fountain packets) that are continuously sent to an intended destination. Then, the original data of the source can be recovered if the destination can obtain a sufficient number of Fountain packets. In [33–37], the PLS systems using FCs were proposed and analyzed. As mentioned in [33], the data transmission between the source and the destination is secure when the destination can receive enough number of Fountain packets before the eavesdropper. Reference [34] proposed a new cooperative jamming approach to protect Fountain packets sent to the destination with assistance of a cooperative relay. The authors of [35] introduced a PLS scheme for the IoT system using FCs. In [36], a MIMO NOMA system was proposed to improve both the reliability and security performance for FCs-based secure transmission, where the source could transmit two Fountain packets to the destination at each time slot. Reference [37] evaluated the security-reliability trade-off for multi-hop Low Energy Adaptive Clustering Hierarchy (LEACH) networks using FCs and CJ. Moreover, in [37], each cluster randomly selects an jammer node to generate noises on the eavesdropper.

This paper proposes an FCs-based PLS scheme in cooperative cognitive radio networks. In the proposed protocol, a secondary source sends Fountain packets to a secondary relay and a secondary destination. After the relay and destination nodes collect enough number of Fountain packets, they send an ACK message back to the source to inform the successful decoding status. If the relay can receive a sufficient number of Fountain packets before the destination, it replaces the source to transmit Fountain packets to the destination. Also in the secondary network, an eavesdropper illegally accumulates Fountain packets for recovering the original data of the source. Hence, if the eavesdropper can sufficiently obtain number of Fountain packets, the source data is intercepted. To protect the source data, a friendly jammer is employed to send noises on the eavesdropper. Moreover, the

jammer is placed near the destination so that they can cooperate with each other to remove the interference components in the signals received at the destination.

In the following, the motivations and main contributions of this paper will be summarized as follows:

- To the best of our knowledge, all the published works related to the PLS systems using FCs (see [33]-[37] and references therein) did not consider the cognitive radio environment. This motivates us to propose and analyze the performance for the FCs-based PLS scheme in UCRNs.
- Similar to [34], cooperative communication and cooperative jamming techniques are employed to enhance the secrecy performance. However, unlike [34], the relay in our proposed scheme does not relay Fountain packets to the destination. Indeed, it will replace the source to transmit the encoded packets when it can recover the original data before the destination. For the cooperative jamming technique proposed in this paper, different with [34], the jammer node in our proposal is near the destination so that the jamming noises at the destination can be removed.
- We propose a simple and efficient transmit power allocation method for the source, relay and jammer nodes to guarantee the outage performance of the primary network.
- We derive an exact closed-form formula of IP for the proposed scheme over Rayleigh fading channel, and verify it by Monte-Carlo simulations.
- For performance comparison, we compare the IP performance of the proposed scheme with the direct transmission scheme which does not use cooperative communication.

The rest of this paper is organized as follows. The system model of the proposed protocol is described in Section 2. Section 3 presents the derived expressions of IP. The simulation results are shown in Section 4. Finally, conclusions are presented in Section 5.

2. System Model

Figure 1 illustrates system model of the proposed scheme. In the primary network, the primary transmitter (PT) communicates with the primary receiver (PR), while in the secondary network, the secondary source (SS) uses FCs to send its data to the secondary destination (SD) via help of the secondary relay (SR). Also in the secondary network, the secondary eavesdropper (SE) attempts to overhear the data of SS. As mentioned above, the secondary jammer (SJ) (near SD) is employed to transmit noises on SE. Assume that all the nodes are

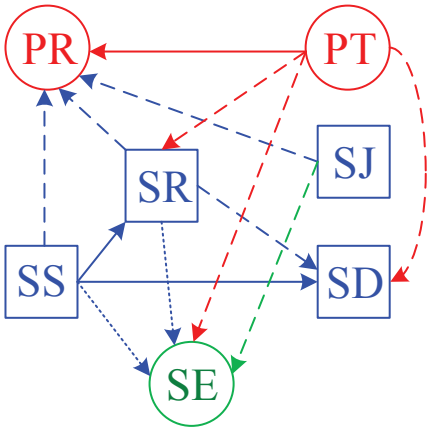

Figure 1. System model of the proposed protocol.

equipped with a single antenna, and operate on a half-duplex mode.

Using FCs, SS divides its original data into small packets with equal length, and some of them are selected, and then appropriately XOR-ed to obtain Fountain packets [36, 37]. Then, SS transmits these encoded packets to SR and SD, while SE attempts to obtain them. To recover the source data, the receivers including SR, SD and SE must obtain at least H Fountain packets [34]-[37]. Due to a delay constraint, total number of Fountain packets that SS and SR can send to SD is limited by $N_{\max}$, where $N_{\max} \geq H$. Moreover, we note that SS and SR will stop their transmission as soon as SD obtains H Fountain packets. As mentioned above, when SE can collect at least H Fountain packets, the source data is intercepted.

Let us denote γ_{XY} as channel gain of the X-Y link, where $X, Y \in \{SS, SR, SD, SE, SJ, PT, PR\}$. Because the considered system operates over Rayleigh fading channel, γ_{XY} is an exponential random variable (RV) whose CDF and PDF are given, respectively as

$$\begin{aligned} F_{\gamma_{XY}}(x) &= 1 - \exp(-\lambda_{XY} x), \\ f_{\gamma_{XY}}(x) &= \lambda_{XY} \exp(-\lambda_{XY} x), \end{aligned} \tag{1}$$

where $\lambda_{XY} = d_{XY}^{\beta}$ [7], d_{XY} is distance between X and Y, and β is path-loss exponential.

2.1. OP of Primary Network

Due to the interference from SX and SJ, $X \in \{S, R\}$, instantaneous signal-to-interference-plus-noise ratio (SINR) of the PT $\rightarrow$ PR link is expressed as

$$\psi_{PTPR} = \frac{P_{PT}\gamma_{PTPR}}{P_{SX}\gamma_{SXPR} + P_{SJ}\gamma_{SJPR} + \sigma_0^2}, \tag{2}$$

where P_{PT}, P_{SX} and P_{SJ} are transmit power of PT, SX and SJ, respectively, and σ_0^2 is variance of additive white Gaussian noise (AWGN) at PT. For ease of presentation, assume that all the AWGNs have zero mean and variance of σ_0^2. From (2), OP of the primary network can be formulated as

$$\begin{aligned}\text{OP} &= \Pr\left(\psi_{\text{PTPR}} < \gamma_{\text{Pth}}\right)\\ &= \Pr\left(\frac{P_{\text{PT}}\gamma_{\text{PTPR}}}{P_{\text{SX}}\gamma_{\text{SXPR}} + P_{\text{SJ}}\gamma_{\text{SJPR}} + \sigma_0^2} < \gamma_{\text{Pth}}\right)\\ &= \Pr\left(\gamma_{\text{PTPR}} < \frac{P_{\text{SX}}\gamma_{\text{Pth}}}{P_{\text{PT}}}\gamma_{\text{SXPR}} + \frac{P_{\text{SJ}}\gamma_{\text{Pth}}}{P_{\text{PT}}}\gamma_{\text{SJPR}} + \frac{\sigma_0^2\gamma_{\text{Pth}}}{P_{\text{PT}}}\right), \quad (3)\end{aligned}$$

where γ_{Pth} is an outage threshold predetermined by the primary network. Using the distributions given in (1), OP in (3) can be computed as

$$\begin{aligned}\text{OP} &= \int_0^{+\infty}\int_0^{+\infty} F_{\gamma_{\text{PTPR}}}\left(\frac{P_{\text{SX}}\gamma_{\text{Pth}}}{P_{\text{PT}}}x + \frac{P_{\text{SJ}}\gamma_{\text{Pth}}}{P_{\text{PT}}}y + \frac{\sigma_0^2\gamma_{\text{Pth}}}{P_{\text{PT}}}\right)\\ &\quad \times f_{\gamma_{\text{SXPR}}}(x) f_{\gamma_{\text{SJPR}}}(y)\, dxdy\\ &= 1 - \frac{\lambda_{\text{SXPR}}P_{\text{PT}}}{\lambda_{\text{SXPR}}P_{\text{PT}} + \lambda_{\text{PTPR}}\gamma_{\text{Pth}}P_{\text{SX}}}\frac{\lambda_{\text{SJPR}}P_{\text{PT}}}{\lambda_{\text{SJPR}}P_{\text{PT}} + \lambda_{\text{PTPR}}\gamma_{\text{Pth}}P_{\text{SJ}}}\\ &\quad \times \exp\left(-\lambda_{\text{PTPR}}\frac{\sigma_0^2\gamma_{\text{Pth}}}{P_{\text{PT}}}\right)\\ &= 1 - \frac{\kappa_{\text{P}}\mu_{\text{X}}\mu_{\text{J}}}{(\mu_{\text{X}} + \theta_{\text{X}})\left(\mu_{\text{J}} + \theta_{\text{J}}\right)}, \quad (4)\end{aligned}$$

where

$$\begin{aligned}\mu_{\text{X}} &= \frac{\lambda_{\text{SXPR}}}{\lambda_{\text{PTPR}}\gamma_{\text{Pth}}}, \mu_{\text{J}} = \frac{\lambda_{\text{SJPR}}}{\lambda_{\text{PTPR}}\gamma_{\text{Pth}}}, \theta_{\text{X}} = \frac{P_{\text{SX}}}{P_{\text{PT}}},\\ \theta_{\text{J}} &= \frac{P_{\text{SJ}}}{P_{\text{PT}}}, \kappa_{\text{P}} = \exp\left(-\lambda_{\text{PTPR}}\frac{\sigma_0^2\gamma_{\text{Pth}}}{P_{\text{PT}}}\right). \quad (5)\end{aligned}$$

2.2. Transmit Power of SS, SR and SJ

To guarantee quality of service (QoS) of the primary network, i.e., OP $\le \varepsilon_{\text{OP}}$ (where ε_{OP} is a pre-determined OP target), the transmit power P_{SX} and P_{SJ} should be adjusted appropriately. We propose a simple transmit power allocation method as follows: At first, we set $P_{\text{SJ}} = \alpha_{\text{X}}P_{\text{SX}}$ (or $\theta_{\text{J}} = \alpha_{\text{X}}\theta_{\text{X}}$) where α_{X} is a constant, and $0 \le \alpha_{\text{X}} < 1$. Next, solving OP $= \varepsilon_{\text{OP}}$, which yields

$$\alpha_{\text{X}}(\theta_{\text{X}})^2 + \left(\alpha_{\text{X}}\mu_{\text{X}} + \mu_{\text{J}}\right)\theta_{\text{X}} + \frac{(1 - \varepsilon_{\text{OP}} - \kappa_{\text{P}})\,\mu_{\text{X}}\mu_{\text{J}}}{1 - \varepsilon_{\text{OP}}} = 0. \quad (6)$$

Our objective now is find positive solutions of θ_{X} in (6). At first, if $1 - \varepsilon_{\text{OP}} - \kappa_{\text{P}} \ge 0$, there does not exist any positive solution. In this case, QoS of the primary network is not guaranteed, and hence SX and SJ are not allowed to access the bands licensed to PT, or their transmit power is set to zero, i.e., $P_{\text{SX}} = P_{\text{SJ}} = 0$. In the case where $1 - \varepsilon_{\text{OP}} - \kappa_{\text{P}} < 0$, we obtain an unique positive solution of θ_{X} as

$$\theta_{\text{X}} = \frac{1}{2\alpha_{\text{X}}} \times \left[\sqrt{\left(\alpha_{\text{X}}\mu_{\text{X}} + \mu_{\text{J}}\right)^2 - \frac{4\alpha_{\text{X}}(1 - \varepsilon_{\text{OP}} - \kappa_{\text{P}})\,\mu_{\text{X}}\mu_{\text{J}}}{1 - \varepsilon_{\text{OP}}}} - \left(\alpha_{\text{X}}\mu_{\text{X}} + \mu_{\text{J}}\right)\right]. \quad (7)$$

Therefore, when $1 - \varepsilon_{\text{OP}} - \kappa_{\text{P}} < 0$, we obtain

$$\begin{cases} P_{\text{SS}} = \theta_{\text{S}}P_{\text{PT}} \\ P_{\text{SJ}} = \alpha_{\text{S}}\theta_{\text{S}}P_{\text{PT}} \end{cases} \text{and} \quad \begin{cases} P_{\text{SR}} = \theta_{\text{R}}P_{\text{PT}} \\ P_{\text{SJ}} = \alpha_{\text{R}}\theta_{\text{R}}P_{\text{PT}} \end{cases} \quad (8)$$

Remark: The SX and SJ nodes must adjust their transmit power before transmitting Fountain packets by using (8). Next, at high P_{PT} values, i.e., $P_{\text{PT}} \to +\infty$, we have $\kappa_{\text{P}} \approx 1$, and equation (7) reduces to

$$\theta_{\text{X}} \approx \frac{1}{2\alpha_{\text{X}}}\left[\sqrt{\left(\alpha_{\text{X}}\mu_{\text{X}} + \mu_{\text{J}}\right)^2 + \frac{4\alpha_{\text{X}}\varepsilon_{\text{OP}}\mu_{\text{X}}\mu_{\text{J}}}{1 - \varepsilon_{\text{OP}}}} - \left(\alpha_{\text{X}}\mu_{\text{X}} + \mu_{\text{J}}\right)\right]. \quad (9)$$

Because θ_{X} in (9) does not depend on P_{PT}, P_{SX} and P_{SJ} are linear functions of P_{PT} at high P_{PT} values.

2.3. Decoding Probability of Fountain Packets

This sub-section calculates the probability that one encoded packet is correctly or incorrectly received by SR, SD and SE. Considering the transmission of one Fountain packet of the source SS; the instantaneous SINR obtained SD, SR and SE can be formulated, respectively as

$$\begin{aligned}\psi_{\text{SSSD}} &= \frac{P_{\text{SS}}\gamma_{\text{SSSD}}}{P_{\text{PT}}\gamma_{\text{PTSD}} + \sigma_0^2},\\ \psi_{\text{SSSR}} &= \frac{P_{\text{SS}}\gamma_{\text{SSSR}}}{P_{\text{PT}}\gamma_{\text{PTSR}} + P_{\text{SJ}}\gamma_{\text{SJSR}} + \sigma_0^2},\\ \psi_{\text{SSSE}} &= \frac{P_{\text{SS}}\gamma_{\text{SSSE}}}{P_{\text{PT}}\gamma_{\text{PTSE}} + P_{\text{SJ}}\gamma_{\text{SJSE}} + \sigma_0^2}. \quad (10)\end{aligned}$$

It is worth noting from (10) that SD can remove the interference caused by SJ while SR and SE cannot. Next, the probability that SD successfully receives one Fountain packet can be calculated as

$$\begin{aligned}\omega_{\text{SD}} &= \Pr\left(\psi_{\text{SSSD}} \ge \gamma_{\text{Sth}}\right)\\ &= \int_0^{+\infty}\left(1 - F_{\gamma_{\text{SSSD}}}\left(\frac{P_{\text{PT}}\gamma_{\text{Sth}}}{P_{\text{SS}}}x + \frac{\sigma_0^2\gamma_{\text{Sth}}}{P_{\text{SS}}}\right)\right) f_{\gamma_{\text{PTSD}}}(x)\, dx\\ &= \frac{\lambda_{\text{PTSD}}\theta_{\text{S}}}{\lambda_{\text{PTSD}}\theta_{\text{S}} + \lambda_{\text{SSSD}}\gamma_{\text{Sth}}}\exp\left(-\lambda_{\text{SSSD}}\frac{\sigma_0^2\gamma_{\text{Sth}}}{P_{\text{SS}}}\right), \quad (11)\end{aligned}$$

where γ_{Sth} is a threshold pre-determined by the secondary network.

For SR; the probability that one Fountain packet is correctly received by SR can be obtained as

$$\begin{aligned}\omega_{\mathrm{SR}} &= \Pr\left(\psi_{\mathrm{SSSR}} \geq \gamma_{\mathrm{Sth}}\right)\\ &= 1 - \int_0^{+\infty}\int_0^{+\infty} F_{\gamma_{\mathrm{SSSR}}}\left(\frac{P_{\mathrm{PT}}\gamma_{\mathrm{Sth}}}{P_{\mathrm{SS}}}x + \frac{P_{\mathrm{SJ}}\gamma_{\mathrm{Sth}}}{P_{\mathrm{SS}}}y + \frac{\sigma_0^2\gamma_{\mathrm{Sth}}}{P_{\mathrm{SS}}}\right)\\ &\quad f_{\gamma_{\mathrm{PTPR}}}(x)\, f_{\gamma_{\mathrm{SJSR}}}(y)\, dxdy\\ &= 1 - \frac{\lambda_{\mathrm{PTSR}}\theta_{\mathrm{S}}}{\lambda_{\mathrm{PTSR}}\theta_{\mathrm{S}} + \lambda_{\mathrm{SSSR}}\gamma_{\mathrm{Sth}}}\frac{\lambda_{\mathrm{SJSR}}}{\lambda_{\mathrm{SJSR}} + \lambda_{\mathrm{SSSR}}\alpha_{\mathrm{S}}\gamma_{\mathrm{Sth}}}\\ &\quad \times \exp\left(-\lambda_{\mathrm{SSSR}}\frac{\sigma_0^2\gamma_{\mathrm{Sth}}}{P_{\mathrm{SS}}}\right). \end{aligned} \tag{12}$$

Similarly, we can calculate probability of the successful decoding at SE as

$$\begin{aligned}\omega_{\mathrm{SE}} &= \Pr\left(\psi_{\mathrm{SSSE}} \geq \gamma_{\mathrm{Sth}}\right)\\ &= \frac{\lambda_{\mathrm{PTSE}}\theta_{\mathrm{S}}}{\lambda_{\mathrm{PTSE}}\theta_{\mathrm{S}} + \lambda_{\mathrm{SSSE}}\gamma_{\mathrm{Sth}}}\frac{\lambda_{\mathrm{SJSE}}}{\lambda_{\mathrm{SJSR}} + \lambda_{\mathrm{SSSE}}\alpha_{\mathrm{S}}\gamma_{\mathrm{Sth}}}\\ &\quad \times \exp\left(-\lambda_{\mathrm{SSSE}}\frac{\sigma_0^2\gamma_{\mathrm{Sth}}}{P_{\mathrm{SS}}}\right). \end{aligned} \tag{13}$$

It is noted from (11)-(13) that probability that SD, SR and SE unsuccessfully decode one Fountain packet from SS can be computed as $1-\omega_{\mathrm{SD}}$, $1-\omega_{\mathrm{SR}}$ and $1-\omega_{\mathrm{SE}}$, respectively.

Now, if SR replaces SS to send the encoded packets to SD, the instantaneous SINRs obtained at SD and SE can be written, respectively as

$$\begin{aligned}\psi_{\mathrm{SRSD}} &= \frac{P_{\mathrm{SR}}\gamma_{\mathrm{SRSD}}}{P_{\mathrm{PT}}\gamma_{\mathrm{PTSD}} + \sigma_0^2},\\ \psi_{\mathrm{SRSE}} &= \frac{P_{\mathrm{SR}}\gamma_{\mathrm{SRSE}}}{P_{\mathrm{PT}}\gamma_{\mathrm{PTSE}} + P_{\mathrm{SJ}}\gamma_{\mathrm{SJSE}} + \sigma_0^2}. \end{aligned} \tag{14}$$

Similarly, we can calculate the successful decoding probability at SD and SE, respectively as

$$\begin{aligned}\chi_{\mathrm{RD}} &= \Pr\left(\psi_{\mathrm{SRSD}} \geq \gamma_{\mathrm{Sth}}\right)\\ &= \frac{\lambda_{\mathrm{PTSD}}\theta_{\mathrm{R}}}{\lambda_{\mathrm{PTSD}}\theta_{\mathrm{R}} + \lambda_{\mathrm{SRSD}}\gamma_{\mathrm{Sth}}}\exp\left(-\lambda_{\mathrm{SRSD}}\frac{\sigma_0^2\gamma_{\mathrm{Sth}}}{P_{\mathrm{SR}}}\right),\\ \chi_{\mathrm{RE}} &= \Pr\left(\psi_{\mathrm{SRSE}} \geq \gamma_{\mathrm{Sth}}\right)\\ &= \frac{\lambda_{\mathrm{PTSE}}\theta_{\mathrm{R}}}{\lambda_{\mathrm{PTSE}}\theta_{\mathrm{R}} + \lambda_{\mathrm{SRSE}}\gamma_{\mathrm{Sth}}}\frac{\lambda_{\mathrm{SJSE}}}{\lambda_{\mathrm{SJSE}} + \lambda_{\mathrm{SRSE}}\alpha_{\mathrm{R}}\gamma_{\mathrm{Sth}}}\\ &\quad \times \exp\left(-\lambda_{\mathrm{SRSE}}\frac{\sigma_0^2\gamma_{\mathrm{Sth}}}{P_{\mathrm{SR}}}\right). \end{aligned} \tag{15}$$

Then, the unsuccessful decoding probability at SD and SE is $1-\chi_{\mathrm{RD}}$ and $1-\chi_{\mathrm{RE}}$, respectively.

3. Performance Analysis

This section evaluates IP of the proposed cooperative communication scheme, named CC. For a base-line comparison, we study the IP performance of the direct transmission (DT) scheme between SS and SD in which the CJ technique is also performed by the SJ node.

3.1. Cooperative Communication Scheme (CC)

IP of the proposed approach can be calculated via 04 cases as follows:

- Case 1: After SS sends $N_{\max}$ Fountain packets to SR and SD, SR receives n_{R} packets, SD receives n_{D} packets and SE receives n_{E} packets, where $n_{\mathrm{R}} \leq H$, $n_{\mathrm{D}} \leq H$ and $n_{\mathrm{E}} \geq H$.

In Case 1, SS stops the data transmission after sending $N_{\max}$ encoded packets. Because SE collects at least H Fountain packets for the data recovery, the source data is intercepted. Therefore, IP can be given as in (16), at the top of next page.

In (16), $\binom{N_{\max}}{n_Z}(\omega_{\mathrm{SZ}})^{n_Z}(1-\omega_{\mathrm{SZ}})^{N_{\max}-n_Z}$ is probability that the SZ node correctly obtains n_Z Fountain packets, where $Z \in \{\mathrm{R}, \mathrm{D}, \mathrm{E}\}$, and $\binom{N_{\max}-1}{H-1}(\omega_{\mathrm{ST}})^{H}(1-\omega_{\mathrm{ST}})^{N_{\max}-H}$ is probability that the ST node successfully receives the $H-$th encoded packet at the last transmission of SS, where $\mathrm{T} \in \{\mathrm{R}, \mathrm{D}\}$.

- Case 2: SD collects enough H encoded packets before SS sends $N_{\max}$ ones. Indeed, SS only sends n_{S} packets, and during the data transmission, SR and SE collect n_{R} and n_{E} Fountain packets, respectively, where $H \leq n_{\mathrm{S}} < N_{\max}$, $n_{\mathrm{R}} \leq H$ and $n_{\mathrm{E}} \geq H$.

In Case 2, SD sends the ACK message to SS as soon as it accumulates enough H packets, and SS intermediately terminates its transmission. However, the source data is still intercepted because $n_{\mathrm{E}} \geq H$. In this case, IP is computed as in (17), at the top of next page.

- Case 3: After SS sends n_{S} packets, SR obtains enough H packets, SD and SE can collect n_{D} and n_{E} ones, respectively, where $H \leq n_{\mathrm{S}} < N_{\max}$, $n_{\mathrm{D}} < H$ and $n_{\mathrm{E}} \geq H$.

In Case 3, SR replaces SS to send Fountain packets to SD. However, because SE collects at least H packets for recovering the source data, it does not need to receive the encoded packets any more. Hence, IP in this case is shown as in (18), at the top of next page.

- Case 4: After SS sends n_{S} packets, SR obtains enough H packets, SD and SE can collect n_{D} and n_{E} ones, respectively, where $H \leq n_{\mathrm{S}} < N_{\max}$, $n_{\mathrm{D}} < H$ and $n_{\mathrm{E}} < H$. Since $H - n_{\mathrm{D}} \leq N_{\max} - n_{\mathrm{S}}$, SR replaces SS to send Fountain packets to SD, and SE attempts to collect more packets from SR. After the data transmission of SR terminates, SE totally receives m_{E} packets with $H \leq m_{\mathrm{E}} \leq N_{\max} - 1$.

Similar to Case 3, SR becomes the new transmitter for SD. In addition, the number of Fountain packets

$$\mathrm{IP}_1 = \left[\binom{N_{\max}-1}{H-1}(\omega_{\mathrm{SD}})^H(1-\omega_{\mathrm{SD}})^{N_{\max}-H} + \sum_{n_{\mathrm{D}}=0}^{H-1}\binom{N_{\max}}{n_{\mathrm{D}}}(\omega_{\mathrm{SD}})^{n_{\mathrm{D}}}(1-\omega_{\mathrm{SD}})^{N_{\max}-n_{\mathrm{D}}}\right] \times \left[\binom{N_{\max}-1}{H-1}(\omega_{\mathrm{SR}})^H(1-\omega_{\mathrm{SR}})^{N_{\max}-H} + \sum_{n_{\mathrm{R}}=0}^{H-1}\binom{N_{\max}}{n_{\mathrm{R}}}(\omega_{\mathrm{SR}})^{n_{\mathrm{R}}}(1-\omega_{\mathrm{SR}})^{N_{\max}-n_{\mathrm{R}}}\right] \times \sum_{n_{\mathrm{E}}=H}^{N_{\max}}\binom{N_{\max}}{n_{\mathrm{E}}}(\omega_{\mathrm{SE}})^{n_{\mathrm{E}}}(1-\omega_{\mathrm{SE}})^{N_{\max}-n_{\mathrm{E}}}. \quad (16)$$

$$\mathrm{IP}_2 = \sum_{n_{\mathrm{S}}=H}^{N_{\max}-1}\left\{\begin{array}{l}\binom{n_{\mathrm{S}}-1}{H-1}(\omega_{\mathrm{SD}})^H(1-\omega_{\mathrm{SD}})^{n_{\mathrm{S}}-H} \\ \times\left[\binom{n_{\mathrm{S}}-1}{H-1}(\omega_{\mathrm{SR}})^H(1-\omega_{\mathrm{SR}})^{n_{\mathrm{S}}-H} + \sum_{n_{\mathrm{R}}=0}^{H-1}\binom{n_{\mathrm{S}}}{n_{\mathrm{R}}}(\omega_{\mathrm{SR}})^{n_{\mathrm{R}}}(1-\omega_{\mathrm{SR}})^{n_{\mathrm{S}}-n_{\mathrm{R}}}\right] \\ \times \sum_{n_{\mathrm{E}}=H}^{n_{\mathrm{S}}}\binom{n_{\mathrm{S}}}{n_{\mathrm{E}}}(\omega_{\mathrm{SE}})^{n_{\mathrm{E}}}(1-\omega_{\mathrm{SE}})^{n_{\mathrm{S}}-n_{\mathrm{E}}}\end{array}\right\}. \quad (17)$$

$$\mathrm{IP}_3 = \sum_{n_{\mathrm{S}}=H}^{N_{\max}-1}\left[\begin{array}{l}\binom{n_{\mathrm{S}}-1}{H-1}(\omega_{\mathrm{SR}})^H(1-\omega_{\mathrm{SR}})^{n_{\mathrm{S}}-H} \times \sum_{n_{\mathrm{D}}=0}^{H-1}\binom{n_{\mathrm{S}}}{n_{\mathrm{D}}}(\omega_{\mathrm{SD}})^{n_{\mathrm{D}}}(1-\omega_{\mathrm{SD}})^{n_{\mathrm{S}}-n_{\mathrm{D}}} \\ \times \sum_{n_{\mathrm{E}}=H}^{n_{\mathrm{S}}}\binom{n_{\mathrm{S}}}{n_{\mathrm{E}}}(\omega_{\mathrm{SE}})^{n_{\mathrm{E}}}(1-\omega_{\mathrm{SE}})^{n_{\mathrm{S}}-n_{\mathrm{E}}}\end{array}\right]. \quad (18)$$

that SR can send to SD is $N_{\max} - n_{\mathrm{S}}$, while the number of Fountain packets that SD has to receive from SR for recovering the source data is $r_{\mathrm{D}} = H - n_{\mathrm{D}}$. It is straightforward that if $r_{\mathrm{D}} > N_{\max} - n_{\mathrm{S}}$, SD cannot collect enough r_{D} packets from SR. In this case, SR will not send the encoded packets to SD, and SE cannot collect more packets from SR.

Therefore, we only consider the case where $1 \le r_{\mathrm{D}} \le N_{\max} - n_{\mathrm{S}}$. Let us denote q_{D} as number of Fountain packets that SD can receive from SR, where $0 \le q_{\mathrm{D}} \le N_{\max} - n_{\mathrm{S}}$. We also denote t_{R} as number of the encoded packets that SR transmits to SD, where $r_{\mathrm{D}} \le t_{\mathrm{R}} \le N_{\max} - n_{\mathrm{S}}$. Then, IP in Case 4 can be expressed as in (19), at the top of next page.

In (19), $\binom{n_{\mathrm{S}}}{H-r_{\mathrm{D}}}(\omega_{\mathrm{SD}})^{H-r_{\mathrm{D}}}(1-\omega_{\mathrm{SD}})^{n_{\mathrm{S}}-H+r_{\mathrm{D}}}$ is probability that SD correctly obtains $H - r_{\mathrm{D}} = n_{\mathrm{D}}$ encoded packets from SS, $m_{\mathrm{E}} - n_{\mathrm{E}}$ is number of Fountain packets that SE can collect from SR, and $\binom{t_{\mathrm{R}}-1}{r_{\mathrm{D}}-1}(\chi_{\mathrm{RD}})^{r_{\mathrm{D}}}(1-\chi_{\mathrm{RD}})^{t_{\mathrm{R}}-r_{\mathrm{D}}}$ is probability that SD can successfully receive r_{D} packets after SR sends t_{R} Fountain packets to SD.

Finally, total IP of the CC scheme is given as

$$\mathrm{IP}_{\mathrm{CC}} = \mathrm{IP}_1 + \mathrm{IP}_2 + \mathrm{IP}_3 + \mathrm{IP}_4. \quad (20)$$

3.2. Direct Transmission Scheme (DT)

In this protocol, SS and SJ continuously send the encoded packets to SD and the jamming noises on SE, respectively. In addition, the transmit power of SS and SJ can be obtained as in (8), and the instantaneous SINRs obtained at SD and SE can be given as in (10). Then, IP of the DT scheme can be calculated as follows:

$$\mathrm{IP}_{\mathrm{DT}} = \sum_{n_{\mathrm{D}}=0}^{H-1}\binom{N_{\max}}{n_{\mathrm{D}}}(\omega_{\mathrm{SD}})^{n_{\mathrm{D}}}(1-\omega_{\mathrm{SD}})^{N_{\max}-n_{\mathrm{D}}} \times \sum_{n_{\mathrm{E}}=H}^{N_{\max}}\binom{N_{\max}}{n_{\mathrm{E}}}(\omega_{\mathrm{SE}})^{n_{\mathrm{E}}}(1-\omega_{\mathrm{SE}})^{N_{\max}-n_{\mathrm{E}}} + \sum_{n_{\mathrm{S}}=H}^{N_{\max}}\binom{n_{\mathrm{S}}-1}{H-1}(\omega_{\mathrm{SD}})^H(1-\omega_{\mathrm{SD}})^{n_{\mathrm{S}}-H} \times \sum_{n_{\mathrm{E}}=H}^{n_{\mathrm{S}}}\binom{n_{\mathrm{S}}}{n_{\mathrm{E}}}(\omega_{\mathrm{SE}})^{n_{\mathrm{E}}}(1-\omega_{\mathrm{SE}})^{n_{\mathrm{S}}-n_{\mathrm{E}}}. \quad (21)$$

4. Simulation Results

This section presents Monte Carlo simulations to verify the closed-form expressions of IP derived in Section 3. Simulation environment is a two-dimensional Oxy

$$\mathrm{IP}_4 = \sum_{m_\mathrm{E}=H}^{N_\mathrm{max}-1} \sum_{n_\mathrm{S}=H}^{N_\mathrm{max}-1} \left\{ \binom{n_\mathrm{S}-1}{H-1} (\omega_\mathrm{SR})^H (1-\omega_\mathrm{SR})^{n_\mathrm{S}-H} \times \sum_{n_\mathrm{E}=0}^{H-1} \left[\binom{n_\mathrm{S}}{n_E} (\omega_\mathrm{SE})^{n_\mathrm{E}} (1-\omega_\mathrm{SE})^{n_\mathrm{S}-n_\mathrm{E}} \times \sum_{r_\mathrm{D}=1}^{N_\mathrm{max}-n_\mathrm{S}} \binom{n_\mathrm{S}}{H-r_\mathrm{D}} (\omega_\mathrm{SD})^{H-r_\mathrm{D}} (1-\omega_\mathrm{SD})^{n_\mathrm{S}-H+r_\mathrm{D}} \times \left(\sum_{q_\mathrm{D}=0}^{r_\mathrm{D}-1} \binom{N_\mathrm{max}-n_\mathrm{S}}{q_\mathrm{D}} (\chi_\mathrm{RD})^{q_\mathrm{D}} (1-\chi_\mathrm{RD})^{N_\mathrm{max}-n_\mathrm{S}-q_\mathrm{D}} \times \binom{N_\mathrm{max}-n_\mathrm{S}}{m_\mathrm{E}-n_\mathrm{E}} (\chi_\mathrm{RE})^{m_\mathrm{E}-n_\mathrm{E}} (1-\chi_\mathrm{RE})^{N_\mathrm{max}-n_\mathrm{S}-m_\mathrm{E}+n_\mathrm{E}} \right) \right. \right. \\ \left. \left. + \sum_{t_\mathrm{R}=r_\mathrm{D}}^{N_\mathrm{max}-n_\mathrm{S}} \binom{t_\mathrm{R}-1}{r_\mathrm{D}-1} (\chi_\mathrm{RD})^{r_\mathrm{D}} (1-\chi_\mathrm{RD})^{t_\mathrm{R}-r_\mathrm{D}} \times \binom{t_\mathrm{R}}{m_\mathrm{E}-n_\mathrm{E}} (\chi_\mathrm{RE})^{m_\mathrm{E}-n_\mathrm{E}} (1-\chi_\mathrm{RE})^{t_\mathrm{R}-m_\mathrm{E}+n_\mathrm{E}} \right) \right] \right\}. \quad (19)$$

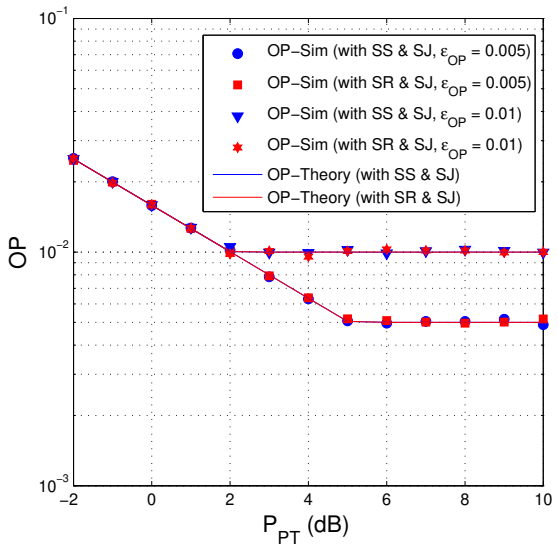

Figure 2. OP of the primary network as a function of P_PT in (dB).

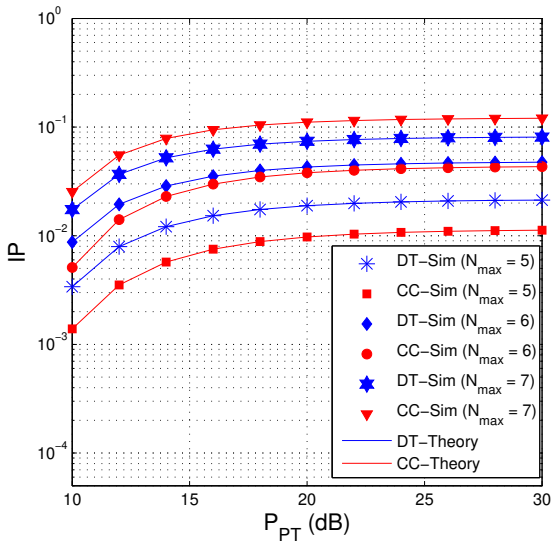

Figure 3. IP as a function of P_PT in (dB) with $\varepsilon_\mathrm{OP} = 0.005$, $x_\mathrm{R} = 0.25$, $y_\mathrm{E} = -0.3$.

plane in which the primary nodes PT and PR are placed at (0.5,1) and (0.5,0.6), respectively, the source SS and the destination SD are placed at (0,0) and (1,0), respectively, the SJ node is assumed to have the same position with the destination SJ, and positions of the SR and SJ nodes are $(x_\mathrm{R}, 0)$ and $(1, y_\mathrm{E})$, respectively. For illustration purpose only, we fix the path-loss exponential (β) by 3, variance of the additive noises (σ_0^2) by 1, the required number of Fountain packets for the data recovery (H) by 4, the outage thresholds (γ_Pth, γ_Sth) by 0.25 ($\gamma_\mathrm{Pth} = \gamma_\mathrm{Sth} = 0.25$), and the coefficients α_S and α_R by 0.1 ($\alpha_\mathrm{S} = \alpha_\mathrm{R} = 0.1$).

Figure 2 presents the outage performance of the primary network as a function of P_PT in dB with different QoS, i.e., $\varepsilon_\mathrm{OP} = 0.005$ and $\varepsilon_\mathrm{OP} = 0.01$. As we can see, when the transmit power P_PT is high enough, OP of the primary network converges to the value of ε_OP. This figure also shows that at low P_PT values, QoS of the primary network is not satisfied, and as mentioned above, the SS, SR and SJ nodes are not allowed to access the licensed band. As observed from Fig. 2, with $\varepsilon_\mathrm{OP} = 0.01$, the secondary network can use the licensed band when P_PT is higher than 2 dB, and with $\varepsilon_\mathrm{OP} = 0.005$, the primary network can share the spectrum with the secondary network when P_PT is higher than 5 dB. We also see from Fig. 2 that the simulation results match very well with the theoretical ones, which validates the expressions of OP of the primary network and the transmit power of the secondary transmitters derived in Section 2.

In Fig. 3, we present the IP performance of the DT and CC schemes as a function of P_PT in dB with different values of N_max. In this figure, QoS of the primary network is set to 0.005 ($\varepsilon_\mathrm{OP} = 0.005$), the SR and SE

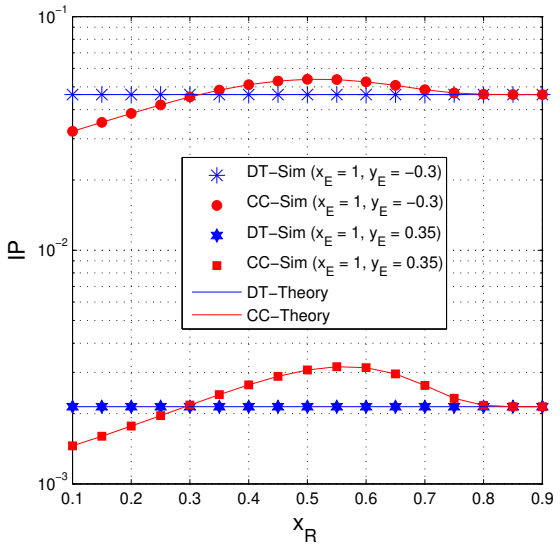

Figure 4. IP as a function of x_R with $\varepsilon_{OP} = 0.005$, $P_{PT} = 25$ dB, $N_{max} = 6$.

nodes are placed at (0.25,0) and (1,-0.3), respectively. Firstly, we see that the IP values in Fig. 3 increase as the transmit power P_{PT} increases. In addition, IP of the considered schemes also increases with the increasing of N_{max}. It is due to the fact that with high N_{max} values, probability that the eavesdropper SE can accumulate enough encoded packets for the data recovery is higher. Next, we can observe that the CC scheme obtains lower IP values than the DT scheme when N_{max} equals to 5 or 6. With $N_{max} = 7$, the IP performance of the CC scheme is worse, which means that the data transmission from SR is less secure than that from SS.

Figure 4 presents IP of the CC and DT schemes as a function of x_R with $\varepsilon_{OP} = 0.005$, $P_{PT} = 25$ dB and $N_{max} = 6$. In Fig. 4, the IP performance of the proposed scheme is best when the relay SR is near the source SS, i.e., $x_R = 0.1$. Due to high impact of the co-channel interference from PT and SJ, we can see that when x_R belongs to the interval (0.4, 0.6), IP of the CC scheme is high. Moreover, the IP value is highest when x_R is about 0.5 or 0.55. As seen from Fig. 4, the IP performance of the CC scheme is better than that of the DT one as $x_R < 0.3$. Moreover, when the relay SR is near the destination SD, i.e., $x_R \geq 0.8$, the performance of both schemes is almost same. Finally, it can be seen that IP of the CC and DT schemes with $y_E = -0.3$ is much higher than that with $y_E = 0.35$. It is due to the fact that when the SE node is at the position (1,-0.3), this node is far the PT node, while the distance d_{SESX} ($X \in \{S, R, J\}$) is slightly different when SE is at (1,-0.3) and (1,0.35).

5. Conclusions

This paper proposed and evaluated the IP performance of the cooperative relaying scheme in underlay cognitive radio networks using Fountain codes and cooperative jamming. We also proposed a simple transmit power for the secondary transmitters to guarantee QoS of the primary network. The obtained results validated the derived expressions of IP. Moreover, the proposed scheme can obtain better performance as compared with the direct transmission one.

References

[1] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty (2015) Physical Layer Security in Wireless Cooperative Relay Networks: State of the Art and Beyond. *IEEE Communications Magazine*, **53**(12): 32–39.

[2] J. Zhang, T. Q. Duong, R. Woods and A. Marshall (2017) Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. *Entropy*, **19**(8): 420.

[3] N. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan and K. Tourki (2018) Secure Massive MIMO With the Artificial Noise-Aided Downlink Training. *IEEE Journal on Selected Areas in Communications*, **36**(4): 802–816.

[4] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober and I. B. Collings (2013) Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels. *IEEE Transactions on Communications*, **61**(1): 144–154.

[5] J. Xiong, Y. Tang, D. Ma, P. Xiao and K. Wong (2015) Secrecy Performance Analysis for TAS-MRC System With Imperfect Feedback. *IEEE Transactions on Information Forensics and Security*, **10**(8): 1617–1629.

[6] N. Yang, H. A. Suraweera, I. B. Collings and C. Yuen (2013) Physical Layer Security of TAS/MRC With Antenna Correlation. *IEEE Transactions on Information Forensics and Security*, **8**(1): 254–259.

[7] J. N. Laneman, D. N. Tse, and G. W. Wornell (2004) Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior. *IEEE Transactions on Information Theory* **50**(12): 3062–3080.

[8] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan and S. Shetty (2015) Physical Layer Security in Wireless Cooperative Relay Networks: State of the Art and Beyond. *IEEE Communications Magazine*, **53**(12): 32–39.

[9] T. T. Duy, Trung Q. Duong, D.B. da Costa, V.N.Q. Bao and M. Elkashlan (2015) Proactive Relay Selection with Joint Impact of Hardware Impairment and Co-channel Interference. *IEEE Transactions on Communications*, **63**(5): 1594–1606.

[10] J. Mo, M. Tao and Y. Liu (2012) Relay Placement for Physical Layer Security: A Secure Connection Perspective. *IEEE Communications Letters*, **16**(6): 878–881.

[11] T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao (2015) Secrecy Performance Analysis with Relay Selection Methods under Impact of Co-channel Interference. *IET Communications*, **9**(11): 1427–1435.

[12] L. Fan, X. Lei, N. Yang, T. Q. Duong and G. K. Karagiannidis (2016) Secure Multiple Amplify-and-Forward Relaying With Co-Channel Interference. *IEEE*

Journal of Selected Topics in Signal Processing, **10**(8): 1494–1505.

[13] X. Jiang, C. Zhong, X. Chen, T. Q. Duong, T. A. Tsiftsis and Z. Zhang (2016) Secrecy Performance of Wirelessly Powered Wiretap Channels. *IEEE Transactions on Communications*, **64**(9): 3858–3871.

[14] J. Chen, L. Yang and M. Alouini (2018) Physical Layer Security for Cooperative NOMA Systems. *IEEE Transactions on Vehicular Technology*, **67**(5): 4645–4649.

[15] Y. Zou, X. Wang, W. Shen and L. Hanzo (2014) Security Versus Reliability Analysis of Opportunistic Relaying. *IEEE Transactions on Vehicular Technology*, **63**(6): 2653–2661.

[16] J. Zhu, Y. Zou and B. Zheng (2017) Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks. *IEEE Access*, **5**: 5313–5320.

[17] P. N. Son and H. Y. Kong (2014) An Integration of Source and Jammer for a Decode-and-Forward Two-way Scheme under Physical Layer Security. *Wireless Personal Communications*, **79**(3): 1741–1764.

[18] F. Jameel, S. Wyne, G. Kaddoum and T. Q. Duong (2019) A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Communications Surveys and Tutorials*, **21**(3): 2734–2771.

[19] X. Ding, T. Song, Y. Zou and X. Chen (2016) Security-Reliability Tradeoff for Friendly Jammer Assisted User-Pair Selection in the Face of Multiple Eavesdroppers. *IEEE Access*, **4**: 8386–8393.

[20] L. Hu, H. Wen, B. Wu, F. Pan, R. F. Liao, H. Song, J. Tang and X. Wang (2018). Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things. *IEEE Internet of Things Journal*, **5**(1): 219–228.

[21] V. L. Nguyen, H. D. Binh, T. D. Dung and Y. Lee (2019) Enhancing Physical Layer Security for Cooperative Non-Orthogonal Multiple Access Networks with Artificial Noise. *EAI Transactions on Industrial Networks and Intelligent Systems*, **6**(20): 1–11.

[22] T. M. Hoang, T. Q. Duong, N.-S. Vo and C. Kundu (2017) Physical Layer Security in Cooperative Energy Harvesting Networks With a Friendly Jammer. *IEEE Wireless Communications Letters*, **6**(2): 174–177.

[23] H. D. Hung, T. T. Duy, and M. Voznak (2020) Secrecy Outage Performance of Multi-hop LEACH Networks using Power Beacon Aided Cooperative Jamming with Jammer Selection Methods. *AEU-International Journal of Electronics and Communications*, **124**(153357):1-23.

[24] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis and A. Nallanathan (2015) On the Security of Cognitive Radio Networks. *IEEE Transactions on Vehicular Technology*, **64**(8): 3790–3795.

[25] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan and Trung Q. Duong (2015) Relay Selection for Security Enhancement in Cognitive Relay Networks. *IEEE Wireless Communications Letter*s, **4**(1): 46–49.

[26] P. T. D. Ngoc, T. T. Duy and H. V. Khuong (2019). Outage Performance of Cooperative Cognitive Radio Networks under Joint Constraints of Co-Channel Interference, Intercept Probability and Hardware Imperfection. *EAI Transactions on Industrial Networks and Intelligent Systems*, **6**(9): 1–8.

[27] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo (2015) Relay-Selection Improves the Security-Reliability Trade-off in Cognitive Radio Systems. *IEEE Transactions on Communications*, **63**(1): 215–228.

[28] Y. Zou (2017) Physical-Layer Security for Spectrum Sharing Systems. *IEEE Transactions on Wireless Communications*, **16**(2): 1319–1329.

[29] N. Q. Sang, N. T. Huy, D. D. Van and W.-J. Hwang (2019) Exact Outage Analysis of Cognitive Energy Harvesting Relaying Networks under Physical Layer Security. *EAI Transactions on Industrial Networks and Intelligent Systems*, **6**(18): 1–15.

[30] T. X. Quach, H. Tran, E. Uhlemann and M. T. Truc (2020) Secrecy Performance of Cooperative Cognitive Radio Networks Under Joint Secrecy Outage and Primary User Interference Constraints. *IEEE Access*, **8**: 18442–18455.

[31] D. J. C. Mackay (2005) Fountain Codes. *IEE Proceedings Communications*, **152**(6): 1062–1068.

[32] J. Castura and Y. Mao (2006) Rateless Coding over Fading Channels. *IEEE Communications Letters*, **10**(1): 46–48.

[33] H. Niu, M. Iwai, K. Sezaki, L. Sun and Q. Du (2014) Exploiting Fountain Codes for Secure Wireless Delivery. *IEEE Communications Letters*, **18**(5): 777–780.

[34] L. Sun, P. Ren, Q. Du and Y. Wang (2016) Fountain-Coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks. *IEEE Transactions on Industrial Informatics*, **12**(1): 291–300.

[35] Q. Du, Y. Xu, W. Li and H. Song (2018) Security Enhancement for Multicast over Internet of Things by Dynamically Constructed Fountain Codes. *Wireless Communications and Mobile Computing*, Article ID **8404219**: 1–11.

[36] D. T. Hung, T. T. Duy, T. T. Phuong, D. Q. Trinh and T. Hanh (2019) Performance Comparison between Fountain Codes-Based Secure MIMO Protocols with and without Using Non-Orthogonal Multiple Access. *Entropy*, **21**(10): 928.

[37] D. T. Hung, T. T. Duy and D. Q. Trinh (2019) Security-Reliability Analysis of Multi-hop LEACH Protocol with Fountain Codes and Cooperative Jamming. *EAI Transactions on Industrial Networks and Intelligent Systems*, **6**(18): 1–7.