IEIE Transactions on Smart Processing and Computing, vol. 6, no. 3, June 2017
https://doi.org/10.5573/IEIESPC.2017.6.3.200

Security-reliability Analysis for a Cognitive Multi-hop Protocol in Cluster Networks with Hardware Imperfections

Phu Tran Tin[1,2], Phạm Minh Nam[2,3], Tran Trung Duy[4], and Miroslav Voznak[1]

[1] VSB Technical University of Ostrava, 17. Listopadu 15/2172, 708 33 Ostrava - Poruba, Czech Republic
[2] Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Ho Chi Minh City, Vietnam
phutrantin@iuh.edu.vn, miroslav.voznak@vsb.cz
[3] PhD Candidate - HCMC University of Technology and Education (HCMUTE), Ho Chi Minh City, VietNam
phamminhnam@iuh.edu.vn, minhnampham@gmail.com
[4] Department of Telecommunications, Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam
trantrungduy@ptithcm.edu.vn

***** Corresponding Author: Tran Trung Duy

Received February 4, 2017; Revised February 27, 2017; Accepted March 20, 2017; Published June 30, 2017

** Regular Paper*

** Extended from a Conference: Preliminary results of this paper were presented at the 18th IEEE International Symposium on Consumer Electronics (ISCE 2014)*

***Abstract*:** In this paper, we investigate the tradeoff between security and reliability for a multi-hop protocol in cluster-based underlay cognitive radio networks. In the proposed protocol, a secondary source communicates with a secondary destination via the multi-hop relay method in the presence of a secondary eavesdropper. To enhance system performance under the joint impact of interference constraint required by multiple primary users and hardware impairments, the best relay node is selected at each hop to relay the source data to the destination. Moreover, the destination is equipped with multiple antennas and employs a selection combining (SC) technique to combine the received data. We derive closed-form expressions of the intercept probability (IP) for the eavesdropping links and the outage probability (OP) for the data links over a Rayleigh fading channel. Finally, the correction of our derivations is verified by Monte-Carlo simulations.

***Keywords*:** Underlay cognitive radio, Cluster-based multi-hop transmission, Physical-layer security, Outage probability, Intercept probability, Rayleigh fading channel

1. Introduction

Multi-hop transmission [1, 2] is an exciting technique where the simple idea is relaying the information from the source to the destination via many intermediate hops. As a result, less transmit power, a lower interference level, higher coverage, and higher spectrum efficiency are obtained while guaranteeing similar data transmission quality. In traditional multi-hop protocols, the source data are relayed hop-by-hop from a source to a destination [1, 2]. Although this protocol is easy to implement, it may not perform well in fading environments. To mitigate the effect of the fading channels, diversity relay methods can be used efficiently in multi-hop networks. Cooperative multi-hop protocols have been proposed and analyzed [3, 4], where intermediate nodes (relays) receive the source data from the previous nodes, and then process the received data appropriately before forwarding them to the next hop. An et al. [5] proposed cooperation-based multi-hop transmission protocols in which cooperative communication [6] is used to enhance the reliability of the data transmission at each hop. Cluster-based multi-hop schemes were investigated [7, 8], where the diversity transmission between two adjacent clusters is realized, relying on channel state information (CSI) between the nodes in two clusters. The results obtained in [3-8] showed that the cooperative multi-hop relay protocols provide high diversity gain, and they significantly reduce the outage probability (OP) and error rates, compared with the traditional multi-hop transmission protocols.

Recently, multi-hop transmission protocols in underlay cognitive radio networks have gained a lot of attention. Underlay cognitive radio [9-11] is an efficient solution to obtain spectrum efficiency while guaranteeing continuous data transmission for the secondary network. In this technique, secondary users (SUs) can use the same licensed bands as primary users (PUs) provided that interference caused by their operations is lower than an interference threshold set by the PUs [9-11]. To improve performance for the secondary networks under the impact of the interference constraint and fading channels, cooperative relay techniques [12, 13] have been proposed. There are several studies addressing the diversity multi-hop transmission protocols in underlay cognitive radio networks. In particular, the authors in [14, 15] proposed algorithms to find an opportunistic route between a secondary source and a secondary destination. Sang et al. [16] evaluated the outage performance of a cluster-based multi-hop underlay cognitive radio scheme over a Rayleigh fading environment.

Physical-layer security (PLS) is a simple technique to obtain security for wireless systems without using complex cryptographic methods [17]. Recently, the PLS issues in underlay cognitive radio have become a hot topic. In [18], the authors proposed various relay and jammer selection schemes to enhance secrecy performance for secondary networks. Duy and Son [19] investigated secured communications in multicast underlay cognitive radio network. Zou et al. [20] studied the security-reliability tradeoff for cooperative cognitive networks by evaluating the intercept probability (IP) at the eavesdropper and the outage probability (OP) at authorized nodes. The published work [21] proposed relay selection methods to improve the outage performance for the data link as well as to reduce the intercept possibility of the eavesdropping link. Moreover, those authors took into account the hardware impairment level when calculating the IP and OP values.

In this paper, we propose a cluster-based multi-hop transmission protocol in underlay cognitive radio networks in the presence of multiple PUs and one secondary eavesdropper. The main contributions of this paper are as follows:

- Similar to [16], the diversity relaying technique with a relay selection method is employed on each hop to improve the reliability of the data transmission. In particular, partial channel state information (CSI) is used to select the next node to forward the source data to the next hop. Moreover, in order to enhance the diversity gain on the last hop, unlike [16], we propose a receive diversity scheme in which the secondary destination is equipped with multiple antennas and employs selection combining (SC) technique to combine the received data.
- We assume that the secondary eavesdropper can receive the source data from all of the hops between the source and the destination (while the eavesdropper in [21] only overhears on the last hop).
- In order to evaluate the performance of the proposed protocol, we first give an exact expression of the end-to-end (e2e) signal-to-noise ratio (SNR) for the data link; we then derive cumulative distribution function (CDF) for this SNR. From the obtained CDF, an exact closed-form formula of the e2e OP over Rayleigh fading channel is derived. Furthermore, we provide an approximate closed-form expression of the OP in order to determine the diversity gain for the proposed system.
- In the same manner, we give an exact closed-form expression for the intercept probability (IP) at the eavesdropper.
- Monte-Carlo simulations are shown to verify the mathematical derivations. The results show that the simulation and theoretical results are in agreement, which verifies the correction of our analysis.
- The results show that the proposed method can obtain high diversity order which equals the minimum value of the number of relays at the clusters and the number of antennas equipped at the secondary destination. Moreover, the number of hops, the number of nodes in each cluster, the position of the eavesdropper and the hardware impairment level significantly affect the OP and IP values.

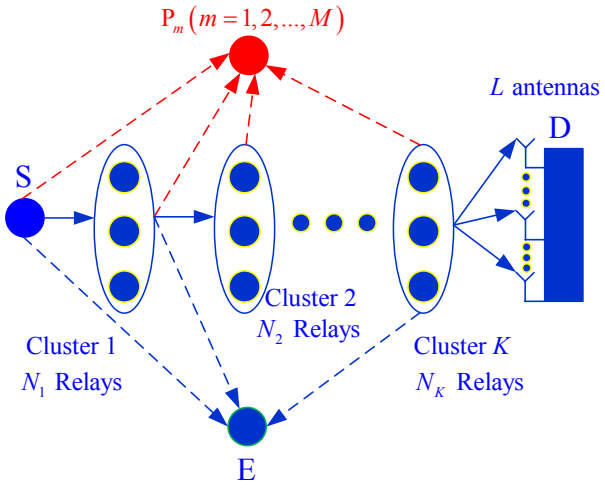

Fig. 1. Cluster-based multi-hop relay protocol in underlay cognitive radio network.

The rest of this paper is organized as follows. The system model of the proposed protocol is described in Section 2. In Section 3, the performance of the protocols is analyzed. The simulation results are presented in Section 4 to verify the theoretical analysis. Finally, the paper is concluded in Section 5.

2. System Model

In Fig. 1, we present the system model of the proposed protocol in the underlay cognitive radio network. In this model, the secondary source (S) attempts to transmit its data to the secondary destination (D) via the cluster-based multi-hop scheme with the presence of M primary users, denoted by $\mathrm{P}_1, \mathrm{P}_2, ..., \mathrm{P}_M$. We assume there are K clusters between S and D, and the j-th cluster has N_j secondary

nodes, where $K \geq 1$, $j = 1,2,...,K$, and $N_j \geq 1$. We also assume that source S and the relays are equipped with a single antenna and operate in half-duplex mode, while destination D is equipped with L antennas. This system model can be applied to the cluster-based wireless sensor networks [22] where the source and the relays play the role of single-antenna wireless sensor nodes while the destination is a base station (or center home).

Next, we introduce notations and definitions used in this paper. First, we denote $\mathrm{R}_j^1, \mathrm{R}_j^2, ..., \mathrm{R}_j^{N_j-1}$ and $\mathrm{R}_j^{N_j}$ as the nodes in the j-th cluster. Second, we denote R_j^c as the selected relay at the j-th cluster for receiving and forwarding the received data to the next hop. Consider the data transmission between secondary transmitter X and secondary receiver Y, where $\mathrm{X} \in \left\{\mathrm{S}, \mathrm{R}_j^k\right\}$, $\mathrm{Y} \in \left\{\mathrm{R}_j^k, \mathrm{D}, \mathrm{E}, \mathrm{P}_m\right\}$, $j = 1,2,...,K$, $k = 1,2, ..., N_j$ and $m = 1,2,...,M$; the signal received at Y due to the transmission of X can be expressed as

$$z_{\mathrm{Y}} = \sqrt{P_{\mathrm{X}}} h_{\mathrm{XY}} \left(x + \chi_t\right) + \chi_r + n_{\mathrm{Y}}. \tag{1}$$

In (1), P_{X} is the transmit power of the secondary transmitter X, x is the transmitted data, h_{XY} is the channel coefficient between nodes X and Y, n_{Y} is the Gaussian noise at secondary receiver Y, χ_t is hardware noise caused by impairments in transmitter X, and χ_r is hardware noise caused by impairments in receiver Y. As in [23, 24], the noises χ_t and χ_r can be modeled as Gaussian random variables (RVs) with zero-mean, and their variances can be given, respectively, by

$$\sigma_{\chi_t}^2 = \xi_{\mathrm{X},t}^2, \ \sigma_{\chi_r}^2 = \xi_{\mathrm{Y},r}^2 P_{\mathrm{X}} |h_{\mathrm{XY}}|^2, \tag{2}$$

where $\xi_{\mathrm{X},t}^2$ and $\xi_{\mathrm{Y},r}^2$ are constants characterizing the level of the hardware impairments.

From (1), the instantaneous SNR received at Y is given by

$$\begin{aligned} \psi_{\mathrm{XY}} &= \frac{P_{\mathrm{X}} |h_{\mathrm{XY}}|^2}{\left(\xi_{\mathrm{X},t}^2 + \xi_{\mathrm{Y},r}^2\right) P_{\mathrm{X}} |h_{\mathrm{XY}}|^2 + N_0} \\ &= \frac{P_{\mathrm{X}} |h_{\mathrm{XY}}|^2}{\kappa_{\mathrm{XY}} P_{\mathrm{X}} |h_{\mathrm{XY}}|^2 + N_0}, \end{aligned} \tag{3}$$

where N_0 is the variance of the Gaussian noise, which is assumed to be the same at all of the receivers and $\kappa_{\mathrm{XY}} = \xi_{\mathrm{X},t}^2 + \xi_{\mathrm{Y},r}^2$ is the total level of hardware impairments.

For ease of presentation and analysis, we denote κ_{D} as the total level of hardware impairments on the data links, $\left(\mathrm{X} \in \left\{\mathrm{S}, \mathrm{R}_j^k\right\}, \mathrm{Y} \in \left\{\mathrm{R}_j^k, \mathrm{D}\right\}\right)$; κ_{E} is the total level of hardware impairments on the eavesdropping links, $\left(\mathrm{X} \in \left\{\mathrm{S}, \mathrm{R}_j^k\right\}, \mathrm{Y} \in \left\{\mathrm{E}\right\}\right)$; and κ_{P} is the total level of hardware impairments on the interference links, $\left(\mathrm{X} \in \left\{\mathrm{S}, \mathrm{R}_j^k\right\}, \mathrm{Y} \in \left\{\mathrm{P}_m\right\}\right)$.

Before transmitting the data, transmitter X must adapt its transmit power to satisfy the interference constraint required by the primary users as in [21]:

$$P_{\mathrm{X}} = \frac{I_{\mathrm{P}}}{\left(1 + \kappa_{\mathrm{P}}\right) \max\limits_{m=1,2,...,M} \left(|h_{\mathrm{XP}_m}|^2\right)}, \tag{4}$$

where I_{P} is the interference constraint, and h_{XP_m} is the channel coefficient between secondary transmitter X and primary user P_m.

From (3) and (4), the obtained SNR on the data and eavesdropping links can be given, respectively as

$$\psi_{\mathrm{XY}} = \frac{\dfrac{Q |h_{\mathrm{XY}}|^2}{\max\limits_{m=1,2,...,M} \left(|h_{\mathrm{XP}_m}|^2\right)}}{\dfrac{\kappa_{\mathrm{D}} Q |h_{\mathrm{XY}}|^2}{\max\limits_{m=1,2,...,M} \left(|h_{\mathrm{XP}_m}|^2\right)} + 1}, \tag{5}$$

$$\psi_{\mathrm{XE}} = \frac{\dfrac{Q |h_{\mathrm{XE}}|^2}{\max\limits_{m=1,2,...,M} \left(|h_{\mathrm{XP}_m}|^2\right)}}{\dfrac{\kappa_{\mathrm{E}} Q |h_{\mathrm{XE}}|^2}{\max\limits_{m=1,2,...,M} \left(|h_{\mathrm{XP}_m}|^2\right)} + 1}, \tag{6}$$

where

$$Q = \frac{I_{\mathrm{P}}}{\left(1 + \kappa_{\mathrm{P}}\right) N_0}.$$

Assume that all the channels are Rayleigh fading; channel gains $|h_{\mathrm{XY}}|^2$ are exponential random variables (RVs). We also denote $\gamma_j^{i,k} = |h_{\mathrm{R}_{j-1}^i, \mathrm{R}_j^k}|^2$ as the channel gain of the link between nodes R_{j-1}^i and R_j^k, where $i = 1,2,...,N_{j-1}$ and $k = 1,2,...,N_j$. In addition, note that $\mathrm{R}_0^i \equiv \mathrm{S}\left(\forall i\right)$. Assume that RVs $\gamma_j^{i,k}$ are independent and identically distributed, i.e., they have the same CDF and PDF, which are given as

$$\begin{aligned} F_{\gamma_j^{i,k}}\left(x\right) &= 1 - \exp\left(-\lambda_j x\right), \\ f_{\gamma_j^{i,k}}\left(x\right) &= \lambda_j \exp\left(-\lambda_j x\right), \end{aligned} \tag{7}$$

Respectively, where λ_j is the parameter of the RV $\gamma_j^{i,k}$ and is modeled as in [6]:

$$\lambda_j = d_j^{\beta}, \tag{8}$$

where d_j is the link distance between nodes belonging to cluster j-1 and cluster j, and β is the path-loss exponent,

which varies from 2 to 6.

Similarly, we denote $\varphi_j^i = |h_{\mathrm{R}_{j-1}^i,\mathrm{E}}|^2$ and $\psi_j^{i,m} = |h_{\mathrm{R}_{j-1}^i,\mathrm{P}_m}|^2$ as the channel gains of the $\mathrm{R}_{j-1}^i \to \mathrm{E}$ and $\mathrm{R}_{j-1}^i \to \mathrm{P}_m$ links, respectively. Also, φ_j^i and $\psi_j^{i,m}$ are exponential RVs with parameters Ω_j and Δ_j, respectively, where $\Omega_j = f_j^\beta$ and $\Delta_j = g_j^\beta$ with f_j as the distance between the nodes in the (j-1)-th cluster and eavesdropper E, while g_j is distance between the nodes in the (j-1)-th cluster and the primary users.

Now, we will describe the operation of the proposed protocol. The data transmission is split into $K+1$ orthogonal time slots. In the first time slot, the source transmits its data to the selected relay $\left(\mathrm{R}_1^c\right)$ which belongs to the first cluster. The relay selection method can be given as the following strategy [16]:

$$\mathrm{R}_1^c : \gamma_1^{i,c} = \max_{k=1,2,\ldots,N_1}\left(\gamma_1^{i,k}\right). \tag{9}$$

Eq. (9) implies that relay R_1^c is considered as the best candidate if the channel gain between this node and the source is highest.

Combining (5), (6) and (9), the instantaneous SNR obtained by the best relay $\left(\mathrm{R}_1^c\right)$ and eavesdropper E can be expressed by

$$\psi_{\mathrm{D},1} = \frac{Q\gamma_1^{i,c} / Z_1^{\max}}{\kappa_{\mathrm{D}} Q\gamma_1^{i,c} / Z_1^{\max} + 1}, \tag{10}$$

$$\psi_{\mathrm{E},1} = \frac{Q\varphi_1^{i} / Z_1^{\max}}{\kappa_{\mathrm{E}} Q\varphi_1^{i} / Z_1^{\max} + 1}, \tag{11}$$

respectively, where $Z_1^{\max} = \max_{m=1,2,\ldots,M}\left(\psi_1^{c,m}\right)$.

Then, relay R_1^c will decode the source data, and then re-encode and forward the encoded data to the next hop in the second time slot.

Generally, the selected relay of the (j-1)-th cluster $\left(\mathrm{R}_{j-1}^c\right)$ will communicate with relay R_j^c of the j-th cluster in the j-th time slot. Similar to (9), relay R_j^c is chosen as follows:

$$\mathrm{R}_j^c : \gamma_j^{c,c} = \max_{k=1,2,\ldots,N_j}\left(\gamma_j^{c,k}\right). \tag{12}$$

Also note that the relay selection process in (12) can be executed in a distributed manner [25], where the relays in the j-th cluster will set a timer to find the best candidate.

As in (10) and (11), we can write the obtained instantaneous SNR of the $\mathrm{R}_j^c \to \mathrm{R}_{j+1}^c$ and $\mathrm{R}_j^c \to \mathrm{E}$ links, respectively, as

$$\psi_{\mathrm{D},j} = \frac{Q\gamma_j^{c,c} / Z_j^{\max}}{\kappa_{\mathrm{D}} Q\gamma_j^{c,c} / Z_j^{\max} + 1}, \tag{13}$$

$$\psi_{\mathrm{E},j} = \frac{Q\varphi_j^{c} / Z_j^{\max}}{\kappa_{\mathrm{E}} Q\varphi_j^{c} / Z_j^{\max} + 1}, \tag{14}$$

where $Z_j^{\max} = \max_{m=1,2,\ldots,M}\left(\psi_j^{c,m}\right)$.

Let us consider the last hop where relay R_K^c of the K-th cluster sends the data to destination D in the (K+1)-th time slot. Because the destination uses the SC technique to combine the received data, the instantaneous SNR received at the secondary destination (D) can be formulated as

$$\begin{aligned}\psi_{\mathrm{D},K+1} &= \max_{l=1,2,\ldots,L}\left(\frac{Q\gamma_{K+1}^{c,l} / Z_{K+1}^{\max}}{\kappa_{\mathrm{D}} Q\gamma_{j+1}^{c,c} / Z_{K+1}^{\max} + 1}\right) \\ &= \frac{Q\max\limits_{l=1,2,\ldots,L}\left(\gamma_{K+1}^{c,l}\right) / Z_{K+1}^{\max}}{\kappa_{\mathrm{D}} Q\max\limits_{l=1,2,\ldots,L}\left(\gamma_{K+1}^{c,l}\right) / Z_{K+1}^{\max} + 1},\end{aligned} \tag{15}$$

where $Z_{K+1}^{\max} = \max_{m=1,2,\ldots,M}\left(\psi_{K+1}^{c,m}\right)$, and $\gamma_{K+1}^{c,l}$ is the channel gain between R_K^c and the l-th antenna at the destination. Also note that RVs $\gamma_{K+1}^{c,l}$ have an exponential distribution with parameter $\lambda_{K+1} = d_{K+1}^\beta$, where d_{K+1} is the link distance between node R_K^c and destination D.

Then, the received SNR at the eavesdropper in this time slot is given as

$$\psi_{\mathrm{E},K+1} = \frac{Q\varphi_{K+1}^{c} / Z_{K+1}^{\max}}{\kappa_{\mathrm{E}} Q\varphi_{K+1}^{c} / Z_{K+1}^{\max} + 1}, \tag{16}$$

To prevent the eavesdropper from combining the received data using maximal ratio combining (MRC) technique, the source and the selected relays employ the randomize-and-forward (RF) technique [19, 26] in which codebooks of the source data are generated randomly on each hop.

Next, combining (10), (13), and (15), we can formulate the end-to-end SNR of the data link as follows:

$$\psi_{\mathrm{e2e}} = \min_{j=1,2,\ldots,K+1}\left(\psi_{\mathrm{D},j}\right). \tag{17}$$

3. Performance Evaluation

In order to derive the CDF of ψ_{e2e} in (17), we have to calculate the CDF of $\psi_{\mathrm{D},j}$. Indeed, from (13), we obtain

$$\begin{aligned}F_{\psi_{\mathrm{D},j}}(x) &= \Pr\left(\frac{Q\gamma_j^{c,c} / Z_j^{\max}}{\kappa_{\mathrm{D}} Q\gamma_j^{c,c} / Z_j^{\max} + 1} < x\right) \\ &= \Pr\left(\left(1-\kappa_{\mathrm{D}} x\right) Q\gamma_j^{c,c} / Z_j^{\max} < x\right) \\ &= \begin{cases} 1, & \text{if } x \ge 1/\kappa_{\mathrm{D}} \\ \Pr\left(\dfrac{\gamma_j^{c,c}}{Z_j^{\max}} < \dfrac{x}{\left(1-\kappa_{\mathrm{D}} x\right) Q}\right), & \text{if } x < 1/\kappa_{\mathrm{D}} \end{cases}\end{aligned} \tag{18}$$

From (18), when $x<1/\kappa_{\mathrm{D}}$, CDF $F_{\psi_{\mathrm{D}j}}(x)$ can be formulated by

$$\begin{aligned} F_{\psi_{\mathrm{D}j}}(x) &= \Pr\left(\gamma_j^{c,c} < \frac{x}{(1-\kappa_{\mathrm{D}}x)Q} Z_j^{\max}\right) \\ &= \int_0^{+\infty} F_{\gamma_j^{c,c}}\left(\frac{x}{(1-\kappa_{\mathrm{D}}x)Q} y\right) f_{Z_j^{\max}}(y)\,dy, \end{aligned} \tag{19}$$

where $F_{\gamma_j^{c,c}}(.)$ and $f_{Z_j^{\max}}(.)$ are the CDF and PDF of RVs $\gamma_j^{c,c}$ and $Z_j^{\max}$, respectively.

Since $\gamma_j^{c,c} = \max\limits_{k=1,2,\ldots,N_j}\left(\gamma_j^{c,k}\right)$, the CDF of $\gamma_j^{c,c}$ can be given as

$$F_{\gamma_j^{c,c}}(x) = \Pr\left(\max_{k=1,2,\ldots,N_j}\left(\gamma_j^{c,k}\right) < x\right) = \left(F_{\gamma_j^{c,k}}(x)\right)^{N_j}. \tag{20}$$

Combining (7) and (20), the CDF of $\gamma_j^{c,c}$ is obtained by

$$\begin{aligned} F_{\gamma_j^{c,c}}(x) &= \left(1-\exp\left(-\lambda_j x\right)\right)^{N_j} \\ &= 1+\sum_{u=1}^{N_j}(-1)^u C_{N_j}^u \exp\left(-u\lambda_j x\right), \end{aligned} \tag{21}$$

where $C_{N_j}^u$ is the binomial coefficient.

Similarly, we can obtain the CDF of $Z_j^{\max}$ with

$$F_{Z_j^{\max}}(y) = \Pr\left(\max_{m=1,2,\ldots,M}\left(\psi_j^{c,m}\right) < y\right) = \left(1-\exp\left(-\Delta_j y\right)\right)^M. \tag{22}$$

Therefore, the PDF of $Z_j^{\max}$ can be given as

$$\begin{aligned} f_{Z_j^{\max}}(y) &= M\Delta_j \exp\left(-\Delta_j y\right)\left(1-\exp\left(-\Delta_j y\right)\right)^{M-1} \\ &= \sum_{v=0}^{M-1}(-1)^v C_{M-1}^v M\Delta_j \exp\left(-(v+1)\Delta_j y\right). \end{aligned} \tag{23}$$

Substituting (21) and (23) into (19), after some manipulations, we obtain

$$\begin{aligned} F_{\psi_{\mathrm{D}j}}(x) = 1+\sum_{u=1}^{N_j}\sum_{v=0}^{M-1}(-1)^{u+v} C_{N_j}^u C_{M-1}^v M\Delta_j \\ \times\frac{(1-\kappa_{\mathrm{D}}x)Q}{u\lambda_j x+(v+1)\Delta_j(1-\kappa_{\mathrm{D}}x)Q}. \end{aligned} \tag{24}$$

In the same manner, the CDF of $\psi_{\mathrm{D},K+1}$ can be given as

$$\begin{aligned} F_{\psi_{\mathrm{D},K+1}}(x) = 1+\sum_{u=1}^{L}\sum_{v=0}^{M-1}(-1)^{u+v} C_L^u C_{M-1}^v M\Delta_{K+1} \\ \times\frac{(1-\kappa_{\mathrm{D}}x)Q}{u\lambda_{K+1}x+(v+1)\Delta_{K+1}(1-\kappa_{\mathrm{D}}x)Q}. \end{aligned} \tag{25}$$

Next, the CDF of ψ_{e2e} can be formulated as

$$\begin{aligned} F_{\psi_{\mathrm{e2e}}}(x) &= \Pr\left(\min_{j=1,2,\ldots,K+1}\left(\psi_{\mathrm{D}j}\right) < x\right) = 1-\prod_{j=1}^{K+1}\left(1-\Pr\left(\psi_{\mathrm{D}j} < x\right)\right) \\ &= 1-\prod_{j=1}^{K+1}\left(1-F_{\psi_{\mathrm{D}j}}(x)\right). \end{aligned} \tag{26}$$

Substituting (24) and (25) into (26) yields

$$\begin{aligned} F_{\psi_{\mathrm{e2e}}}(x) = 1- \\ \prod_{j=1}^{K}\left[\sum_{u=1}^{N_j}\sum_{v=0}^{M-1}\frac{(-1)^{u+v+1} C_{N_j}^u C_{M-1}^v M\Delta_j(1-\kappa_{\mathrm{D}}x)Q}{u\lambda_j x+(v+1)\Delta_j(1-\kappa_{\mathrm{D}}x)Q}\right] \\ \times\left[\sum_{u=1}^{L}\sum_{v=0}^{M-1}\frac{(-1)^{u+v+1} C_L^u C_{M-1}^v M\Delta_{K+1}(1-\kappa_{\mathrm{D}}x)Q}{u\lambda_{K+1}x+(v+1)\Delta_{K+1}(1-\kappa_{\mathrm{D}}x)Q}\right]. \end{aligned} \tag{27}$$

From (18) and (27), the end-to-end outage probability of the proposed method can be computed exactly by

$$\mathrm{OP}=\Pr\left(\psi_{\mathrm{e2e}} < \gamma_{th}\right) = \begin{cases} 1, & \text{if } \gamma_{th} \ge 1/\kappa_{\mathrm{D}} \\ F_{\psi_{\mathrm{e2e}}}(\gamma_{th}), & \text{if } \gamma_{th} < 1/\kappa_{\mathrm{D}} \end{cases} \tag{28}$$

where

$$\begin{aligned} F_{\psi_{\mathrm{e2e}}}(\gamma_{th}) = 1-\prod_{j=1}^{K}\left[\sum_{u=1}^{N_j}\sum_{v=0}^{M-1}\frac{(-1)^{u+v+1} C_{N_j}^u C_{M-1}^v M\Delta_j}{u\lambda_j\rho_{\mathrm{D}}+(v+1)\Delta_j}\right] \\ \times\left[\sum_{u=1}^{L}\sum_{v=0}^{M-1}\frac{(-1)^{u+v+1} C_L^u C_{M-1}^v M\Delta_{K+1}}{u\lambda_{K+1}\rho_{\mathrm{D}}+(v+1)\Delta_{K+1}}\right], \end{aligned} \tag{29}$$

with $\rho_{\mathrm{D}} = \gamma_{th}/(1-\kappa_{\mathrm{D}}\gamma_{th})/Q$.

Next, we evaluate the value of OP at high Q values, i.e., $Q\to+\infty$. Using (21), we can approximate the CDF of $\gamma_j^{c,c}$ in (19) as

$$\begin{aligned} F_{\gamma_j^{c,c}}\left(\frac{x}{(1-\kappa_{\mathrm{D}}x)Q} y\right) &= \left(1-\exp\left(-\frac{\lambda_j x}{(1-\kappa_{\mathrm{D}}x)Q} y\right)\right)^{N_j} \\ &\overset{Q\to+\infty}{\approx} \left(\frac{\lambda_j x}{(1-\kappa_{\mathrm{D}}x)Q} y\right)^{N_j}. \end{aligned} \tag{30}$$

Substituting (23) and (30) into (19), we obtain

$$\begin{aligned} F_{\psi_{\mathrm{D}j}}(x) &\overset{Q\to+\infty}{\approx} \sum_{v=0}^{M-1}(-1)^v C_{M-1}^v M\Delta_j\left(\frac{\lambda_j x}{(1-\kappa_{\mathrm{D}}x)Q}\right)^{N_j} \\ &\quad\times\int_0^{+\infty} y^{N_j}\exp\left(-(v+1)\Delta_j y\right)dy \\ &\overset{Q\to+\infty}{\approx} \sum_{v=0}^{M-1}\frac{(-1)^v N_j! C_{M-1}^v M}{(v+1)^{N_j+1}(\Delta_j)^{N_j}}\left(\frac{\lambda_j x}{(1-\kappa_{\mathrm{D}}x)Q}\right)^{N_j}. \end{aligned} \tag{31}$$

Similarly, we can approximate CDF $F_{\psi_{\mathrm{D},K+1}}(x)$ as

$$F_{\psi_{\mathrm{D},K+1}}(x) \overset{Q\to+\infty}{\approx} \sum_{v=0}^{M-1} \frac{(-1)^v L! C_{M-1}^v M}{(v+1)^{L+1}(\Delta_{K+1})^L} \left(\frac{\lambda_{K+1} x}{(1-\kappa_{\mathrm{D}} x)Q}\right)^L. \quad (32)$$

Using (31) and (32), the asymptotic closed-form expression of the OP can be expressed as follows:

$$\begin{aligned} \mathrm{OP} &= 1-\prod_{j=1}^{K+1}\left(1-F_{\psi_{\mathrm{D},j}}(\gamma_{th})\right) \overset{Q\to+\infty}{\approx} \sum_{j=1}^{K+1} F_{\psi_{\mathrm{D},j}}(\gamma_{th}) \\ &\overset{Q\to+\infty}{\approx} \sum_{j=1}^{K}\sum_{v=0}^{M-1} \frac{(-1)^v N_j! C_{M-1}^v M}{(v+1)^{N_j+1}} \left(\frac{\lambda_j}{\Delta_j}\right)^{N_j} \rho_{\mathrm{D}}^{N_j} \\ &+ \sum_{v=0}^{M-1} \frac{(-1)^v L! C_{M-1}^v M}{(v+1)^{L+1}} \left(\frac{\lambda_{K+1}}{\Delta_{K+1}}\right)^L \rho_{\mathrm{D}}^L. \end{aligned} \quad (33)$$

Using the asymptotic expression of the OP obtained in (33), the definition of the diversity gain in [27, Eq. (17)), and $\rho_{\mathrm{D}} = \gamma_{th}/(1-\kappa_{\mathrm{D}}\gamma_{th})/Q$, the diversity order of the proposed system can be calculated as follows:

$$\begin{aligned} \mathrm{Div} &= -\lim_{Q\to+\infty} \frac{\log(\mathrm{OP})}{\log(Q)} \\ &= -\lim_{\rho_{\mathrm{D}}\to 0} \frac{\log\left(\sum_{j=1}^{K+1} F_{\psi_{\mathrm{D},j}}(\gamma_{th})\right)}{\log\left(\gamma_{th}/(1-\kappa_{\mathrm{D}}\gamma_{th})\right)-\log(\rho_{\mathrm{D}})} \\ &= \min\left(\min_{j=1,2,\ldots,K}(N_j), L\right). \end{aligned} \quad (34)$$

Next, we focus on deriving the intercept probability for the eavesdropping links. At first, we have to formulate the CDF of the SNR $\psi_{\mathrm{E},j}\ (j=1,2,\ldots,K+1)$. Similar to (18), it can be obtained as follows:

$$F_{\psi_{\mathrm{E},j}}(x) = \begin{cases} 1, & \text{if } x \ge 1/\kappa_{\mathrm{E}} \\ \Pr\left(\dfrac{\varphi_j^c}{Z_j^{\max}} < \dfrac{x}{(1-\kappa_{\mathrm{E}}x)Q}\right), & \text{if } x < 1/\kappa_{\mathrm{E}} \end{cases} \quad (35)$$

In the same way we derived (24), we can obtain the exact closed-form expression for $F_{\psi_{\mathrm{E},j}}(x)$ as

$$F_{\psi_{\mathrm{D},j}}(x) = \begin{cases} 1, & \text{if } x \ge 1/\kappa_{\mathrm{E}} \\ 1-\sum_{v=0}^{M-1} \dfrac{(-1)^v C_{M-1}^v M\Delta_j (1-\kappa_{\mathrm{E}}x)Q}{\Omega_j x+(v+1)\Delta_j(1-\kappa_{\mathrm{E}}x)Q}, & \text{if } x < 1/\kappa_{\mathrm{E}} \end{cases} \quad (36)$$

Using (36), we can formulate the probability that eavesdropper E can overhear the source data successfully on the *j*-th hop (or the IP at the *j*-th hop) by

$$\begin{aligned} \mathrm{IP}_j &= \Pr(\psi_{\mathrm{E},j} \ge \gamma_{th}) = 1-F_{\psi_{\mathrm{E},j}}(\gamma_{th}) \\ &= \begin{cases} 0, & \text{if } x \ge 1/\kappa_{\mathrm{E}} \\ \sum_{v=0}^{M-1} \dfrac{(-1)^v C_{M-1}^v M\Delta_j (1-\kappa_{\mathrm{E}}x)Q}{\Omega_j x+(v+1)\Delta_j(1-\kappa_{\mathrm{E}}x)Q}, & \text{if } x < 1/\kappa_{\mathrm{E}} \end{cases} \end{aligned} \quad (37)$$

Here, we have some remarks.

- When eavesdropper E can decode the source data successfully on the *j*-th hop, this node will stop overhearing during the remaining hops.
- The condition where eavesdropper E can overhear successfully on the *j*-th hop requires the data transmission on previous hops (between the nodes R_k^c and R_{k+1}^c, with $k=1,2,\ldots,j-1$, to be successful.

Therefore, the average IP of the eavesdropping link can be formulated as

$$\mathrm{IP} = \mathrm{IP}_1 + \sum_{j=2}^{K+1}\left[\prod_{k=1}^{j-1} \Pr(\psi_{\mathrm{D},k} \ge \gamma_{th}, \psi_{\mathrm{E},k} < \gamma_{th})\right] \mathrm{IP}_j, \quad (38)$$

In (38), IP_1 is the probability that the eavesdropper obtains the data correctly on the first hop, whereas IP_j is the intercept probability on the *j*-th hop. Moreover, $\Pr(\psi_{\mathrm{D},k} \ge \gamma_{th}, \psi_{\mathrm{E},k} < \gamma_{th})$ is the probability that the data transmission and interception on the *k*-th hop is successful and unsuccessful, respectively.

From (13) and (14), we can express probability $\Pr(\psi_{\mathrm{D},k} \ge \gamma_{th}, \psi_{\mathrm{E},k} < \gamma_{th})$ in the following form:

$$\begin{aligned} &\Pr(\psi_{\mathrm{D},k} \ge \gamma_{th}, \psi_{\mathrm{E},k} < \gamma_{th}) = \\ &= \Pr\left((1-\kappa_{\mathrm{D}}\gamma_{th})\frac{\gamma_j^{c,c}}{Z_j^{\max}} \ge \frac{\gamma_{th}}{Q}, (1-\kappa_{\mathrm{E}}\gamma_{th})\frac{\varphi_j^c}{Z_j^{\max}} < \frac{\gamma_{th}}{Q}\right). \end{aligned} \quad (39)$$

If $\gamma_{th} < \min(1/\kappa_{\mathrm{D}}, 1/\kappa_{\mathrm{E}})$, (39) can be rewritten as

$$\begin{aligned} &\Pr(\psi_{\mathrm{D},k} \ge \gamma_{th}, \psi_{\mathrm{E},k} < \gamma_{th}) = \Pr\left(\frac{\gamma_j^{c,c}}{Z_j^{\max}} \ge \rho_{\mathrm{D}}, \frac{\varphi_j^c}{Z_j^{\max}} < \rho_{\mathrm{E}}\right) \\ &= \int_0^{+\infty} f_{Z_j^{\max}}(x)\left[1-F_{\gamma_j^{c,c}}(\rho_{\mathrm{D}}x)\right] F_{\varphi_j^c}(\rho_{\mathrm{E}}x)\,dx, \end{aligned} \quad (40)$$

where $\rho_{\mathrm{E}} = \gamma_{th}/(1-\kappa_{\mathrm{E}}\gamma_{th})/Q$.

Substituting (7), (21), and (23) into (40), after some careful manipulations, we can obtain (41) as follows:

$$\begin{aligned} &\Pr(\psi_{\mathrm{D},k} \ge \gamma_{th}, \psi_{\mathrm{E},k} < \gamma_{th}) = \\ &\sum_{u=1}^{N_j}\sum_{v=0}^{M-1} \frac{(-1)^{u+v+1} C_{N_j}^u C_{M-1}^v M\Delta_j\Omega_j\rho_{\mathrm{E}}}{\left(u\lambda_j\rho_{\mathrm{D}}+(v+1)\Delta_j\right)\left(\left(u\lambda_j\rho_{\mathrm{D}}+\Omega_j\rho_{\mathrm{E}}\right)+(v+1)\Delta_j\right)}. \end{aligned} \quad (41)$$

Substituting (37) and (41) into (38), we obtain the exact

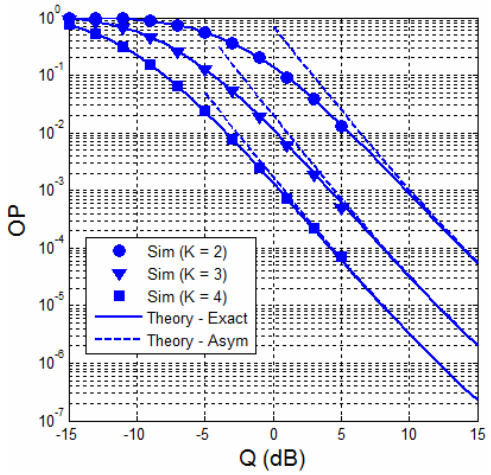

Fig. 2. Outage probability (OP) as a function of Q in dB when $M=2,\ L=2,\ N_j=3\,(\forall j),\ \kappa_{\mathrm{D}}=0.1,\ \kappa_{\mathrm{E}}=0.1,\ \kappa_{\mathrm{P}}=0,\ x_{\mathrm{E}}=0.5,\ y_{\mathrm{E}}=0.5,\ x_{\mathrm{P}}=-0.5,\ y_{\mathrm{P}}=-0.5,$ and $\gamma_{th}=1.$

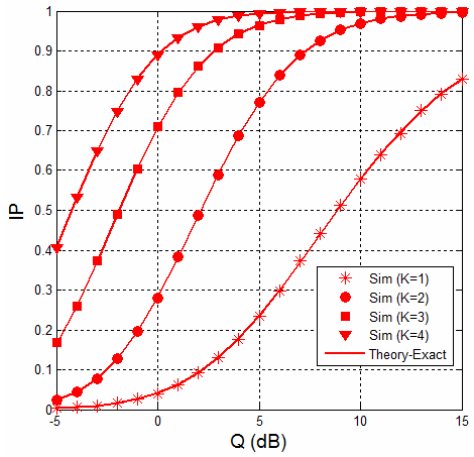

Fig. 3. Intercept probability (IP) as a function of Q in dB when $M=3,\ L=2,\ N_j=3\,(\forall j),\ \kappa_{\mathrm{D}}=0.2,\ \kappa_{\mathrm{E}}=0.2,\ \kappa_{\mathrm{P}}=0,\ x_{\mathrm{E}}=0.5,\ y_{\mathrm{E}}=0.5,\ x_{\mathrm{P}}=-0.5,\ y_{\mathrm{P}}=-0.5,$ and $\gamma_{th}=2.$

closed-form expression of the IP.

4. Simulation Results

In this section, we provide Monte-Carlo simulations in order to verify the theoretical derivations. In the simulation environment, we consider a two-dimensional plane in which the coordinates of the secondary source S , the secondary relays R_j^k , the secondary destination D , the secondary eavesdropper E and the primary users are (0,0), $\left(j/(K+1),0\right)$, (1,0), (x_{E} , y_{E}), and (x_{P} , y_{P}), respectively. Therefore, the distances are calculated as, $d_j=1/(K+1)(\forall j)$, $f_j=\sqrt{\left((j-1)/(K+1)-x_{\mathrm{E}}\right)^2+y_{\mathrm{E}}^2}$, and $g_j=\sqrt{\left((j-1)/(K+1)-x_{\mathrm{P}}\right)^2+y_{\mathrm{P}}^2}$. In all simulations, we assume that path-loss exponential β is equal to 3.

In Fig. 2, we present the outage probability of the proposed scheme as a function of Q in dB. In this simulation, the number of primary users is 2 $(M=2)$, and the primary users are placed at position $(-0.5,-0.5)$. Eavesdropper E is assumed to be located at $(0.5,0.5)$. We also assume that destination D has two antennas $(L=2)$, and the number of nodes in each cluster is 3 $(N_j=3\forall j)$. For the hardware impairments, the values of κ_{D} , κ_{E} and κ_{P} are assigned as 0.1, 0.1 and 0, respectively. Finally, outage threshold γ_{th} is set to 0.1. We can observe from this figure that the outage probability decreases when the value of Q increases. In addition, with higher number of hops (a higher value for K), the proposed system also obtains better performance due to the short distance between two adjacent clusters. It is also seen from Fig. 2 that the simulation results (Sim) match very well with the theoretical results (Theory-Exact), which verifies the correction of our derivations. Moreover, at high Q regions, the asymptotic values (Theory-Asym) rapidly converge to the exact ones and the diversity gain obtained equals 2 for all values of K.

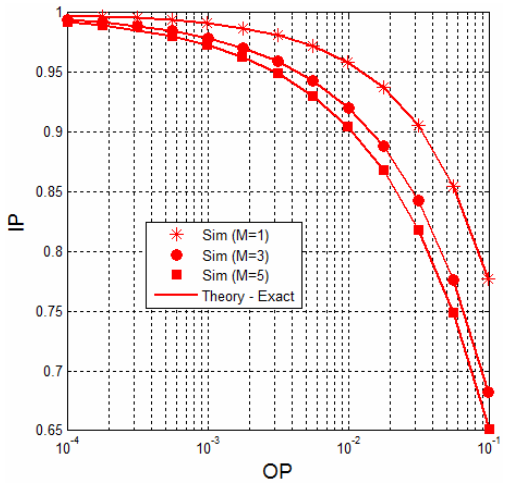

Fig. 4. Intercept probability (IP) as a function of outage probability (OP) when $K=2,\ N_1=N_2=L=5,\ \kappa_{\mathrm{D}}=0.1,\ \kappa_{\mathrm{E}}=0.1,\ \kappa_{\mathrm{P}}=0.1,\ x_{\mathrm{E}}=0.5,\ y_{\mathrm{E}}=0.5,\ x_{\mathrm{P}}=-0.5,\ y_{\mathrm{P}}=-0.5,$ and $\gamma_{th}=1.5.$

Fig. 3 presents the intercept probability as a function of Q in dB when $M=3,\ \kappa_{\mathrm{D}}=\kappa_{\mathrm{E}}=0.2,\ \kappa_{\mathrm{P}}=0,\ L=2,$ $N_j=3(\forall j),\ x_{\mathrm{E}}=y_{\mathrm{E}}=0.5,\ x_{\mathrm{P}}=y_{\mathrm{P}}=-0.5,$ and $\gamma_{th}=2.$ It can be seen in Fig. 3 that the value of the IP increases with the increasing of Q and K. Moreover, we can see that the IP significantly increases with higher number of hops. It is due to the fact that when the number of hops increases, eavesdropper E can overhear the source data more times. Again, the simulation and theoretical results are in good agreement, which validates the theoretical analysis.

In Fig. 4, we investigate the security-reliability tradeoff by presenting IP as a function of OP when $K=2,$

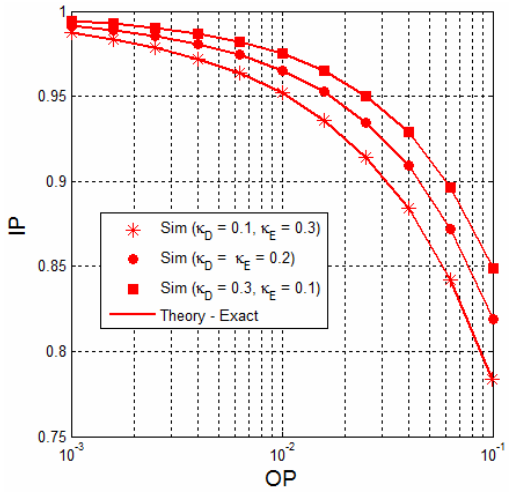

Fig. 5. Intercept probability (IP) as a function of outage probability (OP) when $K=1,\ N_1=4,\ L=3,\ M=2,\ x_E=0.5,\ y_E=0.5,\ x_P=-0.5,\ y_P=-0.5,$ **and** $\gamma_{th}=1.$

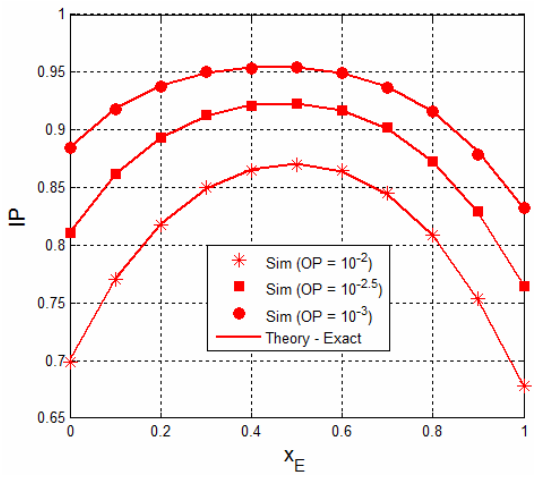

Fig. 6. Intercept probability (IP) as a function of x_E **when** $K=2,\ N_1=7,\ N_2=5,\ L=3,\ \kappa_D=0,\ \kappa_E=0,\ \kappa_P=0,\ M=4,\ y_E=0.5,\ x_P=-0.5,\ y_P=-0.5,$ **and** $\gamma_{th}=2.$

$N_1=N_2=L=5,\ \kappa_D=\kappa_E=\kappa_P=0.1,\ x_E=y_E=0.5,\ x_P=y_P=-0.5,$ and $\gamma_{th}=1.5$. As we can see in this figure, the IP increases with the decreasing of OP. It is also seen from Fig. 4 that with the same value of OP, IP decreases with higher number of primary users (M).

Similar to Fig. 4, Fig. 5 shows that in order to obtain a high quality of service (QoS) for the data link (i.e., a low OP), the proposed system suffers from a high IP. In Fig. 5, the system parameters are set as follows: $K=1,\ N_1=4,\ L=3,\ M=2,\ x_E=y_E=0.5,\ x_P=y_P=-0.5,$ and $\gamma_{th}=1$. In this figure, we consider various scenarios where the hardware impairment levels of the data links (κ_D) and the eavesdropping links (κ_E) change from 0.1 to 0.3. We can see that the value of the IP is lowest when the hardware impairment level of the data links is lower than that of the eavesdropping links, i.e., $\kappa_D=0.1,\ \kappa_E=0.3$.

Fig. 6 investigates the impact of the position of the eavesdropper on the intercept probability with $K=2,\ N_1=7,\ N_2=5,\ L=3,\ \kappa_D=\kappa_E=\kappa_P=0,\ x_P=y_P=-0.5,$ and $\gamma_{th}=2$. In this figure, we fix y_E at 0.5 while changing x_E from 0 to 1. As we can see, the value of IP depends on the position of the eavesdropper. Moreover, the value of IP is highest when x_E is about 0.5.

5. Conclusion

In this paper, we analyzed the security-reliability tradeoff for a multi-hop transmission protocol in cluster-based underlay cognitive radio networks. In particular, the outage and intercept performances were evaluated via both simulations and theory. The interesting results obtained in this paper are as follows:

- The proposed protocol obtains a high diversity order which equals the minimum value of the number of relays at the clusters and the number of antennas equipped at the secondary destination.
- The outage performance can be enhanced by increasing the number of hops. However, the intercept probability also increases with higher number of hops.
- There exists a tradeoff between security and reliability, i.e., in order to obtain high outage performance, the proposed system suffers from a high intercept probability from the secondary eavesdropper.
- To enhance security for the proposed protocol, the authorized nodes such as the source, relays and destination, should be equipped with good transceiver hardware (to reduce the hardware impairment level on the data links).
- The position of the secondary eavesdropper significantly impacts the intercept probability.
- With the same value for outage probability, the value of the intercept probability decreases with higher number of primary users.

Acknowledgement

This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.01-2014.33.

References

[1] M.O. Hasna and M.S. Alouini, "Outage probability of multihop transmission over nakagami fading channels," *IEEE Communication Letters*, vol. 7, no. 5, pp. 216-218, 2003. Article (CrossRef Link)

[2] G. K. Karagiannidis, "Performance bounds of multihop wireless communications with blind relays over generalized fading channels," *IEEE Transactions on Wireless Communications*, vol. 5, no. 3, pp. 498-503, 2006. Article (CrossRef Link)

[3] Z. Yi, M. Ju, H.-K. Song, and I.-M. Kim, "Relay

ordering in a multi-hop cooperative diversity network," *IEEE Transactions on Communications*, vol. 57, pp. 2590-2596, 2009. Article (CrossRef Link)

[4] C. Coone and I1-Min Kim, "Outage Probability of Multi-hop Amplify-and-forward Relay Systems", *IEEE Transactions on Wireless Communications*, vol.9, no.3, pp. 1139-1149, 2010. Article (CrossRef Link)

[5] B. An, T. D. Tran and H.Y. Kong, "A Cooperative Transmission Strategy using Entropy-based Relay Selection in Mobile Ad-hoc Wireless Sensor Networks with Rayleigh Fading Environments", *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 3, no. 2, pp.147-162, 2009. Article (CrossRef Link)

[6] J. N. Laneman, D. N. C. Tse, G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, Vol. 50, No. 12, pp. 3062-3080, 2004. Article (CrossRef Link)

[7] Q. Deng, A. G. Klein, "Diversity of multi-hop cluster-based routing with arbitrary relay selection", *IET Communications*, vol. 6, no. 9, pp. 1054-1060, 2012. Article (CrossRef Link)

[8] P. T. Tin, T. D. Tran, T. T. Phuong and M. Voznak, "Secrecy Performance of Joint Relay and Jammer Selection Methods in Cluster Networks: With and Without Hardware Noises", in *Proc. of AETA2016*, pp. 769-779, 2016. Article (CrossRef Link)

[9] J. Lee, H. Wang, J. G. Andrews and D. Hong, "Outage Probability of Cognitive Relay Networks with Interference Constraints," *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, pp. 390-395, 2011. Article (CrossRef Link)

[10] H. Kim, H. Wang, D. Hong, "On Power Allocation Schemes for Bi-directional Communication in a Spectrum Sharing-based Cognitive Radio System", *IEIE Transactions on Smart Processing and Computing*, vol. 3, no. 5, pp. 285-297, 2014. Article (CrossRef Link)

[11] M. Sundararajan, U. Govindaswamy, "Performance Analysis of Uplink Cognitive Radio Transmission based on Overloaded MC-DS-CDMA", *IEIE Transactions on Smart Processing and Computing*, vol. 3, no. 4, pp. 181-190, 2014. Article (CrossRef Link)

[12] Y. Guo, G. Kang, N. Zhang, W. Zhou, P. Zhang, "Outage Performance of Relay assisted Cognitive-radio System under Spectrum-sharing Constraints," *Electronics Letters*, vol. 46, pp. 182-184, 2010. Article (CrossRef Link)

[13] K. Tourki, K. A. Qaraqe and M.-S. Alouini, "Outage Analysis for Underlay Cognitive Networks Using Incremental Regenerative Relaying," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 2, pp. 721-734, 2013. Article (CrossRef Link)

[14] Khalife, H., Malouch, N.; Fdida, S., "Multihop cognitive radio networks: to route or not to route", *IEEE Network*, vol. 23, no. 4, pp. 23-25, 2009. Article (CrossRef Link)

[15] Y. Shi, Y. T. Hou, S. Kompella, H. D. Sherali, "Maximizing Capacity in Multihop Cognitive Radio Networks under the SINR Model", *IEEE Transactions on Mobile Computing*, vol. 10, no. 7, pp. 954 - 967, 2011. Article (CrossRef Link)

[16] N. Sang, H.Y. Kong, T. T. Duy, "Cognitive Multihop Cluster-based Transmission under Interference Constraint", in *Proc. of ISCE 2014*, pp. 1-3, Jun. 2014. Article (CrossRef Link)

[17] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975. Article (CrossRef Link)

[18] Y. Liu, L. Wang, D. Tran, M. Elkashlan, Trung Q. Duong, "Relay Selection for Security Enhancement in Cognitive Relay Networks", *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 46-49, Feb. 2015. Article (CrossRef Link)

[19] T. T. Duy, P. N. Son, "Secrecy Performances of Multicast Underlay Cognitive Protocols with Partial Relay Selection and without Eavesdropper's Information", *KSII Transactions on Internet and Information Systems*, vol. 9, no. 11, pp. 4623-4643, Nov. 2015. Article (CrossRef Link)

[20] Y. Zou, B. Champagne, W. P. Zhu and L. Hanzo, "Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems," *IEEE Transactions on Communications*, vol. 63, no. 1 pp. 215–228, Nov. 2015. Article (CrossRef Link)

[21] P. T. D. Ngoc, T. T. Duy, V. N. Q. Bao and N. L. Nhat, "Security-Reliability Analysis for Underlay Cognitive Radio Networks with Relay Selection Methods under Impact of Hardware Noises," in *Proc. of ATC 2016*, pp. 174-179, 2016. Article (CrossRef Link)

[22] N. T. T. Nga, N. K. Khanh, S. N. H., "Entropy-based Correlation Clustering for Wireless Sensor Networks in Multi-Correlated Regional Environments", *IEIE Transactions on Smart Processing and Computing*, vol. 5, no. 2, pp. 85-93, 2016. Article (CrossRef Link)

[23] E. Bjornson, M. Matthaiou and M. Debbah, "A New Look at Dual-hop Relaying: Performance Limits with Hardware Impairments," *IEEE Transactions on Communications*, vol. 61, no. 11, pp. 4512–4525, 2013. Article (CrossRef Link)

[24] M. Matthaiou, A. Papadogiannis, "Two-way relaying under the presence of relay transceiver hardware impairments," *IEEE Communications Letters*, vol. 17, no. 6, pp. 1136–1139, 2013. Article (CrossRef Link)

[25] A. Bletsas, A. Khisti, D. P. Reed, A. Lippman, "A Simple Cooperative Diversity Method based on Network Path Selection," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659–672, 2006. Article (CrossRef Link)

[26] J. Mo, M. Tao and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Communications Letters*, vol. 16, no. 6, pp. 878–881, 2012. Article (CrossRef Link)

[27] T. T. Duy and H.Y. Kong, "Performance Analysis of Incremental Amplify-and-Forward Relaying Protocols with Nth Best Partial Relay Selection under

Interference Constraint," *Wireless Personal Communications*, vol. 71, no. 4, pp. 2741-2757, 2013. Article (CrossRef Link)

Phu Tran Tin was born in Khanh Hoa, Vietnam, in 1979. He received the Bachelor degree (2002) and Master degree (2008) from Ho Chi Minh City University of Science. In 2007, he was lecturer at the Faculty of Electronics Technology (FET), Industrial University of Ho Chi Minh City. Since 2015, he has been participating in Ph.D program that had been linked between Technical University of Ostrava, Czech Republic and Ton Duc Thang University, Ho Chi Minh City. His major research interests are wireless communication in 5G, energy harvesting, performance of cognitive radio and physical layer security.

Pham Minh Nam was born in Thanh Hoa, Vietnam, in 1976. He received the B.E degree in 1999 and M.E degree in 2010 from Ho Chi Minh City University of Technology (HCMUT). He became a lecturer at Electronics Engineering Faculty, Industrial University of Ho Chi Minh City (IUH) in 2010. He is participating in Ph.D program at Ho Chi Minh City University of Technology and Education (HCMUTE) in next spring. His major research interests are energy harvesting, multi-hops in communication, performance of cognitive radio and physical layer security.

Tran Trung Duy was born in Nha Trang city, Vietnam, in 1984. He received the B.E. degree in Electronics and Telecommunications Engineering from the French-Vietnamese training program for excellent engineers (PFIEV), Ho Chi Minh City University of Technology, Vietnam in 2007. In 2013, he received the Ph.D degree in electrical engineering from University of Ulsan, South Korea. In 2013, he joined the Department of Telecommunications, Posts and Telecommunications Institute of Technology (PTIT), as a lecturer. His major research interests are cooperative communications, cognitive radio, and physical layer security.

Miroslav Voznak obtained his PhD. in Telecommunications engineering in 2002 from the Faculty in Electrical Engineering and Computer Science, VSB - Technical University of Ostrava and was appointed as an Associate Professor after his habilitation in the same faculty in 2009. Since 2013, he has been leading a Department of Telecommunications in the VSB - Technical University of Ostrava in position of the department chair. He is an IEEE Senior member, actively enganged as a member in numerous conference programme committees and serving as a member of editorial boards in several journals such as Journal of Communications (US), Advances in Electrical and Electronic Engineering (CZ), Communications (TR), etc. He participated in more than fifteen national and three european projects and since 2011 he has been included as a senior researcher into a Czech National Centre of Excellence (National supercomputing centre). His research interests are focused generally on information and communications technology, particularly on Voice over IP, Quality of Experience, Network security, Wireless networks and last several years on Big Data analytics in mobile cellular networks as well.