Analysis of Probability of Non-zero Secrecy Capacity for Multi-hop Networks in Presence of Hardware Impairments over Nakagami-*m* Fading Channels

Tran Tin PHU [1,2], *The Hung DANG* [3], *Trung Duy TRAN* [4], *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
[3] Faculty of Telecommunications, Telecommunications University, Nha Trang City, Vietnam
[4] Department of Telecommunications, Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam

phutrantin79@gmail.com, danghung8384@gmail.com, trantrungduy@ptithcm.edu.vn, miroslav.voznak@vsb.cz

Manuscript received May 19, 2016

Abstract. *In this paper, we evaluate probability of non-zero secrecy capacity of multi-hop relay networks over Nakagami-m fading channels in presence of hardware impairments. In the considered protocol, a source attempts to transmit its data to a destination by using multi-hop randomize-and-forward (RF) strategy. The data transmitted by the source and relays are overheard by an eavesdropper. For performance evaluation, we derive exact expressions of probability of non-zero secrecy capacity (PoNSC), which are expressed by sums of infinite series of exponential functions and exponential integral functions. We then perform Monte Carlo simulations to verify the theoretical analysis.*

Keywords

Hardware impairments, probability of non-zero secrecy capacity, multi-hop networks, Nakagami-*m* fading channel

1. Introduction

Recently, physical-layer security (PLS) has gained much attention as an efficient method to obtain the security in the presence of eavesdroppers, without using complex cryptographic methods [1]. In PLS, the performance is measured by secrecy capacity which is different between channel capacity of the data and eavesdropping links [2]. In addition, important performance metrics such as secrecy outage probability (SOP) and probability of non-zero secrecy capacity (PoNSC) are commonly used to evaluate the system secrecy performance [3].

To improve the secrecy performances for wireless systems, diversity relaying protocols [4], [5] have become a promising technique. In [6] and [7], the authors evaluated the secrecy performances of the relaying networks at the second phase (cooperative phase). In particular, the published work [6] proposed the joint relay and jammer selection methods to enhance the security for secondary networks in underlay cognitive radio. The authors in [7] investigated the impact of co-channel interference on the secrecy performance of various relay selection strategies. In [8] and [9], dual-hop secured communication protocols in one-way and two-way relaying networks were studied, respectively. Moreover, the authors in [8] proposed a switch-and-stay combining method to obtain the security, while the authors in [9] investigated impact of antenna selection on two-way secured communication scenarios. Published works [10], [11] focused on the secured transmission in multi-hop approaches. In [10], cluster-based multi-hop protocols with various relay selection methods applied for each dual-hop were proposed to further improve the secrecy performances, as compared with the random and conventional relay selection methods. The authors in [11] considered the impact of the positions and transmit power of the interference sources (external sources) on the SOP in the limited interference environment.

However, the authors in [10], [11] assumed that transceiver hardware of wireless devices is perfect. In practice, the transceiver hardware is imperfect due to phase noises, amplifier-amplitude non-linearity and in phase and quadrature imbalance (IQI) [12], [13], which degrades performances of wireless relay networks. The authors in [14] studied the effects of the IQI on the secrecy capacity of the wiretap channel. Results in [14] presented that the IQI should be taken into account in the design of secured communication systems.

To the best of our knowledge, only the published work [14] evaluating the secrecy performances in the presence of the hardware imperfection. However, the authors in [14] only considered the effects of the IQI in one-hop orthogonal frequency-division multiple access (OFDMA) communication systems. Unlike [14], this paper investigates the impact of hardware impairments on the probability of non-zero se-

crecy capacity (PoNSC) of a multi-hop transmission scheme, where the data transmitted from a source, via multiple relays, to a destination is overheard by an eavesdropper. In the proposed scheme, the transceiver hardware of the source, relays, destination and eavesdropper is not perfect. Furthermore, the randomize-and-forward (RF) strategy is used by the source and relays so that the eavesdropper cannot combine the received data [15]. For performance evaluation, we derive exact expressions of the PoNSC over Nakagami-m fading channels, which are expressed by sums of infinite series of exponential functions and exponential integral functions. In order to provide insights into the system performance, asymptotic closed-form expressions of the PoNSC at high transmit signal-to-noise ratio (SNR) are also provided. Finally, Monte Carlo simulations are performed to verify the theoretical derivations.

The rest of this paper is organized as follows. The system model of the proposed protocol is described in Sec. 2. In Sec. 3, we evaluate the performance of the considered protocol. The simulation results are shown in Sec. 4. Finally, this paper is concluded in Sec. 5.

2. System Model

In Fig. 1, we present the system model of the proposed protocol, where the source T_0 attempts to transmit its data to the destination T_N via $N-1$ relay nodes, i.e., $\mathrm{T}_1, \mathrm{T}_2, ..., \mathrm{T}_{N-1}$. In this network, there is an eavesdropper E overhearing the data transmitted by the source and relays. We assume that all of the nodes are equipped with a single antenna; therefore, the data transmission is realized by time division multiple access (TDMA). Moreover, the transmitting nodes such as source and relays employ the randomize-and-forward (RF) technique to confuse the eavesdropper. In particular, the source and relays encode the data by randomly generating code-books to avoid the eavesdropper E from combining the received data [15]. We also assume that the eavesdropper E is passive and hence the channel state information (CSI) of the eavesdropping links are not available at the authorized nodes. However, the statistics such as path-loss exponent, link distances between nodes, distributions of the wireless channels are assumed to be available.

Let us denote h_n and g_n as channel gains of the $\mathrm{T}_{n-1} \to \mathrm{T}_n$ and $\mathrm{T}_{n-1} \to \mathrm{E}$ links, respectively, where $n = 1, 2, ..., N$. It is assumed that all of the fading channels between two arbitrary terminals are Nakagami-m [16]. The Nakagami-m fading channel is a generalized model which is widely used to describe different fading environments.

Considering the communication at the nth hop between the nodes T_{n-1} and T_n, the instantaneous SNR received at T_n can be given as in [12, eq. (17)]:

$$\Psi_{\mathrm{D}n} = \frac{P h_n}{\left(\kappa_{t,\mathrm{D}n}^2 + \kappa_{r,\mathrm{D}n}^2\right) P h_n + N_0} = \frac{\psi h_n}{\kappa_{\Sigma,\mathrm{D}n}^2 \psi h_n + 1} = \frac{\chi_n}{\kappa_{\mathrm{D}n}\chi_n + 1}. \quad (1)$$

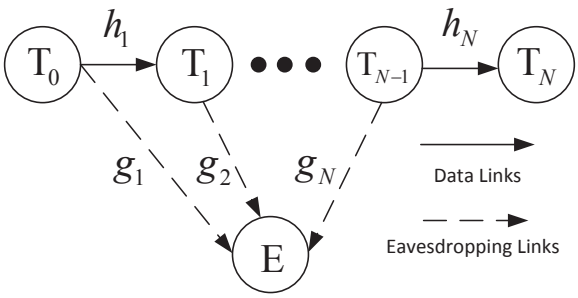

Fig. 1. System model of the proposed protocol.

In (1), P is the transmit power of the node T_{n-1}. It is assumed that all of the transmitters including the source and relays have the same transmit power. The terms N_0 in (1) is variance of zero-mean Gaussian noises at the node T_n. Next, the constants $\kappa_{t,\mathrm{D}n}$ and $\kappa_{r,\mathrm{D}n}$ are the hardware impairment levels at the transmitter T_{n-1} and the receiver T_n, respectively; and $\sqrt{\kappa_{\mathrm{D}n}} = \kappa_{\Sigma,\mathrm{D}n} = \sqrt{\kappa_{t,\mathrm{D}n}^2 + \kappa_{r,\mathrm{D}n}^2}$ is the aggregate level of impairments on the $\mathrm{T}_{n-1} \to \mathrm{T}_n$ link [12]. Finally, the remaining notations in (1) are denoted as follows: $\psi = P/N_0$ and $\chi_n = \psi h_n$.

Similarly, the SNR received at the eavesdropper E from the transmission of the node T_{n-1} is expressed by

$$\Psi_{\mathrm{E}n} = \frac{P g_n}{\left(\kappa_{t,\mathrm{D}n}^2 + \kappa_{r,\mathrm{E}}^2\right) P g_n + N_0} = \frac{\varphi_n}{\kappa_{\mathrm{E}n}\varphi_n + 1} \quad (2)$$

where $\kappa_{r,\mathrm{E}}$ is the level of the hardware impairments at the eavesdropper E; $\kappa_{\mathrm{E}n} = \kappa_{t,\mathrm{D}n}^2 + \kappa_{r,\mathrm{E}}^2$; and $\varphi_n = \psi g_n$.

Because h_n and g_n are channel gains of Nakagami-m fading channels, their probability density functions (PDFs) can be given respectively as (see [17, eq. (7)])

$$f_{h_n}(x) = \frac{1}{\Gamma(m_{\mathrm{D}n})}(m_{\mathrm{D}n}\sigma_n)^{m_{\mathrm{D}n}} x^{m_{\mathrm{D}n}-1} \exp\left(-m_{\mathrm{D}n}\sigma_n x\right),$$
$$f_{g_n}(x) = \frac{1}{\Gamma(m_{\mathrm{E}n})}(m_{\mathrm{E}n}\tau_n)^{m_{\mathrm{E}n}} x^{m_{\mathrm{E}n}-1} \exp\left(-m_{\mathrm{E}n}\tau_n x\right) \quad (3)$$

where $m_{\mathrm{D}n}$ and $m_{\mathrm{E}n}$ are Nakagami-m parameters of the $\mathrm{T}_{n-1} \to \mathrm{T}_n$ and $\mathrm{T}_{n-1} \to \mathrm{E}$ links, respectively; $\sigma_n = 1/\mathcal{E}\{h_n\}$ and $\tau_n = 1/\mathcal{E}\{g_n\}$ ($\mathcal{E}(X)$ is expected value of RV X ($X \in \{h_n, g_n\}$)); and $\Gamma(.)$ is Gamma function [18].

Moreover, since $\chi_n = \psi h_n$ and $\varphi_n = \psi g_n$, χ_n and φ_n are also Nakagami-m random variables (RVs). When $m_{\mathrm{D}n}$ and $m_{\mathrm{E}n}$ are integers, the PDFs of the RVs χ_n and φ_n can be obtained as (see [19, eq. (4)])

$$f_{\chi_n}(x) = \left(\frac{m_{\mathrm{D}n}\sigma_n}{\psi}\right)^{m_{\mathrm{D}n}} \frac{x^{m_{\mathrm{D}n}-1}}{(m_{\mathrm{D}n}-1)!} \exp\left(-\frac{m_{\mathrm{D}n}\sigma_n}{\psi}x\right) = \frac{\lambda_n^{m_{\mathrm{D}n}} x^{m_{\mathrm{D}n}-1}}{(m_{\mathrm{D}n}-1)!} \exp\left(-\lambda_n x\right),$$
$$f_{\varphi_n}(x) = \left(\frac{m_{\mathrm{E}n}\tau_n}{\psi}\right)^{m_{\mathrm{E}n}} \frac{x^{m_{\mathrm{E}n}-1}}{(m_{\mathrm{E}n}-1)!} \exp\left(-\frac{m_{\mathrm{E}n}\tau_n}{\psi}x\right) = \frac{\Omega_n^{m_{\mathrm{E}n}} x^{m_{\mathrm{E}n}-1}}{(m_{\mathrm{E}n}-1)!} \exp\left(-\Omega_n x\right) \quad (4)$$

where $\lambda_n = m_{\mathrm{D}n}\sigma_n/\psi$ and $\Omega_n = m_{\mathrm{E}n}\tau_n/\psi$.

To take path-loss into account, we can model σ_n and τ_n, similarly to [20], as

$$\sigma_n = d_{\mathrm{D}n}^{\beta},\ \tau_n = d_{\mathrm{E}n}^{\beta} \tag{5}$$

where $d_{\mathrm{D}n}$ and $d_{\mathrm{E}n}$ are distances of the $\mathrm{T}_{n-1} \to \mathrm{T}_n$ and $\mathrm{T}_{n-1} \to \mathrm{E}$ links, respectively; and β is path-loss exponent which varies from 2 to 6.

From (4), the corresponding cumulative distribution function (CDF) of the RVs χ_n and φ_n are respectively given by

$$\begin{aligned} F_{\chi_n}(x) &= 1 - \exp(-\lambda_n x) \sum_{t=0}^{m_{\mathrm{D}n}-1} \frac{(\lambda_n x)^t}{t!}, \\ F_{\varphi_n}(x) &= 1 - \exp(-\Omega_n x) \sum_{t=0}^{m_{\mathrm{E}n}-1} \frac{(\Omega_n x)^t}{t!}. \end{aligned} \tag{6}$$

Now, let us consider the secrecy capacity at the nth hop, which can be formulated similarly as in [10]:

$$\begin{aligned} C_n^{\mathrm{Sec}} &= \max\left(0, \frac{1}{N}\log_2(1+\Psi_{\mathrm{D}n}) - \frac{1}{N}\log_2(1+\Psi_{\mathrm{E}n})\right) \\ &= \max\left(0, \frac{1}{N}\log_2\left(\frac{1+\Psi_{\mathrm{D}n}}{1+\Psi_{\mathrm{E}n}}\right)\right) \end{aligned} \tag{7}$$

where the factor $1/N$ indicates that the data transmission is split into N orthogonal time slots.

Because the RF strategy is used by the source and relays, the end-to-end secrecy capacity of the N-hop relaying network can be obtained as

$$C_{\mathrm{e2e}}^{\mathrm{Sec}} = \min_{n=1,2,\ldots,N}\left(C_n^{\mathrm{Sec}}\right). \tag{8}$$

Equation (8) implies that the end-to-end secrecy capacity is dominated by the secrecy capacity of the weakest hop [15].

3. Performance Analysis

In this paper, the secrecy performance of the proposed protocol is evaluated, in terms of the PoNSC [15]. From (1), (2), (7) and (8), the PoNSC can be formulated as

$$\begin{aligned} \mathrm{P}_{\mathrm{NSC}} &= \Pr\left(C_{\mathrm{e2e}}^{\mathrm{Sec}} > 0\right) = \prod_{n=1}^{N} \Pr\left(C_n^{\mathrm{Sec}} > 0\right) \\ &= \prod_{n=1}^{N} \Pr(\Psi_{\mathrm{D}n} > \Psi_{\mathrm{E}n}) \\ &= \prod_{n=1}^{N} \underbrace{\Pr\left(\frac{\chi_n}{\kappa_{\mathrm{D}n}\chi_n + 1} > \frac{\varphi_n}{\kappa_{\mathrm{E}n}\varphi_n + 1}\right)}_{\mathrm{P}_n}. \end{aligned} \tag{9}$$

Moreover, the probability P_n can be rewritten as follows:

$$\mathrm{P}_n = \begin{cases} \Pr(\chi_n > \varphi_n); & \text{if } \kappa_{\mathrm{D}n} = \kappa_{\mathrm{E}n} \\ \Pr\left(\varphi_n < \frac{\chi_n}{1+\Delta_1\chi_n}\right); & \text{if } \kappa_{\mathrm{D}n} > \kappa_{\mathrm{E}n} \\ \Pr\left(\chi_n > \frac{\varphi_n}{1+\Delta_2\varphi_n}\right); & \text{if } \kappa_{\mathrm{D}n} < \kappa_{\mathrm{E}n} \end{cases} \tag{10}$$

where $\Delta_1 = \kappa_{\mathrm{D}n} - \kappa_{\mathrm{E}n}$ and $\Delta_2 = \kappa_{\mathrm{E}n} - \kappa_{\mathrm{D}n}$.

As presented in (10), depending on values of $\kappa_{\mathrm{D}n}$ and $\kappa_{\mathrm{E}n}$, we consider three cases as follows:

Case 1: $\kappa_{\mathrm{D}n} = \kappa_{\mathrm{E}n}$

In this case, the authorized node T_n and the eavesdropper E are assumed to have the same hardware structure (e.g., both are mobile users), hence their hardware impairment levels are same (see [13]). Then, from (10), the PoNSC at the nth hop is formulated by

$$\mathrm{P}_n = \int_0^{+\infty} \left(1 - F_{\chi_n}(x)\right) f_{\varphi_n}(x)\,\mathrm{d}x. \tag{11}$$

Substituting the results given in (4) and (6) into (11); and using [18, eq. (3.351.3)] for the corresponding integrals, we can obtain

$$\mathrm{P}_n = \sum_{t=0}^{m_{\mathrm{D}n}-1} \frac{(t+m_{\mathrm{E}n}-1)!}{t!\,(m_{\mathrm{E}n}-1)!} \frac{\lambda_n^t \Omega_n^{m_{\mathrm{E}n}}}{(\lambda_n+\Omega_n)^{t+m_{\mathrm{E}n}}}. \tag{12}$$

It can be observed from (12) that the PoNSC P_n does not depend on the transmit SNR $\psi(P/N_0)$ as well as the hardware impairment levels.

Case 2: $\kappa_{\mathrm{D}n} > \kappa_{\mathrm{E}n}$

In this case, the eavesdropper is equipped with a better transceiver, as compared with that of the nodes $\mathrm{T_n}$, e.g., the node E is a base station while $\mathrm{T_n}$ is a mobile user. Then, the PoNSC in (10) can be formulated by

$$\mathrm{P}_n = \int_0^{+\infty} F_{\varphi_n}\left(\frac{x}{1+\Delta_1 x}\right) f_{\chi_n}(x)\,\mathrm{d}x. \tag{13}$$

Combining (4), (6) and (13), after some manipulations, it can be obtained that

$$\begin{aligned} \mathrm{P}_n = 1 - &\sum_{t=0}^{m_{\mathrm{E}n}-1} \frac{\Omega_n^t}{t!} \frac{\lambda_n^{m_{\mathrm{D}n}}}{(m_{\mathrm{D}n}-1)!} \\ &\times \int_0^{+\infty} \frac{x^{t+m_{\mathrm{D}n}-1}}{(1+\Delta_1 x)^t} \exp\left(-\frac{\Omega_n x}{1+\Delta_1 x} - \lambda_n x\right). \end{aligned} \tag{14}$$

Next, by changing variable $y = 1 + \Delta_1 x$, we can rewrite (14) under the following form:

$$\begin{aligned} \mathrm{P}_n = 1 - &\sum_{t=0}^{m_{\mathrm{E}n}-1} \frac{\Omega_n^t}{t!} \frac{\lambda_n^{m_{\mathrm{D}n}}}{(m_{\mathrm{D}n}-1)!} \frac{1}{\Delta_1^{t+m_{\mathrm{D}n}}} \exp\left(\frac{\lambda_n - \Omega_n}{\Delta_1}\right) \\ &\times \int_1^{+\infty} \frac{(y-1)^{t+m_{\mathrm{D}n}-1}}{y^t} \exp\left(\frac{\Omega_n}{\Delta_1 y}\right) \exp\left(-\frac{\lambda_n}{\Delta_1} y\right) \mathrm{d}y. \end{aligned} \tag{15}$$

Next, applying binomial expansion for $(y-1)^{t+m_{\mathrm{D}n}-1}$; and substituting this result into (15), we arrive at

$$\mathrm{P}_n = 1 - \sum_{t=0}^{m_{\mathrm{E}n}-1} \frac{\Omega_n^t}{t!} \frac{\lambda_n^{m_{\mathrm{D}n}}}{(m_{\mathrm{D}n}-1)!} \frac{1}{\Delta_1^{t+m_{\mathrm{D}n}}} \exp\left(\frac{\lambda_n - \Omega_n}{\Delta_1}\right) \times \sum_{v=0}^{t+m_{\mathrm{D}n}-1} (-1)^v C_{t+m_{\mathrm{D}n}-1}^v \times \int_1^{+\infty} y^{m_{\mathrm{D}n}-v-1} \exp\left(\frac{\Omega_n}{\Delta_1 y}\right) \exp\left(-\frac{\lambda_n}{\Delta_1} y\right) \mathrm{d}y. \quad (16)$$

Remark 1: It can be observed that the PoNSC P_n is expressed by sum of integrals because it is impossible to find a closed-form expression for the integrals given in (16). However, it is too difficult to use integral-form expressions to design and optimize the system, which motivates us to express P_n by a more useful form: infinite series of closed-form expressions (see [21]).

At first, the exponential function $\exp(\Omega_n/\Delta_1/y)$ in (16) can be expressed by an infinite series as

$$\exp\left(\frac{\Omega_n}{\Delta_1 y}\right) = \sum_{w=0}^{+\infty} \frac{1}{w!} \left(\frac{\Omega_n}{\Delta_1 y}\right)^w. \quad (17)$$

Substituting (17) into (16), which yields

$$\mathrm{P}_n = 1 - \sum_{t=0}^{m_{\mathrm{E}n}-1} \frac{\Omega_n^t}{t!} \frac{\lambda_n^{m_{\mathrm{D}n}}}{(m_{\mathrm{D}n}-1)!} \frac{1}{\Delta_1^{t+m_{\mathrm{D}n}}} \exp\left(\frac{\lambda_n - \Omega_n}{\Delta_1}\right) \times \sum_{v=0}^{t+m_{\mathrm{D}n}-1} \sum_{w=0}^{+\infty} \frac{(-1)^v}{w!} C_{t+m_{\mathrm{D}n}-1}^v \left(\frac{\Omega_n}{\Delta_1}\right)^w \times \underbrace{\int_1^{+\infty} y^{m_{\mathrm{D}n}-v-w-1} \exp\left(-\frac{\lambda_n}{\Delta_1} y\right) \mathrm{d}y}_{I_1}. \quad (18)$$

In order to calculate the integral I_1 in (18), we have to consider three cases as follows:

- $m_{\mathrm{D}n} - w - v - 1 = 0$ or $w = m_{\mathrm{D}n} - v - 1$

  In this case, it is obvious that

$$I_1 = \frac{\Delta_1}{\lambda_n} \exp\left(-\frac{\lambda_n}{\Delta_1}\right). \quad (19)$$

- $m_{\mathrm{D}n} - w - v - 1 > 0$ or $w < m_{\mathrm{D}n} - v - 1$

  At first, using [18, 2.321.2], we obtain a following result:

$$\int_1^{+\infty} x^r \exp(-ax)\,\mathrm{d}x = \exp(-a) \sum_{k=0}^{r} k! C_r^k / a^{k+1} \quad (20)$$

where r is a positive integer, a is positive constant and $C_r^k = r!/k!/(r-k)!$. From (20), the integral I_1 in this case can be calculated by

$$I_1 = \exp\left(-\frac{\lambda_n}{\Delta_1}\right) \sum_{k=0}^{m_{\mathrm{D}n}-w-v-1} k! C_{m_{\mathrm{D}n}-w-v-1}^k \left(\frac{\Delta_1}{\lambda_n}\right)^{k+1}. \quad (21)$$

- $m_{\mathrm{D}n} - w - v - 1 < 0$ or $w > m_{\mathrm{D}n} - v - 1$

  In this case, by employing [18, 3.351.4], we have

$$\int_1^{+\infty} \frac{\exp(-ax)}{x^r} \mathrm{d}x = \exp(-a) \sum_{k=0}^{r-2} \frac{(-1)^k a^k}{\prod_{l=0}^{k} (r-1-l)} + \frac{(-1)^{r-1} a^{r-1}}{(r-1)!} E_1(a) \quad (22)$$

where r is a positive integer, a is positive constant and $E_1(.)$ is exponential integral function [18]. Therefore, we can calculate I_1 by

$$I_1 = \int_1^{+\infty} \frac{1}{y^{v+w+1-m_{\mathrm{D}n}}} \exp\left(-\frac{\lambda_n}{\Delta_1} y\right) \mathrm{d}y = \exp\left(-\frac{\lambda_n}{\Delta_1}\right) \sum_{k=0}^{w+v-m_{\mathrm{D}n}-1} \frac{(-1)^k (\lambda_n/\Delta_1)^k}{\prod_{l=0}^{k} (w+v-m_{\mathrm{D}n}-l)} + \frac{(-1)^{w+v-m_{\mathrm{D}n}} (\lambda_n/\Delta_1)^{w+v-m_{\mathrm{D}n}}}{(w+v-m_{\mathrm{D}n})!} E_1\left(\frac{\lambda_n}{\Delta_1}\right). \quad (23)$$

From (18), (19), (21) and (23), an exact expression of the PoNSC P_n can be given as in (24).

However, equation (24) is still complex which does not provide any insights into system performance, which motivates us to find simpler expressions for P_n.

At first, when the transmit SNR ψ is high, we can approximate P_n in (10) by

$$\mathrm{P}_n \overset{\psi\to+\infty}{\approx} \Pr\left(\varphi_n < \frac{1}{\Delta_1}\right) = F_{\varphi_n}\left(\frac{1}{\Delta_1}\right) \overset{\psi\to+\infty}{\approx} 1 - \exp\left(-\frac{\Omega_n}{\Delta_1}\right) \sum_{t=0}^{m_{\mathrm{E}n}-1} \frac{1}{t!} \left(\frac{\Omega_n}{\Delta_1}\right)^t. \quad (25)$$

Moreover, (25) can be approximated by a simpler expression as follows:

$$\mathrm{P}_n \overset{\psi\to+\infty}{\approx} F_{\varphi_n}\left(\frac{1}{\Delta_1}\right) \overset{\psi\to+\infty}{\approx} \frac{1}{m_{\mathrm{E}n}!} \left(\frac{\Omega_n}{\Delta_1}\right)^{m_{\mathrm{E}n}}. \quad (26)$$

Substituting the results obtained by (25) and (26) into (9), the PoNSC can be approximated by the following closed-form formulas:

$$\mathrm{P}_{\mathrm{NSC}} \overset{\psi\to+\infty}{\approx} \prod_{n=1}^{N} \left[1 - \exp\left(-\frac{\Omega_n}{\Delta_1}\right) \sum_{t=0}^{m_{\mathrm{E}n}-1} \frac{1}{t!} \left(\frac{\Omega_n}{\Delta_1}\right)^t\right], \quad (27)$$

$$\mathrm{P}_{\mathrm{NSC}} \overset{\psi\to+\infty}{\approx} \prod_{n=1}^{N} \frac{1}{m_{\mathrm{E}n}!} \left(\frac{\Omega_n}{\Delta_1}\right)^{m_{\mathrm{E}n}}. \quad (28)$$

$$\mathrm{P}_n = 1 - \sum_{t=0}^{m_{\mathrm{E}n}-1} \frac{\Omega_n^t}{t!} \frac{\lambda_n^{m_{\mathrm{D}n}}}{(m_{\mathrm{D}n}-1)!} \frac{1}{\Delta_1^{t+m_{\mathrm{D}n}}} \exp\left(\frac{\lambda_n - \Omega_n}{\Delta_1}\right) \times \sum_{v=0}^{t+m_{\mathrm{D}n}-1} \left[\begin{array}{l} \frac{(-1)^v}{(m_{\mathrm{D}n}-v-1)!} C_{t+m_{\mathrm{D}n}-1}^v \left(\frac{\Omega_n}{\Delta_1}\right)^{m_{\mathrm{D}n}-v-1} \frac{\Delta_1}{\lambda_n} \exp\left(-\frac{\lambda_n}{\Delta_1}\right) \\ + \sum_{w=0}^{m_{\mathrm{D}n}-v-2} \frac{(-1)^v}{w!} C_{t+m_{\mathrm{D}n}-1}^v \left(\frac{\Omega_n}{\Delta_1}\right)^w \exp\left(-\frac{\lambda_n}{\Delta_1}\right)^{m_{\mathrm{D}n}-w-v-1} \sum_{k=0} k! C_{m_{\mathrm{D}n}-w-v-1}^k \left(\frac{\Delta_1}{\lambda_n}\right)^{k+1} \\ + \sum_{w=m_{\mathrm{D}n}-v}^{+\infty} \frac{(-1)^v}{w!} C_{t+m_{\mathrm{D}n}-1}^v \left(\frac{\Omega_n}{\Delta_1}\right)^w \\ \times \left(\exp\left(-\frac{\lambda_n}{\Delta_1}\right)^{w+v-m_{\mathrm{D}n}-1} \sum_{k=0}^{k} \frac{(-1)^k (\lambda_n/\Delta_1)^k}{\prod_{l=0}^{k} (w+v-m_{\mathrm{D}n}-l)} + \frac{(-1)^{w+v-m_{\mathrm{D}n}} (\lambda_n/\Delta_1)^{w+v-m_{\mathrm{D}n}}}{(w+v-m_{\mathrm{D}n})!} E_1\left(\frac{\lambda_n}{\Delta_1}\right) \right) \end{array} \right]. \quad (24)$$

Remark 2: From (25), it is obvious that the PoSNC P_n at high transmit SNR ψ depends on ψ and $m_{\mathrm{E}n}$. In particular, P_n decreases when the value of ψ increases, which means that as $\kappa_{\mathrm{D}n} > \kappa_{\mathrm{E}n}$, the secrecy performance is worse with increasing of the transmit power. Moreover, the performance also degrades with higher value of the Nakagami-m parameter of the eavesdropping link ($m_{\mathrm{E}n}$). Indeed, as shown in (26) and (28), the P_n and $\mathrm{P}_{\mathrm{NSC}}$ decrease with the slope of $m_{\mathrm{E}n}$ and $\sum_{n=1}^{N} m_{\mathrm{E}n}$, respectively.

Case 3: $\kappa_{\mathrm{D}n} < \kappa_{\mathrm{E}n}$

In this case, the hardware transceiver of the nodes $\mathrm{T_n}$ is better that of the eavesdropper, e.g., $\mathrm{T_n}$ can be a base station while E is only a mobile user. Similarly, we can rewrite P_n in (10) under the following form:

$$\begin{aligned} \mathrm{P}_n &= \int_0^{+\infty} \left(1 - F_{\chi_n}\left(\frac{x}{1+\Delta_2 x}\right)\right) f_{\varphi_n}(x)\,\mathrm{d}x \\ &= \sum_{t=0}^{m_{\mathrm{D}n}-1} \frac{\lambda_n^t}{t!} \frac{\Omega_n^{m_{\mathrm{E}n}}}{(m_{\mathrm{E}n}-1)!} \frac{1}{\Delta_2^{t+m_{\mathrm{E}n}}} \exp\left(\frac{\Omega_n - \lambda_n}{\Delta_2}\right) \\ &\times \sum_{v=0}^{t+m_{\mathrm{E}n}-1} \sum_{w=0}^{+\infty} \frac{(-1)^v}{w!} C_{t+m_{\mathrm{E}n}-1}^v \left(\frac{\lambda_n}{\Delta_2}\right)^w \\ &\times \underbrace{\int_1^{+\infty} y^{m_{\mathrm{E}n}-v-w-1} \exp\left(-\frac{\Omega_i}{\Delta_2} y\right) \mathrm{d}y}_{I_2}. \end{aligned} \quad (29)$$

Similarly, when $w = m_{\mathrm{E}n} - v - 1$, $w < m_{\mathrm{E}n} - v - 1$ and $w > m_{\mathrm{E}n} - v - 1$, the integral I_2 in (29) can be calculated respectively by

$$\begin{aligned} I_2 &= \frac{\Delta_2}{\Omega_n} \exp\left(-\frac{\Omega_n}{\Delta_2}\right), \\ I_2 &= \exp\left(-\frac{\Omega_n}{\Delta_2}\right) \sum_{k=0}^{m_{\mathrm{E}n}-w-v-1} k! C_{m_{\mathrm{E}n}-w-v-1}^k \left(\frac{\Delta_2}{\Omega_n}\right)^{k+1}, \\ I_2 &= \exp\left(-\frac{\Omega_n}{\Delta_2}\right) \sum_{k=0}^{w+v-m_{\mathrm{E}n}-1} \frac{(-1)^k (\Omega_n/\Delta_2)^k}{\prod_{l=0}^{k} (w+v-m_{\mathrm{E}n}-l)} \\ &+ \frac{(-1)^{w+v-m_{\mathrm{E}n}} (\Omega_n/\Delta_2)^{w+v-m_{\mathrm{E}n}}}{(w+v-m_{\mathrm{E}n})!} E_1\left(\frac{\Omega_n}{\Delta_2}\right). \end{aligned} \quad (30)$$

From the results obtained above, an exact expression of P_n can be given by (31).

Also, considering the value of P_n at high ψ regions, we obtain the following result:

$$\begin{aligned} \mathrm{P}_n &\overset{\psi\to+\infty}{\approx} \Pr\left(\gamma_n > \frac{1}{\Delta_2}\right) \\ &\overset{\psi\to+\infty}{\approx} \sum_{t=0}^{m_{\mathrm{D}n}-1} \frac{1}{t!} \left(\frac{\lambda_n}{\Delta_2}\right)^t \exp\left(-\frac{\lambda_n}{\Delta_2}\right). \end{aligned} \quad (32)$$

From (9) and (32), the approximate closed-form expression of the PoNSC at high transmit SNR can be expressed as follows:

$$\mathrm{P}_{\mathrm{NSC}} \overset{\psi\to+\infty}{\approx} \prod_{n=1}^{N} \left[\sum_{t=0}^{m_{\mathrm{D}n}-1} \frac{1}{t!} \left(\frac{\lambda_n}{\Delta_2}\right)^t \exp\left(-\frac{\lambda_n}{\Delta_2}\right) \right]. \quad (33)$$

Remark 3: We can observe from (32) and (33) that as $\kappa_{\mathrm{D}n} < \kappa_{\mathrm{E}n}$, the value of PoNSC at the nth hop increases when the transmit power increases. Furthermore, the PoNSC performance is also better with high value of the Nakagami-m parameter of the data link.

4. Simulation Results

In this section, we perform Monte-Carlo simulations to verify the theoretical derivations provided in Section 3. For each Monte-Carlo simulation, we performed 10^6 trials in which the channel coefficients between two nodes X and Y are randomly generated, where $\mathrm{X}, \mathrm{Y} \in \{\mathrm{T}_0, \mathrm{T}_1, ..., \mathrm{T}_N, \mathrm{E}\}$. Then, the simulated PNSC is computed by the number of trials that the end-to-end secrecy capacity is higher than zero divided by the number of trials (10^6). In the simulation environment, the source is placed at the position (0, 0), the destination is located at (1, 0), the position of the relay node $\mathrm{T_n}$ is $(n/N, 0)$, where $n = 1, 2, ..., N-1$, and the position of the eavesdropper is $(x_{\mathrm{E}}, y_{\mathrm{E}})$, where $0 \le x_{\mathrm{E}}, y_{\mathrm{E}} \le 1$. In all of the simulations, the path-loss exponent β is fixed by 3. In order to present the impact of the hardware imperfection on the secrecy performance clearly, we can assume that the

$$\mathrm{P}_n = \sum_{t=0}^{m_{\mathrm{D}n}-1} \frac{\lambda_n^t}{t!} \frac{\Omega_n^{m_{\mathrm{E}n}}}{(m_{\mathrm{E}n}-1)!} \frac{1}{\Delta_2^{t+m_{\mathrm{E}n}}} \exp\left(\frac{\Omega_n - \lambda_n}{\Delta_2}\right) \times \sum_{v=0}^{t+m_{\mathrm{E}n}-1} \left[\begin{array}{l} \frac{(-1)^v}{(m_{\mathrm{E}n}-v-1)!} C_{t+m_{\mathrm{E}n}-1}^{v} \left(\frac{\lambda_n}{\Delta_2}\right)^{m_{\mathrm{E}n}-v-1} \frac{\Delta_2}{\Omega_n} \exp\left(-\frac{\Omega_n}{\Delta_2}\right) \\ + \sum_{w=0}^{m_{\mathrm{E}n}-v-2} \frac{(-1)^v}{w!} C_{t+m_{\mathrm{E}n}-1}^{v} \left(\frac{\lambda_n}{\Delta_2}\right)^{w} \exp\left(-\frac{\Omega_n}{\Delta_2}\right) \sum_{k=0}^{m_{\mathrm{E}n}-w-v-1} k! C_{m_{\mathrm{E}n}-w-v-1}^{k} \left(\frac{\Delta_2}{\Omega_n}\right)^{k+1} \\ + \sum_{w=m_{\mathrm{E}n}-v}^{+\infty} \frac{(-1)^v}{w!} C_{t+m_{\mathrm{E}n}-1}^{v} \left(\frac{\lambda_n}{\Delta_2}\right)^{w} \\ \times \left(\exp\left(-\frac{\Omega_n}{\Delta_2}\right) \sum_{k=0}^{w+v-m_{\mathrm{E}n}-1} \frac{(-1)^k (\Omega_n/\Delta_2)^k}{\prod_{l=0}^{k} (w+v-m_{\mathrm{E}n}-l)} + \frac{(-1)^{w+v-m_{\mathrm{E}n}} (\Omega_n/\Delta_2)^{w+v-m_{\mathrm{E}n}}}{(w+v-m_{\mathrm{E}n})!} E_1\left(\frac{\Omega_n}{\Delta_2}\right) \right) \end{array} \right]. \quad (31)$$

hardware impairment levels on the data links (the eavesdropping links) are same, i.e., $\kappa_{\mathrm{D}n} = \kappa_{\mathrm{D}}$ ($\kappa_{\mathrm{E}n} = \kappa_{\mathrm{E}}$) for all n. Also, it is also assumed that $m_{\mathrm{D}n} = m_{\mathrm{D}}$ and $m_{\mathrm{E}n} = m_{\mathrm{E}}$ for all n. Moreover, for the theoretical results, we truncate infinite series at first 100 terms.

In Fig. 2, we present the PoNSC as a function of the transmit SNR $\psi(P/N_0)$ in dB. In this simulation, the number of hops (N) is fixed by 4, the Nakagami-m parameters $\mathrm{m_D}$ is set by 2, the hardware impairment levels κ_{D} and κ_{E} equals to 0.2 and 0.1, respectively, the eavesdropper is located at the position (0.5, 0.5). We can see that the secrecy performance significantly degrades with the increasing of the transmit SNR. Moreover, the PoNSC of the proposed protocol is also worse when the channels of the eavesdropping links are better (m_{E} is higher). Finally, it is worth noting that the simulation results (denoted by Sim) match very well with the theoretical ones (denoted by Exact), which validates our derivations.

In Fig. 3, we verify the approximate closed-form expressions given in (27) and (28) by presenting the theoretical results of PoNSC at high transmit SNR. The parameters used for this simulation are $N = 5$, $m_{\mathrm{D}} = 2$, $\kappa_{\mathrm{D}} = 0.2$, $\kappa_{\mathrm{E}} = 0$, $x_{\mathrm{E}} = 0.3$ and $y_{\mathrm{E}} = 0.4$. It can be seen that the asymptotic values (denoted by Appro) in (27) rapidly converges to the exact ones at low and medium ψ region, while that of (28) reaches to the exact ones at medium and high ψ regime. Moreover, we can also observe from this figure that the slope of the curves equals to the number of Nm_{E}, which verifies the result obtained in (28).

Figure 4 presents the PoNSC as a function of the transmit SNR ψ in dB when the hardware transceiver of the authorized nodes is better than that of the eavesdropper, i.e., $\kappa_{\mathrm{D}} < \kappa_{\mathrm{E}}$. In this figure, we set the value of the parameters by $N = 3$, $m_{\mathrm{E}} = 3$, $\kappa_{\mathrm{D}} = 0.05$, $\kappa_{\mathrm{E}} = 0.1$ and $x_{\mathrm{E}} = y_{\mathrm{E}} = 0.3$. As illustrated in Fig. 4, the PoNSC increases when the transmit SNR ψ increases. In addition, the performance is also better when the Nakagami-m parameter of the data link is higher. Again, the simulation and theoretical results are in good agreement, while the asymptotic PoNSC converges to the exact PoNSC at medium and high ψ regimes.

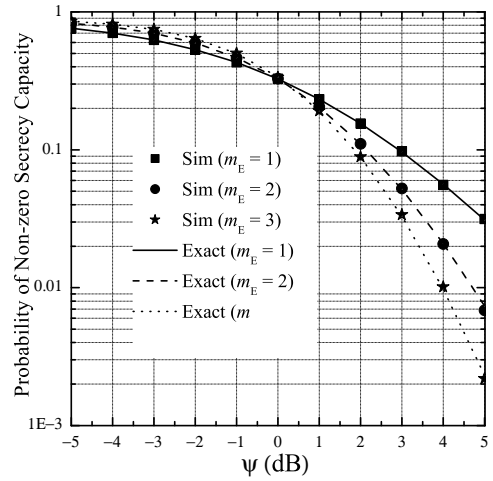

Fig. 2. Probability of non-zero secrecy capacity as a function of the transmit SNR ψ in dB with different values of m_{E}, when $N = 4$, $m_{\mathrm{D}} = 2$, $\kappa_{\mathrm{D}} = 0.2$, $\kappa_{\mathrm{E}} = 0.1$ and $x_{\mathrm{E}} = y_{\mathrm{E}} = 0.5$.

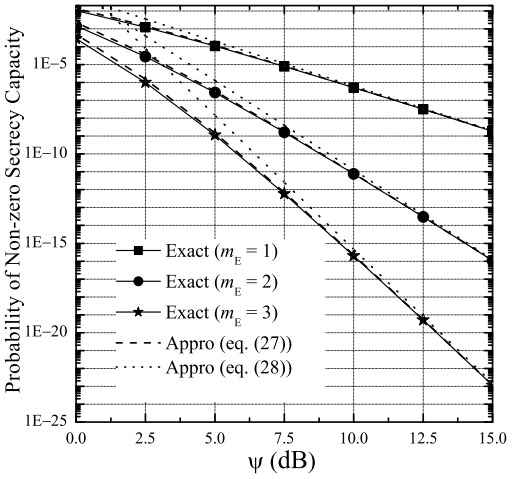

Fig. 3. Probability of non-zero secrecy capacity as a function of the transmit SNR ψ in dB with different values of m_{E}, when $N = 5$, $m_{\mathrm{D}} = 2$, $\kappa_{\mathrm{D}} = 0.2$, $\kappa_{\mathrm{E}} = 0$, $x_{\mathrm{E}} = 0.3$ and $y_{\mathrm{E}} = 0.4$.

In Fig. 5, we investigate the impact of the number of hops on the secrecy performance of the proposed protocol when $\psi = 0$dB, $m_{\mathrm{D}} = 1$, $m_{\mathrm{E}} = 2$, $\kappa_{\mathrm{D}} = 0.05$, $\kappa_{\mathrm{E}} = 0.1$ and $x_{\mathrm{E}} = y_{\mathrm{E}} = 0.5$. An interesting result presented in this figure

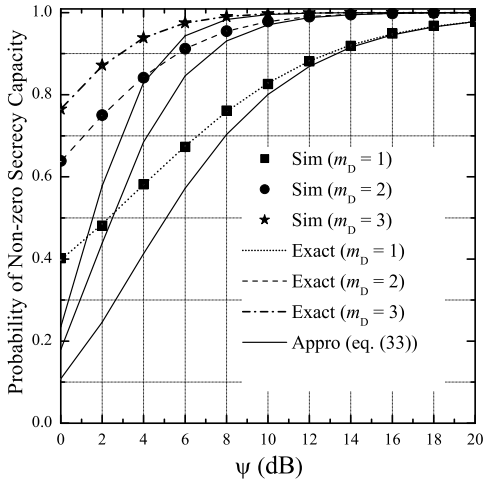

Fig. 4. Probability of non-zero secrecy capacity as a function of the transmit SNR ψ in dB with different values of m_D, when $N = 3$, $m_E = 3$, $\kappa_D = 0.05$, $\kappa_E = 0.1$ and $x_E = y_E = 0.3$.

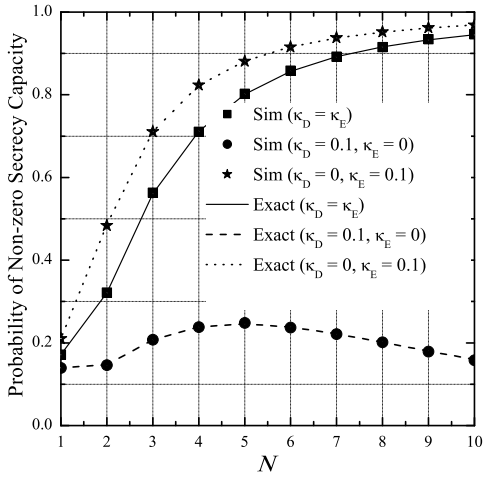

Fig. 5. Probability of non-zero secrecy capacity as a function of the number of hops N with different values of κ_D and κ_E, when $\psi = 0$dB $m_D = 1$, $m_E = 2$, $\kappa_D = 0.05$, $\kappa_E = 0.1$ and $x_E = y_E = 0.5$.

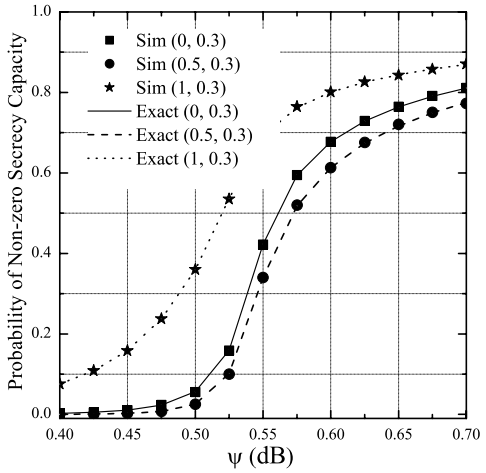

Fig. 6. Probability of non-zero secrecy capacity as a function of κ_E with various positions of the eavesdropper when $\psi = 0$dB, $N = 4$, $m_D = 1$, $m_E = 2$, $\kappa_D = 0.55$.

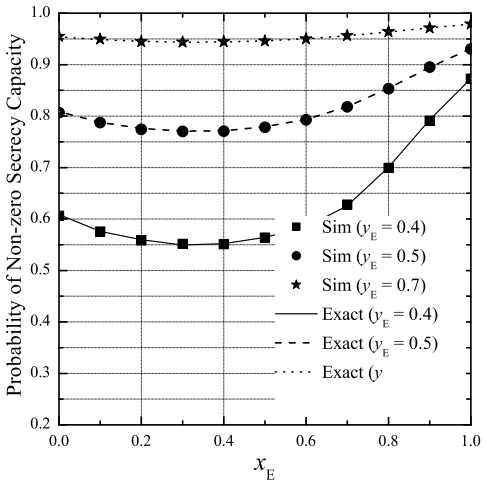

Fig. 7. Probability of non-zero secrecy capacity as a function of x_E with various values of y_E when $N = 3$, $m_D = m_E = 2$ and $\kappa_D = \kappa_E$.

is that when the hardware impairment level at the authorized nodes is lower or equal to that of the eavesdropper, the PoNSC increases when the number of hops increases. It is also seen that in case where $\kappa_D > \kappa_E$, the secrecy performance changes with the increasing of the number of hops. Moreover, it is worth noting that there exists an optimal value of N at which the PoNSC is highest, i.e., $N = 5$.

Figure 6 presents the impact of the hardware impairment level κ_E on the PoNSC with different positions of the eavesdropper, i.e., (0, 0.3), (0.5, 0.3) and (1, 0.3). The remaining parameters are set by $\psi = 0$dB, $N = 4$, $m_D = 1$, $m_E = 2$ and $\kappa_D = 0.55$. As expected, the secrecy performance of the proposed protocol is better when the hardware impairment level κ_E increases. Moreover, the eavesdropper's position affects on the system performance. For example, in this figure, the PoNSC is highest when the eavesdropper is near the destination $(x_E, y_E) = (1, 0.3)$), and the PoNSC is lowest when the eavesdropper is located at (0.5, 0.3).

In Fig. 7, we investigate the impact of the eavesdropper's position on the secrecy performance when $\kappa_D = \kappa_E$, $N = 3$, $m_D = m_E = 2$. In particular, we fix the value of y_E, while changing that of x_E from 0 to 1. As we can see, the secrecy performance significantly improves when the eavesdropper is far the authorized nodes, i.e., y_E increases. Similar to Fig. 6, it is also seen that the PoNSC is highest when the eavesdropper is near the destination. Moreover, for each value of y_E, there exists a value of x_E at which the PoNSC is lowest.

5. Conclusion

In this paper, the impact of hardware impairments on the probability of non-zero secrecy capacity (PoNSC) of the multi-hop RF relaying protocol was investigated. The obtained results in this paper can be listed as follows:

- We derive exact expressions of the PoNSC over Nakagami-m fading channels. These formulas are expressed by infinite series of exponential functions and

exponential integral functions. Moreover, Monte Carlo simulations are also performed to validate the correction of our derivations. Results presented that simulation and theoretical results are in good agreement when we truncate infinite series at first 100 terms.

- The hardware impairment level significantly affects on the secrecy performance. In particular, the PoNSC rapidly increases with low impairment level at the authorized nodes and high impairment level at the eavesdropper. In addition, when the transceiver hardware of the eavesdropper is better that of the authorized nodes, the system performance seriously degrades, where the performance-degradation slope equals to the Nakagami-*m* parameter of the eavesdropping link.
- When the hardware impairment level at the authorized nodes are better than that of the eavesdropper, the PoNSC increases with the increasing of the transmit SNR and the number of hops. Furthermore, with the same impairment levels at all of the nodes, the secrecy performance does not depend on the transmit SNR as well as the hardware impairments.
- The position of the eavesdropper also affects on the value of the PoNSC, i.e., the system performance is better when the eavesdropper is near the destination.

The results obtained in this paper are useful for designing and optimizing the multi-hop secured communication networks. In future works, we will study secured relaying protocols with relay selection methods in presence of hardware impairments.

Acknowledgments

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

References

[1] WYNER, A. D. The wire-tap channel. *The Bell System Technical Journal*, 1975, vol. 54, no. 8, p. 1355–1387. DOI: 10.1002/j.1538-7305.1975.tb02040.x

[2] GOPALA, P. K., LAI, L., GAMAL, H. E. On the secrecy capacity of fading channels. *IEEE Transactions on Information Theory*, 2008, vol. 54, no. 10, p. 4687–4698. DOI: 10.1109/TIT.2008.928990

[3] WANG, L., YANG, N., ELKASHLAN, M., et al. Physical layer security of Maximal ratio combining in two-wave with diffuse power fading channels. *Transactions on Information Forensics and Security*, 2014, vol. 9, no. 2, p. 247 – 258. DOI: 10.1109/TIFS.2013.2296991

[4] KAKITANI, M., BRANTEB, G., SOUZAS, R. Energy efficiency analysis of a two dimensional cooperative wireless sensor network with relay selection. *Radioengineering*, 2013, vol. 22, no. 2, p. 549–557. ISSN: 1805-9600

[5] WANG, G., GUO, D., LIU, A., et al. Multiuser cooperation with hybrid network coding in wireless networks. *Radioengineering*, 2014, vol. 23, no. 1, p. 435–444. ISSN: 1805-9600

[6] LIU, Y., WANG, L., DUY, T. T., et al. Relay selection for security enhancement in cognitive relay networks. *IEEE Wireless Communications Letters*, 2015, vol. 4, no. 1, p. 46–49. DOI: 10.1109/LWC.2014.2365808

[7] DUY, T. T., DUONG, T. Q., THANH, T. L., et al. Secrecy performance analysis with relay selection methods under impact of co-channel interference. *IET Communications*, 2015, vol. 9, no. 11, p. 1427–1435. DOI: 10.1049/iet-com.2014.1128

[8] FAN, L., ZHANG, S., DUONG, T. Q., et al. Secure switch-and-stay combining (SSSC) for cognitive relay networks. *IEEE Transactions on Communications*, 2016, vol. 64, no. 1, p. 70–82. DOI: 10.1109/TCOMM.2015.2497308

[9] DING, Z., MA, Z., FAN, P. Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise. *IEEE Transactions on Wireless Communications*, 2014, vol. 13, no. 4, p. 2189–2203. DOI: 10.1109/TWC.2014.022714131252

[10] DUY, T. T., KONG, H. Y. Secrecy performance analysis of multihop transmission protocols in cluster networks. *Wireless Personal Communications*, 2015, vol. 82, no. 4, p. 2505–2518. DOI: 10.1007/s11277-015-2361-y

[11] SANG, N. Q., KONG, H. Y. Exact outage analysis of the effect of co-channel interference on secured multi-hop relaying networks. *International Journal of Electronics*, 2016, vol. 103, no. 11, p. 1822–1838. DOI: 10.1080/00207217.2016.1138534

[12] BJORNSON, E., MATTHAIOU, M., DEBBAH, M. A new look at dual-hop relaying: Performance limits with hardware impairments. *IEEE Transactions on Communications*, 2013, vol. 61, no. 11, p. 4512–4525. DOI: 10.1109/TCOMM.2013.100913.130282

[13] DUY, T. T., DUONG, T. Q., DA COSTA, D. B., et al. Proactive relay selection with joint impact of hardware impairment and co-channel interference. *IIEEE Transactions on Communications*, 2015, vol. 63, no. 5, p. 1594–1606. DOI: 10.1109/TCOMM.2015.2396517

[14] BOULOGEORGOS, A. A., KARAS, D. S., KARAGIANNIDIS, G. K. How much does I/Q Imbalance affect secrecy capacity? *IEEE Communications Letters*, 2016, vol. 20, no. 7, p. 1305–1308. DOI: 10.1109/LCOMM.2016.2558561

[15] MO, J., TAO, M., LIU, Y. Relay placement for physical layer security: A secure connection perspective. *IEEE Communications Letters*, 2012, vol. 16, no. 6, p. 878–881. DOI: 10.1109/LCOMM.2012.042312.120582

[16] DENG, Y., WANG, L., ELKASLAN, M., et al. Generalized selection combining for cognitive relay networks over Nakagami-*m* fading. *IEEE Transactions on Signal Processing*, 2015, vol. 63, no. 8, p. 1993–2006. DOI: 10.1109/TSP.2015.2405497

[17] LEE, S., LEE, H., CHOI, H. H., et al. Outage probability of decode-and-forward relaying systems with efficient partial relay selection in Nakagami fading channels. *ETRI Journal*, 2014, vol. 36, no. 1, p. 22–30. DOI: 10.4218/etrij.13.0113.0348

[18] GRADSHTEYN, I., RYZHIKR, I. *Table of Integrals, Series, and Products*. 7th ed. New York (USA): Academic Press, Inc., 2007. ISBN: 978-0123736376

[19] YANG, N., ELKASLAN, M., YUAN, J. Outage probability of multiuser relay networks in Nakagami-*m* fading channels. *IEEE Transactions on Vehicular Technology*, 2010, vol. 59, no. 5, p. 2120–2132. DOI: 10.1109/TVT.2010.2042828

[20] LANEMAN, J. N., TSE, D. N. C., WORNELL, G. W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Transactions on Information Theory*, 2004, vol. 50, no. 12, p. 3062 – 3080. DOI: 10.1109/TIT.2004.838089

[21] ALVI, S. H., WYNE, S. Error analysis of fixed-gain AF relaying with MRC over Nakagami-*m* fading channels. *Radioengineering*, 2016, vol. 25, no. 1, p. 106–113. DOI: 10.13164/re.2016.0106

About the Authors ...

Tran Tin PHU 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 ChiMinh 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.

The Hung DANG was born in Ha Tinh, Vietnam, in 1983. He received the B.E. degree in Telecommunication Technological Command from Telecommunications University (TCU), Nha Trang, Khanh Hoa, in 2006 and M.Eng. degree in Telecommunications Engineering from Posts and Telecommunications Institute of Technology (PTIT), Ho Chi Minh city, Vietnam, in 2014, respectively. He is currently a Lecturer in the Faculty of Telecommunications Professional of Telecommunications University. His major research interests are Cooperative Communications, Cognitive Radio, and Physical Layer Security.

Trung Duy TRAN (corresponding author) 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 Ph.D. 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.