Exploiting Secure Performance of Full-Duplex Decode and Forward in Optimal Relay Selection Networks

Thu-Thuy Thi Dao[1], Ngoc-Long Nguyen[2], Hong-Nhu Nguyen[2,3], Si-Phu Le[2,4], Dinh-Thuan Do[5], Quyet Nguyen[1], Miroslav Voznak[2], Lukas Sevcik[2], Jaroslav Zdralek[2]
[1]*Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Vietnam*
[2]*VSB Technical University of Ostrava, Ostrava, Czech Republic*
[3]*Faculty of Electronics and Telecommunications, Sai Gon University, Vietnam*
[4]*Faculty of Refrigeration Engineering, Van Lang University, Vietnam*
[5]*Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam*
dodinhthuan@tdt.edu.vn

***Abstract*—In the presence of an illegitimate user, we investigate the secrecy outage probability (SOP) of the optimal relay selection (ORS) networks by applying decode-and-forward (DnF) based full-duplex (FD) relaying mode. The closed-form expressions for the allocations of the end-to-end signal-to-interference-plus-noise ratio (SINR) in each wireless network are derived as well as the closed-form expression for the exact SOP of the proposed ORS system is presented under Rayleigh fading schemes. As an important achievement, SOP is also compared between orthogonal multiple access (OMA) and non-orthogonal multiple access (NOMA) schemes. Our results reveal that the SOP of the suggested scheme can be considerably influenced by several parameters involved, including the number of relays, the average signal-to-noise ratio (SNR) of eavesdropper links, transmit power and the average residual self-interference (SI) enforced on the FD relays.**

***Keywords*—Full-duplex; Optimal relay selection; Secrecy outage probability.**

I. INTRODUCTION

To enable secure communication in wireless networks, it will take advantage of the physical characteristics of wireless channels in term of secrecy rate and amount of securely transmitted information transmitted to the expected receiver. In particular, a wireless relaying system with energy harvesting capability is investigated under the impact of the jamming signal [1]. Simultaneously, for improving the spectral efficiency of the wireless networks and widening the radio coverage thanks to relaying schemes [2], [3], a valuable method which has been arising is an implementation of half-duplex (FD) based relaying technologies in cooperative communication systems. However, the happening at the same time of proper receivers and eavesdroppers in the equivalent network may turn the legitimate responding information of receivers be vulnerable to security attacks, although cooperative communication technology has published several technical advantages [4]. In [5], an optimal power allocation design introduced for performing full-duplex relaying (FDR) shows the outperformance between FDR and the typical half- duplex relaying (HDR) in terms of outage performance. The FDR technique investigated in [6] reveals that it could raise the physical layer security rate in multi-hop relaying systems. Furthermore, Shafie *et al.* considered the physical-layer security cases of an FD multiple-input multiple-output (MIMO) relaying channel with fixed power transmissions as well as suggesting an artificial-noise aided secure system for attaining an improvement in average secrecy rate in [7].

Recently, the current multiple access techniques can be mainly categorized into two classes including orthogonal multiple access and non-orthogonal multiple access (NOMA), by distinctive considering on a specific resource block occupied by more than one user [8]. In the NOMA technique, it is further categorized some kinds, so-called as code-domain NOMA and power-domain NOMA through examining the multiplexing gain gathered from the different domains. Ding *et al.* [9] explored randomly scenario of roaming users to examine the performance of the NOMA downlink. Moreover, Qin *et al.* considered NOMA systems in large-scale networks with respect to physical layer security in case of NOMA users and eavesdroppers are spatially arranged at random position [10].

Motivated by previous works and to fill the gap related to

Manuscript received 20 November, 2017; accepted 23 June, 2018.

relaying scheme in [11], [12], the main aim of this paper is enhancing the secrecy performance of a full duplex relay network with DnF scheme. More importantly, the main contribution is that secrecy performance is compared in both OMA and NOMA scheme.

The rest of the paper is organized as follows: in Section II, system model shows secure full-duplex with OSR. In Section III and IV, we investigate the secrecy performance with DnF relay schemes for OMA, NOMA respectively. Section V shows numerical simulations to verify the analysis. Finally, the paper is concluded in Section VI.

Notations: Mathematical expectation is denoted by $E[.]$, $\Pr[.]$ stands for probability, $Ei(.)$ is the exponential integral, $f_X(.)$ and $F_X(.)$ define the probability density function (PDF) and cumulative distribution function (CDF) of a given random variable (RV) X, respectively.

II. System Model

As shown in Fig. 1, consider a system composed of one source S, one destination D, N full- duplex DnF relays R_k with k = {1, ..., N}, and an eavesdropper E. The source, destination, and the eavesdropper are assumed to have a single antenna while the relays have two antennas, one for reception and the other for transmission. The direct links between the source and the destination or the eavesdropper are unavailable due to severe fading and path-loss, and thus communication can be established only via relays. Also, we concentrate on the situation that the eavesdropper may only overhear the confidential message from the source through the relays' transmission.

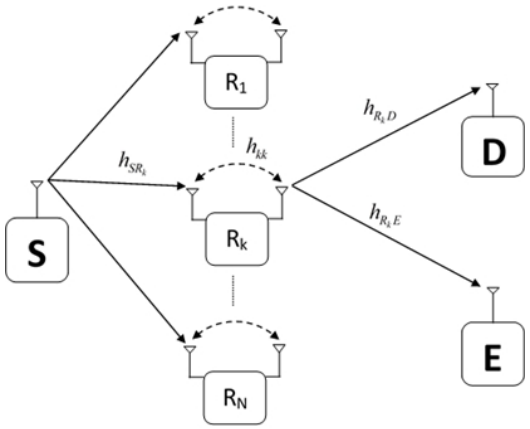

Fig. 1. System Model for OMA and NOMA.

The channel coefficients for S → R_k, R_k → D, R_k → E and R_k → R_k are denoted as h_{SR_k}, h_{R_kD}, h_{R_kE} and h_{kk}, respectively. It is considered that a quasi-static block-fading Rayleigh channel between two nodes with h_{SR_k}, h_{R_kD}, h_{R_kE} and h_{kk} which are modelled as zero mean complex Gaussian random variables with variances $\delta^2_{SR_k}$, $\delta^2_{R_kD}$, $\delta^2_{R_kE}$, and $\delta^2_{R_k}$ respectively. The noise associated with each channel is modelled as mutually independent additive white Gaussian noise (AWGN) with zero mean and variance N_0. We assume that the source and the relays transmit signal with fixed powers P_S and P_R, respectively.

III. Secrecy Outage Probability in OMA Scheme

A. Secrecy Outage Probability for the System with Full-Duplex DnF Relays

Secrecy outage probability is defined as the probability that the instantaneous secrecy rate of the system is less than a predefined target rate R_o (in bits/s/Hz). We denote γ_{mn} is SNR of link $m \to n$. Mathematically, the concerned SOP, i.e. $SOP_o = \Pr(C_{R_o} < R_o)$ can be expressed as [11], [12]

$$SOP_o = \prod_{k=1}^{N} \Pr\left[\frac{1+\min\left(\frac{\gamma_{SR_k}}{\gamma_{kk}+1}, \gamma_{R_kD}\right)}{1+\gamma_E} < 2^{R_o}\right] = \prod_{k=1}^{N} \int_0^{\infty} F_{Z_K}(a+by) f_{\gamma_E}(y)dy, \quad (1)$$

where $Z_k = \min\left(\frac{\gamma_{SR_k}}{\gamma_{kk}+1}, \gamma_{R_kD}\right)$, $a = 2^{R_o} - 1$, $b = 2^{R_o}$.

After some analysis we have the following result [13]

$$SOP_o = \prod_{k=1}^{N} \left(1 - Ae^{\mu\beta} Ei(\mu\beta)\right), \quad (2)$$

where $A = \frac{\lambda_{SR_k}}{b\lambda_{R_kE}\lambda_{R_k}} e^{-a\left(\frac{1}{\lambda_{SR_k}} + \frac{1}{\lambda_{R_kD}}\right)}$, $\beta = \frac{\lambda_{SR_k} + \lambda_{R_k}}{b\lambda_{R_k}}$, $\mu = \frac{b}{\lambda_{SR_k}} + \frac{b}{\lambda_{R_kD}} + \frac{1}{\lambda_{R_kE}}$

B. Secrecy Outage Probability for the System with Half-Duplex DnF Relays

In this section we consider the SOP of the system using HD DnF relays. Similarly, secrecy outage probability for the system with Half-Duplex DnF relays can be expressed as

$$SOP_o^H = \prod_{k=1}^{N} \Pr\left[\frac{1+\min(\gamma_{SR_k}, \gamma_{R_kD})}{1+\gamma_E} < 2^{2R_o}\right] = \prod_{k=1}^{N} \int_0^{\infty} F_{Z_k^H}(a_1+b_1y) f_{\gamma_E}(y)dy, \quad (3)$$

where $Z_k^H = \min(\gamma_{SR_k}, \gamma_{R_kD})$, $a_1 = 2^{2R_o} - 1$, $b_1 = 2^{2R_o}$.

After some analysis we have the following result [11], [12]

$$SOP_o^H = \prod_{k=1}^{N} \left(1 - \frac{e^{-a_1\left(\frac{1}{\lambda_{SR_k}} + \frac{1}{\lambda_{R_kD}}\right)}}{\frac{b_1\lambda_{R_kE}}{\lambda_{SR_k}} + \frac{b_1\lambda_{R_kE}}{\lambda_{R_kD}} + 1}\right). \quad (4)$$

IV. SECRECY OUTAGE PROBABILITY IN FULL-DUPLEX NOMA SCHEME

In this scenario, the transmit signal at source X_S is composed signal intended to two different services, i.e. the first component for IoT data transfer, another for video streaming transmission. Following principle of NOMA with power allocation factors are a_1, a_2 satisfying $a_1 + a_2 = 1$ and hence it can be obtained the received signals at R_k

$$y_{R_k} = h_{SR_k}(\sqrt{a_1 P_S} X_{S_1} + \sqrt{a_1 P_S} X_{S_1}) + \\ + \sqrt{P_R} h_{kk} X_{R_k} + n_{R_k}. \quad (5)$$

At relay, the composited signal is decoded to obtain signal X_{S1} while considering X_{S2} as interference. After using SIC to detect X_{S2}. The received SNRs for detecting X_{S1} and X_{S2} are given respectively by:

$$\begin{cases} \gamma^1_{R_k} = \dfrac{\dfrac{a_1 P_S}{N_0}\left|h_{SR_k}\right|^2}{\dfrac{a_2 P_S}{N_0}\left|h_{SR_k}\right|^2 + \dfrac{P_R}{N_0}\left|h_{kk}\right|^2 + 1} = \dfrac{a_1 \gamma_{SR_k}}{a_2 \gamma_{SR_k} + \gamma_{kk} + 1}, \\ \gamma^2_{R_k} = \dfrac{\dfrac{a_2 P_S}{N_0}\left|h_{SR_k}\right|^2}{\dfrac{P_R}{N_0}\left|h_{kk}\right|^2 + 1} = \dfrac{a_2 \gamma_{SR_k}}{\gamma_{kk} + 1}. \end{cases} \quad (6)$$

Then, SOP for signal X_{S_1} can be expressed by

$$SOP^1_o = \Pr(C_{R_o} < R_o) = \\ = \prod_{k=1}^{N} \Pr\left[\frac{1 + \min\left(\dfrac{a_1 \gamma_{SR_k}}{a_2 \gamma_{SR_k} + \gamma_{kk} + 1}, \gamma_{R_k D}\right)}{1 + \gamma_E} < 2^{R_o}\right] = \\ = \prod_{k=1}^{N} \int_0^{\infty} F_{Z_{k1}}(a + by) f_{\gamma_E}(y) dy, \quad (7)$$

where $Z_{k1} = \min\left(\dfrac{a_1 \gamma_{SR_k}}{a_2 \gamma_{SR_k} + \gamma_{kk} + 1}, \gamma_{R_k D}\right)$.

After some analysis, we have the following result

$$SOP^1_o = \prod_{k=1}^{N}\left(1 - \frac{1}{\lambda_{R_k E}} \int_0^{\omega} A(a + by) e^{\frac{-y}{\lambda_{R_k E}}} dy\right). \quad (8)$$

where

$$A(z) = \frac{\lambda_{SR_k}(a_1 - a_2 z)}{z\lambda_{R_k} + \lambda_{SR_k}(a_1 - a_2 z)} e^{-z\left(\frac{1}{\lambda_{SR_k}(a_1 - a_2 z)} + \frac{1}{\lambda_{R_k D}}\right)},$$

$$\omega = \frac{1}{a_2 b} - 1, \omega < \frac{a_1}{a_2}.$$

Proof: See Appendix A.

In special case as $\lambda_{SR_k} \to \infty$, $A(z)\big|_{\lambda_{SR_k} \to \infty} = e^{-z\left(\frac{1}{\lambda_{R_k D}}\right)}$

$$SOP^1_o\Big|_{\lambda_{SR_k} \to \infty} = \prod_{k=1}^{N}\left(1 - \frac{1}{\lambda_{RE}} \int_0^{\omega} e^{-(a+by)\left(\frac{1}{\lambda_{R_k D}}\right)} e^{\frac{-y}{\lambda_{RE}}} dy\right) = \\ = 1 + \frac{1}{\left(\dfrac{b\lambda_{RE}}{\lambda_{R_k D}} + 1\right)}\left(e^{-\omega\left(\frac{b}{\lambda_{R_k D}} + \frac{1}{\lambda_{RE}}\right) - \frac{a}{\lambda_{R_k D}}} - e^{-\frac{a}{\lambda_{R_k D}}}\right). \quad (9)$$

When $\lambda_{R_k D} \to \infty$, we have $A_1(z) = A(z)\big|_{\lambda_{R_k D} \to \infty} =$

$$= \frac{\lambda_{SR_k}(a_1 - a_2 z)}{z\lambda_{R_k} + \lambda_{SR_k}(a_1 - a_2 z)} e^{-z\left(\frac{1}{\lambda_{SR_k}(a_1 - a_2 z)}\right)}$$ and hence, we obtain

$$SOP^1_o\Big|_{\lambda_{R_k D} \to \infty} = \prod_{k=1}^{N}\left(1 - \frac{1}{\lambda_{RE}} \int_0^{\omega} A_1(a + by) e^{\frac{-y}{\lambda_{RE}}} dy\right). \quad (10)$$

Finally, in case of $\lambda_{R_k E} \to \infty$, we have $SOP^1_o\,|_{\lambda_{R_k E} \to \infty} = 1$.

Similarly, in OMA case, SOP for signal X_{S2} can be computed by

$$SOP^2_o = \prod_{k=1}^{N}\left(1 - A_n e^{\mu_n \beta_n} E_1(\mu_n \beta_n)\right), \quad (11)$$

where $A_n = \dfrac{a_2 \lambda_{SR_k}}{b\lambda_{R_k E}\lambda_{R_k}} e^{-a\left(\frac{1}{a_2 \lambda_{SR_k}} + \frac{1}{\lambda_{R_k D}}\right)}$,

$\mu_n = \dfrac{b}{a_2 \lambda_{SR_k}} + \dfrac{b}{\lambda_{R_k D}} + \dfrac{1}{\lambda_{R_k E}}$, $\beta_n = \dfrac{a_2 \lambda_{SR_k} + \lambda_{R_k}}{b\lambda_{R_k}}$.

When $\lambda_{SR_k} \to \infty$

$$SOP_o\,|_{\lambda_{SR_k} \to \infty,} = \prod_{k=1}^{N}\left(1 - \frac{e^{-a/\lambda_{R_k D}}}{1 + b\dfrac{\lambda_{R_k E}}{\lambda_{R_k D}}}\right). \quad (12)$$

When $\lambda_{R_k D} \to \infty$

$$SOP^2{}_o\,|_{\lambda_{R_k D} \to \infty} = \prod_{k=1}^{N}\left(1 - A_{n1} e^{\mu_{n1}\beta_{n1}} E_1(\mu_{n1}\beta_{n1})\right), \quad (13)$$

where $A_{n1} = \frac{a_2\lambda_{SR_k}}{b\lambda_{R_kE}\lambda_{R_k}} e^{-a\frac{1}{a_2\lambda_{SR_k}}}$, $\mu_{n1} = \frac{b}{a_2\lambda_{SR_k}} + \frac{1}{\lambda_{R_kE}}$, $\beta_1 = \frac{a_2\lambda_{SR_k} + \lambda_{R_k}}{b\lambda_{R_k}}$.

Finally, when $\lambda_{R_kE} \to \infty$, we have $A \to 0$ and $SOP_o\,|_{\lambda_{\mathrm{R_kE}} \to \infty} = 1$.

Remark 1: It difficult of evaluate how the related parameter, i.e. the number of relay, P_S, P_R, which affect on system performance by analytical expressions. Fortunately, they can be determined through following simulation results for find optimal SOP.

V. SIMULATION RESULTS

In this section, several Monte Carlo simulation results of the proposed relay section network and existing half-duplex relaying (HDR), full-duplex relaying (FDR) schemes are presented. In the simulations, the transmit power of source and relay are changed to find optimal outage performance. In this paper, we assume that the self-interference is the residual self-interference exists small amount after the imperfect self-interference suppression. For outage probability evaluation, we assume that the interference is at noise level and channel gain of each channel as $R_0 = 0.5, \left|\lambda_{SR_1}\right|^2, \left|\lambda_{SR_2}\right|^2 = 1.1, 1.3, \left|\lambda_{R_1D}\right|^2, \left|\lambda_{R_2D}\right|^2 = 1.1, 1.2$ $\left|\lambda_{R_1E}\right|^2, \left|\lambda_{R_2E}\right|^2 = 0.2, 0.5$, which can be achieved through numerical simulation.

Figure 2 plots the SOP of the scenario in which we change the transmit power at the source and the transmit power at the relay.

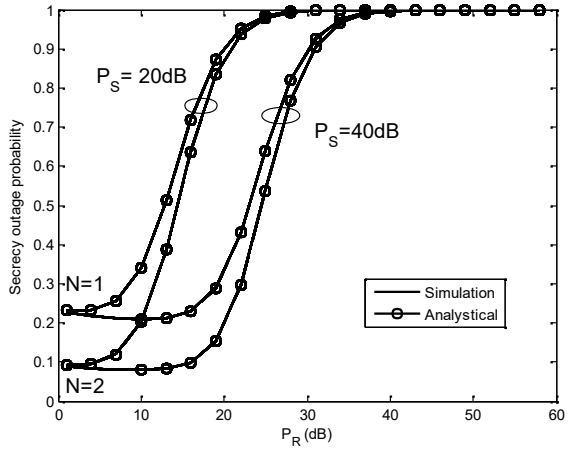

Fig. 2. Secrecy outage probability in OMA versus P_R of FD DnF relays with N = 1, 2 relays and P_S = 20 dB, 40 dB.

We can observe that as expected, the SOP decreases to an optimal point as approximately with mathematical programs such as Matlab, i.e, $P_S = 40(dB)$, $P_R = 9.1(dB)$ with N = 2 and $P_S = 40(dB)$, $P_R = 9.2(dB)$ with N = 1. Another option for enhancing the physical layer security is to choose power allocation between the source and the relay properly since it reduces the total outage probability. It is also worth noting that having the best outage performance if we choose P_S, P_R in right manner.

In Fig. 3 and Fig. 4, we compare SOP of OMA and NOMA.

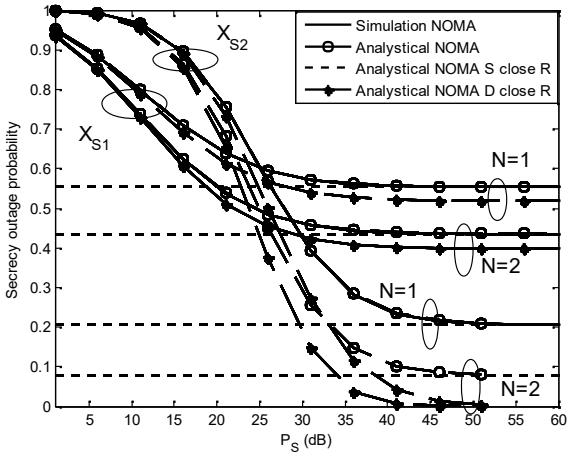

Fig. 3. Secrecy outage probability of the ORS scheme versus P_S of FD DnF relays in NOMA with N = 1, 2 relays and P_R = 10 dB of two signals X_{S1}, X_{S2}.

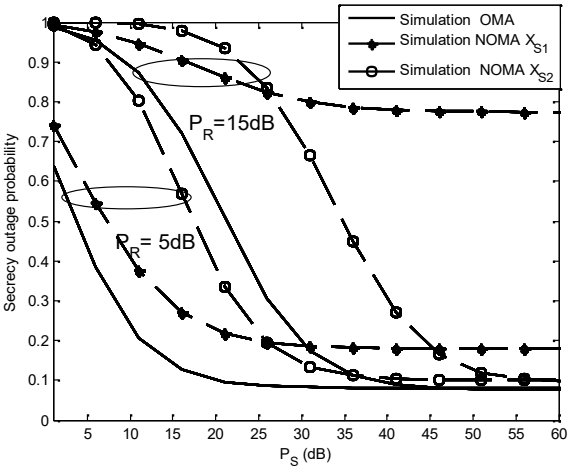

Fig. 4. Secrecy outage probability of the ORS scheme versus P_S of FD DnF relays OMA and NOMA with N = 2, $a_1 = 0.95, a_2 = 0.05$ and P_R = 5 dB, 15 dB.

The results confirmed that SOP performance of X_{S1} and X_{S2} lower than SOP performance of OMA due to lower power allocated for each signal. In this case the transmit power at relay P_R contribute to change SOP performance at high region P_S and the cross point is approximately 25 dB–30 dB.

VI. CONCLUSIONS

In this paper, we studied the secrecy outage probability of the FDR by comparing performance of OMA and NOMA scenarios with relay selection scheme. We suggested a novel FDR operation, where each FDR receives the information signal from the previous node as well as transmits the jamming signal to the eavesdropper at the same time. The transmit power allocations for FDRs are calculated by a

numerical approach to minimize the lower bound of the secrecy outage performance. Numerical results have revealed that the mentioned FDR operation with the high number of the relay significantly enhanced the outage performance compared with the conventional FDR operation with the only relay.

APPENDIX A

It is noted that

$$Z_{k1} = \min\left(\frac{a_1\gamma_{SR_k}}{a_2\gamma_{SR_k} + \gamma_{kk} + 1}, \gamma_{R_kD}\right) = \min(X_{k1}, Y_k). \quad \text{(A1)}$$

We consider outage event below

$$F_{Z_{k1}}(z) = 1 - (1 - F_{X_{k1}}(z))(1 - F_{Y_k}(z)). \quad \text{(A2)}$$

We first derive F_{X_k} as follows with x > 0

$$F_{X_{k1}}(x) = \Pr\left(\frac{a_1\gamma_{SR_k}}{a_2\gamma_{SR_k} + \gamma_{kk} + 1} < x\right) = \\ = \Pr((a_1 - a_2x)\gamma_{SR_k} < x(\gamma_{kk} + 1)). \quad \text{(A3)}$$

We divide two cases

$$F_{X_{k1}}(x) = \begin{cases} \Pr\left(\gamma_{SR_k} > \dfrac{x(\gamma_{kk}+1)}{(a_1 - a_2x)}\right) = 1, x \geq \dfrac{a_1}{a_2}, \\ \Pr\left(\gamma_{SR_k} < \dfrac{x(\gamma_{kk}+1)}{(a_1 - a_2x)}\right), \quad x < \dfrac{a_1}{a_2}. \end{cases} \quad \text{(A4)}$$

Substituting $F_{\gamma_{SR_k}}(x) = 1 - e^{\frac{-x}{\lambda_{SR_k}}}, f_{\gamma_{R_k}}(y) = \frac{1}{\lambda_{R_k}} e^{\frac{-y}{\lambda_{R_k}}}$

into (A3), we obtain:

$$F_{X_{k1}}(x) = \begin{cases} 1 & , x \geq \dfrac{a_1}{a_2} \\ \int_0^\infty (1 - e^{\frac{-z(y+1)}{\lambda_{SR_k}(a_1 - a_2z)}}) \frac{1}{\lambda_{R_k}} e^{\frac{-y}{\lambda_{R_k}}} dy, & x < \dfrac{a_1}{a_2} \end{cases}, \quad \text{(A5)}$$

$$F_{X_{k1}}(x) = \begin{cases} 1, \quad x \geq \dfrac{a_1}{a_2}, \\ 1 - \dfrac{\lambda_{SR_k}(a_1 - a_2z) e^{\frac{-z}{\lambda_{SR_k}(a_1 - a_2z)}}}{z\lambda_{R_k} + \lambda_{SR_k}(a_1 - a_2z)}, x < \dfrac{a_1}{a_2}. \end{cases} \quad \text{(A6)}$$

Combining (A2) and (A4) we have

$$F_{Z_{k1}}(z) = \begin{cases} 1, \quad \text{when} \quad z \geq \dfrac{a_1}{a_2}, \\ 1 - A(z), \quad \text{when} \quad z < \dfrac{a_1}{a_2}. \end{cases} \quad \text{(A7)}$$

As a result, it can be shown that

$$SOP_o^1 = \prod_{k=1}^{N} \int_0^\infty F_{Z_{k1}}(a + by) f_{\gamma_E}(y) dy = \\ = \prod_{k=1}^{N} \left(1 - \frac{1}{\lambda_{R_kE}} \int_0^\omega A(a + by) e^{\frac{-y}{\lambda_{R_kE}}} dy\right), \quad \text{(A8)}$$

in which:

$$A(z) = \frac{\lambda_{SR_k}(a_1 - a_2z)}{z\lambda_{R_k} + \lambda_{SR_k}(a_1 - a_2z)} e^{-z\left(\frac{1}{\lambda_{SR_k}(a_1 - a_2z)} + \frac{1}{\lambda_{R_kD}}\right)}, \quad \text{(A9)}$$

$$(\omega = \frac{1}{a_2b} - 1) < \frac{a_1}{a_2}. \quad \text{(A10)}$$

REFERENCES

[1] N. Q. Le, Dinh-Thuan Do, B. An, "Secure wireless powered relaying networks: energy harvesting policies and performance analysis", *International Journal of Communication Systems (Wiley)*, vol. 30, no. 18, 2017. DOI: 10.1002/dac.3369.

[2] Dinh-Thuan Do, H-S Nguyen, "A tractable approach to analyze the energy-aware two-way relaying networks in presence of co-channel interference", *EURASIP Journal on Wireless Communications and Networkin*g, vol. 271, 2016. DOI: 10.1186/s13638-016-0777-z.

[3] Thanh-Luan Nguyen, Dinh-Thuan Do, "A new look at AF two-way relaying networks: energy harvesting architecture and impact of co-channel interference", *Annals of Telecommunications*, vol. 72, no. 11, pp. 669–678, 2017. DOI: 10.1007/s12243-017-0590-7.

[4] Y. Feng, Z. Yang, S. YanNon, "Orthogonal multiple access and artificial-noise aided secure transmission in FD relay networks", in *Proc. of IEEE Globecom*, 2017, pp. 1–6. DOI: 10.1109/GLOCOMW.2017.8269229.

[5] X-X Nguyen, Dinh-Thuan Do, "Optimal power allocation and throughput performance of full-duplex DF relaying networks with wireless power transfer-aware channel", *EURASIP Journal on Wireless Communications and Networking,* vol. 152, 2017. DOI: 10.1186/s13638-017-0936-x.

[6] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems", *IEEE Commun*. Lett., vol. 19, no. 4, pp. 525–528, 2015. DOI: 10.1109/LCOMM.2015.2401551.

[7] A. E. Shafie, D. Niyato, N. Al-Dhahir, "Artificial-noise-aided secure MIMO full-duplex relay channels with fixed-power transmissions", *IEEE Commun.* Lett., vol. 20, no. 8, pp. 1591–1594, 2016. DOI: 10.1109/LCOMM.2016.2579623.

[8] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, F. L. Hanzo, ''Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks", *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, 2017. DOI: 10.1109/TWC.2017.2650987.

[9] Z. Ding, Z. Yang, P. Fan, H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users", *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, 2014. DOI: 10.1109/LSP.2014.2343971.

[10] Z. Qin, Y. Liu, Z. Ding, Y. Gao, M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks", in *Proc. IEEE Int. Conf. Commun. (ICC 2016)*, Kuala Lumpur, Malaysia, 2016, pp. 1–6. DOI: 10.1109/ICC.2016.7510755.

[11] Binh V. Nguyen, K. Kim, "Secrecy outage probability of optimal relay selection for secure AnF cooperative networks", *IEEE Communications Letters*, vol. 19, no. 12, 2015. DOI: 10.1109/LCOMM.2015.2486768.

[12] Binh V. Nguyen, K. Kim, "Single relay selection for secure communication in a cooperative system with multiple full-duplex decode-and-forward relays", 2015 *IEEE Int. Workshop on Information Forensics and Security (WIFS 2015)*, Rome, Italy, 2015. DOI: 10.1109/WIFS.2015.7368590.

[13] I. S. Gradshteyn, I. M. Ryzhik, *Table of Integrals, Series, and Products.* Amsterdam, The Netherlands: Elsevier, 2007.