On Secure Cooperative Non-orthogonal Multiple Access Network with RF Power Transfer

Duy-Hung Ha[1], Dac-Binh Ha[2](✉), and Miroslav Voznak[1]

[1] Faculty of Electrical Engineering and Computer Science,
VSB - Technical University of Ostrava,
17. lisltopadu 2172/15, 708 00 Ostrava, Czechia
haduyhung@tdtu.edu.vn, miroslav.voznak@vsb.cz

[2] Faculty of Electrical and Electronics Engineering, Duy Tan University,
Da Nang, Vietnam
hadacbinh@duytan.edu.vn

Abstract. In this paper, we investigate the secrecy performance of the cooperative non-orthogonal multiple access (NOMA) network with radio frequency (RF) power transfer. Specifically, this considered network consists of one RF power supply station, one source and multiple energy constrained NOMA users in the presence of a passive eavesdropper. The better user helps the source to forward the message to worse user by using the energy harvested from the power station. The expression of secrecy outage probability for the scenario of wiretaping from user-to-user link is derived by using the statistical characteristics of signal-to-noise ratio (SNR) and signal-to-interference-plus-noise ratio (SINR) of transmission links. In order to understand more detail about the behaviour of this considered system, the numerical results are provided according to the system key parameters, such as the transmit power, number of users, time switching ratio and power allocation coefficients. The simulation results are also provided to confirm the correctness of our analysis.

Keywords: Non-orthogonal multiple access · Relaying network · Physical layer secrecy · RF power transfer · Secrecy outage probability

1 Introduction

The next generation wireless networks have been developing to satisfy human being non-stop growing need, i.e., big data rate (5G is 100 times compare to 4G), large number of users and secure transmission. Some emerging techniques, such as relaying, NOMA, MIMO techniques etc., are deployed to meet these requirements. Relaying technique with amplify-and-forward (AF) or decode-and-forward (DF) scheme allows to extend the coverage and improve the performance of wireless networks [1–3]. On the other hand, NOMA technique is employed in

T. Q. Duong et al. (Eds.): INISCOM 2019, LNICST 293, pp. 117–129, 2019.
https://doi.org/10.1007/978-3-030-30149-1_10

power domain to achieve multiple access strategies. It has the potential to be integrated with conventional orthogonal multiple access, i.e., frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA). The combination between relaying and NOMA applied in wireless network is studied in a number of works [4–12].

Moreover, due to diverse functions of wireless devices, the energy is the most concerned issue to last long the lifetime of wireless devices and extend the coverage of network. Wireless energy harvesting is approach that the wireless devices can harvest the energy from the environment (e.g., via solar, wind, thermal, and RF power sources) and convert it into electrical energy for the energy constrained devices. Among them, RF power transfer is the emerging technique that allows the energy constrained wireless devices to harvest the energy from RF sources (e.g., base station, TV/radio broadcast station, microwave station, satellite earth station etc.). A significant works [13–18] have studied the impact of RF energy harvesting (EH) on the performance of wireless networks when they took into account the RF energy harvesting in their system. This service of RF energy harvesting is predicted to be available on the future mobile networks [19].

In wireless networks, due to the broadcast nature of wireless links, the data transmission is vulnerable to be attacked and wiretapped. Although we have a number of solutions (e.g., the public-key system developed by Rivest, Shamir, and Adleman (RSA) and the data encryption standard (DES), etc.) to protect the transmit data, these solutions have not covered all of scenarios of wireless networks (e.g., error physical layer link between transmitter and receiver, powerfull computational power of eavesdropper with efficient algorithms). Physical layer security (PLS) is a novel approach that can employs the random variation characteristics of wireless links to enhance the secure transmission of wireless communication [20–22]. There are a number of works in recent to investigate PLS in NOMA relaying network without RF energy harvesting [23–29]. The work of [23] evaluated the PLS of simple NOMA model of large-scale networks through the secrecy outage probability (SOP). The better PLS performance of overall communication process has been proven in case that there is not much difference in the level of priority between legitimate users of downlink NOMA system in [24], in which users' QoS requirements to perform NOMA. The work in [25] provided the secrecy performance analysis of a two-user downlink NOMA systems with two considered SISO and MISO schemes. The authors concluded that the secrecy performance for the far user with fixed power allocation scheme degraded as the transmit power beyond the threshold and then reaches a floor as the interference from the near user increases. In [26], the artificial noise is deployed at the base station to enhance the security ability of a beamforming-aided multiple-antenna system. The PLS for cooperative NOMA systems is studied in [27], in which the AF and DF schemes are considered. They found that AF and DF schemes nearly achieve the same secrecy performance and it is independent of the channel conditions between the relay and the worse user.

Unlike above works, in this work we study the PLS performance for the cooperative NOMA network with RF energy harvesting. This considered network consists of one RF power supply station, one source and multiple energy constrained NOMA users in the presence of a passive eavesdropper. The better user harvests the RF energy from the power station to help the source to forward the message to worse user. The expression of secrecy outage probability for the scenario of wiretaping from user-to-user link is derived by using the statistical characteristics of signal-to-noise ratio (SNR) and signal-to-interference-plus-noise ratio (SINR) of transmission links. In order to understand more detail about the behaviour of this considered system, the numerical results are provided according to the system key parameters, such as the transmit power, number of users, time switching ratio and power allocation coefficients. The correctness of our analysis is confirmed by simulation results.

The remain of this paper is organized as follows. The system model is presented in Sect. 2. Secrecy performance analysis is provided in Sect. 3. The numerical results are shown in Sect. 4. Finally, we conclude our work in Sect. 5.

2 System Model Description

Figure 1 depicts a downlink RF EH cooperative NOMA system. A power supply station P intends to transfer RF power to energy-constrained users. A source S, i.e., base station, intends to transmit information to M energy constrained mobile users denoted as D_i, $(1 \leq i \leq M)$ in the presence of a passive eavesdropper E. In this considered system, we can divided M users into multiple pairs, such as $\{D_m, D_n\}$ $(m < n)$, to perform NOMA [4]. We design that the better user D_m forward the information of the poor user D_n after use applying successive interference cancellation (SIC) to detect the D_m's signal. We investigate the scenario that D_n and E can not hear from S due to the severe shadowing environment. In other words, E only tries to extract the message s_n of D_n from D_m.

Without loss of generality, assuming that all the channel gains between S and D_i follow the order of $|h_{SD_1}|^2 \geq ... \geq |h_{SD_m}|^2 \geq |h_{SD_n}|^2 \geq ... \geq |h_{SD_M}|^2$, where $|h_{SD_m}|^2$ and $|h_{SD_n}|^2$ are denoted as the ordered channel gains of the m^{th} user and the n^{th} user, respectively. And $|h_{PD_m}|^2$, $|h_{mn}|^2$, $|h_{SE}|^2$, $|h_{D_mE}|^2$ are the channel gains of the links $P - D_m$, $D_m - D_n$, $S - E$ and $D_m - E$, respectively. All the user nodes are single-antenna devices and operate in half-duplex mode, i.e., sensor nodes. All wireless links are assumed to undergo independent frequency non-selective Rayleigh block fading and additive white Gaussian noise (AWGN) with zero mean and the same variance σ^2, i.e., $\sim \mathcal{CN}(0, \sigma^2)$. We also denote $d_{PD_m}, d_{SD_m}, d_{mn}, d_{D_mE}$ as the Euclidean distances of $P - D_m, S - D_m, D_m - D_n, D_m - E$, respectively and θ denote the path-loss exponent. Let $X_1 \triangleq |h_{PD_m}|^2$, $X_2 \triangleq |h_{SD_m}|^2$, $X_3 \triangleq |h_{mn}|^2$, and $Z_3 \triangleq |h_{D_mE}|^2$.

The triple-phase protocol for this RF EH cooperative NOMA system is proposed as follows

(1) In the first phase: P transfers RF energy to the users with power P_0 in the time αT ($\alpha \in (0, 1)$: time switching ratio; T: block time).

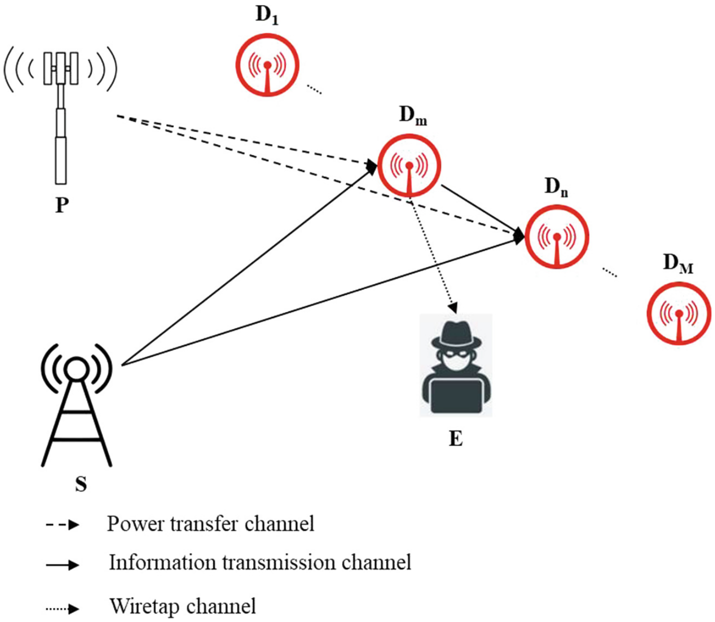

Fig. 1. System model for secured RF EH cooperative NOMA network

(2) In the second phase: S transmits information signal $x = \sqrt{a_m}s_m + \sqrt{a_n}s_n$ with power P_S to user pair $\{D_m, D_n\}$ in the time of $(1-\alpha)T/2$, where s_m and s_n are the message for the m^{th} user D_m and the n^{th} user D_n, respectively; a_m and a_n are the power allocation coefficients satisfied the conditions: $0 < a_m < a_n$ and $a_m + a_n = 1$ by following the NOMA scheme.

(3) In the third phase: Applying NOMA, D_m uses SIC to detect message s_n and subtracts this component from the received signal to obtain its own message s_m, then re-encodes and forwards s_n to D_n in the remain time of $(1-\alpha)T/2$ with the energy harvested from P.

Next, we present the RF EH NOMA relaying-based transmission in mathematical manner.

2.1 The First Phase

In this phase, the energy harvested by D_m in the time of αT can be expressed as

$$E_{D_m} = \frac{\eta P_0 |h_{PD_m}|^2 \alpha T}{d_{PD_m}^{\theta}}, \tag{1}$$

where η denotes as the energy conversion efficiency $(0 < \eta < 1)$.

2.2 The Second Phase

In the second phase, the source S broadcasts information to the user pair in duration of $(1-\alpha)T/2$. The received signal at D_m is given by

$$y_{SD_m} = \sqrt{\frac{P_S}{d_{SD_m}^{\theta}}}(\sqrt{a_m}s_m + \sqrt{a_n}s_n)h_{SD_m} + n_{SD_m}, \tag{2}$$

where $n_{SD_m} \sim \mathcal{CN}(0, \sigma^2)$.

The instantaneous SINR at D_m to detect s_n transmitted from S can be written as

$$\gamma_{SD_m}^{s_n} = \frac{a_n\bar{\gamma}_S|h_{SD_m}|^2}{a_m\bar{\gamma}_S|h_{SD_m}|^2 + d_{SD_m}^{\theta}} = \frac{b_2X_2}{b_1X_2+1}, \tag{3}$$

where $\bar{\gamma}_S = \frac{P_S}{\sigma^2}$, $b_1 = \frac{a_m\bar{\gamma}_S}{d_{SD_m}^{\theta}}$, $b_2 = \frac{a_n\bar{\gamma}_S}{d_{SD_m}^{\theta}}$.

2.3 The Third Phase

In this phase, D_m uses the harvested energy E_{Dm} as (1) to forward s_n to D_n in duration of $(1-\alpha)T/2$. Here, we ignore the processing power required by the transmit/receive circuitry of D_m. The transmit power of D_m is given by

$$P_{D_m} = \frac{\eta\alpha P_0|h_{PD_m}|^2}{(1-\alpha)d_{PD_m}^{\theta}}. \tag{4}$$

The received signal at D_n is expressed as

$$y_{mn} = \sqrt{\frac{P_{D_m}}{d_{mn}^{\theta}}}h_{mn}s_n + n_{mn}, \tag{5}$$

where $n_{mn} \sim \mathcal{CN}(0, \sigma^2)$. From (4) and (5), the instantaneous SNR at D_n in the last phase is as follows

$$\gamma_{mn} = \frac{P_{D_m}|h_{mn}|^2}{\sigma^2 d_{mn}^{\theta}} = c_1X_1X_3, \tag{6}$$

where $c_1 = \frac{\eta\alpha\bar{\gamma}_0}{(1-\alpha)d_{PD_m}^{\theta}d_{mn}^{\theta}}$, $\bar{\gamma}_0 = \frac{P_0}{\sigma^2}$ is denoted as the average transmit SNR of $D_m - D_n$ link.

Due to we consider the scenario that the passive eavesdropper E tries to extract the poor user's message s_n from the links $D_m - D_n$ without any attacks, the received signal at E is written as

$$y_{D_mE} = \sqrt{\frac{P_{D_m}}{d_{D_mE}^{\theta}}}h_{D_mE}s_n + n_{D_mE}, \tag{7}$$

where $n_{D_mE} \sim \mathcal{CN}(0,\, \sigma_E^2)$. Similarly, the instantaneous SNR at E in this phase is given by

$$\gamma_{D_mE} = c_2 X_1 Z_3, \tag{8}$$

where $c_2 = \frac{\eta\alpha\bar{\gamma}_{0E}}{(1-\alpha)d_{PD_m}^{\theta}d_{DmE}^{\theta}}$, $\bar{\gamma}_{0E} = \frac{P_0}{\sigma_E^2}$ is denoted as the average transmit SNR of $D_m - E$ link.

The i.i.d. Rayleigh channel gains ($|h_{PDm}|^2$, $|h_{SDm}|^2$, $|h_{mn}|^2$, and $|h_{DmE}|^2$) follow exponential distributions with parameters λ_{PDm}, λ_{SDm}, λ_{mn}, and λ_{DmE}, respectively. According to [30], the probability density function (PDF) and the cumulative distribution function (CDF) of ordered random variable X_2 are respectively written as follows

$$f_{X_2}(x) = \frac{M!}{(M-m)!(m-1)!}\frac{1}{\lambda_{SD_m}}\sum_{k=0}^{m-1} C_k^{m-1}(-1)^k e^{\frac{-x(M-m+k+1)}{\lambda_{SD_m}}}, \tag{9}$$

$$F_{X_2}(x) = \frac{M!}{(M-m)!(m-1)!}\sum_{k=0}^{m-1}\frac{C_k^{m-1}(-1)^k}{M-m+k+1}\left[1-e^{\frac{-x(M-m+k+1)}{\lambda_{SD_m}}}\right]. \tag{10}$$

Under Rayleigh fading, the PDF and CDF of random variable V are respectively expressed as

$$f_V(x) = \frac{1}{\lambda}e^{-\frac{x}{\lambda}}, \tag{11}$$

$$F_V(x) = 1 - e^{-\frac{x}{\lambda}}, \tag{12}$$

where $V \in (X_1, X_3, Z_3)$, $\lambda \in \{\lambda_{PD_m}, \lambda_{mn}, \lambda_{DmE}\}$.

3 Secrecy Performance Analysis

In this section, we analyze the secrecy performance by derivation the expression of secrecy outage probability. Notice that, in this considered system we only consider the case of the eavesdropper tries to hear the message of D_n at D_m without any attacks. Therefore, the instantaneous secrecy capacity for $D_m - D_n$ is given by

$$C_S = \begin{cases} \frac{(1-\alpha)}{2}\log_2\left(\frac{1+\gamma_{mn}}{1+\gamma_{D_mE}}\right), & \gamma_{mn} > \gamma_{D_mE} \\ 0, & \gamma_{mn} \le \gamma_{D_mE} \end{cases}, \tag{13}$$

Here, for simplicity we assume $B = 1\,\text{Hz}$. SOP is defined as the probability that the instantaneous secrecy capacity falls below a predetermined secrecy rate threshold $R_S > 0$ or $SOP = Pr(C_S < R_S)$.

For further calculation, we derive the following proposition.

Proposition 1. *Under Rayleigh fading, the joint CDF of γ_{mn} and γ_{D_mE} is given by*

$$F_{\gamma_{mn},\gamma_{D_mE}}(x,y) = 1 - u\mathcal{K}_1(u) - v\mathcal{K}_1(v) + t\mathcal{K}_1(t), \tag{14}$$

where $u = 2\sqrt{\frac{x}{c_1\lambda_{PD_m}\lambda_{mn}}}$, $v = 2\sqrt{\frac{y}{c_2\lambda_{PD_m}\lambda_{D_mE}}}$, $t = 2\sqrt{\frac{c_2\lambda_{D_mE}x+c_1\lambda_{mn}y}{c_1c_2\lambda_{PD_m}\lambda_{mn}\lambda_{D_mE}}}$, $\mathcal{K}_v(.)$ is the modified Bessel function of the second kind and v^{th} order [31].

Proof. See Appendix A.

In this considered scenario, the secrecy outage event occurs when D_m cannot detect s_n or D_m can detect s_n but the secrecy capacity is below the secrecy threshold. Therefore, the secrecy outage probability at the D_m is calculated as follows

$$\begin{aligned} SOP &= \Pr(\gamma_{SD_m}^{s_n} < \gamma_t) + \Pr(\gamma_{SD_m}^{s_n} > \gamma_t, C_{S_3} < R_S) \\ &= \Pr(\gamma_{SD_m}^{s_n} < \gamma_t) + \Pr(\gamma_{SD_m}^{s_n} > \gamma_t)\Pr(C_{S_3} < R_S), \end{aligned} \tag{15}$$

where γ_t is denoted as the SNR threshold to ensure successful detection at the D_m for a given target data rate R and $\gamma_t = 2^{\frac{2R}{1-\alpha}} - 1$.

Theorem 1. *Under Rayleigh fading, the SOP of the link $D_m - D_n$ is given by*

$$SOP = \varPhi_1 + (1-\varPhi_1)\varPhi_2, \tag{16}$$

where

$$\varPhi_1 = \begin{cases} \frac{M!}{(M-m)!(m-1)!}\sum\limits_{k=0}^{m-1}\frac{C_k^{m-1}(-1)^k}{M-m+k+1}\left[1 - e^{-\frac{\gamma_t(M-m+k+1)}{(b_2-b_1\gamma_t)\lambda_{SDm}}}\right], & \gamma_t < \frac{a_n}{a_m} \\ 1, & \gamma_t > \frac{a_n}{a_m} \end{cases}$$

$$\varPhi_2 = 1 - \frac{2c_1\lambda_{mn}}{c_1\lambda_{mn} + c_2\lambda_{D_mE}\varOmega_S}\sqrt{\frac{\varOmega_S - 1}{c_1\lambda_{PD_m}\lambda_{mn}}}\mathcal{K}_1\left(2\sqrt{\frac{\varOmega_S - 1}{c_1\lambda_{PD_m}\lambda_{mn}}}\right).$$

where $\varOmega_S = 2^{\frac{2R_S}{1-\alpha}}$.

Proof. See Appendix B.

4 Numerical Results and Discussion

In this section, we provide the numerical results to clarify the physical layer secrecy performance of proposed protocol for this considered RF EH NOMA relaying system. Further more, Monte-Carlo simulation results are also provided to verify our analytical results.

Figure 2 plots the curves of SOP of this system at D_m versus the transmit power of P and different average transmit SNR of link $D_m - D_n$. This result shows that when we increase the transmit power from P to the better user D_m, SOP of the system decreases. This means that we can improve the secrecy performance by increasing the transmit power to provide more energy to legitimate users.

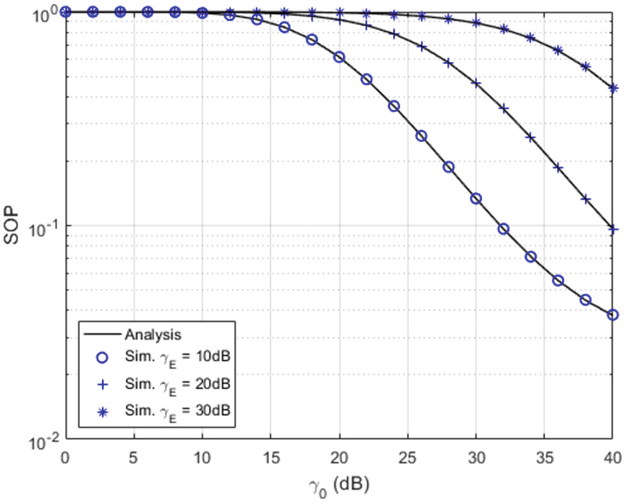

Fig. 2. SOP vs. the transmit power of P and different average transmit SNR of link $D_m - D_n$ with $\gamma_S = 20\,\text{dB}$, $a_n = 0.9$, $M = 4$, $m = 2$, $n = 3$, $R = 1\,\text{bps/Hz}$, $R_S = 1\,\text{bps/Hz}$, $\alpha = 0.3$, $\eta = 0.9$, $d_{PD_m} = d_{SD_m} = d_{mn} = d_{D_mE} = 1$, $\theta = 2$.

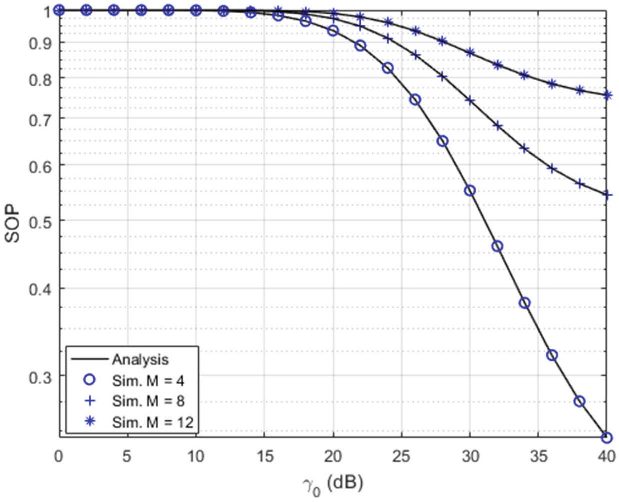

Fig. 3. SOP vs. the transmit power of P with different number of users M with $\gamma_S = 20\,\text{dB}$, $\gamma_E = 20\,\text{dB}$, $a_n = 0.9$, $m = 2$, $n = 3$, $R = 1\,\text{bps/Hz}$, $R_S = 1\,\text{bps/Hz}$, $\alpha = 0.3$, $\eta = 0.9$, $d_{PD_m} = d_{SD_m} = d_{mn} = d_{D_mE} = 1$, $\theta = 2$.

The curves of SOP of this system at D_m versus the transmit power of P with different number of users M are plotted in Fig. 3. From this figure, we can see that the secrecy performance degrades when increasing the number of users.

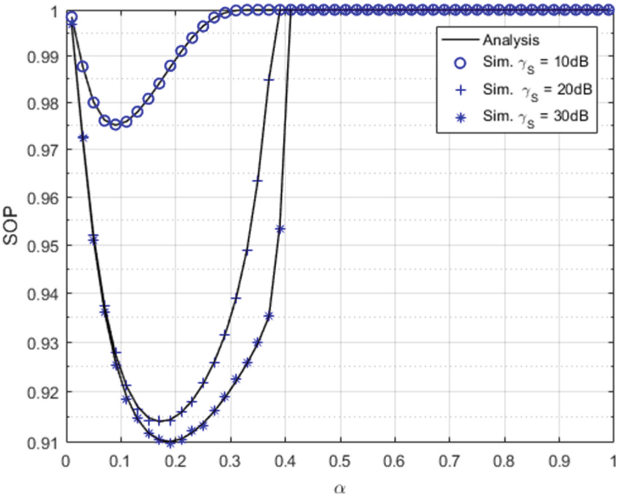

Fig. 4. SOP vs. time switching ratio α with different average transmit SNR of link $S - D_m$ with $\gamma_0 = 20\,\text{dB}$, $\gamma_E = 20\,\text{dB}$, $a_n = 0.9$, $M = 4$, $m = 2$, $n = 3$, $R = 1\,\text{bps/Hz}$, $R_S = 1\,\text{bps/Hz}$, $\eta = 0.9$, $d_{PD_m} = d_{SD_m} = d_{mn} = d_{D_mE} = 1$, $\theta = 2$.

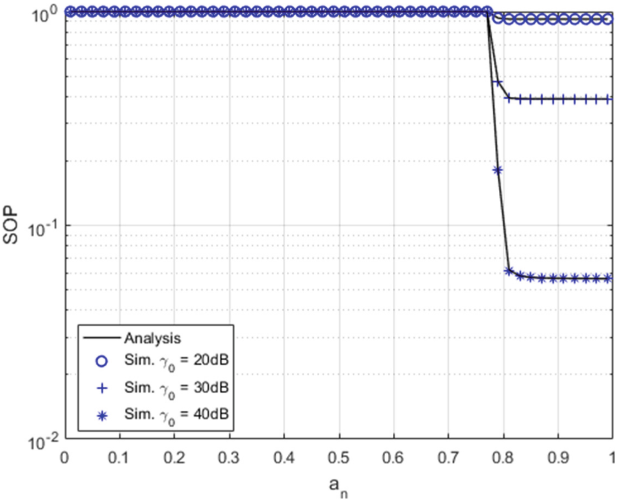

Fig. 5. SOP vs. power allocation coefficient a_n with different average transmit SNR of link $P - D_m$ with $\gamma_S = 20\,\text{dB}$, $\gamma_E = 20\,\text{dB}$, $M = 4$, $m = 2$, $n = 3$, $R = 1\,\text{bps/Hz}$, $R_S = 1\,\text{bps/Hz}$, $\eta = 0.9$, $d_{PD_m} = d_{SD_m} = d_{mn} = d_{D_mE} = 1$, $\theta = 2$.

This can be explained that the more number of users the more opportunities to wiretape the message of s_n.

The numerical results for SOP of this system at D_m versus time switching ratio α with different average transmit SNR of link $S - D_m$ are provided in Fig. 4.

We can observe from this figure that when time switching ratio α is small, α increases SOP decreases. This can be explained that there is more time to power the users as α grows. When α continue to increase, SOP inversely increases. It means that there exists a specific value of α^* to help SOP to reach the lowest value. The reason is that there is less time for message transmitting when α is greater than α^* value. When α is greater than $1-\frac{2R}{\log_2\left(\frac{a_n}{a_m}+1\right)}$ then SOP reaches 1. Obviously, we can select the best time switching ratio α to achieve the optimal secrecy performance of this system.

Figure 5 depicts the SOP's curve according to power allocation coefficient a_n with different average transmit SNR of link $P-D_m$. From this figure, we can see that when $a_n \to 1$, SOP degrades. In other words, the secrecy performance can be improved by allocating more power for the worse user's signal. However, at that time the power leaves for the better user's signal will be smaller. Due to the constrain of γ_t (i.e., $\gamma_t = 2^{\frac{2R}{1-\alpha}} - 1 < \frac{a_n}{a_m}$), by the given value of R and α, the SOP reaches 1 when $\frac{a_n}{a_m} < 2^{\frac{2R}{1-\alpha}} - 1$.

From above Figures, it is observed that the analysis and simulation results are matching very well. It means that the correctness of our analysis is verified.

5 Conclusion

In this paper, we have presented the secrecy performance analysis of downlink RF EH cooperative NOMA network with triple-phase transmission protocol. The expression of secrecy outage probability for this considered system has been derived. We have found that the secrecy performance is enhanced by increasing the transmit power for energy harvesting and/or increasing the transmit power for message signal. Moreover, the existence of best time switching ratio is proven to achieve the optimal secrecy performance of this system. Due to the limitation of this paper, we leave the best time switching ratio algorithm for future work.

Acknowledgements. This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2017.301.

Appendix A - Proof of Proposition 1

Here, we derive the expression of the joint CDF of γ_{mn} and γ_{D_mE} as follows

$$\begin{aligned} F_{\gamma_{mn},\gamma_{D_mE}}(x,y) &= \int_0^\infty F_{\gamma_{mn},\gamma_{D_mE}|X_1}(x,y|z) f_{X_1}(z)dz \\ &= \int_0^\infty F_{\gamma_{mn}|X_1}(x|z) F_{\gamma_{D_mE}|X_1}(y|z) f_{X_1}(z)dz \\ &= \int_0^\infty \left(1-e^{-\frac{x}{c_1\lambda_{mn}z}}\right)\left(1-e^{-\frac{y}{c_2\lambda_{D_mE}z}}\right)\frac{1}{\lambda_{PD_m}}e^{-\frac{z}{\lambda_{PD_m}}}dz \\ &= 1 - u\mathcal{K}_1(u) - v\mathcal{K}_1(v) + t\mathcal{K}_1(t), \end{aligned} \tag{17}$$

where $u = 2\sqrt{\frac{x}{c_1\lambda_{PD_m}\lambda_{mn}}}$, $v = 2\sqrt{\frac{y}{c_2\lambda_{PD_m}\lambda_{D_mE}}}$, $t = 2\sqrt{\frac{c_2\lambda_{D_mE}x+c_1\lambda_{mn}y}{c_1c_2\lambda_{PD_m}\lambda_{mn}\lambda_{D_mE}}}$. This concludes the proof.

Appendix B - Proof of Theorem 1

By means of (15), Φ_1 and Φ_2 are respectively calculated as follows

$$\begin{aligned}\Phi_1 &= \Pr\left(\frac{b_2X_2}{b_1X_2+1} < \gamma_t\right) = F_{X_2}\left(\frac{\gamma_t}{b_2 - b_1\gamma_t}\right)\\ &= \begin{cases} \frac{M!}{(M-m)!(m-1)!}\sum\limits_{k=0}^{m-1}(-1)^k C_k^{m-1}\frac{1}{M-m+k+1}\left[1 - e^{-\frac{\gamma_t(M-m+k+1)}{(b_2-b_1\gamma_t)\lambda_{SDm}}}\right], & \gamma_t < \frac{a_n}{a_m}\\ 1, & \gamma_t > \frac{a_n}{a_m}\end{cases}\end{aligned}$$

$$\begin{aligned}\Phi_2 &= \Pr\left(\frac{1+\gamma_{mn}}{1+\gamma_{D_mE}} < \Omega_S\right) = \int_0^\infty \left[\frac{\partial F_{\gamma_{mn},\gamma_{D_mE}}(x,y)}{\partial y}\right]_{x=\Omega_S(1+y)-1} dy\\ &= -\frac{2}{c_2\lambda_{PD_m}\lambda_{D_mE}}\int_0^\infty \mathcal{K}_0\left(\sqrt{\frac{y}{c_2\lambda_{PD_m}\lambda_{D_mE}}}\right)dy\\ &\quad + \frac{2}{c_2\lambda_{PD_m}\lambda_{D_mE}}\int_0^\infty \mathcal{K}_0\left(\sqrt{\frac{(c_1\lambda_{mn}+c_2\lambda_{D_mE}\Omega_S)y + c_2\lambda_{D_mE}(\Omega_S-1)}{c_1c_2\lambda_{PD_m}\lambda_{mn}\lambda_{D_mE}}}\right)dy\\ &= \int_0^\infty v\mathcal{K}_0(v)dv - \frac{2c_1\lambda_{mn}}{c_1\lambda_{mn}+c_2\lambda_{D_mE}\Omega_S}\int_{2\sqrt{\frac{\Omega_S-1}{c_1\lambda_{PD_m}\lambda_{mn}}}}^\infty s\mathcal{K}_0(s)ds\\ &= 1 - \frac{2c_1\lambda_{mn}}{c_1\lambda_{mn}+c_2\lambda_{D_mE}\Omega_S}\sqrt{\frac{\Omega_S-1}{c_1\lambda_{PD_m}\lambda_{mn}}}\mathcal{K}_1\left(2\sqrt{\frac{\Omega_S-1}{c_1\lambda_{PD_m}\lambda_{mn}}}\right), \qquad (18)\end{aligned}$$

where $\Omega_S = 2^{\frac{2R_S}{1-\alpha}}$, $s = \sqrt{\frac{(c_1\lambda_{mn}+c_2\lambda_{D_mE}\Omega_S)y+c_2\lambda_{D_mE}(\Omega_S-1)}{c_1c_2\lambda_{PD_m}\lambda_{mn}\lambda_{D_mE}}}$.

This is the end of our proof.

References

1. Wu, H., Wang, C., Tzeng, N.F.: Novel self-configurable positioning technique for multihop wireless networks. IEEE/ACM Trans. Netw. **13**(3), 609–621 (2005)
2. Kim, K.J., Duong, T.Q., Poor, H.V.: Performance analysis of cyclic prefixed single-carrier cognitive amplify-and-forward relay systems. IEEE Trans. Wirel. Commun. **12**(1), 195–205 (2013)
3. Thanh, T.L., Hoang, T.M.: Cooperative spectrum-sharing with two-way AF relaying in the presence of direct communications. EAI Endorsed Trans. Ind. Netw. Intell. Syst. **5**(14), 1–9 (2018)
4. Ding, Z., Peng, M., Poor, H.V.: Cooperative non-orthogonal multiple access in 5G systems. IEEE Commun. Lett. **19**(8), 1462–1465 (2015)
5. Do, N.T., Costa, D.B.D., Duong, T.Q., An, B.: A BNBF user selection scheme for NOMA-based cooperative relaying systems with SWIPT. IEEE Commun. Lett. **21**(3), 664–667 (2017)

6. Islam, S.M.R., Avazov, N., Dobre, O.A., Kwak, K.S.: Power-domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges. IEEE Commun. Surv. Tutor. **19**(2), 721–742 (2017)
7. Nguyen, V.D., Tuan, H.D., Duong, T.Q., Poor, H.V., Shin, O.S.: Precoder design for signal superposition in MIMO-NOMA multicell networks. IEEE J. Sel. Areas Commun. **35**(12), 2681–2695 (2017)
8. Tran, D.D., Tran, H.V., Ha, D.B., Kaddoum, G.: Cooperation in NOMA networks under limited user-to-user communications: solution and analysis. In: IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018 (2018)
9. Lee, S., Duong, T.Q., da Costa, D.B., Ha, D.B., Nguyen, S.Q.: Underlay cognitive radio networks with cooperative non-orthogonal multiple access. IET Commun. **12**(3), 359–366 (2018)
10. Do, T.N., da Costa, D.B., Duong, T.Q., An, B.: Improving the performance of cell-edge users in NOMA systems using cooperative relaying. IEEE Trans. Commun. **66**(5), 1883–1901 (2018)
11. Do, T.N., da Costa, D.B., Duong, T.Q., An, B.: Improving the performance of cell-edge users in MISO-NOMA systems using TAS and SWIPT-based cooperative transmissions. IEEE Trans. Green Commun. Netw. **2**(1), 49–62 (2018)
12. Tuan, H.D., Nasir, A.A., Nguyen, H.H., Duong, T.Q., Poor, H.V.: Non-orthogonal multiple access with improper gaussian signaling. IEEE J. Sel. Topics Signal Process. **13**, 496–507 (2019)
13. Nasir, A.A., Zhou, X., Durrani, S., Kennedy, R.A.: Relaying protocols for wireless energy harvesting and information processing. IEEE Trans. Wireless Commun. **12**(7), 3622–3636 (2013)
14. Ha, D.B., Tran, D.D., Tran-Ha, V., Hong, E.K.: Performance of amplify-and-forward relaying with wireless power transfer over dissimilar channels. Elektronika ir Elektrotechnika J. **21**(5), 90–95 (2015)
15. Du, G., Xiong, K., Qiu, Z.: Outage analysis of cooperative transmission with energy harvesting relay: time switching versus power splitting. Math. Probl. Eng. **2015**, 1–9 (2015)
16. Chen, X., Zhang, Z., Chen, H.H., Zhang, H.: Enhancing wireless information and power transfer by exploiting multi- antenna techniques. IEEE Commun. Mag. **53**(4), 133–141 (2015)
17. Cvetkovic, A., Blagojevic, V., Ivanis, P.: Performance analysis of nonlinear energy-harvesting DF relay system in interference-limited Nakagami-m fading environment. ETRI J. **39**(6), 803–812 (2017)
18. Xu, K., Shen, Z., Wang, Y., Xia, X.: Beam-domain hybrid time-switching and power splitting SWIPT in full-duplex massive MIMO system. EURASIP J. Wirel. Commun. Netw., 1–21 (2018)
19. Lu, X., Wang, P., Niyato, D., Kim, D.I., Han, Z.: Wireless networks with RF energy harvesting: a contemporary survey. IEEE Commun. Surv. Tutor. **17**(2), 757–789 (2014)
20. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)
21. Wyner, A.: The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
22. Bloch, M., Barros, J., Rodrigues, M.R., McLaughlin, S.W.: Wireless information-theoretic security. IEEE Trans. Inf. Tech. **54**(6), 2515–2534 (2008)
23. Liu, Y., Qin, Z., Elkashlan, M., Gao, Y., Hanzo, L.: Enhancing the physical layer security of nonorthogonal multiple access in large-scale networks. IEEE Trans. Wirel. Commun. **16**(3), 1656–1672 (2017)

24. Tran, D.D., Ha, D.B.: Secrecy performance analysis of QoS-based non-orthogonal multiple access networks over nakagami-m fading. In: The International Conference on Recent Advances in Signal Processing, Telecommunications and Computing (SigTelCom), HCMC, Vietnam (2018)
25. Lei, H., Zhang, J., Park, K.H., Xu, P., Ansari, I.S., Pan, G.: On secure NOMA systems with transmit antenna selection schemes. IEEE Access **5**, 17450–17464 (2017)
26. Lv, L., Ding, Z., Ni, Q., Chen, J.: Secure MISO-NOMA transmission with artificial noise. IEEE Trans. Veh. Technol. **67**(7), 6700–6705 (2018)
27. Chen, J., Yang, L., Alouini, M.S.: Physical layer security for cooperative NOMA systems. IEEE Trans. Veh. Technol. **67**(5), 4645–4649 (2018)
28. Kieu, T.N., Tran, D.D., Ha, D.B., Voznak, M.: On secure QoS-based NOMA networks with multiple antennas and eavesdroppers over Nakagami-m fading. IETE J. Res., 1–13 (2019)
29. Tran, D.D., Tran, H.V., Ha, D.B., Kaddoum, G.: Secure transmit antenna selection protocol for MIMO NOMA networks over Nakagami-m channels. IEEE Syst. J., 1–12 (2019)
30. Men, J., Ge, J.: Performance analysic of non-orthogonal multiple access in downlink cooperative network. IET Commun. **9**(18), 2267–2273 (2015)
31. Gradshteyn, I., Ryzhik, I.: Table of Integrals, Series, and Products. Elsevier Academic Press, Cambridge (2007)