Multi-destination Two-Hop Untrusted AF Relay Networks with Destination-Aided Cooperative Jamming

Hui Shi(✉), Weiwei Yang, Yueming Cai, Yongxing Jia, and Wendong Yang

College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
lgdhpkry@aliyun.com

Abstract. We consider a multi-destination two-hop untrusted amplify-and-forward (AF) relay networks, where each node is equipped with a single antenna and the confidential information communication needs the aid of the untrusted relay over the Nakagami-m channel. Because the relay is energy-constrained, the relay needs to harvest energy from the received information and the jamming signals by applying the power splitting relaying (PSR) protocol. The confidential information can be protected from the untrusted relay eavesdropping with destination-aided cooperative jamming. We focus on the secure and reliable performance of the presented system. The secrecy outage probability (SOP) and the connection outage probability (COP) are specially examined, which mainly show in the closed-form expressions of SOP and COP. In addition, the effective secrecy throughput (EST) performance is also investigated to comprehensively measure the secure and reliable performance. Moreover, we also present the asymptotic analysis of EST at the high signal-to-noise ratio (SNR). The Monte Carlo simulation is applied to validate the accuracy of the derived expressions and reveals the effects of different parameters, such as the transmit SNR, the power allocation factor, the fading factor and other parameters on the EST.

Keywords: Multi-destination · Untrusted relay · Energy harvesting · Performance analysis · Power splitting relaying · Nakagami-m fading

1 Introduction

The relaying technique has been applied to improve the throughput and coverage area of wireless communication systems [1–6]. The two main protocols applied in relay systems are amplify-and-forward (AF) and decode-and-forward (DF), respectively [7]. However, due to the constrained energy, the application of the relay is limited. The energy harvesting (EH) has been particularly noticed to prolong the lifetime of the relay [8–11]. The power splitting and time switching methods are the two main energy harvesting methods [12–14]. The power splitting relaying (PSR) protocol is one of the two relaying protocols. The energy

X. B. Zhai et al. (Eds.): MLICOM 2019, LNICST 294, pp. 58–71, 2019.
https://doi.org/10.1007/978-3-030-32388-2_6

harvesting technique has been applied with the relaying technique. In [15], the authors applied the PSR protocol to divide the harvested energy at the relay.

It is well known that the Nakagami-m fading channel is more practical and general when characterizing the fading effect over wireless channels. The literatures in [15–20], the transmissions were Nakagami-m fading channels. In [15,16], all nodes were equipped with a single antenna and the relay was trusted. The authors in [15] focused on a two-way AF communication system, where consisted the source, the destination, and the relay. With harvesting energy from the surrounding radio frequency environment, the relay assisted the transmission between the source and the destination. In [16], the source node transmitted the information to the destination node via the DF relay, where the average symbol error rate was analyzed under two relaying scenarios, i.e., the existence or non-existence of direct link between the source and the destination.

In [17], Mahendra *et al.* analyzed the cellular multiuser two-way relay network, where consisted a multi-antenna base station, a single-antenna trusted relay and several single-antenna mobile stations. The overall outage probability expressions and optimal power allocation were investigated. In [18], the authors considered a dual-hop multiple-input multiple-output (MIMO) relay system, where each node was equipped with multiple antennas. The eavesdropper could intercept the transmission between the source and the destination, aided by the trusted relay under the DF protocol. The authors examined the secrecy outage probability and ergodic secrecy rate to evaluate the secrecy performance. Fan *et al.* [19] studied the system outage probability in the multiple AF relay network, where the best relay was chosen to maximize the received signal-to-noise ratio (SNR) at the destination. In [20], both antenna and relay selection were jointed to improve the system capacity, and the outage probability expression was examined.

However, when assisting the confidential information transmission, the relay may eavesdrop or decode the information at the same time. Utilizing the inherent nature of wireless channels, the secure communications could be realized with the physical-layer security (PLS) technology.

The works in [21], the authors investigated the secrecy outage probability (SOP) of the dual-hop AF untrusted relay networks with a single destination, besides the minimal SOP with optimal power allocation scheme. However, the authors just presented the tight closed-form and asymptotic expressions for the lower and upper bounds of SOP under Nakagami-m fading channels, rather than the closed-form expression of the SOP. The authors in [22] considered the secure communication in nonorthogonal multiple access (NOMA) networks with an untrusted AF relay, where the exact and asymptotic expressions for effective secrecy throughput (EST) over Nakagami-m fading was derived. In the first time slot, one of the two users were chosen to transmit the jamming signal to protect the information. Distinguished from the works in [22], our works considered all the destinations transmitted the jamming signals to the untrusted relay, without the user choice.

To the best of our knowledge, the connection outage probability (COP) and EST performance in the multi-destination two-hop untrusted AF relay networks have been relatively litter analyzed in the literatures. Motivated by this, the paper examines the multi-destination two-hop untrusted AF relay networks, where all nodes have a single antenna and the untrusted relay assists the confidential information communication between the source and the destinations over the Nakagami-m channel. In view of the untrusted relay may eavesdrop the confidential information when forwarding the information to the destinations, the destination-aided cooperative jamming technique is considered. The SOP, COP and EST performance are investigated to evaluate the secure transmission in the proposed system. The main contributions can be summarized as follows.

- We derive the closed-form expressions of SOP, COP, and EST in the multi-destination two-hop untrusted AF relay networks with destination-aided cooperative jamming over Nakagami-m fading channel. Moreover, we also derive the closed-form asymptotic expression for the EST at the high transmit SNR. The accuracy of these expressions are verified by the Monte Carlo simulations.
- The simulation results show that the EST increases with gradually increasing the transmit SNR and then tends to the constant, which can be validated by the asymptotic analysis of the EST. The number of the destinations can improve the EST to some extent. The simulations also demonstrate how the other parameters affect the EST.

The remainder of the paper is organized as follows. Section 2 describes the proposed system model and the secure communication process. Section 3 presents the analytical expressions for the SOP, COP, and EST, as well as the asymptotic analytical expression for the EST. In Sect. 4, we validate the derived expressions with the Monte Carlo simulation and illustrate the parameters impact on the EST. Finally, Sect. 5 summarizes the conclusions.

2 System Model

Consider a one-source multi-destination two-hop untrusted relay network depicted in Fig. 1. Each node is equipped with a single antenna and in a half-duplex mode. Assuming that the direct links between the source S and the destinations D_n ($n \in \{1, ..., N\}$) are unavailable [10], thus all the communications are aided by the untrusted relay R, which is assumed to be honest but curious. The channels between the source and the relay, the relay and the destinations are subject to the Nakagami-m fading, distributed independently and identically, denoted by h_{SR} and $\mathbf{h_{RD}} \in \mathbb{C}^{1\times N}$ with parameters $\bar{\gamma}_{SR}$ and $\bar{\gamma}_{RD}$, respectively ($\mathbf{h_{RD}} = \mathbf{h_{DR}}$ [23,24]). The N destinations are close to each other and subject to the same Nakagami-m fading.

Applying PSR protocol, the total transmitted power P of the system is divided into two parts with the power allocation factor $\beta \in (0, 1)$. The information communication between the S and the D_n is divided into two equal

hops. In the first hop $T/2$, the S transmits the confidential information to R with power βP, meanwhile, all the destinations D_n apply the maximal ratio transmission (MRT) technique to send the jamming signals to R with power $(1-\beta)P$, making it impossible for the R to eavesdrop the confidential information. The R splits the received signal power into two parts with the power splitting factor $\rho \in (0,1)$. The ρ part of the received signal power is applied to harvest energy and the remaining part is utilized to transmit the information.

Then the received instantaneous signal-to-interference-plus-noise ratio (SINR) at the R is given by

$$\gamma_R = \frac{(1-\rho)\beta\lambda X}{(1-\rho)(1-\beta)\lambda Y + 1}, \tag{1}$$

where $X = |h_{SR}|^2$, $Y = \|\mathbf{h_{DR}}\|^2$, $\lambda = P/N_0$. λ is the transmit SNR, and the N_0 denotes the zero mean additive white Gaussian noise (AWGN) power at the relay. $\|\bullet\|$ represents the Frobenius Norm.

Therefore, the transmit power at the R can be expressed as

$$P_R = \omega\eta\rho PG, \tag{2}$$

where $G = \beta X + (1-\beta)Y$. The parameters ω and η denote the allocation factor of the harvested energy and the energy conversion efficiency factor of the harvested energy at the R, respectively. Both ω and η range from 0 to 1.

The harvested energy at the R is divided into ω and $(1-\omega)$ parts. The ω proportion is applied for forwarding the confidential information to D_n and the other proportion is utilized to eavesdrop and decode consumption.

In the second hop, the R amplifies and forwards the information to D_n with the normalization factor $1/\sqrt{PG+N_0}$, and the D_n receive the information with

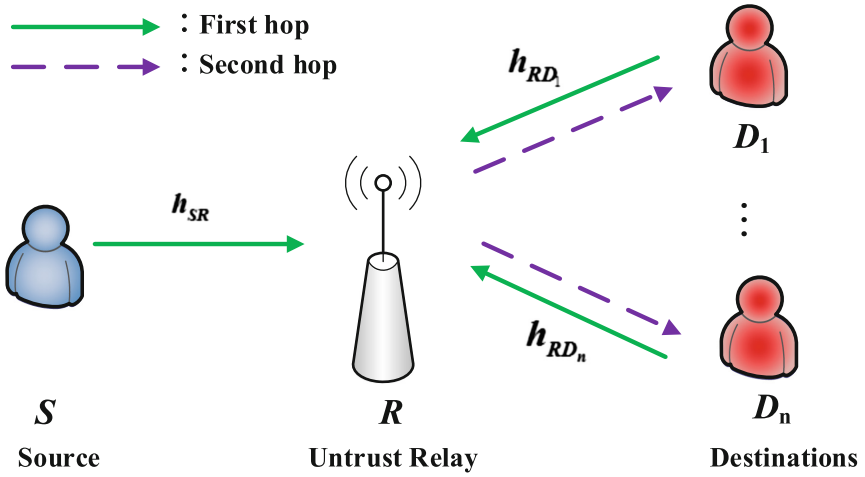

Fig. 1. System model.

maximal ratio combining (MRC) technique. Then the received instantaneous SINR of D_n is given by

$$\gamma_D \approx \frac{\omega\eta\rho(1-\rho)\beta\lambda XY}{\omega\eta\rho Y + 1 - \rho}. \tag{3}$$

where the approximation bases on the fact that 1 item could be neglected campared with $((\omega\eta\rho Y + 1 - \rho)\,\lambda G)$, when the SNR is high compared with the transmit power and channel gains [10,23,25].

3 Performance Analysis

Firstly, we derive the closed-form expressions for the SOP and the COP to evaluate the secure and the reliable performance. Then the closed-form expression and the asymptotic analysis at high transmit SNR of EST are also applied to evaluate the comprehensive performance of the system.

3.1 Preliminaries

Notations: Both $X = |h_{SR}|^2$ and $Y = \|\mathbf{h_{DR}}\|^2$ undergo the Nakagami-m fading distribution, therefore, the probability density function (PDF) of X and Y can be therefore given by

$$f(x) = \left(\frac{m_1}{\bar{\gamma}_{SR}}\right)^{m_1} \frac{x^{m_1-1} e^{-\frac{m_1 x}{\bar{\gamma}_{SR}}}}{\Gamma(m_1)} \tag{4}$$

and

$$f_N(y) = \left(\frac{m_2}{\bar{\gamma}_{RD}}\right)^{m_2 N} \frac{y^{m_2 N-1} e^{-\frac{m_2 y}{\bar{\gamma}_{RD}}}}{\Gamma(m_2 N)}, \tag{5}$$

where $\Gamma(\bullet)$ is the Gamma function, m_1 and m_2 are the Nakagami-m fading parameters for the channel between S and R, between R and D_n. Both m_1 and m_2 range from $1/2$ to ∞. Obviously, when $m_1 = 1$, the Nakagami-m distribution is Rayleigh fading distribution.

3.2 Secrecy Outage Probability

The secrecy outage event may occur when the channel capacity of the untrusted relay is higher than the positive difference between the codeword transmission rate R_{ct} and the confidential information rate R_{ci}, which is the definition of the SOP. Therefore, the SOP is given by

$$P_{SOP} = \mathbf{Pr}\{C_R > R_{dif}\}, \tag{6}$$

where $C_R = 1/(2\log_2(1+\gamma_R))$, $R_{dif} = R_{ct} - R_{ci}$.

Plugging (1) into (6), (6) can rewritten as

$$P_{SOP} = \mathbf{Pr}\left\{X > \frac{(1-\beta)\vartheta_1 Y}{\beta} + \frac{\vartheta_1}{(1-\rho)\beta\lambda}\right\} = \int_0^{\infty}\int_{X_1}^{\infty} f(x)f_N(y)\mathrm{d}x\mathrm{d}y, \tag{7}$$

where $X_1 = \frac{(1-\beta)\vartheta_1 Y}{\beta} + \frac{\vartheta_1}{(1-\rho)\beta\lambda}$, $\vartheta_1 = 2^{2R_{dif}} - 1$.

Substituting (4) and (5) into (7), the close-form expression of the SOP can be calculated as

$$P_{SOP} = \sum_{i=0}^{m_1-1}\sum_{k=0}^{i}\binom{i}{k}\frac{1}{i!}(m_2)^{m_2N}(m_1\vartheta_1)^i e^{-\frac{m_1\vartheta_1}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}} \times \frac{\Gamma(m_2N+k)(\beta\bar{\gamma}_{SR})^{m_2N+k-i}((1-\rho)\lambda)^{k-i}((1-\beta)\bar{\gamma}_{RD})^k}{\Gamma(m_2N)((1-\beta)m_1\vartheta_1\bar{\gamma}_{RD} + m_2\beta\bar{\gamma}_{SR})^{m_2N+k}}. \tag{8}$$

The Eq. (8) shows that the SOP is associated with the fading factors m_1 and m_2, the number of the destinations N, the power allocation factor β, the power splitting factor ρ and other parameters.

3.3 Connection Outage Probability

The connection outage event would occur when the channel capacity of the destinations is less than the R_{ct}, which is the definition of the COP. Thus, the COP is given by [26].

$$P_{COP} = \mathbf{Pr}\{C_D < R_{ct}\}, \tag{9}$$

where $C_D = \log_2(1+\gamma_D)/2$.

Substituting (3) into (9), the expression of the COP can be rewritten as

$$P_{COP} = \mathbf{Pr}\left\{X < \frac{\vartheta_2}{(1-\rho)\beta\lambda} + \frac{\vartheta_2}{\omega\eta\rho\beta\lambda Y}\right\} = \int_0^{\infty}\int_0^{X_2} f(x)f_N(y)\mathrm{d}x\mathrm{d}y, \tag{10}$$

where $X_2 = \frac{\vartheta_2}{(1-\rho)\beta\lambda} + \frac{\vartheta_2}{\omega\eta\rho\beta\lambda Y}$, $\vartheta_2 = 2^{2R_{ct}} - 1$.

Substituting (4) and (5) into (10), the closed-form expression of the COP can be obtained as

$$P_{COP} = 1 - \sum_{i=0}^{m_1-1}\sum_{k=0}^{i}\binom{i}{k}\frac{1}{i!}\frac{2e^{\frac{-m_1\vartheta_2}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}}(m_1\vartheta_2)^{\frac{m_2N+2i-k}{2}}}{\Gamma(m_2N)(1-\rho)^{i-k}} \times \frac{(m_2)^{\frac{k+m_2N}{2}}\mathrm{K}_{(m_2N-k)}\left(\sqrt{\frac{4m_1m_2\vartheta_2}{\omega\eta\rho\beta\lambda\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right)}{(\beta\lambda\bar{\gamma}_{SR})^{\frac{m_2N+2i-k}{2}}(\omega\eta\rho\bar{\gamma}_{RD})^{\frac{m_2N+k}{2}}}, \tag{11}$$

where $\mathrm{K}_z(\bullet)$ represents the z^{th} order modified Bessel functions of second kind.

Equation (11) indicates that the COP is related to the fading factors, the number of the destinations, the allocation factor of the harvested energy ω, the energy conversion efficiency factor η and other parameters.

3.4 Effective Secrecy Throughput

The confidential information needs to be secure and reliable when transmitted between the S and the D_n, aided by the untrusted relay. To measure the secure and reliable performance of the transmission information, the EST is defined as follows.

$$\begin{aligned}\zeta &= \frac{R_{ci}}{2}\mathbf{Pr}\left\{C_R < R_{dif}, C_D > R_{ct}\right\} \\ &= \frac{R_{ci}}{2}\left\{X < \frac{(1-\beta)\vartheta_1 Y}{\beta} + \frac{\vartheta_1}{(1-\rho)\beta\lambda},\ X > \frac{\vartheta_2}{(1-\rho)\beta\lambda} + \frac{\vartheta_2}{\omega\eta\rho\beta\lambda Y}\right\} \\ &= \frac{R_{ci}}{2}\int_u^{\infty}\int_{X_2}^{X_1} f(x)dx f_N(y)dy, \end{aligned} \tag{12}$$

where $u = \left(b + \sqrt{b^2 + 4ac}\right)/2a$, $a = \omega\eta\rho\lambda(1-\rho)(1-\beta)\vartheta_1$, $b = \omega\eta\rho(\vartheta_2 - \vartheta_1)$, and $c = (1-\rho)\vartheta_2$.

Based on (4) and (5), and after some manipulations, the closed-form expression of EST is calculated as

$$\zeta^{PSR} = \frac{R_{ci}}{2}\left\{\Xi_1 - \Xi_2\right\}, \tag{13}$$

where Ξ_1 and Ξ_2 are given by

$$\begin{aligned}\Xi_1 = &\sum_{i=0}^{m_1-1}\sum_{k=0}^{i}\sum_{j=0}^{\infty}\binom{i}{k}(-1)^j\frac{1}{i!j!}e^{\frac{-m_1\vartheta_2}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}}\left(\frac{m_1\vartheta_2}{\beta\lambda\bar{\gamma}_{SR}}\right)^{i+j}\left(\frac{m_2}{\omega\eta\rho\bar{\gamma}_{RD}}\right)^{k+j} \\ &\times\frac{\Gamma\left(m_2N - j - k, \frac{m_2u}{\bar{\gamma}_{RD}}\right)}{\Gamma(m_2N)(1-\rho)^{i-k}}\end{aligned} \tag{14}$$

and

$$\begin{aligned}\Xi_2 = &\sum_{i=0}^{m_1-1}\sum_{k=0}^{i}\binom{i}{k}\frac{1}{i!}\frac{e^{-\frac{m_1\vartheta_1}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}}(m_1\vartheta_1)^i(m_2)^{m_2N}((1-\beta)\bar{\gamma}_{RD})^k(\beta\bar{\gamma}_{SR})^{m_2N+k-i}}{\Gamma(m_2N)((1-\rho)\lambda)^{i-k}((1-\beta)m_1\vartheta_1\bar{\gamma}_{RD} + m_2\beta\bar{\gamma}_{SR})^{m_2N+k}} \\ &\times\Gamma\left(m_2N + k, \frac{((1-\beta)m_1\vartheta_1\bar{\gamma}_{RD} + m_2\beta\bar{\gamma}_{SR})u}{\beta\bar{\gamma}_{SR}\bar{\gamma}_{RD}}\right).\end{aligned} \tag{15}$$

When $\lambda \to \infty$, the asymptotical expression of EST can be given by

$$\lim_{\lambda\to\infty} \zeta = \frac{\mathrm{R}_{ci}}{2}\left\{1 - \sum_{i=0}^{m_1-1} \frac{1}{i!}\frac{\Gamma\left(m_2N+i\right)\left(m_2\beta\bar{\gamma}_{SR}\right)^{m_2N}\left(\left(1-\beta\right)m_1\vartheta_1\bar{\gamma}_{RD}\right)^{i}}{\Gamma\left(m_2N\right)\left(\left(1-\beta\right)m_1\vartheta_1\bar{\gamma}_{RD}+m_2\beta\bar{\gamma}_{SR}\right)^{m_2N+i}}\right\}. \tag{16}$$

4 Numerical Results

In this section, we present the numerical results of the SOP, COP, and EST under different parameters to demonstrate the secure and reliable performance of the proposed system. Without loss of generality, the parameters in each figure are set as $N = 3$, $\beta = 0.5, \rho = 0.5, \omega = 0.9, \eta = 0.5$, $R_{ct} = 2$bit/s/Hz, $R_{ci} = 1$bit/s/Hz. It is assumed that the fading factors are the same, i.e., $m_1 = m_2$. The solid curves denote the numerical analysis, and the symbols '□', 'o' and '∇' represent the figures under the fading factors $m = 1$, $m = 2$, $m = 4$, successively.

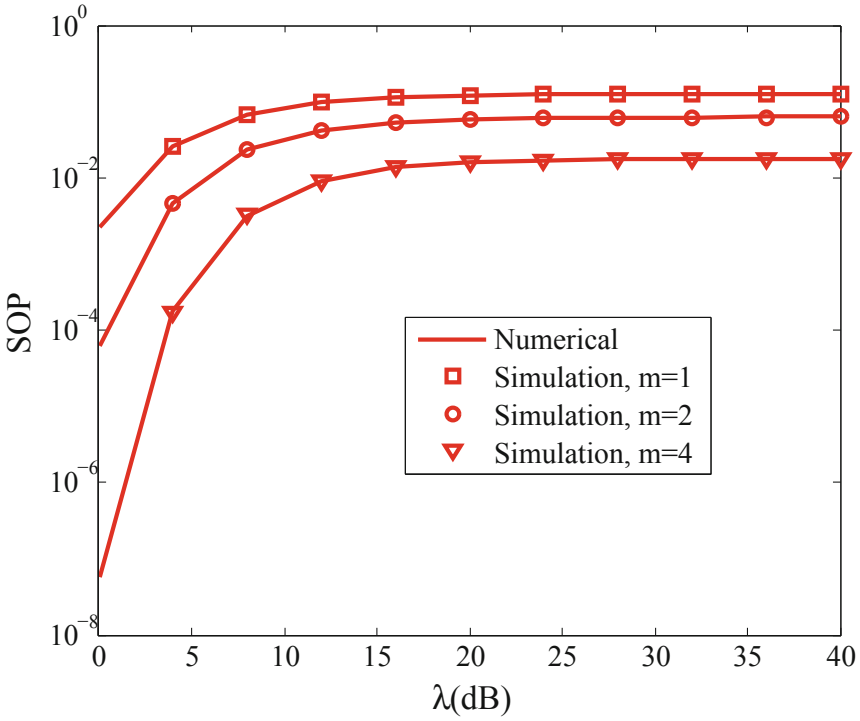

Fig. 2. The SOPs versus λ.

Figures 2 and 3 show the SOPs and COPs of the proposed system with various values of the transmit SNR λ, respectively. It is observed that: (1) When the transmit SNR λ increases, the SOPs increase and then approaches the constant. The reason is that the untrusted relay R can acquire more confidential information with λ increase at first. However, when λ is high, the destinations send the jamming signals to protect the information from eavesdropping. (2) The COPs decrease with increasing λ. It is due to that the destinations can receive more confidential information in the higher the transmit SNR regime. (3) With increasing the value of the fading factor, the channel fading gradually becomes smaller, which leads to decrease the SOP and the COP.

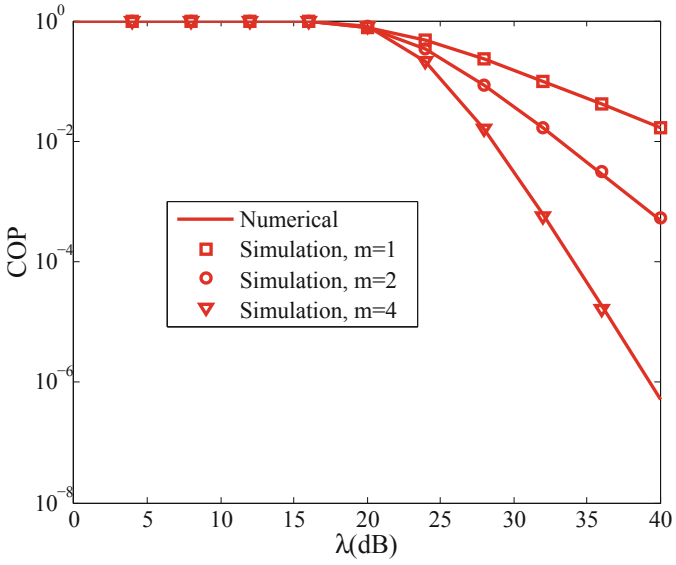

Fig. 3. The COPs versus λ.

In Fig. 4, the ESTs are presented as the function of the transmit SNR λ for the different fading factor m. The corresponding EST asymptotic analysis curves are demonstrated with the dashed lines. Two observations can be obtained as follows. (1) When the fading factors are fixed, the ESTs gradually increase with increasing the transmit SNR λ. The net result is that the EST tends to a constant, which can be validated by the asymptotic analysis curves. (2) When the transmit SNR λ is fixed, it is obvious that the ESTs increase with increasing the fading factor values. The reason is the same as the Figs. 2 and 3.

Figure 5 plots the impact of the number of the destinations on the ESTs. We observe that the ESTs become larger by increasing the number of the destinations N firstly. However, when the number N is larger than 20, the ESTs increase slowly, at this moment, it does not make much sense to increase the number N of the destinations anymore.

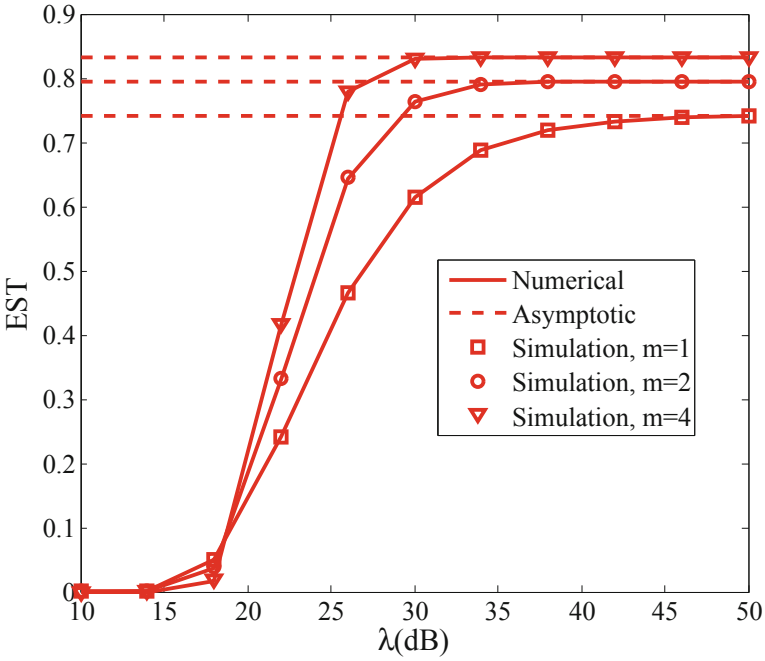

Fig. 4. The ESTs versus λ.

Figures 6 and 7 show the ESTs under different values of the power splitting factor ρ and the power allocation factor β, respectively. It is observed that the ESTs increase firstly and then turn to decrease along with increasing the parameters ρ and β. Therefore, there are the optimal values ρ and β, which could maximize the ESTs. The larger power splitting factor ρ demonstrates that the received signal power at R applied to harvest energy is larger, on the contrary, the received signal power at R utilized to transmit the information is smaller. The power allocation factor β is bigger, the power applied to transmit the confidential information to R is larger. Conversely, the power utilized to transmit the jamming signals to R is smaller. Figure 8 describes the EST versus both the parameters ρ and β in detail.

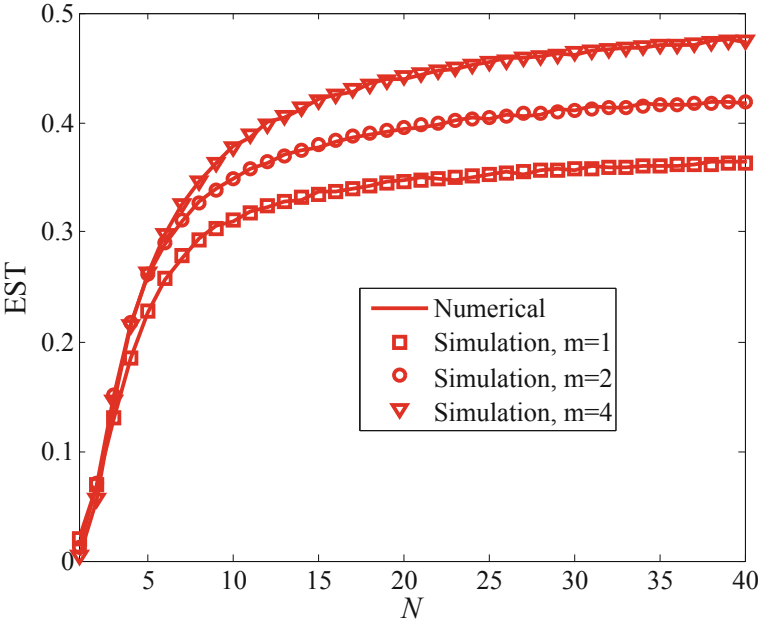

Fig. 5. The ESTs versus N.

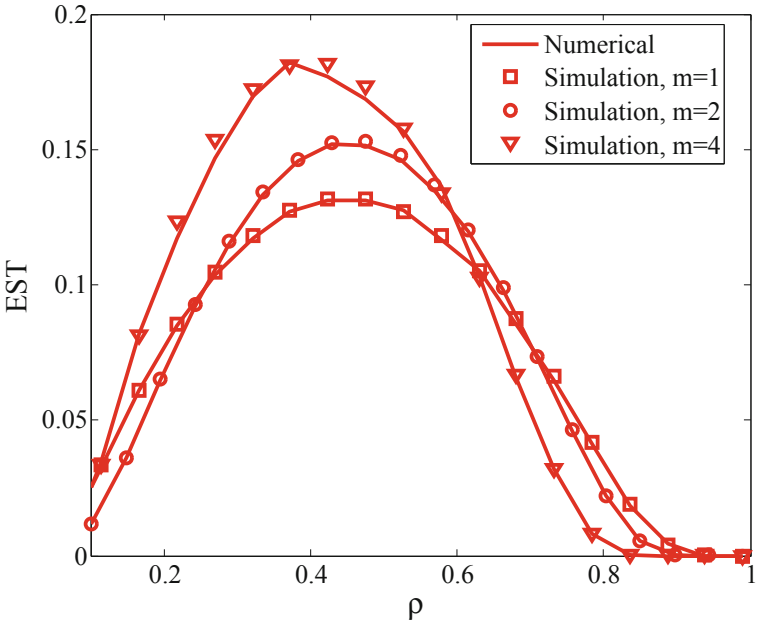

Fig. 6. The ESTs versus ρ.

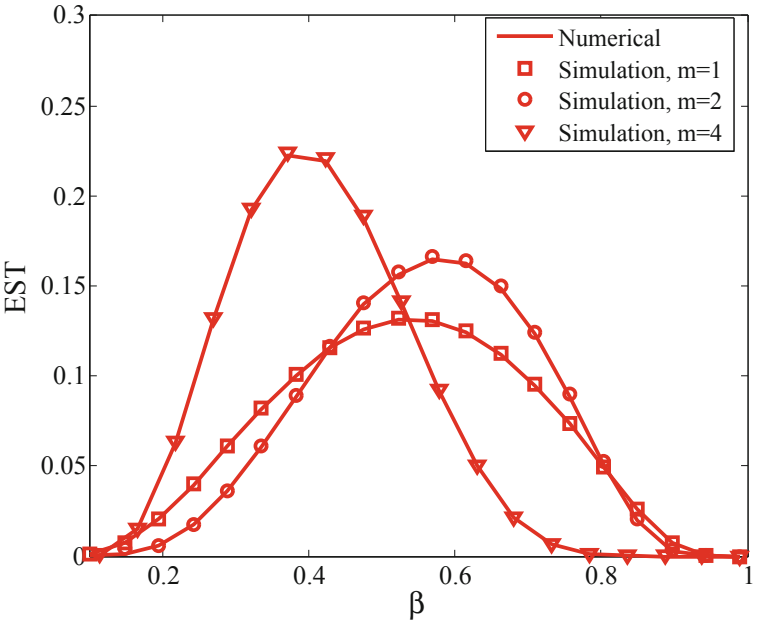

Fig. 7. The ESTs versus β.

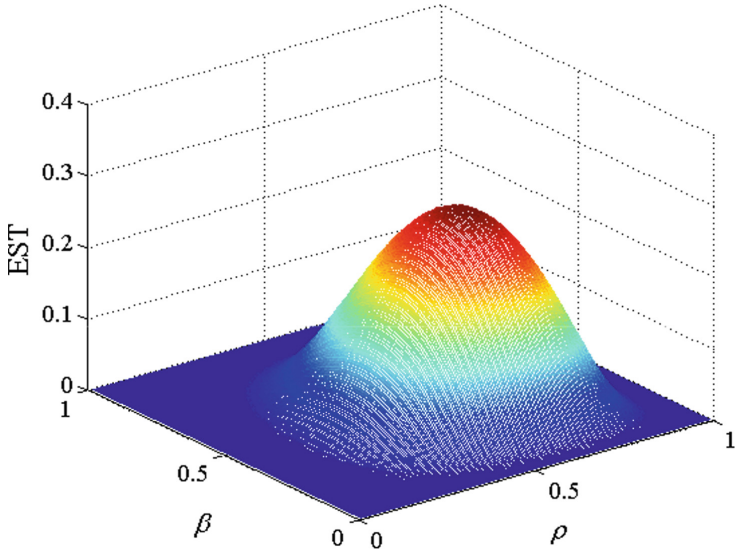

Fig. 8. The EST versus ρ and β with $m = 2$.

5 Conclusion

The multi-destination two hops untrusted and energy-limited relay network over Nakagami-m channel is proposed and analyzed. In the proposed networks, all the nodes are equipped with a single antenna, the untrusted relay can harvest energy both from the confidential information and the jamming signals. The destination-aided cooperative jamming is utilized to prevent the untrusted relay from eavesdropping. The closed-form expressions of the SOP, COP, and EST have been derived under different fading factors, as well as the asymptotic expressions of EST. The Monte Carlo simulations show that the effect of different parameters on the EST performance. In the future work, we will extend this work to analyze the performance of multiple untrusted relays, multiple destinations and multiple antennas communications scenario.

References

1. Hasna, M.O., Alouini, M.: End-to-end performance of transmission systems with relays over Rayleigh-fading channels. IEEE Trans. Wirel. Commun. **2**(6), 1126–1131 (2003)
2. Pabst, R., Walke, B., Schultz, D.C., et al.: Relay-based deployment concepts for wireless and mobile broadband radio. IEEE Commun. Mag. **42**(9), 80–89 (2004)
3. Ye, Y., Li, Y., et al.: Dynamic asymmetric power splitting scheme for SWIPT-based two-way multiplicative AF relaying. IEEE Signal Process. Lett. **25**(7), 1014–1018 (2018)
4. Zhang, Z., Ma, Z., Ding, Z., et al.: Full-duplex two-way and one-way relaying: average rate, outage probability, and tradeoffs. IEEE Trans. Wirel. Commun. **15**(6), 3920–3933 (2016)
5. Peng, C., Li, F., Liu, H., et al.: Optimal power splitting in two-way decode-and-forward relay networks. IEEE Commun. Lett. **21**(9), 2009–2012 (2017)
6. Van Nguyen, B., Kim, K.: Secrecy outage probability of optimal relay selection for secure AnF cooperative networks. IEEE Commun. Lett. **19**(12), 2086–2089 (2015)
7. Peter Hong, Y.-W., Huang, W.-J., et al.: Cooperative Communications and Networking. Springer, New York (2014)
8. Ulukus, S., Yener, A., Erkip, E., et al.: Energy harvesting wireless communications: a review of recent advances. IEEE J. Sel. Areas Commun. **33**(3), 360–381 (2015)
9. Qi, N., Xiao, M., Tsiftsis, T.A., et al.: Efficient coded cooperative networks with energy harvesting and transferring. IEEE Trans. Wirel. Commun. **16**(10), 6335–6349 (2017)
10. Nasir, A.A., Zhou, X., Durrani, S., et al.: Relaying protocols for wireless energy harvesting and information processing. IEEE Trans. Wirel. Commun. **12**(7), 3622–3636 (2013)
11. Yao, R., Xu, F., Mekkawy, T., et al.: Optimised power allocation to maximise secure rate in energy harvesting relay network. Electron. Lett. **52**(22), 1879–1881 (2016)
12. Liu, L., Zhang, R., Chua, K.C., et al.: Wireless information and power transfer: a dynamic power splitting approach. IEEE Trans. Commun. **61**(9), 3990–4001 (2013)
13. Zhou, X., Zhang, R., Ho, C.K., et al.: Wireless information and power transfer: architecture design and rate-energy tradeoff. IEEE Trans. Commun. **61**(11), 4754–4767 (2013)

14. Liu, L., Zhang, R., Chua, K.C., et al.: Wireless information transfer with opportunistic energy harvesting. IEEE Trans. Wirel. Commun. **12**(1), 288–300 (2013)
15. Bao, V.N., Van Toan, H., Le, K.N., et al.: Performance of two-way AF relaying with energy harvesting over Nakagami-m fading channels. IET Commun. **12**(20), 2592–2599 (2018)
16. Kumar, P., Dhaka, K.: Performance analysis of wireless powered DF relay system under Nakagami-m fading. IEEE Trans. Veh. Technol. **67**(8), 7073–7085 (2018)
17. Shukla, M.K., Yadav, S., Purohit, N., et al.: Performance evaluation and optimization of traffic-aware cellular multiuser two-way relay networks over Nakagami-m fading. IEEE Syst. J. **12**(2), 1933–1944 (2018)
18. Zhao, R., Lin, H., He, Y., et al.: Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI. IEEE Trans. Commun. **66**(2), 546–559 (2018)
19. Fan, L., Zhao, N., Lei, X., et al.: Outage probability and optimal cache placement for multiple amplify-and-forward relay networks. IEEE Trans. Veh. Technol. **67**(12), 12373–12378 (2018)
20. Zhang, Y., Ge, J.: Joint antenna-and-relay selection in MIMO decode-and-forward relaying networks over Nakagami-m fading channels. IEEE Signal Process. Lett. **24**(4), 456–460 (2017)
21. Ding, F., Wang, H., Zhou, Y., et al.: Impact of relays eavesdropping on untrusted amplify-and-forward networks over Nakagami-m fading. IEEE Wirel. Commun. Lett. **7**(1), 102–105 (2018)
22. Xiang, Z., Yang, W., Pan, G., et al.: Secure transmission in non-orthogonal multiple access networks with an untrusted relay. IEEE Wirel. Commun. Lett. 1 (2019)
23. Kalamkar, S.S., Banerjee, A.: Secure communication via a wireless energy harvesting untrusted relay. IEEE Trans. Veh. Technol. **66**(3), 2199–2213 (2017)
24. Huang, J., Mukherjee, A., Swindlehurst, A.L., et al.: Secure communication via an untrusted non-regenerative relay in fading channels. IEEE Trans. Signal Process. **61**(10), 2536–2550 (2013)
25. Wang, Z., Chen, Z., Xia, B., et al.: Cognitive relay networks with energy harvesting and information transfer: design, analysis, and optimization. IEEE Trans. Wirel. Commun. **15**(4), 2562–2576 (2016)
26. Chen, D., Cheng, Y., Yang, W., et al.: Physical layer security in cognitive untrusted relay networks. IEEE Access **6**, 7055–7065 (2018)