Secure Communications in Three-Step Two-Way Energy Harvesting DF Relaying

DOI:
10.1109/LCOMM.2017.2772244

Document Version
Accepted author manuscript

Secure Communications in Three-step Two-way Energy Harvesting DF Relaying

Furqan Jameel, Shurjeel Wyne, and Zhiguo Ding

Abstract

Energy harvesting relaying is predicted to play a pivotal role in large scale energy constrained networks. This letter evaluates the secrecy performance of a system that employs a three-step two-way decode-and-forward relay with the energy harvesting capability. More specifically, we derive a closed-form expression for the eavesdropping probability when the main and wiretap links experience independent $\kappa-\mu$ shadowed fading. We evaluate the impact of the fading parameters, and the power splitting factor at the relay, on the secrecy performance. Our results indicate that for a small relay reception interval, secrecy can be enhanced by allocating more power for information decoding. Numerical results are provided to validate the derived results.

Index Terms

Three-step two-way decode-and-forward relay, Intercept probability, Power splitting.

I. Introduction

Cooperative systems that employ relays can extend the radio coverage significantly compared to non-cooperative systems. The application of the simultaneous wireless information and power transfer (SWIPT) strategy to relaying can maximize the lifetime of energy constrained relays [1]. The authors in [1] considered a system with multiple energy-harvesting (EH) decode-and-forward (DF) relays. They proposed three relay selection methods and demonstrated that when the DF relays are clustered close to the source, the same diversity gain as that with conventional self-powered relays can be achieved. In [2], the authors compared the secrecy performance of DF and amplify-and-forward (AF) relays equipped with a power-splitting architecture for EH. They showed that the DF relaying outperforms AF relaying by achieving a smaller secrecy outage probability for different values of the power-splitting factor. The two-way relaying (TWR), which describes the information exchange between two nodes sharing a common relay, can alleviate the spectral efficiency constraints of one-way relaying with half-duplex (HD) nodes. The TWR can be performed either in 2 steps, i.e., the relay receives signals from both source nodes in step one and transmits to both nodes in step two; or in 3 steps, i.e., the relay receives signals from both source nodes in two orthogonal channel uses and transmits to both nodes in the third channel use [3]. The increased spectral efficiency of the 2-step scheme comes at the price of multiple-access interference suffered by the relay when both source nodes use the same transmission frequency. On the other hand, the 3-step scheme trades-off the spectral efficiency against lesser interference and allows for a simpler relay design [3]. Secure communications in two-way DF relaying networks has been studied extensively [4], [5]. In [4] an optimal relay selection scheme was proposed to increase the secrecy capacity of a two-way DF relaying network. In [5], the authors proposed a secure transmission scheme in the presence of an untrusted DF relay. They provided a secure key exchange method and showed that the secrecy performance can be enhanced by increasing the buffer size of the secret key queue. Recently in [3], the authors investigated 3-step two-way DF (TT-DF) relaying with EH capability at the relay. They derived an analytical expression for the throughput and showed that the TT-DF relaying achieves a higher throughput than the two-way multiplicative relaying scheme.

The $\kappa-\mu$ shadowed fading distribution accurately models the fading in practical scenarios such as device-to-device communications under human shadowing [6] and land mobile satellite communications [7]. The $\kappa-\mu$ shadowed distribution is a clustered multipath model that also includes shadow fading [8]. The κ parameter is a ratio between the sum powers of the dominant cluster paths and the diffuse cluster paths, μ is the number of clusters. The distribution parameter m represents shadowing variance with an increasing m corresponding to a smaller shadowing

This work was supported by the EU-funded project ATOM-690750, approved under call H2020-MSCA-RISE-2015. The associate editor coordinating the review of this letter and approving it for publication was Yansha Deng. (Corresponding author: Shurjeel Wyne.)

F. Jameel and S. Wyne are with the Department of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad 45550, Pakistan (e-mail: shurjeel.wyne@comsats.edu.pk).

Z. Ding is with the School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, U.K.

variance. This distribution includes other conventional models such as Nakagami-m and Shadowed Rician as its special cases [8]. This work aims to investigate the secrecy performance of a TT-DF EH relaying system, Our novel contributions are listed as follows:

- A closed-form expression for the intercept probability of a TT-DF EH relaying system is derived.
- The impact of $\kappa-\mu$ shadowed fading parameters on the secrecy performance of the system is evaluated.

To the authors' best knowledge, this is the first work to evaluate the secrecy performance of TT-DF EH relaying for $\kappa-\mu$ shadowed fading links. The remainder of this paper is organized as follows. In Sec. II the system model is given, followed by Sec. III that contains derivation of the intercept probability. In Sec. IV numerical results are provided. Finally, Sec. V concludes this work.

II. SYSTEM MODEL

Consider nodes A and B exchange information through a shared relay node R in the presence of a single eavesdropper E, as shown in Fig. 1. Assume all nodes operate in the HD mode and are equipped with single antennas. The direct link between A and B is considered in deep fade such that these nodes cannot communicate directly. Let $h_{ij}\ \forall\ i,j \in \{A,B,E,R\}$ and $i \neq j$ denote the $\kappa-\mu$ shadowed channel gains between the respective nodes in a quasi-static fading model. Furthermore, channel reciprocity is assumed such that $h_{ij}=h_{ji}$. We consider R to be pre-selected based on its ability to successfully decode the corresponding messages of A and B [9]. Moreover, A, B, E, and R are assumed to have the channel state information (CSI) for their respective links. The eavesdropper itself is assumed to be a legitimate receiver in the network for some signals and acts as an eavesdropper for others as in a multicast and unicast scenario so that its CSI is available in the system [10]. Each quasi-static fading block of time duration T units is sub-divided into three intervals as shown in Fig. 1. During the first two intervals $T_1=T_2=T\alpha$, $0\leq\alpha<0.5$, the relay operates in reception mode while for the remaining time $T_3=T(1-2\alpha)$, it broadcasts its received information. During the reception mode, the radio-frequency (RF) signal received at R is power-split into two streams: one stream with power ratio $0\leq\rho\leq1$, is used for EH while the other stream with fractional power $(1-\rho)$ is used for information decoding (ID). Consider the relayed transmission between the links

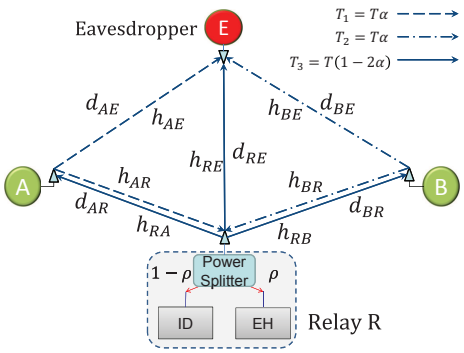

Fig. 1. System Model.

A→R→B. During T_1, A transmits the message s_A with power P_A and the signal received at R is given by

$$y_{AR}=\sqrt{\frac{P_A}{d_{AR}^{\eta}}}h_{AR}s_A+n_{AR}, \tag{1}$$

where d_{AR} is the separation distance between A and R, η is the pathloss exponent, and n_{AR} is the zero-mean additive white Gaussian noise (AWGN) with variance N_0 due to the receiver electronics at R. Without loss of generality we assume $P_A=P_B=P$ throughout this work. The EH relay uses a fixed power-splitting factor ρ to split the received RF power into two parts: $\sqrt{1-\rho}\left(\sqrt{\frac{P_A}{d_{AR}^{\eta}}}h_{AR}s_A+n_{AR}\right)$ is used for ID, while the fractional power $\sqrt{\rho}\left(\sqrt{\frac{P_A}{d_{AR}^{\eta}}}h_{AR}s_A+n_{AR}\right)$ is used for EH. The fixed-value ρ at R affords a simple and inexpensive hardware architecture [3]. The amount of harvested energy during T_1 and T_2 is $E=2\rho\alpha\zeta TP\left(\frac{|h_{AR}|^2}{N_0d_{AR}^{\eta}}+\frac{|h_{RB}|^2}{d_{RB}^{\eta}N_0}\right)$, where d_{RB} is the separation distance between R and B, and $0<\zeta<1$ denotes the energy harvesting efficiency of R.

The signals received at R, from A and B, are decoded and then re-encoded using an appropriate network coding scheme [11]. In the third time slot T_3, R uses $\tilde{P}$ the power harvested during T_1 and T_2 to broadcast the signal $s = \frac{\breve{s}_A + \breve{s}_B}{\sqrt{2}}$, where $\breve{s}_A$ and $\breve{s}_B$ are the decoded signals from A and B during the first two time slots. Since B already knows its own transmitted signal, it can detect the signal of A by using an appropriate self-interference cancellation scheme [3]. The signal received at B can be written as

$$y_{RB} = \sqrt{\frac{\tilde{P}}{d_{RB}^{\eta}}} h_{RB} \frac{\breve{s}_A}{\sqrt{2}} + n_{RB}, \tag{2}$$

where $\tilde{P} = \left(\frac{\zeta \rho \alpha P}{1-2\alpha}\right) \left(\frac{d_{BR}^{\eta}|h_{AR}|^2 + d_{AR}^{\eta}|h_{BR}|^2}{d_{AR}^{\eta} d_{BR}^{\eta}}\right)$. From (1) and (2), the instantaneous signal to noise ratios (SNR)s at R and B are $\gamma_{AR} = \frac{P\zeta(1-\rho)|h_{AR}|^2}{d_{AR}^{\eta} N_0}$ and $\gamma_{RB} = \frac{\tilde{P}|h_{RB}|^2}{2 d_{RB}^{\eta} N_0}$, respectively. Due to the broadcast nature of the wireless transmission from A→R→B, the RF signal is also intercepted twice by a nearby eavesdropper; the instantaneous SNR at the eavesdropper during T_1 is $\gamma_{AE} = \frac{P|h_{AE}|^2}{d_{AE}^{\eta} N_0}$, and during T_3 it is $\gamma_{RE} = \frac{\tilde{P}|h_{RE}|^2}{2 d_{RE}^{\eta} N_0}$.

III. Intercept Probability Analysis

An intercept event occurs when the secrecy capacity becomes negative ($C_{sec} < 0$), i.e., the channel capacity of the main link becomes less than that of the wiretap link and the eavesdropper can successfully decode the source message [12]. A smaller probability of the intercept event, i.e., *intercept probability* is desirable for secure transmission against eavesdropping. Now, for the relayed transmission A→R→B, $C_{sec,1} = \log_2\left\{\frac{1+\gamma_1}{1+\gamma_{e1}}\right\}$, where $\gamma_1 = \min\{\gamma_{AR}, \gamma_{RB}\}$ and $\gamma_{e1} = \gamma_{AE} + \gamma_{RE}$. The eavesdropper's SNR follows from the eavesdropper combining its observations over two hops to create a virtual single-input multiple-output channel for decoding A's message [13]. Similarly, the achievable secrecy capacity for the relayed transmission B→R→A can be written as $C_{sec,2} = \log_2\left\{\frac{1+\gamma_2}{1+\gamma_{e2}}\right\}$, where $\gamma_2 = \min\{\gamma_{BR}, \gamma_{RA}\}$ and $\gamma_{e2} = \gamma_{BE} + \gamma_{RE}$. The end-to-end intercept probability for the transmission A↔R↔B is[1]

$$\begin{aligned} P_{int} &= \Pr\{\min(C_{sec,1}, C_{sec,2}) < 0\} \\ &= \Psi(\bar{\gamma}_{AR}, \bar{\gamma}_{e1}) \Psi(\bar{\gamma}_{RB}, \bar{\gamma}_{e1}) (\bar{\gamma}_{RB})^{\lambda} (\bar{\gamma}_{AR})^{\lambda} \times \frac{\Psi(\bar{\gamma}_{BR}, \bar{\gamma}_{e2}) \Psi(\bar{\gamma}_{RA}, \bar{\gamma}_{e2}) [\Gamma(\lambda)]^4 (\bar{\gamma}_{BR})^{\lambda} (\bar{\gamma}_{RA})^{\lambda}}{(\mu(1+\kappa))^{4\lambda}}, \end{aligned} \tag{3}$$

where $\Psi(a,b) = \frac{\mu^{3\mu} m^{3m} (1+\kappa)^{3\mu} \Gamma(\mu) \Omega}{\Gamma(1+3\mu)\Gamma(m)(\mu\kappa+m)^{3m}(a)^{\mu}(b)^{-2\mu}} \times \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \sum_{l=0}^{\infty} \frac{(2\mu-2m)_i (2m)_i \Gamma(m+l)}{(1+2\mu)_{i+j} \Gamma(\mu+l) i! j! l!} \left(\frac{-\mu(1+\kappa)}{b}\right)^i$ $\times \left(\frac{-\mu(1+\kappa)m}{b(\mu\kappa+m)}\right)^j \left(\frac{\mu^2\kappa(1+\kappa)\Omega}{(\mu\kappa+m)a}\right)^l$, $(k)_l = \frac{\Gamma(k+l)}{\Gamma(k)}$ is the Pochhammer symbol [15, Eq. (1.1.3)] and $\Gamma(.)$ is the Gamma function.

Proof. The proof is given in Appendix. ■

IV. Numerical results

This section provides some numerical examples for the analytical results derived in Sec. III. Unless stated otherwise, the parameter values used in plotting the results are as follows: $\bar{\gamma}_{AR} = \bar{\gamma}_{RB} = \bar{\gamma}_{BR} = \bar{\gamma}_{RA} = \bar{\gamma}_m = 5$ dB, $\bar{\gamma}_{e1} = \bar{\gamma}_{e2} = \bar{\gamma}_e = -5$ dB, $m = 20$, $\kappa = 5$, $\mu = 2$, $\eta = 2$, ρ=0.1, $\alpha = 0.25$, and $\zeta = 0.9$.

Fig. 2 plots the intercept probability against increasing values of $\bar{\gamma}_m$ for several values of the $\kappa - \mu$ shadowed fading parameters. It can be observed from Fig. 2 that an increase in the parameter μ, which corresponds to an increase in number of multipath clusters in the model, rapidly decreases the intercept probability. Similarly, the intercept probability decreases with an increase in κ which corresponds to a larger sum power of the dominant cluster paths. More specifically, for $\kappa = 10$, $\mu = 2$ and $\bar{\gamma}_m = 14$ dB, the figure shows that by increasing the parameter m from 5 to 20, which corresponds to lesser shadowing variance in the $\kappa - \mu$ shadowed model, the intercept probability is reduced from 0.1 to 0.003. This shows that the parameter m has a prominent role in determining the intercept probability of the considered TT-DF relaying system.

[1]The worst-case scenario and thus a lower bound on the secrecy performance is considered here by assuming that the eavesdropper can decode the message of one user and performs backward decoding to decode the other user's message [14].

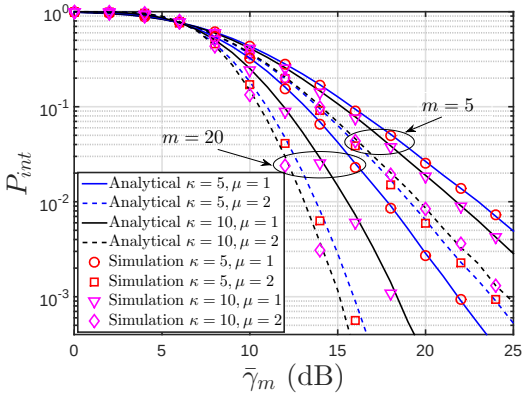

Fig. 2. P_{int} versus $\bar{\gamma}_m$.

Fig. 3 plots P_{int} against $\frac{d_{AR}}{d_{AE}}$ to depict the effect of the distance ratio on the intercept probability. It can be observed that an increase in $\frac{d_{AR}}{d_{AE}}$ or $\bar{\gamma}_e$, increases the intercept probability. More importantly, we note that for any constant values of μ, the intercept probability curves come closer when $\frac{d_{AR}}{d_{AE}} > 1$. This shows that the impact of fading on intercept probability diminishes when either source is placed far away from relay or eavesdropper is placed very near to the source. In addition, for any particular values of $\frac{d_{AR}}{d_{AE}}$, $\bar{\gamma}_m$, $\bar{\gamma}_e$ and μ, we can see that the gap of the curves of intercept probability reduces when α decreases from 0.2 to 0.1. Similar observations made for node B are not illustrated here for brevity.

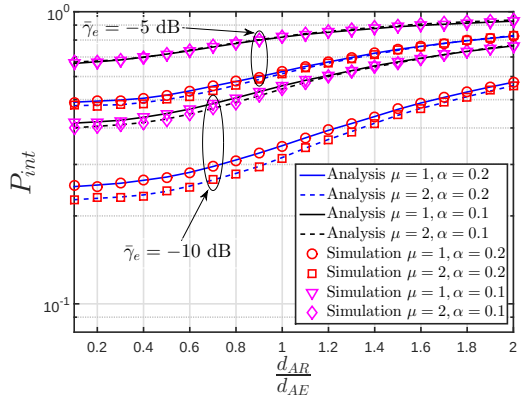

Fig. 3. P_{int} as a function of $\frac{d_{AR}}{d_{AE}}$.

Fig. 4 emphasizes on the impact of ρ on the intercept probability. It can be seen that a large ρ increases the message intercept probability; for instance at $\frac{d_{AR}}{d_{AE}} = 0.9$ and $\rho = 0.01$, the intercept probability increases from 0.4 to 0.7 when α is decreased from 0.2 to 0.1. In particular, for small values of ρ and $\frac{d_{AR}}{d_{AE}}$, the intercept probability decreases and the gap between the graphs of both $\alpha = 0.1$ and $\alpha = 0.2$ considerably increases. This indicates that the secrecy at smaller values of α can be ensured by allocating more power for ID at the relay.

V. Conclusion

This work analyzed the secrecy performance of a TT-DF relay with energy harvesting capability. We derived a closed-form expression for the intercept probability under $\kappa - \mu$ shadowed fading and evaluated the impact of the fading distribution parameters and the node locations on the intercept probability. The impact of the power-splitting factor ρ, at the relay, on the intercept probability was also quantified and it was shown that more power is required for ID at the relay to improve the secrecy performance. Our results are useful for analyzing the intercept probability of energy harvesting TT-DF relays with $\kappa - \mu$ shadowed fading links.

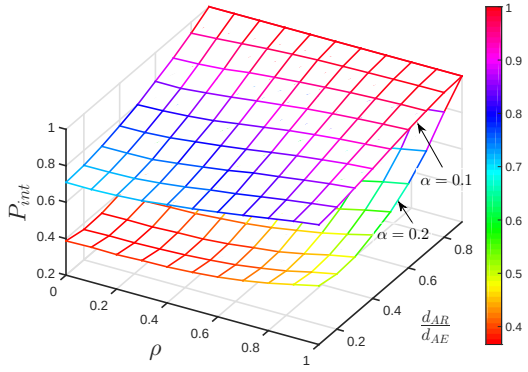

Fig. 4. P_{int} versus $\frac{d_{AR}}{d_{AE}}$ and ρ.

APPENDIX
PROOF OF (3)

The intercept probability can be written as

$$\begin{aligned} P_{int} &= \Pr\{\min(C_{sec,1}, C_{sec,2}) < 0\} \\ &= 1 - [(1 - P_{int(A,R,B)})(1 - P_{int(B,R,A)})] \end{aligned} \tag{4}$$

where $P_{int(A,R,B)}$ is the intercept probability for the link A→R→B which is given by

$$\begin{aligned} P_{int(A,R,B)} &= \Pr\{\min\{\gamma_{AR}, \gamma_{RB}\} < \gamma_{e1}\} \\ &= 1 - \Pr\{\gamma_{AR} > \gamma_{e1}, \gamma_{RB} > \gamma_{e1}\}. \end{aligned} \tag{5}$$

By exploiting the independence of γ_{AR} and γ_{RB}, we get

$$P_{int(A,R,B)} = 1 - (1 - P_{\gamma_{AR}}(\gamma_{e1}))(1 - P_{\gamma_{RB}}(\gamma_{e1})). \tag{6}$$

Similarly, the intercept probability $P_{int(B,R,A)}$ for the link B→R→A can be written as

$$P_{int(B,R,A)} = 1 - (1 - P_{\gamma_{BR}}(\gamma_{e2}))(1 - P_{\gamma_{RA}}(\gamma_{e2})). \tag{7}$$

Now, the probability $P_{\gamma_{AR}}(\gamma_{e1})$ can be derived as

$$P_{\gamma_{AR}}(\gamma_{e1}) = 1 - \tau, \tag{8}$$

where

$$\tau = \int_0^\infty F_{\gamma_{e1}}(\gamma_{AR}) f_{\gamma_{AR}}(\gamma_{AR}) d\gamma_{AR}. \tag{9}$$

The probability density function of the $\kappa - \mu$ shadowed distribution is expressed as [8, Eq.(4)]

$$\begin{aligned} f_Z(z) = &\frac{\mu^\mu m^m (1+\kappa)^\mu}{\Gamma(\mu)\bar{\gamma}_z(\mu\kappa + m)^m} \left(\frac{\gamma_z}{\bar{\gamma}_z}\right)^{\mu-1} \exp\left(-\frac{\mu(1+\kappa)\gamma_z}{\bar{\gamma}_z}\right) \\ &\times_1 F_1\left(m; \mu; \frac{\mu^2\kappa(1+\kappa)}{\mu\kappa + m}\frac{\gamma_z}{\bar{\gamma}_z}\right), \end{aligned} \tag{10}$$

where ${}_1F_1(.)$ is the Kummer confluent hypergeometric function [16] and $\bar{\gamma}_z$ represents the mean value. The cumulative distribution function of the sum of two $\kappa - \mu$ shadowed variates is written as [8, Eq.(11)]

$$\begin{aligned} F_Z(z) = &\frac{1}{\Gamma(1 + M\mu)} \frac{\mu^{2\mu} m^{2m} (1+\kappa)^{2\mu}}{(\mu\kappa + m)^{2m}} \left(\frac{1}{\bar{\gamma}_z}\right)^{2\mu} \gamma^{2\mu} \\ &\times \Phi_2\Bigg(2\mu - 2m, 2m; 1 + 2\mu; -\frac{\mu(1+\kappa)\gamma_z}{\bar{\gamma}_z}, \\ &- \frac{\mu(1+\kappa)}{\bar{\gamma}_z}\frac{m\gamma_z}{\mu\kappa + m}\Bigg), \end{aligned} \tag{11}$$

where $\Phi_2(.)$ is the bivariate confluent hypergeometric function [16]. Substituting (10), (11) into (9) we obtain

$$\begin{aligned}\tau = &\frac{\mu^{3\mu} m^{3m} (1+\kappa)^{3\mu} \Omega}{\Gamma(1+3\mu)(\mu\kappa+m)^{3m} \bar{\gamma}_{e1}^{2\mu} \bar{\gamma}_{AR}^{\mu}} \\ &\times \int_0^\infty \gamma_{AR}^{3\mu-1} \exp\left(-\frac{\mu(1+\kappa)\gamma_{AR}}{\bar{\gamma}_{AR}}\right) \Phi_2\Bigg(2\mu-2m, \\ &2m; 1+2\mu; \frac{-\mu(1+\kappa)\gamma_{AR}}{\bar{\gamma}_{e1}}, \frac{-\mu(1+\kappa)\gamma_{AR}}{\bar{\gamma}_{e1}} \frac{m}{\mu\kappa+m}\Bigg) \\ &\times_1 F_1\left(m; \mu; \frac{\Omega\mu^2\kappa(1+\kappa)}{\mu\kappa+m} \frac{\gamma_{AR}}{\bar{\gamma}_{AR}}\right) d\gamma_{AR}. \end{aligned} \tag{12}$$

where $\Omega = \frac{2d_{AR}^{\eta} d_{BR}^{\eta}(1-2\alpha)}{\zeta\rho\alpha}$. Simplifying and using the identities [16, Eqs. (3.326),(9.14),(9.261)] in (12) and replacing the same in (8), we get

$$\begin{aligned} P_{\gamma_{AR}}(\gamma_{e1}) = 1 - &\sum_{i,j,l=0}^{\infty} \frac{\mu^{3\mu} m^{3m} (1+\kappa)^{3\mu} \Omega \Gamma(\mu)}{\Gamma(1+3\mu)\Gamma(m)(\mu\kappa+m)^{3m} (\bar{\gamma}_{AR})^{\mu}} \\ &\times \frac{\Gamma(\lambda)(\bar{\gamma}_{AR})^{\lambda} (2\mu-2m)_i (2m)_i \Gamma(m+l)}{(\bar{\gamma}_{e1})^{-2\mu} (\mu(1+\kappa))^{\lambda} (1+2\mu)_{i+j} \Gamma(\mu+l) i! j! l!} \\ &\times \left(\frac{-\mu(1+\kappa)}{\bar{\gamma}_{e1}}\right)^i \left(\frac{-\mu(1+\kappa)m}{\bar{\gamma}_{e1}(\mu\kappa+m)}\right)^j \left(\frac{\Omega\mu^2\kappa(1+\kappa)}{(\mu\kappa+m)\bar{\gamma}_{AR}}\right)^l, \end{aligned} \tag{13}$$

where $\lambda = 3\mu + i + j + l$. Similarly, we can obtain

$$\begin{aligned} P_{\gamma_{RB}}(\gamma_{e1}) = 1 - &\sum_{i,j,l=0}^{\infty} \frac{\mu^{3\mu} m^{3m} (1+\kappa)^{3\mu} \Gamma(\mu) \Omega}{\Gamma(1+3\mu)\Gamma(m)(\mu\kappa+m)^{3m} (\bar{\gamma}_{RB})^{\mu}} \\ &\times \frac{\Gamma(\lambda)(\bar{\gamma}_{RB})^{\lambda} (2\mu-2m)_i (2m)_i \Gamma(m+l)}{(\bar{\gamma}_{e1})^{-2\mu} (\mu(1+\kappa))^{\lambda} (1+2\mu)_{i+j} \Gamma(\mu+l) i! j! l!} \\ &\times \left(\frac{-\mu(1+\kappa)}{\bar{\gamma}_{e1}}\right)^i \left(\frac{-\mu(1+\kappa)m}{\bar{\gamma}_{e1}(\mu\kappa+m)}\right)^j \left(\frac{\Omega\mu^2\kappa(1+\kappa)}{(\mu\kappa+m)\bar{\gamma}_{RB}}\right)^l. \end{aligned} \tag{14}$$

To obtain the intercept probability for the link B→R→A, we have to first evaluate the terms $P_{\gamma_{BR}}(\gamma_{e2})$ and $P_{\gamma_{RA}}(\gamma_{e2})$ in (7). By following the approach of (13) and (14), we get

$$\begin{aligned} P_{\gamma_{BR}}(\gamma_{e2}) = 1 - &\sum_{i,j,l=0}^{\infty} \frac{\mu^{3\mu} m^{3m} (1+\kappa)^{3\mu} \Gamma(\mu) \Omega}{\Gamma(1+3\mu)\Gamma(m)(\mu\kappa+m)^{3m} (\bar{\gamma}_{BR})^{\mu}} \\ &\times \frac{\Gamma(\lambda)(\bar{\gamma}_{BR})^{\lambda} (2\mu-2m)_i (2m)_i \Gamma(m+l)}{(\bar{\gamma}_{e2})^{-2\mu} (\mu(1+\kappa))^{\lambda} (1+2\mu)_{i+j} \Gamma(\mu+l) i! j! l!} \\ &\times \left(\frac{-\mu(1+\kappa)}{\bar{\gamma}_{e2}}\right)^i \left(\frac{-\mu(1+\kappa)m}{\bar{\gamma}_{e2}(\mu\kappa+m)}\right)^j \left(\frac{\mu^2\kappa(1+\kappa)\Omega}{(\mu\kappa+m)\bar{\gamma}_{BR}}\right)^l, \end{aligned} \tag{15}$$

$$\begin{aligned} P_{\gamma_{RA}}(\gamma_{e2}) = 1 - &\sum_{i,j,l=0}^{\infty} \frac{\mu^{3\mu} m^{3m} (1+\kappa)^{3\mu} \Gamma(\mu) \Omega}{\Gamma(1+3\mu)\Gamma(m)(\mu\kappa+m)^{3m} (\bar{\gamma}_{RA})^{\mu}} \\ &\times \frac{\Gamma(\lambda)(\bar{\gamma}_{RA})^{\lambda} (2\mu-2m)_i (2m)_i \Gamma(m+l)}{(\bar{\gamma}_{e2})^{-2\mu} (\mu(1+\kappa))^{\lambda} (1+2\mu)_{i+j} \Gamma(\mu+l) i! j! l!} \\ &\times \left(\frac{-\mu(1+\kappa)}{\bar{\gamma}_{e2}}\right)^i \left(\frac{-\mu(1+\kappa)m}{\bar{\gamma}_{e2}(\mu\kappa+m)}\right)^j \left(\frac{\Omega\mu^2\kappa(1+\kappa)}{(\mu\kappa+m)\bar{\gamma}_{RA}}\right)^l. \end{aligned} \tag{16}$$

Substituting (13), (14) into (6) and (15), (16) into (7) and replacing (6), (7) in (4) yields the intercept probability in (3).

REFERENCES

[1] Z. Ding, I. Krikidis, B. Sharif, and H. V. Poor, "Wireless information and power transfer in cooperative networks with spatially random relays," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4440–4453, 2014.

[2] P. N. Son and H. Y. Kong, "Cooperative communication with energy-harvesting relays under physical layer security," *IET Commun.*, vol. 9, no. 17, pp. 2131–2139, 2015.

[3] N. T. P. Van, S. F. Hasan, X. Gui, S. Mukhopadhyay, and H. Tran, "Three-step two-way decode and forward relay with energy harvesting," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 857–860, April 2017.

[4] N. Zhou, X. Chen, C. Li, and Q. Lai, "Relay selection for physical layer security in decode-and-forward two-way relay networks," *J. Info. Comput. Sci.*, vol. 10, no. 18, pp. 5821–5828, 2013.

[5] A. El Shafie, A. Sultan, A. Mabrouk, K. Tourki, and N. Al-Dhahir, "Secret-Key-Aided Scheme for Securing Untrusted DF Relaying Networks," *ArXiv e-prints*, Jun. 2017.

[6] S. L. Cotton, "Human Body Shadowing in Cellular Device-to-Device Communications: Channel Modeling Using the Shadowed $\kappa - \mu$ fading model," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 111–119, 2015.

[7] S. Kumar, "Approximate outage probability and capacity for κ-μ shadowed fading," *IEEE Commun. Lett.*, vol. 4, no. 3, pp. 301–304, 2015.

[8] J. F. Paris, "Statistical characterization of $\kappa - \mu$ shadowed fading," *IEEE Trans. Veh. Technol.*, vol. 63, no. 2, pp. 518–526, 2014.

[9] Z. Ding, S. M. Perlaza, I. Esnaola, and H. V. Poor, "Power allocation strategies in energy harvesting wireless cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 846–860, 2014.

[10] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, 2014.

[11] B. Zhong and Z. Zhang, "Secure full-duplex two-way relaying networks with optimal relay selection," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1123–1126, May 2017.

[12] Y. Zou and G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Trans. Ind. Informat*, vol. 12, no. 2, pp. 780–787, 2016.

[13] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, 2012.

[14] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[15] H. Exton, *Multiple hypergeometric functions and applications*. Horwood, 1976.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.