AUT Jouranl of Modeling and Simulation

AUT J. Model. Simul., 52(2) (2020) 167-178
DOI: 10.22060/miscj.2020.17653.5190

Security and Reliability Trade-off in Device to Device Communications with Untrusted Relays

Marzieh Izanlou[1], Abbas Mohammadi[2*], Mohamad Dosaranian-Moghadam[1]

[1] Faculty of Electrical, Biomedical and Mechatronics Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran.
[2] Electrical Engineering Department, Amirkabir University of Technology, Tehran, Iran

ABSTRACT: In this paper, we investigate the trade-off between reliability and security in a device to device (D2D) network including a pair of D2D, an untrusted relay, and a jammer. The untrusted relay is used as aiding to D2D communications but due to untrusting the relay, data protection from eavesdropping by relay is very important. According to this, two protocols direct transmission (DT) and relay transmission (RT) are considered for transmission in network. In the DT protocol, D2D pair directly and without relay aid and in the RT protocol, D2D pair use from relay for communication. In this paper, first, secrecy outage probability (SOP) and intercept probability and then trade-off between reliability and security presenting the closed-form relations for two protocols are investigated. Simulation results show the reliability of analytic relationships and show that in a steady intercept probability, DT protocol into RT protocol has a higher reliability. Also, the simulation results show that in RT, intercept probability is lower into the DT protocol and consequently security increases in RT into the DT protocol. Also the results confirm that increasing security increases the likelihood of loss of communication, and increasing the likelihood of reliable communication reduces communications security.

Review History:
Received:Jan. 04, 2020
Revised:Feb. 16, 2020
Accepted:Aug. 01, 2020
Available Online:Dec. 01,2020

Keywords:
Device to Device
Intercept Probability
Physical Layer Security
Security and Reliability Trade-off
Secrecy Outage Probability

1- INTRODUCTION

Due to the nature of wireless networks, information signals exchanged between legal transmitters and receivers can easily be available to eavesdroppers; so data security is a vital issue in wireless communication networks. Recently, physical layer security (PLS) has been paid much attention. In [1], a cellular network based on a two-way untrusted relay has been considered in presence of an external jammer. Considering the physical layer security, network security rate has been improved. In [2], a wireless network including a transmitter, a receiver and an untrusted amplify-and-forward (AF) relay has been considered which use of destination based cooperative jamming (DBCJ). In this reference, outage probability has been investigated and indicated that optimal power allocation (OPA) compared to the allocation of the same power, is resulted to reducing network outage probability. Unlike the cellular network, PLS in device to device (D2D) communication hasn't been paid much attention. In [3], a vast study about D2D communications and their taxonomy has been done and in [4] D2D communications security has been investigated comprehensively. References [5] to [10] have researched PLS in D2D communications. In [5], D2D pair can work in underlay or overlay states. By calculating the probability of outage and confidential capacity in each mode, it's determined that physical layer security can be controlled with mode selection. In [6] a D2D pair, communicates directly or using trusted relay. The D2D transmission capacity has been calculated for underlay and overlay states and indicated that the more relay density the more D2D transmission capacity. In [7], a D2D network is considered. D2D pair acts in both states of direct and relay communication. Available sum rate in both cases is calculated and shown when the conditions of the communication channels are good, the use of the relay can raise the rate of the sum. In [8], physical layer security in a D2D network is investigated using untrusted relay. Considering with and without jammer states of ergodic secrecy rate (ESR) of network was calculated and shown that the presence of the jammer provides more security for the physical layer.

References [9] to [16] have been made to study the reliability and security of cellular networks. Ref. [9] examines the possibility of connection outage probability (COP) and secrecy outage probability (SOP) in a relay network. Then security and reliability trade-off (SRT) is considered. The simulation results show that the use of a jamming signal increases network security and, as security increases, network reliability decreases. In [10], a relay selection plan is provided that the transmitter and receiver communicate through a relay in the presence of an eavesdropper. This plan in single and multi-relay states is investigated. The simulation results show that the more relay numbers the less intercept probability. Ref. [11] has studied the SRT in a cyber-physical cooperative system. They have investigated the probability of cutting off

*Corresponding author's email:abm125@aut.ac.ir

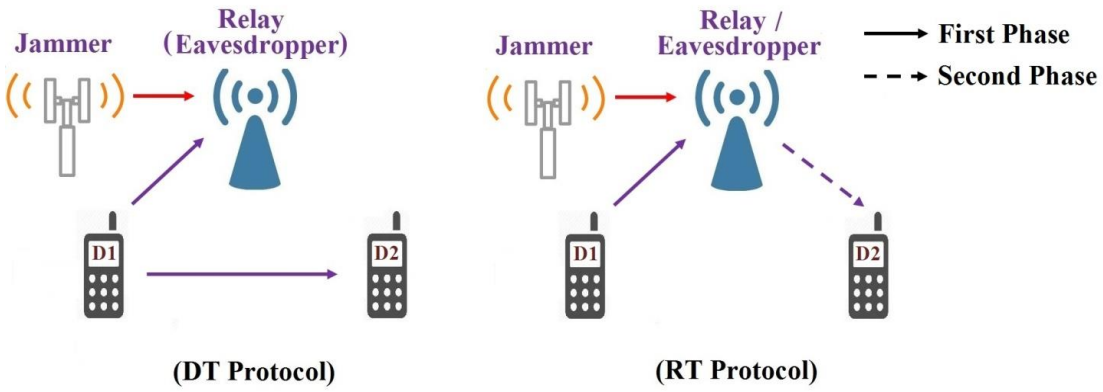

Fig. 1. Relaying between D1 and D2 via untrusted amplify-and-forward (AF) relay in the presence of a jammer for DT and RT protocols

the communication and intercept probability in two states of direct and relay communication using DBCJ. The simulation results show the direct communication increases the SRT and relay using state decreases the SRT. Ref. [12] considers two sources which communicate through an untrusted relay with together and investigates the probability of communication cutting off and intercept probability for without and with jammer states. The simulation results show that using a jammer decreases the intercept probability but increases the cutting off probability. In [13], one source and one destination communicate through many trusted relays in presence of an eavesdropper with together. By selecting the best relay, outage and intercept probability and also trade-off between these states are investigated. The simulation results show that the best relay selection plan, results to improving the SRT and whatever the relay number gets high, the SRT gets better. Ref. [14] has considered a communicative network including an origin, a destination, many trusted relays and an eavesdropper. In this reference, an opportunistic relay selection plan has been proposed and SRT analyzed. Then opportunistic relay selection plan results in SRT improvement and by increasing the relays number, intercept and outage probability decrease.

In Reference [15], the SRT in the IoT (internet of things) network in untrusted and selfish relay-assisted D2D communication has been evaluated. In this scenario, the relay is both untrusted, trying to eavesdrop information, and selfish, using available resources only for relaying its own packets. The SRT is examined both in the instantaneous state when channel state information (CSI) is available and in the statistical state when CSI is not available.

In this paper, despite the [9] to [14] which investigate the security analyzes and reliability in cellular networks, we will study the SRT in D2D transmission. For this purpose, an overlay D2D pair is considered which transmit with together through an AF relay and in presence of a jammer. Also, in contrast to [15], which only considered the relay protocol, this paper examines both relayed and direct transmission between D2D pairs. Despite [10], [12] to [14] which have considered a trusted relay, in this paper an untrusted relay has been used. Based on this fact that the D2D pair transmission is directly established or used with an untrusted relay, two protocols are considered for the system: 1) Direct transmission (DT) protocol and 2) Relay transmission (RT) protocol. For each protocol, the first step is to analyze the outage probability and intercept probability, and new package relationships are achieved. Then, the compromise between security and reliability is studied analytically by providing closed form relationships. Numerical simulations show the validity of analytical results and show that the higher the reliability of the network, the lower the network security, and vice versa.

The rest of this paper is organized as follow. In Section 2, system model is presented. In Section 3 and Section 4, we provide the performance analyses of the SOP and the intercept probability in two protocols, respectively. In addition, in Section 5, the SRT will be studied. In Section 6, the trusted relay scenario and the calculation of the SOP for the two protocols are discussed. In Section 7, the numerical results are given, and then, we conclude this paper in Section 8.

2- SYSTEM MODEL

The system model includes a D2D transmitter (D1), a D2D receiver (D2), an untrusted AF relay, and a jammer. Similar to [1], jammer is considered as output power seller which becomes active for improving the security in network. All nodes act as half-duplex.

The Gaussian channels are complex and from D1-to-D2, D1-to-relay, relay-to-D2, and jammer-to-relay, are respectively shown $h_{12} \sim CN(0,\mu_{12})$, $h_{1r} \sim CN(0,\mu_{1r})$, $h_{r2} \sim CN(0,\mu_{r2})$, and $h_{jr} \sim CN(0,\mu_{jr})$, where μ_{12}, μ_{1r}, μ_{r2}, and μ_{jr} are channel gains between the D2D pair, D1 and relay, the relay and D2, and the jammer and relay, respectively. Additive white Gaussian noise (AWGN) in each receiver is $n_m\left(m \in \{r,d\}\right)$ with zero average and N_0 variance. Transmit power in each node is P_n and transmit power to noise ratio is $\rho_n = \frac{P_n}{N_0}$ where $n \in \{1,r,j\}$. Channel gain is $\lambda_{kl} = |h_{kl}|^2$ where define as $k,l \in \{1,2,r,j\}$. For this network, two direct transmission (DT) protocol and relay transmission (RT) protocol are considered.

In this study, D2D pair in overlay state have considered and doesn't receive any interference from cellular network [3]. In addition, with the assumption of distributing the cell

spectrum vertically between D2D users, the interference from other D2D users, which probably use the same resources as the D2D pair, is not entered in the D2D pair [5]. In Figure 1, the DT and RT protocols are represented. In the following, we will describe the two protocols

A. DT PROTOCOL

In the DT protocol, the D2D pair communicate with together directly, and an untrusted relay appears only in the role of eavesdropper. In this way, D1 sends a signal to D2, which is also received by the relay. To prevent eavesdropping in the relay, the jammer generates a jamming signal simultaneously by sending message signal by D1. If we supposed x_s and x_j are transmitted signals from D1 and jamming signals respectively, the received signal in the relay and D2 are respectively expressed as:

$$y_R = \sqrt{P_1} h_{1r} x_s + \sqrt{P_j} h_{jr} x_j + n_r, \tag{1}$$

$$y_D = \sqrt{P_1} h_{12} x_s + n_d. \tag{2}$$

So,signal-to-interference-plus-noise ratio (SINR) in relay and signal to noise ratio (SNR) in D2 are respectively presented as follow:

$$\begin{aligned} \gamma_R &= \frac{P_1 |h_{1r}|^2}{P_j |h_{jr}|^2 + N_0} = \frac{\rho_1 \lambda_{1r}}{\rho_j \lambda_{jr} + 1} \\ &\cong \frac{\rho_1 \lambda_{1r}}{\rho_j \lambda_{jr}} = \frac{\rho_1}{\rho_j} \nu \quad \text{if SNR} \gg 1, \end{aligned} \tag{3}$$

$$\gamma_D = \frac{P_1 |h_{12}|^2}{N_0} = \rho_1 \lambda_{12}. \tag{4}$$

where in Eq. (3), $\nu = \frac{\lambda_{1r}}{\lambda_{jr}}$ and approximation of this relationship with hypothesis high SNR ($\rho_n \lambda_{kl} \gg 1$ where $n \in \{1, r, j\}$ and $k, l \in \{1, 2, r, j\}$) are resulted.

B. RT protocol

In the RT protocol, the D2D pair communicates through untrusted relay, and according to Fig. 1, message transmission is achieved in two phases. In the first phase, D1 sends a signal to the relay, and simultaneously the jammer sends a jamming signal to the relay. In the second phase, the relay sends the received signal from the first phase to D2. Assuming that x_s and x_j are the signals transmitted from D1 and jammer respectively, the received signal in the relay in the first phase is expressed as:

$$y_R = \sqrt{P_1} h_{1r} x_s + \sqrt{P_j} h_{jr} x_j + n_r. \tag{5}$$

The relay, after receiving the D1 data, amplifies and sends it as $x_R = G y_R$, where G is the relay's amplification factor, and is calculated from the following equation:

$$G = \sqrt{\frac{P_r}{P_1 |h_{1r}|^2 + P_j |h_{jr}|^2 + N_0}}. \tag{6}$$

So in the second phase, the received signal in D2 is calculated as follows:

$$\begin{aligned} y_D &= x_R h_{r2} + n_d = G y_R h_{r2} + n_d \\ &= G h_{r2} \left(\sqrt{P_1} h_{1r} x_s + \sqrt{P_j} h_{jr} x_j + n_r \right) + n_d \\ &= G \sqrt{P_1} h_{r2} h_{1r} x_s + G \sqrt{P_j} h_{r2} h_{jr} x_j + G h_{r2} n_r + n_d \\ &= G \sqrt{P_1} h_{r2} h_{1r} x_s + G h_{r2} n_r + n_d. \end{aligned} \tag{7}$$

It is noteworthy that Eq. (7) is calculated with the assumption that the pre-shared jamming signal is known to the jammer and D2 but is unknown to the untrusted relay. Therefore, D2 can omit the jamming to extract more information [1].

Now, using Eqs. (5) -(7), the SINR in the relay and D2 are obtained as follows, respectively:

$$\begin{aligned} \gamma_R &= \frac{P_1 |h_{1r}|^2}{P_j |h_{jr}|^2 + N_0} = \frac{\rho_1 \lambda_{1r}}{\rho_j \lambda_{jr} + 1} \cong \\ &\frac{\rho_1 \lambda_{1r}}{\rho_j \lambda_{jr}} = \frac{\rho_1}{\rho_j} \nu \quad \text{if SNR} \gg 1, \end{aligned}$$

$$\begin{aligned} \gamma_D &= \frac{G^2 P_1 |h_{1r}|^2 |h_{r2}|^2}{G^2 |h_{r2}|^2 N_0 + N_0} \\ &= \frac{P_1 P_r |h_{1r}|^2 |h_{r2}|^2}{P_r |h_{r2}|^2 N_0 + N_0 \left(P_1 |h_{1r}|^2 + P_j |h_{jr}|^2 + N_0 \right)} \\ &= \frac{P_1 P_r |h_{1r}|^2 |h_{r2}|^2}{N_0^2 \left(\frac{P_r |h_{r2}|^2}{N_0} + \frac{P_1 |h_{1r}|^2}{N_0} + \frac{P_j |h_{jr}|^2}{N_0} + 1 \right)} \\ &= \frac{\rho_1 \rho_r \lambda_{1r} \lambda_{r2}}{\rho_1 \lambda_{1r} + \rho_r \lambda_{r2} + \rho_j \lambda_{jr} + 1} \\ &= \frac{\rho_1 \rho_r \lambda_{1r} \lambda_{r2}}{\rho_1 \lambda_{1r} + \rho_r \lambda_{r2} + \rho_j \lambda_{jr}} \end{aligned} \tag{8}$$

$$\underline{z} \frac{\rho_1 \rho_r \lambda_{r2} \nu}{\rho_1 \nu + \rho_r \frac{\lambda_{r2}}{\lambda_{jr}} + \rho_j} \quad \text{if SNR} \gg 1. \tag{9}$$

where in Eq. (8) and Eq. (9), ν is calculated similar to Eq. (3), and the approximation of these relations is obtained by assuming a high SNR.

3- PERFORMANCE ANALYSIS OF SECRECY OUTAGE PROBABILITY

In order to ensure that the data is sent successfully to the destination, the instantaneous secrecy rate must be higher than the threshold of the data rate. The probability that the instantaneous secrecy rate is lower than the optimal information rate is called the SOP, which is displayed with P_{out}. In this section, the probability of secrecy outage for both DT and RT protocols is investigated.

A. DT Protocol

The instantaneous secrecy rate in the DT protocol is as follows:

$$R_s^{DT} = I_{12}^{DT} - I_{1r}^{DT}, \tag{10}$$

where I_{12}^{DT} and I_{1r}^{DT} are the mutual information between D1 and D2, and between D1 and relay, respectively, obtained by the following relationships:

$$I_{12}^{DT} = \log_2\left(1+\gamma_D\right) = \log_2\left(1+\rho_1\lambda_{12}\right), \tag{11}$$

$$I_{1r}^{DT} = \log_2\left(1+\gamma_R\right) = \log_2\left(1+\frac{\rho_1}{\rho_j}\nu\right), \tag{12}$$

Now, if R is the target transmission rate, the SOP is as follows:

$$\begin{aligned}
&P_{out}^{DT} = \Pr\left\{R_s^{DT} < R\right\} = \Pr\left\{I_{12}^{DT} - I_{1r}^{DT} < R\right\} \\
&= \Pr\left\{\log_2\left(1+\rho_1\lambda_{12}\right) - \log_2\left(1+\frac{\rho_1}{\rho_j}\nu\right) < R\right\} \\
&= \Pr\left\{\log_2\frac{\left(1+\rho_1\lambda_{12}\right)}{\left(1+\frac{\rho_1}{\rho_j}\nu\right)} < R\right\} = \Pr\left\{\frac{\left(1+\rho_1\lambda_{12}\right)}{\left(1+\frac{\rho_1}{\rho_j}\nu\right)} < 2^R\right\} \\
&\cong \Pr\left\{\left(1+\rho_1\lambda_{12}\right) < 2^R\right\} = \Pr\left\{\lambda_{12} < \frac{2^R-1}{\rho_1}\right\} \quad \text{if} \quad \nu \ll 1 \\
&= F_{\lambda_{12}}\left(\frac{2^R-1}{\rho_1}\right) = 1-\exp\left(-\frac{2^R-1}{\rho_1\mu_{12}}\right).
\end{aligned} \tag{13}$$

The approximation of the above equation is obtained by assuming $\nu \ll 1$ or $\lambda_{jr} \gg \lambda_{1r}$.

From Eq. (13), the following result follows:

1)The probability of secrecy outage in the DT protocol depends only on the gain of the channel between the D2D pairs, so that if the channel gain between the D2D pairs increases, the confidential outage probability decreases.

2)As the transmit SNR increases, the SOP decreases.

3)As the optimal transmit rate increases, the SOP increases as well.

B. RT Protocol

In the RT protocol, data transfer takes place in two phases. Therefore, the rate of confidentiality is calculated as follows [1]:

$$R_s^{RT} = \left[\frac{1}{2}\log_2\Phi\right]^+, \tag{14}$$

where $\Phi = \frac{1+\gamma_D}{1+\gamma_R}$ and $[x]^+ = \max\{0,x\}$.

Therefore, the SOP in the RT protocol is obtained as follows:

$$\begin{aligned}
&P_{out}^{RT} = \Pr\left\{R_s^{RT} < R\right\} = \Pr\left\{\max\left\{0,\frac{1}{2}\log_2\frac{1+\gamma_D}{1+\gamma_R}\right\} < R\right\} \\
&= \Pr\left\{\frac{1}{2}\log_2\frac{1+\gamma_D}{1+\gamma_R} < R\right\} = \Pr\left\{\frac{1+\gamma_D}{1+\gamma_R} < 2^{2R}\right\} \\
&= \Pr\left\{\frac{\left(1+\frac{\rho_1\rho_r\lambda_{r2}\nu}{\rho_1\nu+\rho_r\frac{\lambda_{r2}}{\lambda_{jr}}+\rho_j}\right)}{1+\frac{\rho_1}{\rho_j}\nu} < 2^{2R}\right\} \\
&\cong \Pr\left\{\left(1+\frac{\rho_1\rho_r\lambda_{r2}\nu}{\rho_j}\right) < 2^{2R}\right\} \quad \text{if} \quad \left(\nu \ll 1, \lambda_{jr} \gg \lambda_{r2}\right) \\
&= \Pr\left\{\lambda_{r2} < \frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\nu}\right\} = \Pr\left\{\lambda_{r2} < \frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\nu}\middle|\nu\right\} \\
&E_\nu\left(F_{\lambda_{r2}}\left(\frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\nu}\right)\right) = 1-E_\nu\left(\exp\left(-\frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\mu_{r2}\nu}\right)\right) \\
&= 1-e^{\frac{\rho_j\mu_{jr}\left(2^{2R}-1\right)}{2\rho_1\rho_r\mu_{1r}\mu_{r2}}} W_{-1,-\frac{1}{2}}\left(\frac{\rho_j\mu_{jr}\left(2^{2R}-1\right)}{\rho_1\rho_r\mu_{1r}\mu_{r2}}\right),
\end{aligned} \tag{15}$$

where the approximation of the above equation is obtained by assuming $\nu \ll 1$ or $\lambda_{jr} \gg \lambda_{1r}$, as well as $\lambda_{jr} \gg \lambda_{r2}$. In other words, the relay-jammer distance is much longer than the relay-D2D pair distance. Also, W is the Wittaker function, calculated as follows in [16- Eq. 9.224]:

$$W_{\mu,\frac{1}{2}+\mu}\left(z\right) = z^{\mu+1}e^{-\frac{1}{2}z}\int_0^\infty\left(1+t\right)^{2\mu}e^{-zt}dt = z^{-\mu}e^{\frac{1}{2}z}\int_z^\infty t^{2\mu}e^{-t}dt. \tag{16}$$

From (15), the following result follows:

1)The SOP in the RT protocol is increased by increasing the channel gain between the jammer and the relay and decreasing with the increase in the channel efficiency between the relays with D1 and D2.

2) As the transmit SNR increases, the SOP decreases.

It should be noted that the calculation of Eq. (15) is in

Appendix A.

It is worth mentioning that, to maintain confidentiality, as in [17] and [18], secrecy coding was used. To make codes secret, sending confidential information, the transmitter sends additional information about the codeword as well. If the codeword rate is R_c and the information confidentiality rate is R_s, the total rate sent by the transmitter would be $R_t = \left(R_c - R_s\right)$. In this case, the cost to maintain confidentiality against information eavesdropping is $R_c - R_s$. Also, if the main and eavesdrop channel capacities are C_d and C_e respectively, then $C_e < R_t < C_d$ to prevent zconfidentiality outage.

4- PERFORMANCE ANALYSIS OF INTERCEPT PROBABILITY

The probability of eavesdropping happens when the capacity of the main channel decreases from the capacity of the intercept channel. In this case, an untrusted relay can eavesdrop the signal. The probability that an untrusted relay can successfully eavesdrop the signal is called the IP, which is displayed with P_{int}. In the following, the IP for the two protocols, DT and RT, is investigated.

A. DT Protocol

The intercept probability in the DT protocol is as follows:

$$\begin{aligned} P_{int}^{DT} &= \Pr\left\{\log_2\left(1+\gamma_R\right) > R\right\} = \\ &\Pr\left\{\log_2\left(1+\frac{\rho_1}{\rho_j}\nu\right) > R\right\} \\ &= 1-\Pr\left\{\left(1+\frac{\rho_1}{\rho_j}\nu\right) < 2^R\right\} \\ &= 1-\Pr\left\{\nu < \frac{\rho_j}{\rho_1}\left(2^R-1\right)\right\} \\ &= 1-F_\nu\left(\frac{\rho_j}{\rho_1}\left(2^R-1\right)\right) \\ &= \frac{\mu_{1r}}{\mu_{1r}+\frac{\rho_j}{\rho_1}\left(2^R-1\right)\mu_{jr}}. \end{aligned} \tag{17}$$

The calculation of Eq. (17) is given in Appendix B. Eq. (17) shows that as R increases, the intercept probability is closer to zero. Also, as the channel gain between the relay and the jammer increases, the intercept probability to zero and the greater the channel gain between the relay and D1 increases, the intercept probability is closer to 1.

B. RT Protocol

Given that the intercept probability in the RT protocol is calculated as $P_{int} = \Pr\left\{\frac{1}{2}\log_2\left(1+\gamma_R\right) > R\right\}$ and given that γ_R is equal in RT and DT, the intercept probability in the RT protocol, like the DT protocol, is obtained by the difference in the R coefficient as follows:

$$P_{int}^{RT} = \frac{\mu_{1r}}{\mu_{1r}+\frac{\rho_j}{\rho_1}\left(2^{2R}-1\right)\mu_{jr}}. \tag{18}$$

From Eq. (18), conclusions are derived such as Eq. (17). Also, in Eq. (18), the more the R is, the lower the eavesdropping of the relation with Eq. (17) doubles.

5- ANALYSIS OF SECURITY AND RELIABILITY TRADE-OFF

Reliability means that the sent data is sent successfully from the source to the destination, and security means that we trust that the sent data from the source remains confidential. Some issues, such as increasing transmitter's transmit power or decreasing transmitter data rates, can increase network reliability, but network security is at risk. So there must be a trade-off between reliability and security. In this section, for each of the DT and RT protocols, the SRT is examined.

A. DT Protocol

By combining Eq. (13) and Eq. (17), the SRT for the DT protocol is obtained as follows:

$$P_{out}^{DT} = 1-\exp\left(-\frac{\mu_{1r}\left(\left(P_{int}^{DT}\right)^{-1}-1\right)}{\rho_j\mu_{12}\mu_{jr}}\right), \tag{19}$$

$$P_{int}^{DT} = \frac{\mu_{1r}}{\mu_{1r}-\rho_j\mu_{12}\mu_{jr}\ln\left(1-P_{out}^{DT}\right)}. \tag{20}$$

From Eq. (19) and Eq. (20), the following result follows:

1)SRT is independent from R.

2)As the transfer SNR increases, the SOP decreases and the intercept probability increases.

3) If $P_{int}^{DT} \to 0$ then $P_{out}^{DT} \to 1$ and vice versa.

B. RT Protocol

By combining Eq. (15) and Eq. (18), SRT for the RT protocol is obtained as follows:

$$P_{out}^{RT} = 1-e^{\frac{\left(\left(P_{int}^{RT}\right)^{-1}-1\right)}{2\rho_r\mu_{r2}}}W_{-1,-\frac{1}{2}}\left(\frac{\left(\left(P_{int}^{RT}\right)^{-1}-1\right)}{\rho_r\mu_{r2}}\right). \tag{21}$$

From Eq. (21), the following result follows:

1)Like the DT protocol, in this protocol, the SRT is independent of R.

2)As P_{int}^{RT} increases, P_{out}^{RT} decreases and vice versa.

6- TRUSTED RELAY SCENARIO

In this scenario, the D2D pair exchange information using a trusted relay, therefore jamming is not necessary. Similar to the untrusted relay scenario, this scenario was examined in both direct communication and relay communication.

A. DT Protocol

In this mode, the D2D pair communicate directly and the relay plays no role in the exchange of information and while intercepting the information, it is trusted. In this case, the signal received in the trusted relay is:

$$y_R = \sqrt{P_1} h_{1r} x_s + n_r. \tag{22}$$

The signal received in D2 is similar to Eq. (2).

So, the SNR in the relay is:

$$\gamma_R = \frac{P_1 |h_{1r}|^2}{N_0} = \rho_1 \lambda_{1r}. \tag{23}$$

The SNR in D2 is also similar to Eq. (4).

B. RT protocol

In this mode, the D2D pair communicates through a trusted relay in two phases. In the first phase, D1 sends the signal to the relay and in the second phase, the relay sends the signal received in the first phase to D2. Therefore, the signal received in the relay in the first phase is obtained similar to Eq. (22) and the relay's amplification factor is calculated as follows:

$$G = \sqrt{\frac{P_r}{P_1 |h_{1r}|^2 + N_0}}. \tag{24}$$

Also in the second phase, the signal received in D2 is calculated as follows:

$$\begin{aligned} y_D &= x_R h_{r2} + n_d = G y_R h_{r2} + n_d \\ &= G h_{r2} \left(\sqrt{P_1} h_{1r} x_s + n_r \right) + n_d \\ &= G \sqrt{P_1} h_{r2} h_{1r} x_s + G h_{r2} n_r + n_d. \end{aligned} \tag{25}$$

According to Eq. (22), the SNR in the relay is obtained similar to Eq. (23). Also, considering Eqs. (24) and (25), the SNR in D2 is obtained as:

$$\begin{aligned} \gamma_D &= \frac{G^2 P_1 |h_{1r}|^2 |h_{r2}|^2}{G^2 |h_{r2}|^2 N_0 + N_0} = \frac{P_1 P_r |h_{1r}|^2 |h_{r2}|^2}{P_r |h_{r2}|^2 N_0 + N_0 \left(P_1 |h_{1r}|^2 + N_0 \right)} \\ &= \frac{P_1 P_r |h_{1r}|^2 |h_{r2}|^2}{N_0^2 \left(\frac{P_r |h_{r2}|^2}{N_0} + \frac{P_1 |h_{1r}|^2}{N_0} + 1 \right)} = \frac{\rho_1 \rho_r \lambda_{1r} \lambda_{r2}}{\rho_1 \lambda_{1r} + \rho_r \lambda_{r2} + 1} \\ &= \frac{\rho_1 \rho_r \lambda_{r2}}{\rho_1 + \rho_r \vartheta + \frac{1}{\lambda_{1r}}} \cong \frac{\rho_1 \rho_r \lambda_{r2}}{\rho_1 + \rho_r \vartheta} \quad \text{if SNR} \gg 1. \end{aligned} \tag{26}$$

In Eq. (26) $\vartheta = \lambda_{r2} / \lambda_{1r}$ and is approximated by assuming high SNR.

We will now proceed to calculate the SOP in both DT and RT protocols.

6-1 SOP in DT protocol:

Since the relay is trusted and there is no eavesdropping in the system, the instantaneous secrecy rate is the rate that reaches D2 and is obtained as:

$$R_{s,T}^{DT} = I_{12}^{DT}, \tag{27}$$

where I_{12}^{DT} is obtained as in Eq. (11). In this case, SOP assuming that the optimal transmission rate is R is achieved as follows:

$$\begin{aligned} P_{out,T}^{DT} &= \Pr\left\{ R_{s,T}^{DT} < R \right\} = \Pr\left\{ I_{12}^{DT} < R \right\} \\ &= \Pr\left\{ \log_2 \left(1 + \rho_1 \lambda_{12} \right) < R \right\} \\ &\Pr\left\{ \left(1 + \rho_1 \lambda_{12} \right) < 2^R \right\} = \Pr\left\{ \lambda_{12} < \frac{2^R - 1}{\rho_1} \right\} \\ &= F_{\lambda_{12}} \left(\frac{2^R - 1}{\rho_1} \right) = 1 - \exp\left(-\frac{2^R - 1}{\rho_1 \mu_{12}} \right). \end{aligned} \tag{28}$$

Eq. (28) is obtained like Eq. (13) except that Eq. (28) is exact but Eq. (13) is obtained by approximation. Therefore, the results obtained in Eq. (13) can be applied to Eq. (28).

6-2 SOP in RT protocol:

In this scenario, since the data transfer is in two phases and there is no eavesdropping, the secrecy rate is calculated as:

$$R_{s,T}^{RT} = \frac{1}{2} \log_2 \gamma_D, \tag{29}$$

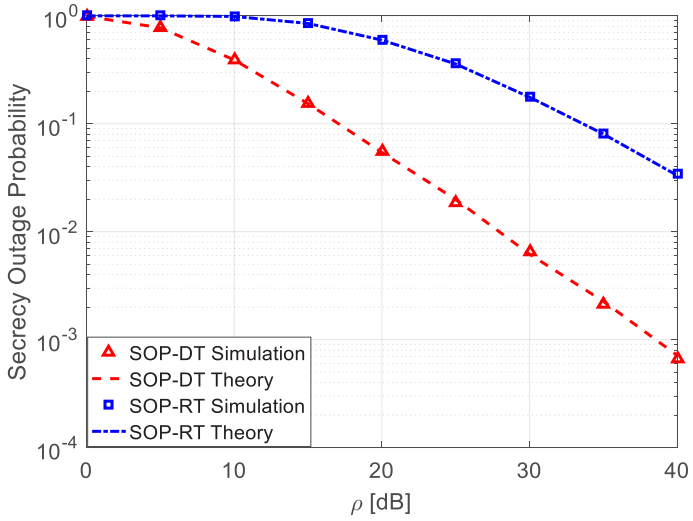

Fig.2. Comparing SOP versus transmit SNR (ρ) in [*dB*] for both DT and RT protocols.

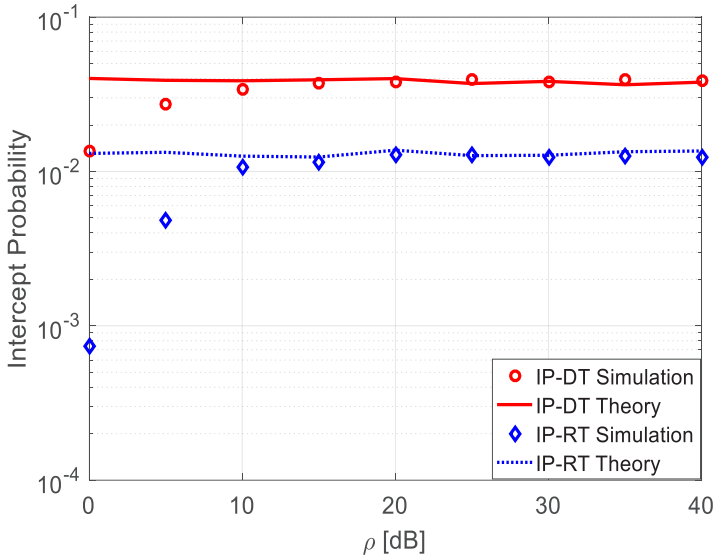

Fig.3. Comparing intercept probability versus transmit SNR (ρ) in [*dB*] for both DT and RT protocols.

Accordingly, SOP in the RT protocol is calculated as follows:

$$
\begin{aligned}
P_{out,T}^{RT} &= \Pr\left\{R_{s,T}^{RT} < R\right\} = \Pr\left\{\frac{1}{2}\log_2(1+\gamma_D) < R\right\} \\
&= \Pr\left\{1+\gamma_D < 2^{2R}\right\} = \Pr\left\{1+\frac{\rho_1\rho_r\lambda_{r2}}{\rho_1+\rho_r\vartheta} < 2^{2R}\right\} \\
&= \Pr\left\{\lambda_{r2} < \frac{(\rho_1+\rho_r\vartheta)(2^{2R}-1)}{\rho_1\rho_r}\right\} \\
&= \Pr\left\{\lambda_{r2} < \frac{(\rho_1+\rho_r\vartheta)(2^{2R}-1)}{\rho_1\rho_r}\middle|\vartheta\right\} \\
&\quad E_\vartheta\left(F_{\lambda_{r2}}\left(\frac{(\rho_1+\rho_r\vartheta)(2^{2R}-1)}{\rho_1\rho_r}\right)\right) \\
&= 1-E_\vartheta\left(\exp\left(-\frac{(\rho_1+\rho_r\vartheta)(2^{2R}-1)}{\rho_1\rho_r\mu_{r2}}\right)\right) \\
&= 1-\frac{2^{2R}-1}{\rho_1\mu_{1r}}e^{\frac{(2^{2R}-1)}{\rho_r\mu_{r2}}}e^{\frac{(2^{2R}-1)}{\rho_1\mu_{1r}}}E_i\left(-\frac{2^{2R}-1}{\rho_1\mu_{1r}}\right).
\end{aligned}
\tag{30}
$$

The proof of Eq. (30) is mentioned in Appendix C.

From Eq. (30), the following result follows:

1) The probability of a secrecy outage decreases by increasing channel gain between the relays, and D1 and D2 (μ_{1r} and μ_{r2}), and the increase in μ_{1r} is greater than in μ_{r2} .

2) Increase in transfer SNR decreases SOP.

Note that since the relay is trusted, probability of eavesdropping is not important, and in the trusted relay scenario calculation of SOP suffice.

7- NUMERICAL RESULTS

In this section, we will examine the simulation results in two protocols, DT and RT, to verify the validity of the calculated relationships. In this study, D1, D2, untrusted relay and jamming are assumed to be located at (-1, 0), (1, 0), (0, 0) and (0, 0.2) points,

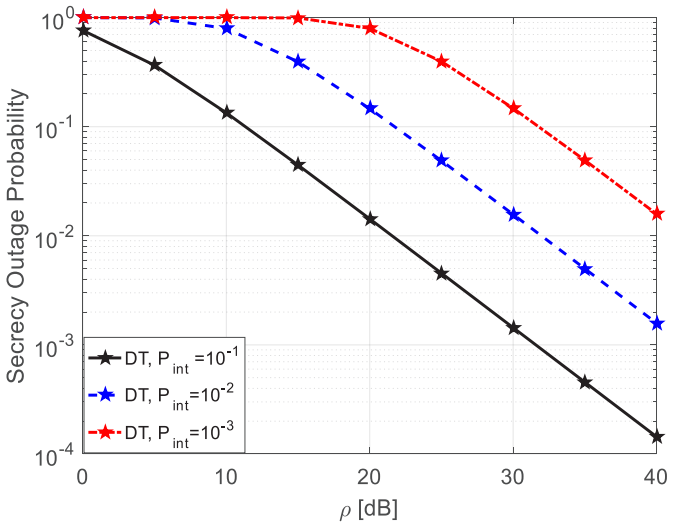

Fig.4. Trade-off between the secrecy outage and intercept probability for DT protocol.

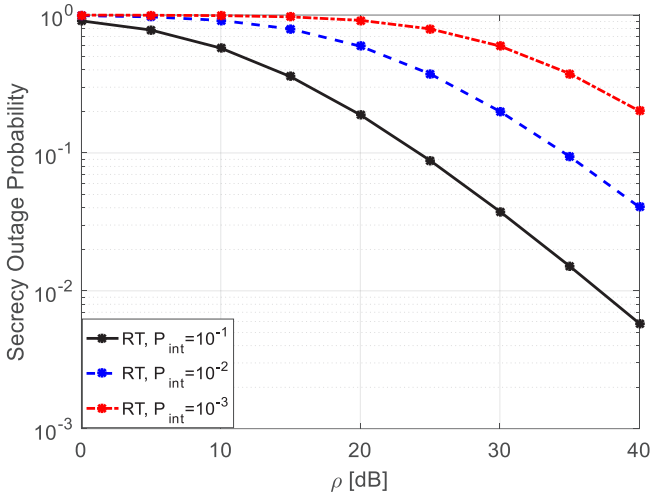

Fig.5. Trade-off between secrecy outage and intercept probability for RT protocol.

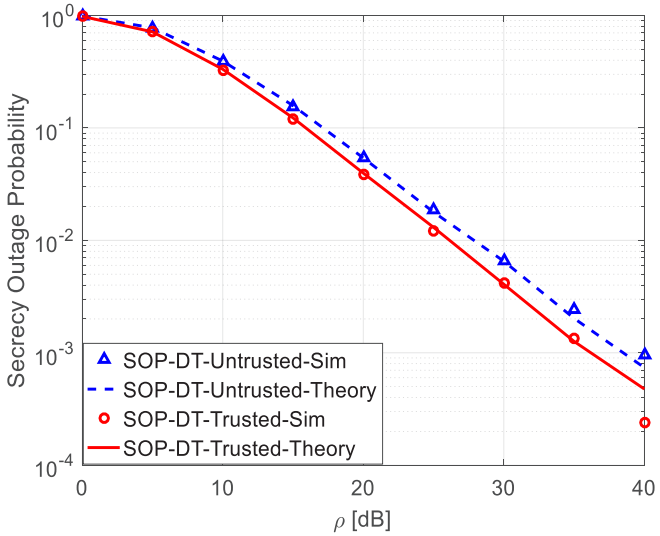

Fig. 6. Comparison of the SOP for the trusted and untrusted relay scenarios in the DT protocol.

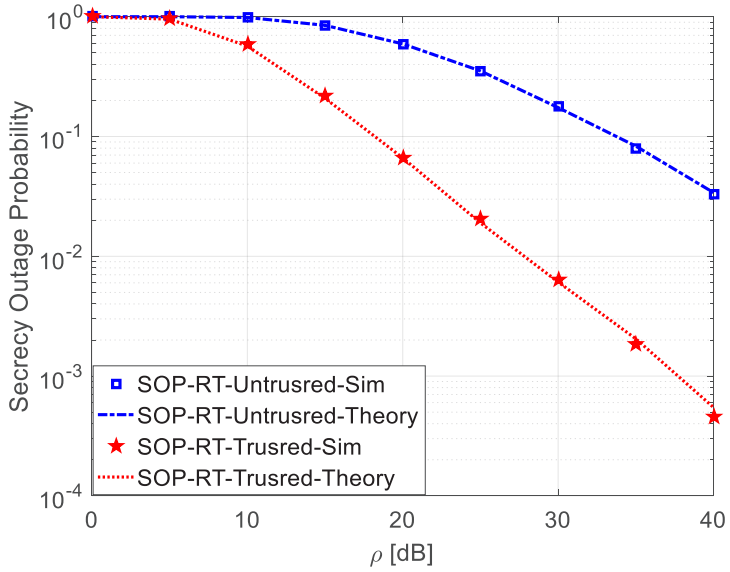

Fig. 7. Comparison of the SOP for the trusted and untrusted relay scenarios in the RT protocol.

respectively. The waste path component is considered $n=2$ and the channel gain between the i and j nodes is changed to $\mu_{ij}=d_{ij}^{-n}$, where d_{ij} is the distance between the nodes i and j. The system data rate is $R=1$ and assumes that $\rho_1=\rho_r=\rho_j=\rho$ and $\lambda_{jr}\gg(\lambda_{1r},\lambda_{r2})$.

Fig. 2 shows the intercept probability in terms of transmit SNR (ρ) for DT and RT protocols. The results show that they follow the analytic relations well. Simulation results show that the higher the transmit SNR, the lower the SOP in both protocols. In addition, with the increase of transmit SNR, the SOP in the DT protocol begins to decrease initially and decreases in higher rate more than the RT protocol, while in the RT protocol, the SOP in transmit SNRs is a lower than one and it begins to decrease with increasing transmit SNR and about $\rho=10dB$ later on. In other words, reliability in the DT protocol is greater than the RT protocol, and this reliability increases with increasing ρ in both protocols.

In Fig. 3, the intercept probability in terms of transmit SNR (ρ) for both the DT and RT protocols has been investigated. On this basis, it is seen that the intercept probability in both protocols in a higher SNR reaches a constant value of less than one. This value is lower for the RT protocol than the DT protocol, which indicates that the intercept probability in the RT protocol is lower than the DT protocol. In other words, security in the RT protocol is more than the DT protocol. Also, in both protocols for probing more than $\rho=15dB$, the intercept probability is fixed and the simulation results are as valid as the analyzes.

Fig. 4 shows a trade-off between the SOP and the probability of eavesdropping for the DT protocol. It is noted that the probability of eavesdropping decrease, the intercept outage probability increases. In other words, increasing the security increases the probability of loss of communication, and increasing the probability of secure communication reduces the security of communications.

Fig. 5 shows the trade-off between the SOP and the intercept probability for the RT protocol. As much as DT protocol, as the intercept probability increases the SOP decreases. For example, $P_{int}=10^{-3}$ is more secure than $P_{int}=10^{-1}$, but the probability of loss of communication becomes higher. Therefore, there must be a trade-off between security and reliability.

Also, by comparing Figs. 4 and 5, it can be seen that in a defined intercept probability, the SOP in the DT protocol decreases as compared to the RT protocol. This indicates that with a defined security, the DT protocol is more reliable than the RT protocol.

In Figs. 6 and 7, SOP of the trusted and untrusted relays are compared in DT and RT protocols, respectively. It is worth mentioning that the location of nodes and other simulation parameters are considered the same for the trusted and untrusted relay scenarios. Simulation results show that in both protocols, the SOP in the trusted relay scenario is lower than in the untrusted relay scenario, and the difference is more significant in the RT protocol. Since the DT protocol does not use a relay for communication, the untrusted relay that appears in this protocol as the eavesdropper, does not make much difference. However, in the RT protocol in which a relay is used to assist communication, the existence of a trusted relay greatly decreases the SOP and with the increase in SNR this decrease occurs more rapidly.

8- CONCLUSION

In this paper, the SRT in a D2D network was investigated. In the system model, an AF untrusted relay can be involved to assist the D2D communication. Furthermore, a jammer may help to improve the secrecy performance. Based on the dual role of the relay in the form of an eavesdropper and D2D communication facilitator, the DT and RT protocols were investigated. For this purpose, first, for two protocols, the SOP and the intercept probability was analyzed by providing

the closed form relations. Then SRT was examined by providing closed relationships. The simulation results showed the correction of analytic relationships and provided a good insight into the design of D2D networks with trading-off between reliability and security.

APPENDIX A

Assuming that $F_X(x)$ is the probability distribution (cdf) function of the random variable (rv) X and the probability density function (pdf) for λ_{r2}, follows the exponential distribution $f_{\lambda_{r2}}(x)=\left(\left(1/\mu_{r2}\right)e^{-x/\mu_{r2}}\right)$, $F_{\lambda_{r2}}$ is obtained in Eq. (15) as follows:

$$F_{\lambda_{r2}}\left(\frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\nu}\right)=\int_0^{\frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\nu}} f_{\lambda_{r2}}(x)\,dx$$
$$=\int_0^{\frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\nu}}\left(\frac{1}{\mu_{r2}}\right)e^{-\frac{x}{\mu_{r2}}}dx=1-\exp\left(-\frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\mu_{r2}\nu}\right). \tag{A.1}$$

To obtain Eq. (15) with the definition of $\nu=\frac{\lambda_{1r}}{\lambda_{jr}}$, and assuming that the probability density functions for λ_{1r} and λ_{jr} follow the exponential distributions $f_{\lambda_{1r}}(x)=\left(1/\mu_{1r}\right)e^{-x/\mu_{1r}}$ and $f_{\lambda_{jr}}(x)=\left(1/\mu_{jr}\right)e^{-x/\mu_{jr}}$, the probability density function ν is calculated as follows:

$$f_\nu(x)=\frac{\partial}{\partial x}F_\nu(x)=\frac{\partial}{\partial x}\left(\Pr\{\nu<x\}\right)$$
$$=\overbrace{\frac{\partial}{\partial x}\int_0^\infty\int_0^{\beta x} f_{\lambda_{1r}}(\alpha)f_{\lambda_{jr}}(\beta)\,d\alpha\,d\beta}^{A_1}$$
$$=\int_0^\infty\left(\frac{\partial}{\partial x}\int_0^{\beta x} f_{\lambda_{1r}}(\alpha)\,d\alpha\right)f_{\lambda_{jr}}(\beta)\,d\beta \tag{A.2}$$
$$=\int_0^\infty\left(\overbrace{\beta f_{\lambda_{1r}}(\beta x)}^{A_2}\right)f_{\lambda_{jr}}(\beta)\,d\beta=\overbrace{\frac{\mu_{1r}}{\mu_{jr}}\left(\frac{1}{\left(x+\frac{\mu_{1r}}{\mu_{jr}}\right)^2}\right)}^{A_3},$$

where A_1 is derived from the independence of λ_{1r} and λ_{jr}. Also, A_2 follows [16-Eq.0.410], and A_3 obtained after inserting pdfs of λ_{1r} and λ_{jr} and using [16-Eq.4.381.4]. Accordingly, we have:

$$E_\nu\left(\exp\left(-\frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\mu_{r2}\nu}\right)\right)=\int_0^\infty e^{-\frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\mu_{r2}\nu}} f_\nu(x)\,dx$$
$$=\overbrace{\frac{\mu_{1r}}{\mu_{jr}}\int_0^\infty e^{-\frac{\rho_j\left(2^{2R}-1\right)}{\rho_1\rho_r\mu_{r2}}\times\frac{1}{x}}\left(\frac{1}{\left(x+\frac{\mu_{1r}}{\mu_{jr}}\right)^2}\right)dx}^{A_4} \tag{A.3}$$
$$=e^{\frac{\rho_j\mu_{jr}\left(2^{2R}-1\right)}{2\rho_1\rho_r\mu_{1r}\mu_{r2}}}W_{-1,-\frac{1}{2}}\left(\frac{\rho_j\mu_{jr}\left(2^{2R}-1\right)}{\rho_1\rho_r\mu_{1r}\mu_{r2}}\right).$$

where A_4 is obtained from the pdf placement of the function ν and Eq. (A.3) with respect to [16-Eq. 3.471.7].

Appendix B

With the definition of $N=\frac{\lambda_{1r}}{\lambda_{jr}}$ and $\nu=\frac{\rho_j}{\rho_1}\left(2^R-1\right)$ and assuming that the probability density functions for λ_{1r} and λ_{jr} follow exponential distributions $f_{\lambda_{1r}}(x)=\left(1/\mu_{1r}\right)e^{-x/\mu_{1r}}$ and $f_{\lambda_{jr}}(x)=\left(1/\mu_{jr}\right)e^{-x/\mu_{jr}}$; we have:

$$F_N(\nu)=\Pr\{N\le\nu\}=\Pr\left\{\frac{\lambda_{1r}}{\lambda_{jr}}\le\nu\right\}=\Pr\left\{\lambda_{1r}\le\nu\lambda_{jr}\right\}$$
$$=\Pr\left\{\lambda_{1r}\le\nu\lambda_{jr}\,\middle|\,\lambda_{jr}\right\}=$$
$$E_{\lambda_{jr}}\left(\Pr\left\{\lambda_{1r}\le\nu\lambda_{jr}\,\middle|\,\lambda_{jr}\right\}\right)=E_{\lambda_{jr}}\left(F_{\lambda_{1r}}\left(\nu\lambda_{jr}\right)\right) \tag{B.1}$$
$$=E_{\lambda_{jr}}\left(1-e^{-\frac{\nu\lambda_{jr}}{\mu_{1r}}}\right)=1-\int_0^\infty e^{-\frac{\nu\lambda_{jr}}{\mu_{1r}}}f_{\lambda_{jr}}(x)\,dx\ \backslash$$
$$=1-\frac{\mu_{1r}}{\mu_{1r}+\frac{\rho_j}{\rho_1}\left(2^R-1\right)\mu_{jr}}.$$

APPENDIX C

Similar to Appendix A, assuming $F_X(x)$ as the function of probability distribution of the random variable X and the probability density function for λ_{r2} follows the exponential distribution $f_{\lambda_{r2}}(x)=\left(1/\mu_{r2}\right)e^{-x/\mu_{r2}}$, in Eq. (30) $f_{\lambda_{r2}}$ is obtained as:

$$F_{\lambda_{r2}}\left(\frac{\left(\rho_1+\rho_r\vartheta\right)\left(2^{2R}-1\right)}{\rho_1\rho_r}\right)$$
$$=\int_0^{\frac{\left(\rho_1+\rho_r\vartheta\right)\left(2^{2R}-1\right)}{\rho_1\rho_r}} f_{\lambda_{r2}}(x)\,dx$$
$$=\int_0^{\frac{\left(\rho_1+\rho_r\vartheta\right)\left(2^{2R}-1\right)}{\rho_1\rho_r}}\left(\frac{1}{\mu_{r2}}\right)e^{\frac{-x}{\mu_{r2}}}dx \tag{C.1}$$
$$=1-\exp\left(-\frac{\left(\rho_1+\rho_r\vartheta\right)\left(2^{2R}-1\right)}{\rho_1\rho_r\mu_{r2}}\right),$$

T

o obtain Eq. (30) by defining $\vartheta=\frac{\lambda_{r2}}{\lambda_{1r}}$ assuming that the probability density functions for λ_{1r} and λ_{r2} follow the exponential distributions $f_{\lambda_{1r}}(x)=\left(1/\mu_{1r}\right)e^{-x/\mu_{1r}}$ and $f_{\lambda_{r2}}(x)=\left(1/\mu_{r2}\right)e^{-x/\mu_{r2}}$ respectively, the probability density function is calculated as:

$$
\begin{aligned}
f_{\vartheta}(x) &= \frac{\partial}{\partial x} F_{\vartheta}(x) = \frac{\partial}{\partial x}\left(\Pr\{\vartheta < x\}\right) \\
&= \overbrace{\frac{\partial}{\partial x}\int_0^{\infty}\int_0^{\beta x} f_{\lambda_{r2}}(\alpha) f_{\lambda_{1r}}(\beta)\, d\alpha\, d\beta}^{C_1} \\
&= \int_0^{\infty}\left(\frac{\partial}{\partial x}\int_0^{\beta x} f_{\lambda_{r2}}(\alpha)\, d\alpha\right) f_{\lambda_{1r}}(\beta)\, d\beta \\
&= \int_0^{\infty}\left(\overbrace{\beta f_{\lambda_{r2}}(\beta x)}^{C_2}\right) f_{\lambda_{1r}}(\beta)\, d\beta \\
&= \overbrace{\frac{\mu_{r2}}{\mu_{1r}}\left(\frac{1}{\left(x+\frac{\mu_{r2}}{\mu_{1r}}\right)^2}\right)}^{C_3},
\end{aligned}
\tag{C.2}
$$

The value of C_1 is obtained by λ_{1r} and λ_{r2} being independent. Also, C_2 is based on [16-Eq. 0.410] and C_3 is obtained by inserting pdfs λ_{1r} and λ_{r2} and based on [16-Eq. 3.353.3].

Accordingly, we have [16-Eq. 3.353.3]:

$$
\begin{aligned}
E_{\vartheta}\left(\exp\left(-\frac{(\rho_1+\rho_r\vartheta)\left(2^{2R}-1\right)}{\rho_1\rho_r\mu_{r2}}\right)\right) &= \int_0^{\infty} e^{-\frac{(\rho_1+\rho_r\vartheta)\left(2^{2R}-1\right)}{\rho_1\rho_r\mu_{r2}}} f_{\vartheta}(x)\, dx \\
&= \overbrace{\frac{\mu_{r2}}{\mu_{1r}}\int_0^{\infty} e^{-\frac{\left(2^{2R}-1\right)}{\rho_1\mu_{r2}}\times\left(\frac{\rho_1}{\rho_r}+x\right)}\left(\frac{1}{\left(x+\frac{\mu_{r2}}{\mu_{1r}}\right)^2}\right) dx}^{C_4} \\
&= \frac{2^{2R}-1}{\rho_1\mu_{1r}} e^{-\frac{\left(2^{2R}-1\right)}{\rho_r\mu_{r2}}} e^{\frac{\left(2^{2R}-1\right)}{\rho_1\mu_{1r}}} E_i\left(-\frac{2^{2R}-1}{\rho_1\mu_{1r}}\right).
\end{aligned}
\tag{C.3}
$$

where C_4 is obtained by inserting pdf ϑ.

REFERENCES

[1]A. Kuhestani, A. Mohammadi, and P. L. Yeoh, "Optimal Power Allocation and Secrecy Sum Rate in Two-Way Untrusted Relaying Networks with an External Jammer," *IEEE Transactions on Communications,* vol. 66, no. 6, pp. 2671-2684, 2018.

[2]A. Kuhestani and A. Mohammadi, "Destination-based Cooperative Jamming in Untrusted Amplify-and-Forward Relay Networks: Resource Allocation and Performance Study," *IET Communications,* vol. 10, no. 1, pp. 17-23, Jan. 2016.

[3]A. Asadi, Q. Wang, and V. Mancuso, "A Survey on Device-to-Device Communication in Cellular Networks," *IEEE Communications Surveys & Tutorials,* vol. 16, pp. 1801-1819, 2014.

[4]O. N. Hamoud, T. Kenaza, and Y. Challal, "Security in Device-to-Device Communications: A Survey," *IET Networks,* vol. 7, no. 1, pp. 14-22, Jan. 2018.

[5]Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode Selection and Spectrum Partition for D2D Inband Communications: A Physical Layer Security Perspective," *IEEE Transactions on Communications,* Feb. 2018.

[6]Y. Yang, Y. Zhang, L. Dai, J. Li, S. Mumtaz, and J. Rodriguez, "Transmission Capacity Analysis of Relay-Assisted Device-to-Device Overlay/Underlay Communication," *IEEE Transactions on Industrial Informatics,* vol. 13, pp. 380-389, 2017.

[7]S. N. Islam, M. A. Mahmud, and A. M. T. Oo, "Achievable Sum Rate Analysis of Relay Aided Overlay Device to Device Communication Among Multiple Devices," *Journal of Communications and Networks,* vol. 19, pp. 309-318, 2017.

[8]M. Izanlou, A. Mohammadi, and M. Dosaranian-Moghadam, "Optimal Power Allocation for Physical Layer Security in Device-to-Device Communications using Untrusted Relays," *Transactions on Emerging Telecommunications Technologies*, https://doi.org/10.1002/ett.3623, 26 Apr. 2019.

[9]D. Chen,L. Wang,T. Yin, X. Xu, W. Yang,Y. Cai, and W. Yang, "Reliability and Security Performance Analysis of Non-Regenerative Untrusted Relay Networks," *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, Nanjing, pp. 1-5, 2015.

[10]J. Zhu, Y. Zou, B. Champagne, W. Zhu and L. Hanzo, "Security–Reliability Tradeoff Analysis of Multirelay-Aided Decode-and-Forward Cooperation Systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp. 5825-5831, July 2016.

[11]A. Kuhestani, A. Mohammadi and P. L. Yeoh, "Security-Reliability Trade-off in Cyber-Physical Cooperative Systems with Non-Ideal Untrusted Relaying," *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, pp. 552-557, 2018.

[12]M. T. Mamaghani and R. Abbas, "Security and Reliability Performance Analysis for Two-Way Wireless Energy Harvesting based Untrusted Relaying with Cooperative Jamming," *IET Communications*, vol. 13, no. 4, pp. 449-459, 2019.

[13]J. Zhu, Z. Liu, Y. Jiang and Y. Zou, "Security-Reliability Tradeoff for Relay Selection in Cooperative Amplify-and-Forward Relay Networks," *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, Nanjing, 2015, pp. 1-4, 2015.

[14]Y. Zou, X. Wang, W. Shen and L. Hanzo, "Security Versus Reliability Analysis of Opportunistic Relaying," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 6, pp. 2653-2661, July 2014.

[15]C. Zhang, J. Ge, F.Gong, F. Jia, and N. Guo, "Security-Reliability Tradeoff for Untrusted and Selfish Relay-Assisted D2D Communications in Heterogeneous Cellular Networks for IoT," *IEEE Systems Journal*, pp. 1-10, 11 Sept 2019.

[16]I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products,* 7th ed. New York: Academic, 2007.

[17]B. He, Y. She, and V. K. N. Lau, "Artificial Noise Injection for Securing Single-Antenna Systems", *IEEE Transactions on Vehicular Technology,* vol. 66, no. 10, pp. 9577 - 9581, Oct. 2017.

[18]T.-X. Zheng, H.-M. Wang, H. Deng, "Improving Anti-Eavesdropping Ability without Eavesdropper's CSI: A Practical Secure Transmission Design Perspective," *IEEE Wireless Communications Letters*, vol. 7, no. 6, pp. 946 - 949, Dec. 2018.

HOW TO CITE THIS ARTICLE

M.Izanlou, A.Mohammadi, M.Dosaranian-Moghadaz, Security and Reliability Trade-off in Device to Device Communications with Untrusted Relays, AUT J. Model. Simul., 52(2) (2020) 167-178.

DOI: 10.22060/miscj.2020.17653.5190