Jurnal Rekayasa Elektrika Vol. 19, No. 3, September 2023, page 115-121
ISSN. 1412-4785; e-ISSN. 2252-620X, Accredited by Kemendikbudristek No. 105/E//KPT/2022
DOI: 10.17529/jre.v19i3.29486

Secrecy Capacity of Cooperative D2D Multi-relay Communication System with Multiple Protocols Based on Max-Min Relay Selection

Nurul Maulida Fitri, Yunida Yunida, Melinda Melinda, and Nasaruddin Nasaruddin*
Department of Electrical and Computer Engineering, Universitas Syiah Kuala
Jln. Tgk. Syech Abdurrauf No. 7 Kopelma Darussalam, Banda Aceh 23111
*e-mail: nasaruddin@usk.ac.id

***Abstract*—The utilization of other devices as relays in cooperative device-to-device (D2D) communication systems does not fully guarantee the security of confidential information from being intentionally or unintentionally accessed by eavesdroppers. Therefore, the implementation of a method to enhance the security performance of information is highly necessary. This paper proposes the application of relay selection mechanisms in a communication system with three relay protocols: amplify-and-forward (AF), decode-and-forward (DF), and quantize-and-forward (QF). The research method employs a mathematical modeling approach and simulations. The simulation results demonstrate an improvement in the level of information security in cooperative D2D communication systems using the proposed method in multiple relay protocols. The relay selection method has been evaluated and compared based on the secrecy outage probability (SOP), which is one of the parameters for information security in the communication system. The SOP achieved is smaller with the implementation of the max-min relay selection technique in multi-relay cooperative communication networks. Considering the presence or absence of eavesdroppers, the SOP of the DF relay is smaller compared to other protocols. The impact of distance on secrecy capacity also indicates that the DF protocol utilizing multiple relays achieves higher results compared to other protocols, and the increased usage of relays also affects the simulation outcomes.**

Keywords: ***cooperative d2d, eavesdropper, max-min relay selection, relay protocol, secrecy outage probability***

I. Introduction

The ease of wireless communication technology has brought us to an era where there is a high demand for services with high data rates and Quality-of-Service (QoS), including cellular and multimedia communication. Device-to-device (D2D) is a wireless communication system implemented in Fifth Generation (5G) technology due to its reliability in improving spectrum efficiency through cellular spectrum reuse and enhancing QoS by utilizing links established between neighboring devices [1]. In D2D communication, two neighboring devices can communicate directly without involving the base station (BS), making the system more efficient. However, due to the limitation of the distance between devices, the transmission quality deteriorates, necessitating the use of relays between these devices [2]. Communication systems that employ other devices as relays are referred to as cooperative communication systems.

Cooperative communication systems employ three main protocols that are commonly used, namely amplify-and-forward (AF), decode-and-forward (DF), and quantize-and-forward (QF). These three protocols determine how the received information signal from the source is processed by the relay before being forwarded to the destination. The use of relays in D2D cooperative communication has a drawback in that during the relay's transmission of information, there is no standardized recognition among the devices. This is due to the lack of centralized supervision and control of the relay by the base station during the process of transmitting information from the source to the destination, resulting in the potential disclosure of confidential information to eavesdroppers, intentionally or unintentionally, leading to a decrease in the communication system's performance [3]. D2D devices can be cellular subscribers or other devices, including low-power Internet-of-Things (IoT) devices. Paper [4] examines the secrecy capacity of a cooperative scheme where D2D users must perform sensing of channel availability during a specific time period before using that channel. If the cellular user's link is active, the D2D user will transmit artificial noise to disrupt eavesdroppers in the vicinity, known as friendly jamming, which is a concept in physical layer security [4].

Physical layer security for wireless communication offers a solution to enhance security by leveraging the fading characteristics of wireless channels. Fading occurring in wireless communication scenarios can improve secure communication capabilities in the presence of eavesdroppers, without relying on the network layer [5]. This concept was initially proposed by Shannon and Wyner [6], where the fundamental principle of physical

Received 13 December 2022; Revised 1 July 2023; Accepted 31 July 2023

layer security is to exploit the physical characteristics of wireless channels to prevent eavesdropping interference during an ongoing communication. This selection process operates proactively before transmitting the information signal, employing single relay selection and considering the presence of eavesdroppers [7].

Despite its advantages in terms of spectrum efficiency, improved user experience, and high-speed data transmission for short-range communication, there are several challenges in terms of mode selection, device discovery, and interference management. Study [8] focuses on analyzing the secrecy rate for D2D cases with cellular communication under the influence of time-frequency resource allocation within a cell, considering four strategies: (a) single eavesdropper scenario; (b) cooperative multiple eavesdroppers capable of interfering with each other; (c) cooperative multiple eavesdroppers capable of interfering with both interference and artificial noise; and (d) multiple eavesdroppers acting simultaneously.

The study [9] explains that previous studies have not adequately considered important parameters such as power influence. In a simple scenario, a BS and each user utilize fixed power levels and are unable to adjust the power according to the varying distance requirements. Additionally, power control can also conserve energy consumption and reduce potential interference among communications using the same spectrum. Therefore, further research [9] develops a theoretical model of D2D communication networks to test the secrecy capacity, which involves multiple BSs, paired D2D devices, cellular users, and eavesdroppers, where the eavesdropper can intercept information from user devices. User devices are defined as capable of adjusting transmission power according to the required threshold standards.

The purpose of this paper is to enhance the security performance of cooperative D2D communication systems through the use of relay selection methods with multiple protocols. The paper proposes a relay selection method where the selected relay for forwarding information from the source is capable of maximizing secrecy capacity, taking into account the presence of eavesdroppers, using the distance ratio information between the source-to-relay and relay-to-destination/relay-to-eavesdropper. Furthermore, the paper evaluates and compares the performance of secrecy outage probability (SOP) with respect to signal-to-noise ratio (SNR) and secrecy capacity with respect to the distance ratio, considering the goal of achieving higher secrecy capacity and power savings, which are parameters for information security in the physical layer. The proposed method utilizes the AF, DF, and QF protocols in the cooperative D2D system and proves useful for characterizing the trade-off between reliability and security more accurately.

The remaining parts of this work are formatted as follows. The literature review and system model for cooperative D2D communication systems with multi-relay are presented in Section II and Section III, respectivelty. The simulation result and discussion are provided in Section IV. Finally, a brief conclusion is presented in Section V.

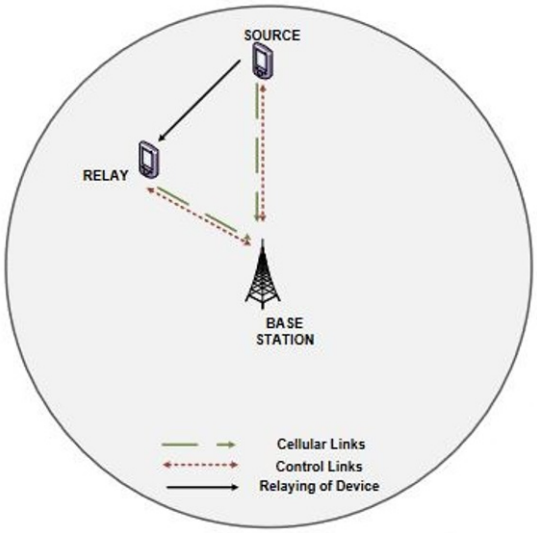

Figure 1. Cooperative D2D communication system with BS as the controller [11]

II. Literature Review

A. Cooperative D2D Communication

In wireless systems, D2D communication can be enabled in a condition known as two-tier networks, consisting of the macro cell network and the device network itself [10]. The difference between D2D communication and conventional cellular communication is that conventional cellular communication is supported through the macro cell tier, while D2D communication is supported by the device tier, where guaranteed and reliable services can be obtained by each device located at the edge/outer area of the cell and devices within high-traffic areas of the cell. When a group of devices within the cell region establishes direct D2D communication, the BS has partial or full access control over the communication process among those devices [11].

Cooperative D2D communication is one type of D2D communication system where a device (source) located at the cell edge or with a poor coverage area can communicate with the BS by forwarding information through other nearby devices (relays). An illustration of the cooperative D2D communication system is shown in Figure 1. All processes involved in establishing communication among the devices are directly handled by the BS, thereby improving the resilience of user devices [11]. This system facilitates cooperation between nodes in a network and can reduce transmission energy consumption. The benefits of this technique include improved reliability, throughput, capacity, and wireless transmission range [12].

B. Cooperative D2D Protocols

Based on the relay method in cooperative D2D

communication systems, there are three commonly used protocols, namely amplify and forward (AF), decode and forward (DF), and quantize and forward (QF).

1. Amplify-and-forward (AF): A simple protocol that allows a relay to amplify and retransmit the received signal from the source to the destination. One advantage of using the AF protocol in a simple implementation is that AF relays only forward the received signal from the source without relying on any decoding operations. However, a disadvantage is that the noise received at the relay can also be forwarded to the destination, resulting in a degraded performance at the destination during the decoding of the source signal [13].
2. Decode-and-forward (DF): A cooperative method in which the relay detects the received information signal from the source. Then, the detected information signal is decoded and subsequently forwarded to the destination [13].
3. Quantize-and-forward (QF): A cooperative method in which the relay performs quantization on the received information signal from the source before forwarding it to the destination with an improved signal quality [14].

C. Security in Cooperative D2D Communication Systems

Security is one of the primary concerns that need to be addressed properly before D2D techniques are widely implemented. Wireless transmission characteristics, such as Wi-Fi and Bluetooth communication, are vulnerable to various attacks that can compromise the three basic principles of security: information confidentiality, information integrity, and service availability [10]. Therefore, there is a need for robust security enhancements in D2D communication to counteract the factors or types of disruptions present in wireless communication.

There are several factors that influence and disrupt D2D communication systems, including [15]:

1. Eavesdropping attack, where an attacker passively listens to the channel between devices to obtain sensitive data.
2. Impersonation attack, where an attacker can impersonate a legitimate device to gain access to data traffic.
3. Forgery attack, where an attacker can forge content and send fake data to all devices, deceiving the system.
4. Free riding attack is an attack aimed at reducing availability in D2D communication. The attacker may control multiple devices to consume their energy, thus preventing them from transmitting content to others while still receiving data requests from other devices.
5. Active attack on control data, where an attacker attempts to modify control data.
6. Privacy breach, which includes sensitive private data such as identity, location, and others that are more related to D2D services, thus requiring the protection of this personal information from unauthorized parties.
7. Denial-of-Service (DoS) attacks cause the unavailability of services in D2D communication.

At the physical layer, this method is to explore the physical characteristics of the wireless channel to prevent eavesdroppers from interrupting ongoing wireless communication. The mechanisms of confidentiality and security at the physical layer can further be categorized into methods that silently or securely transmit information using the characteristics of the wireless medium, and methods that extract secret message information from the wireless medium. There are several fundamental research studies related to security systems that work at the physical layer. First, the fading phenomenon in wireless communication serves to enhance the ability to communicate silently and securely. Second, the broadcast nature of the wireless medium allows one to introduce interference into the medium, which can jeopardize the attacker's capability while strengthening the communication capabilities of two legitimate nodes [5]. However, in this study, we focus only on the secrecy capacity of the D2D system with considered eavesdropping attacks between communicating devices.

D. Relay Selection Method

The relay selection method is one of the techniques used in efforts to enhance the security of cooperative D2D communication systems. In this technique, the source transmits information to several relays in its vicinity. Then, the source determines the best relay that can maximize the secrecy capacity of the communication system as the relay is authorized to forward the information to the destination. The relay selection process consists of a conventional scheme through max-min relay selection, where the best relay is chosen based on the maximum of the minimum SNR between the first and second nodes, known as a proactive relay selection strategy before the information is transmitted by the source. The relay node will first send the channel state information (CSI), typically in the form of SNR information, as a measure for the source to determine the best relay to be selected [16].

III. System Model

The proposed cooperative D2D communication system model in this paper is a multi-relay model based on relay selection using multiple relay protocols, namely AF, DF, and QF. The system model can be seen in Figure 2, which consists of one source (S) that wants to communicate with the destination (D) through eight nearby relay nodes (R_1, R_2, R_3, R_4, R_5, R_6, R_7, and R_8) and one eavesdropper. The eavesdropper is an attacking device that passively listens to the channel between devices to obtain information data from the source. The relay selection method is used to select the best relay to forward the information to D. The relay selection method considered in this paper is the

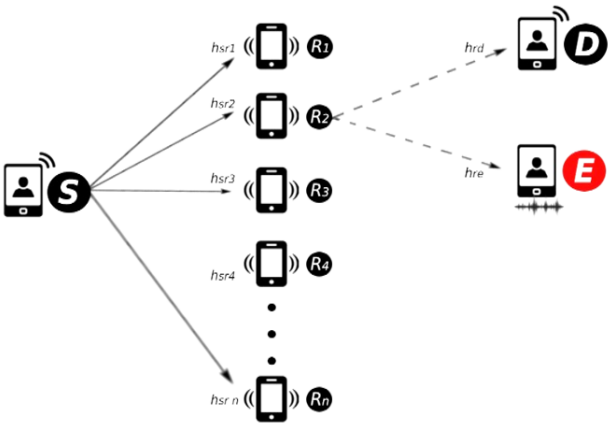

Figure 2. The model of a cooperative D2D system with an eavesdropper located near the destination

max-min method, which involves estimating the channel quality or CSI through an estimation process before the information is transmitted. This is done by sending training bits first to determine the SNR quality between the source (S), relay (R), and destination (D). This then becomes the basis for selecting the best relay for the multi-relay cooperative D2D communication system.

The system model in this paper assumes the use of a half-duplex mode, where each node cannot transmit and receive information signals simultaneously. Before the actual communication phase occurs, there is a training phase where S sends training bits to all R nodes to determine the SNR quality between the S-R-D links, which is the basis for selecting the best relay. Meanwhile, the half-duplex communication phase in this paper is divided into two time slots. In the first slot, S broadcasts the information signal to all three nearby R nodes. The received signal at each R node (R_1, R_2, R_3) can be written as follows:

$$y_{sr_k} = h_{sr_k} x_s + n_{r_k} \tag{1}$$

where h_{srk} is the channel coefficient between S and the k^{th} R, where k = 1, 2, 3, and n_{rk} is a random variable of additive white Gaussian noise (AWGN) at the k^{th} R with variance σ^2.

Furthermore, the received signal at each R node will undergo processing based on the considered cooperative protocol, namely AF, DF, or QF. After this processing, the relay with the best SNR value, which was selected during the training phase, will forward the information signal to the destination in the second phase. Based on the feedback obtained from the destination, the source calculates the SNR value to determine the best relay (r_b) using the max-min method through the following equation [17]:

$$r_b = \arg\max_{k=1,2,3} \left\{ \min\left(\mathrm{SNR}_{sr_k}, \mathrm{SNR}_{r_k d} \right) \right\} \tag{2}$$

where SNR_{srk} and SNR_{rkd} respectively are the SNR values between the source (S) and the k^{th} relay node, where k=1, 2, 3.

The signal forwarded by the selected relay (r_b) to the destination for each relaying protocol, AF, DF, and QF.

1. AF Protocol: The signal forwarded by the selected relay r_b to D in the second phase can be written as:

$$y_{r_b}^{AF} = \alpha y_{sr_b}, \tag{3}$$

where α is the amplification factor of the AF protocol, which can be calculated using the equation [13]:

$$\alpha = \sqrt{\frac{p_{r_b}}{\left|h_{sr_b}\right|^2 + p_s + n_{r_b}}} \tag{4}$$

with p_{rb} and p_s being the average transmission powers of S and the selected relay r_b, respectively. Furthermore, the received signal at the destination can be expressed as follows:

$$y_{r_b d}^{AF} = \alpha h_{r_b d}\, y_{sr_b} + n_d \tag{5}$$

where h_{rbd} is the channel coefficient of the link between the selected relay R to D, and n_d is the additive white Gaussian noise (AWGN) variable at node D with variance σ^2.

2. DF Protocol: The signal forwarded by the selected relay R to D in the second phase can be written as:

$$y_{r_b}^{DF} = \hat{y}_{sr_b}, \tag{6}$$

where $\hat{y}_{srb}$ is the decoded information signal from S to the selected relay R. Furthermore, the received signal at the destination can be expressed as follows:

$$y_{r_b d}^{DF} = h_{r_b d}\, \hat{y}_{sr_b} + n_d. \tag{7}$$

3. QF Protocol: The signal forwarded by the selected relay R to D in the second phase can be written as:

$$y_{r_b}^{QF} = Q\left(y_{sr_b}\right) \tag{8}$$

where $Q(y_{srb})$ is the quantization function of the received signal at the selected relay R from S. Furthermore, the received signal at the destination can be expressed as follows:

$$y_{r_b d}^{QF} = h_{r_b d}\, Q\left(y_{sr_b}\right) + n_d. \tag{9}$$

The second phase, in which the information transmitted by the selected relay to the destination is also intercepted by an eavesdropper in its vicinity, poses a security threat as the attacker attempts to obtain information from the source. This leads to a decrease in the performance and security level of the system's information. Therefore, it is necessary to analyze the secrecy capacity with performance parameters in the form of SOP, which will be explained in the following section.

In this section, the SOP parameter will be analyzed to determine the extent of performance degradation in cooperative multi-relay D2D communication systems using relay selection methods. The parameter used to analyze the SOP is the value of secrecy capacity between node D and the eavesdropper (E). Secrecy capacity is

defined as the difference between the channel capacity from the source to the destination and from the source to the eavesdropper [18]. The measurement of secrecy capacity is developed from an information-theoretic perspective and is denoted by the difference between the channel capacity from the source to the destination and from the source to the eavesdropper. If the secrecy capacity is negative, the eavesdropper will be able to decode the source code, and interception events will occur [19]. Therefore, the value of secrecy capacity must be positive, which can be expressed mathematically as follows:

$$C_{Secrecy} = \left[C_{r_b d} - C_{r_b e}\right]^{+} = \begin{cases} \frac{1}{2}\log_2\left(1+SNR_{r_b d}\right) - \frac{1}{2}\log_2\left(1+SNR_{r_b e}\right), C_{r_b d} > C_{r_b e} \\ 0, C_{r_b d} \le C_{r_b e}\ . \end{cases} \quad (10)$$

where C_{rbd} and C_{rbe} are the channel capacities of the R-D and R-E links, respectively, and their difference should be positive. SNR_{rbd} and SNR_{rbe} represent the SNR values of the R-D and R-E links, respectively, while n_d and n_e are the AWGN variables at D and E, respectively, with a variance of σ^2. Meanwhile, for each type of relay protocol, the secrecy capacity can be explained in the following sub-sections.

1. AF Protocol: The channel capacities R-D and R-E in the AF protocol, as referenced in [15], respectively are expressed as follows:

$$y_{r_b d}^{QF} = h_{r_b d}\, Q\left(y_{sr_b}\right) + n_d\,. \quad (9)$$

$$C_{r_b d}^{AF} = \log_2\left(1 + \frac{\left|h_{sr_b}\right|^2 \left|h_{r_b d}\right|^2}{\left|h_{r_b d}\right|^2 + \left|h_{sr_b}\right|^2}\gamma\right) \quad (11)$$

   where $\gamma = P/N_0$ is the system SNR, with P being the total transmission power and N_0 being the noise power.

2. Protocol DF: The channel capacity of R-D and R-E in DF protocol, as referenced in [15], respectively are expressed as follows:

$$C_{r_b d}^{DF} = \left[\gamma \min\left(\left|h_{sr_b}\right|^2, \left|h_{r_b d}\right|^2\right)\right] \quad (13)$$

$$C_{r_b e}^{DF} = \left[1 + \gamma\left|h_{r_b e}\right|^2\right]. \quad (14)$$

3. Protocol QF: For the QF protocol, the secrecy capacity of the R-D link is equal to R-E link that can be expressed as follows [20]:

$$C_{r_b d}^{QF} = C_{r_b e}^{QF} = \left[\gamma \max\left(\left|h_{sr_b}\right|^2, \left|h_{r_b d}\right|^2\right)\right]. \quad (15)$$

In a wireless communication system, a parameter used to measure the outage probability for secure communication is the SOP. SOP is defined as the probability that the secrecy capacity is lower than the minimum capacity or bit rate requirement (R_b) of the user [21]. SOP serves as a benchmark that indicates the extent to which information leaks during the transmission process or, technically speaking, the achieved secrecy rate of the system being less than the specified secrecy rate [19]. The mathematical equation for SOP can be seen as follows:

$$P_{\text{sec\_out}} = P_r\left[C_{Secrecy} < R_b\right]. \quad (16)$$

IV. Result and Discussion

The results in this paper are divided based on the protocol types for each scenario. The cooperative D2D communication system is considered in the first scenario without an eavesdropper, and the second scenario involves an eavesdropper. In the cooperative communication system, the SNR can be calculated based on the distance between the source, relay, and destination [22]:

$$\gamma_{s,r} = \frac{p_{s,r}}{d_{s,r^{\alpha}}} \quad (17)$$

$$\gamma_{r,d} = \frac{p_{r,d}}{d_{r,d^{\alpha}}} \quad (18)$$

$$\gamma_{r,e} = \frac{p_{r,e}}{d_{r,e^{\alpha}}}. \quad (19)$$

where $\gamma_{s,r}$ is the SNR from the source to the relay, $\gamma_{r,d}$ is the SNR from the relay to the destination, and $\gamma_{r,e}$ is the SNR from the relay to the eavesdropper.

We assume that the distance ratio from the source to the destination is 1, calculated as the ratio of the distance $d_{s,r}/d_{s,d}$. The distance for D2D communication is determined by the ratio of the distance from the source to the relay and from the relay to the destination/relay to the eavesdropper. The power at the source and relay is set to be the same for all protocols used. All simulations were conducted using MATLAB 2019a.

Simulation of secrecy capacity against distance ratio is performed to observe the influence of the number of relays using DF, AF, and QF protocols in the presence of an eavesdropper near the destination. In this simulation, 2 relays, 4 relays, 6 relays, and 8 relays are used, assuming a distance ratio between the source and destination ranging from 0.1 to 0.9.

The simulation results of secrecy capacity against distance ratio for the DF protocol can be seen in Figure 3, where in this simulation, using 8 relays resulted in a secrecy capacity of 2.04 bps/Hz. Figure 4 shows that the AF protocol, using 8 relays, resulted in a secrecy capacity of 1.38 bps/Hz, which is higher compared to using 2, 4, and 6 relays.

The next simulation shown in Figure 5 is the secrecy capacity against distance ratio for the QF protocol. This simulation also demonstrates the use of different numbers of relays, namely 2 relays, 4 relays, 6 relays, and 8 relays. The secrecy capacity value for 8 relays is 1.20 bps/Hz, which is significantly higher compared to the others.

The simulation presented in Figure 6 compares the secrecy capacity against distance ratio for the three

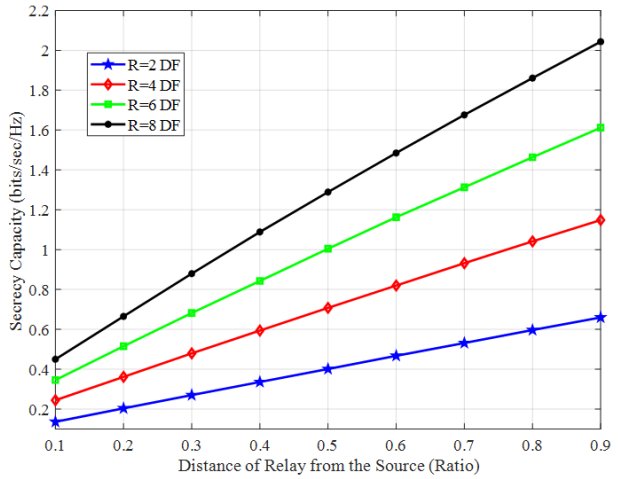

Figure 3. The model of a cooperative D2D system with an eavesdropper located near the destination

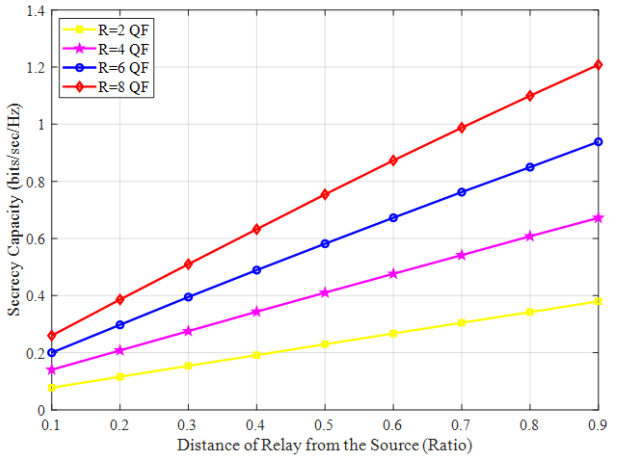

Figure 5. Secrecy capacity with respect to the distance ratio for the QF protocol

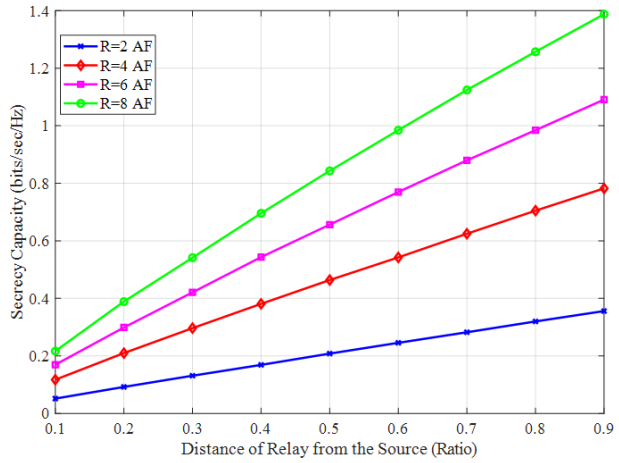

Figure 4. Secrecy capacity with respect to the distance ratio for the AF protocol

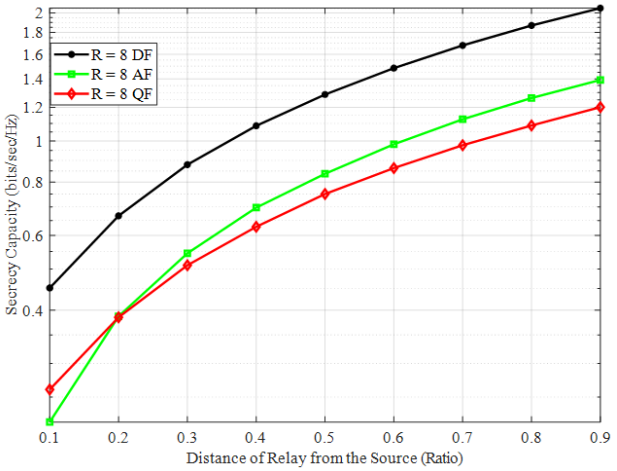

Figure 6. Secrecy capacity with respect to the distance ratio for the DF, AF, and QF protocols

protocols: DF, AF, and QF, using 2, 4, 6, and 8 relays. From the results of all three protocols, it can be observed that DF outperforms AF and QF with a higher secrecy capacity of 2.05 bps/Hz. This outcome is attributed to the signal amplification in AF, followed by noise amplification, while QF only involves quantization. The results of all three simulations demonstrate that the system performs better when using multiple relays. This is because an increased number of relays allows for more freedom in selecting the most suitable relay, resulting in a higher achieved secrecy capacity.

Figure 7 shows the SOP values against SNR by comparing the three protocols used: DF, AF, and QF. The simulation results in the graph depict the SOP for each protocol, demonstrating that DF outperforms AF and QF. The secure communication system's secrecy capacity and secrecy outage probability, achieved through cooperative communication with relay protocols DF, AF, and QF using the max-min technique, indicate that adding relays and selecting the best relay improves secrecy capacity and reduces SOP in the proposed model. The placement of relays at specific distances depends on the destination and eavesdropper locations [23]. Better and more secure system performance can be achieved to mitigate eavesdropping issues.

V. Conclusion

This paper has analyzed the performance of secrecy outage probability in cooperative communication systems using DF, AF, and QF protocols with the max-min relay selection technique. The paper has mathematically modeled and simulated the proposed method to enhance system security. Furthermore, the paper has simulated secrecy capacity with varying numbers of relays, specifically 2, 4, 6, and 8 relays. The simulation results demonstrate that the SOP using the DF protocol is higher compared to the other protocols (AF and QF), indicating successful information transmission from source to destination in the cooperative multi-relay network. Based on the distance ratio, the DF method yields higher values with an increasing number of relays, as the increased number of relays allows for greater freedom in selecting the most suitable relay and achieving higher secrecy capacity.

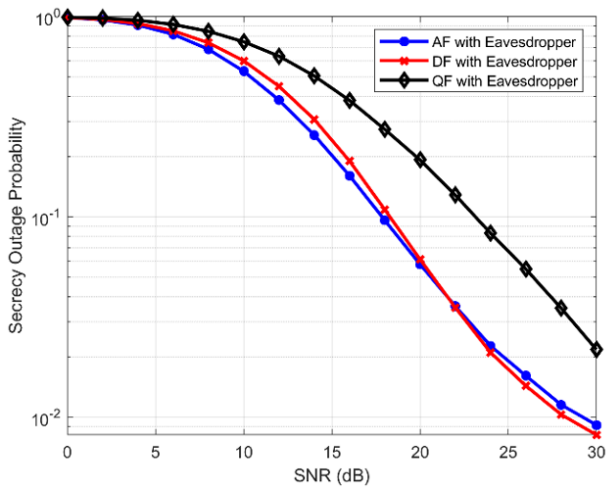

Figure 7. SOP with respect to SNR for the DF, AF, and QF protocols

REFERENCES

[1] S. Naderi, M. R. Javan and A. Aref, "Secrecy outage analysis of cooperative amplify and forward relaying in device to device communications," in Proc. 24th Iranian Conference on Electrical Engineering, 2016, pp. 40-44.

[2] Y. Cao, T. Jiang and C. Wang, "Cooperative device-to-device communications in cellular networks," *IEEE Wireless Communications*, vol. 22, no. 3, pp. 124-129, 2015.

[3] V. Nhan Vo, D. Tran, C. So-In, and H. Tran, "Secrecy performance analysis for fixed-gain energy harvesting in an internet of things with untrusted relays," *IEEE Access*, vol. 6, pp. 48247-48258, 2018.

[4] Y. L. Foo, "Secrecy capacity and energy efficiency in D2D-enabled cellular networks," *Telecommunication Systems*, vol. 77, no. 2, pp. 351-357, 2021.

[5] R Liu, and W. Trappe, *Securing Wireless Communication at the Physical Layer,* vol.7. New York, NY, USA:Springer, 2010.

[6] A. Zhang, L. Zhou, and L. Wang, *Security-Aware Device-to-Device Communications Underlaying Cellular Networks*, part of Book Series Springer Briefs in Electrical and Computer Engineering, 1st Ed, New York, NY, USA: Springer, 2016.

[7] T. Mekkawy, R. Yao, N. Qi, and Y. Lu, "Secure relay selection for two way amplify-and-forward untrusted relaying networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 11979-11987, 2018.

[8] Y. J. Tolossa, S. Vuppala, G. Kaddoum, and G. Abreu, "On the uplink secrecy capacity analysis in D2D-enabled cellular network." *IEEE Systems Journal*, vol. 12 no. 3, pp. 2297-2307, 2017.

[9] M. Zhang, B. Yang, S. Zhao, and L. Ma, "Secrecy capacity analysis in D2D-enabled cellular networks under power control," in Proc. International Conference on Networking and Network Applications (NaNA), 2019, pp. 81-84.

[10] S. K. Surinder, B. Manju, and S. B. Sukhvinder, "5G Cellular Networks's Device to Device Communication : A State of The Art Survey," *International Journal of Advanced Research in Computer Science,* vol. 9, pp. 645-649, 2018

[11] P. Gandotra and R. K. Jha, "Device-to-device communication in cellular networks: A survey," *Journal of Network and Computer Applications*, vol.71, pp. 99–117, 2016.

[12] M. Aishwarya and S. Kirthiga, "Relay assisted cooperative communication for wireless sensor networks," in Proc. 2nd International Conference on Advances in Electronics, Computers and Communications (ICAECC), *2018*, pp. 1-6.

[13] Y. Zou, and J. Zhu, *Physical-Layer Security for Cooperative Relay Networks*, New York: Springer International Publishing, 2016.

[14] B. Djeumou, S. Lasaulce, and A. G. Klein, "Practical quantize-and-forward schemes for the frequency division relay channel," *EURASIP Journal on Wireless Communication and Networking*, vol. 2008, no. 020258, 2008.

[15] 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, 2018

[16] M. Xia and S. Aïssa, "Fundamental relations between reactive and proactive relay-selection strategies," *IEEE Communications Letters*, vol. 19, no. 7, pp. 1249-1252, 2015.

[17] Y. Yunida, R. Muharar, Y. Away, and N. Nasaruddin. "Efficient relay selection algorithm for non-orthogonal amplify-and-forward cooperative systems over block-fading channels." *Radioengineering*, vol. 29, no.2, 2020.

[18] Y. Zou, X. Wang and W. Shen, "Optimal Relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099-2111, 2013.

[19] L. Wang, *Physical Layer Security in Wireless Cooperative Networks*. Berlin/Heidelberg, Germany: Springer International Publishing, 2018.

[20] Liu, Ruoheng. *Securing Wireless Communications at The Physical Layer*. Ed. Wade Trappe, vol. 7. New York: Springer, 2010.

[21] B. V. Nguyen and K. Kim, "Secrecy outage probability of optimal relay selection for secure AnF cooperative networks," *IEEE Communications Letters,* vol. 19, no. 12, pp. 2086-2089, 2015.

[22] Shams, F.; Bacci, G.; and Luise, M, "Energy-efficient power control for multiple-relay cooperative networks using q-learning," *IEEE Transactions on Wireless Communications*, vol. 14, no. 3, pp. 1567-1580, 2014.

[23] B. Kasiri, H. Meshgi, M. Naderi and B. Abolhassani, "Diversity-based relay selection for multihop cellular networks," in Proc. International Conference on Advanced Computer Theory and Engineering, 2008, pp. 740-743.