Physical Layer Security in 5G and Beyond Wireless Networks Enabling Technologies

by

©Majid Hamoud Ahmed Khoshafa

A dissertation submitted to the School of Graduate Studies
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Faculty of Engineering and Applied Science
Memorial University of Newfoundland

February 2022

St. John's, Newfoundland

Abstract

Information security has always been a critical concern for wireless communications due to the broadcast nature of the open wireless medium. Commonly, security relies on cryptographic encryption techniques at higher layers to ensure information security. However, traditional cryptographic methods may be inadequate or inappropriate due to novel improvements in the computational power of devices and optimization approaches. Therefore, supplementary techniques are required to secure the transmission data. Physical layer security (PLS) can improve the security of wireless communications by exploiting the characteristics of wireless channels. Therefore, we study the PLS performance in the fifth generation (5G) and beyond wireless networks enabling technologies in this thesis. The thesis consists of three main parts.

In the first part, the PLS design and analysis for Device-to-Device (D2D) communication is carried out for several scenarios. More specifically, in this part, we study the underlay relay-aided D2D communications to improve the PLS of the cellular network. We propose a cooperative scheme, whereby the D2D pair, in return for being allowed to share the spectrum band of the cellular network, serves as a friendly jammer using full-duplex (FD) and half-duplex (HD) transmissions and relay selection to degrade the wiretapped signal at an eavesdropper. This part aims to show that spectrum sharing is advantageous for both D2D communications and cellular networks concerning reliability and robustness for the former and PLS enhancement for the latter. Closed-form expressions for the D2D

outage probability, the secrecy outage probability (SOP), and the probability of non-zero secrecy capacity (PNSC) are derived to assess the proposed cooperative system model. The results show enhancing the robustness and reliability of D2D communication while simultaneously improving the cellular network's PLS by generating jamming signals towards the eavesdropper. Furthermore, intensive Monte-Carlo simulations and numerical results are provided to verify the efficiency of the proposed schemes and validate the derived expressions' accuracy.

In the second part, we consider a secure underlay cognitive radio (CR) network in the presence of a primary passive eavesdropper. Herein, a secondary multi-antenna full-duplex destination node acts as a jammer to the primary eavesdropper to improve the PLS of the primary network. In return for this favor, the energy-constrained secondary source gets access to the primary network to transmit its information so long as the interference to the latter is below a certain level. As revealed in our analysis and simulation, the reliability and robustness of the CR network are improved, while the security level of the primary network is enhanced concurrently.

Finally, we investigate the PLS design and analysis of reconfigurable intelligent surface (RIS)-aided wireless communication systems in an inband underlay D2D communication and the CR network. An RIS is used to adjust its reflecting elements to enhance the data transmission while improving the PLS concurrently. Furthermore, we investigate the design of active elements in RIS to overcome the double-fading problem introduced in the RIS-aided link in a wireless communications system. Towards this end, each active RIS element amplifies the reflected incident signal rather than only reflecting it as done in passive RIS modules. As revealed in our analysis and simulation, the use of active elements leads to a drastic reduction in the size of RIS to achieve a given performance level. Furthermore, a practical design for active RIS is proposed.

To my father and mother ...
To my lovely wife and kids ...
To my sister and brothers ...
To my entire family and friends ...

Acknowledgments

All praise and thanks be to Almighty Allah, the one and only who helps us in every aspect of our lives. After thanking Almighty "ALLAH" for His blessing and guidance to complete this work, I would like to express deep gratefulness and appreciation to my thesis supervisors Prof. Telex M. N. Ngatched and Prof. Mohamed H. Ahmed, for their continuous help, guidance, and encouragement throughout this work. They spent a lot of their precious time helping me and advising me at each step. I would like to acknowledge the financial support provided by my supervisors, and the School of Graduate Studies at Memorial University of Newfoundland.

The final word of acknowledgment is reserved to my parents for their unconditional support to my two sisters and two brothers for their love, to my friends all over the world, to my sweetheart and lovely wife and our kids for their patience and for motivating me. Finally, I would like to say that "*I am nothing without you all*."

Co-Authorship Statement

I, Majid Khoshafa, hold a principle author status for all the manuscript chapters (Chapters 2 - 7) in this dissertation. However, each manuscript is co-authored by my supervisors and co-researchers, whose contributions have facilitated the development of this work as described below.

- **Chapter 2**:
  - Majid H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "On the Physical Layer Security of Underlay Relay-Aided Device-to-Device Communications", *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 7609-7621, July. 2020.
- **Chapter 3**:
  - Majid H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and I. Ahmed, "Enhancing Physical Layer Security Using Underlay Full-Duplex Relay-Aided D2D Communications," *IEEE Wireless Communications and Networking Conference (WCNC)*, Seoul, South Korea, pp. 1-7, Mar. 2020.
  - Majid H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and I. Ahmed, "Improving Physical Layer Security of Cellular Networks Using Full-Duplex Jamming Relay-Aided D2D Communications," *IEEE Access*, vol. 8, pp. 53575-53586, Mar. 2020.

  - Majid H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and I. Ahmed, "Secure Transmission in Wiretap Channels Using Full-Duplex Relay-Aided D2D Communications with Outdated CSI," *IEEE Wireless Communications Letters*, vol. 9, pp. 1216-1220, Aug. 2020.

- **Chapter 4**:

  - Majid H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "Secure Transmission in Underlay D2D Communications Using Optimal Relay Selection," *IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, Victoria, BC, Canada, pp. 1-6, Aug. 2020.
  - Majid H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "Relay Selection for Improving Physical layer Security in D2D Underlay Communications," under second round of review in *IEEE Transactions on Mobile Computing.*
  - Majid H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "On the Physical Layer Security of Underlay Multihop Device-to-Ddevice Relaying," *IEEE Wireless Communications and Networking Conference (WCNC)*, Marrakesh, Morocco, pp. 1-6, Apr. 2019.

- **Chapter 5**:

  - Majid H. Khoshafa, J. M. Moualeu, T. M. Ngatched, and M. H. Ahmed, "On the Performance of Secure Underlay Cognitive Radio Networks with Energy Harvesting and Dual-Antenna Selection," *IEEE Communications Letter,* vol. 25, pp. 1815-1819, Jun. 2021.

- **Chapter 6**:

  - Majid H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "Reconfigurable Intelligent Surfaces-Aided Physical Layer Security Enhancement in D2D Underlay

Communications," *IEEE Communications Letter,*vol. 25, no. 5, pp. 1443-1447, May 2021.

- Majid H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. R. Ndjiongue, "Active Reconfigurable Intelligent Surfaces-Aided Wireless Communication System," *IEEE Communications Letter,* vol. 25, no. 11, pp. 3699-3703, Nov. 2021.

- **Chapter 7**:

  - Majid H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "Secure Underlay Cognitive Radio Networks Using Reconfigurable Intelligent Surface," under review for publication in *IEEE Transactions on Vehicular Technology.*

_____ _____

Majid Khoshafa Date

Table of Contents

List of Figures

List of Abbreviations

6G	Sixth Generation
AF	Amplify-and-Forward
AI	Artificial Intelligence
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BS	Base Station
CDF	Cumulative Distribution Function
CJ	Cooperative Jamming
CR	Cognitive Radio
CSI	Channel State Information
CU	Cellular User
D2D	Device-to-Device
DF	Decode-and-Forward
DRL	Deep Reinforcement Learning

EH	Energy Harvesting
EM	Electromagnetic
FD	Full-Duplex
HD	Half-Duplex
ISM	Industrial, Scientific and Medical
IT	Information Transmission
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
MRC	Maximum Ratio Combining
ORS	Optimal Relay Selection
PB	Power Beacon
PCB	printed circuit board
PDF	Probability Density Function
PN	Primary Network
PNSC	Probability of Non-zero Secrecy Capacity
QoS	Quality of Service
RF	Radio Frequency
RIS	Reconfigurable Intelligent Surface
RV	Random Variable

SC	Selection Combining
SI	Self-Interference
SINR	Signal-to-Interference-and-Noise Ratio
SN	Secondary Network
SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
SRS	Suboptimal Relay Selection
SU	Secondary User
TAS	Transmit Antenna Selection
TS	Time-Switching
UAV	Unmanned Aerial Vehicle

Chapter 1

Introduction

1.1 Background

1.1.1 Physical Layer Security

Nowadays, wireless networks have been widely utilized in daily life applications to transmit essential and secure information. Consequently, security is considered a critical issue for future 5G and beyond wireless networks due to the broadcasting nature of the open wireless medium [1]. Traditionally, security depends on cryptographic encryption techniques and related protocols at higher layers to guarantee information security. Nevertheless, with the development of mobile Internet, traditional cryptographic techniques maybe inadequate or even inappropriate as an extra secure channel is needed for private key exchanges [2]. More importantly, due to novel improvements in the computational power of devices and optimization approaches. Therefore, new supplementary security strategies from information theory fundamentals, which focus on the propagation channel's secrecy capacity, are essential to protect information from unauthorized devices [3].

Physical layer security, first explored by Wyner [4], is considered a novel strategy for improving wireless security by only exploiting the characteristics of wireless channels, e.g.,

noise, interference, and fading. The benefits of applying physical layer security strategies for 5G and beyond wireless networks compared to traditional cryptography techniques are twofold. First, PLS is independent of the computational complexity compared to cryptography in the higher layers [5]. Accordingly, even though the eavesdroppers have high powerful computational abilities, secure and reliable communications can be guaranteed. The second one is that PLS strategies have high scalability [6]. It is important to remark that PLS can be employed as a supplementary level of security on top of the current security approaches. To elaborate, PLS can be integrated with the other security solutions to provide confidential and private communication data in 5G and beyond wireless networks [2].

Many techniques, such as cooperative beamforming [7], artificial noise [8], and multi-antenna beamforming [9], have been investigated to degrade the quality of the wiretapped signals at the eavesdropper. Moreover, cooperative jamming (CJ) has been extensively studied to safeguard wireless communications. In CJ, a relay terminal is chosen by the authorized receiver to degrade the eavesdroppers signal by sending a jamming signal [10], [11]. In cooperative scenarios, CJ and cooperative relaying [12], [13] are considered as promising techniques to efficiently increase the secrecy capacity.

The secrecy capacity (i.e., the maximum transmission rate at which the eavesdropper is unable to decode any information) is equal to the difference between the main channel and the eavesdropper channel. The main performance metrics used in this work to evaluate the security level are the secrecy outage probability (SOP) and the probability of non-zero secrecy capacity (PNSC). The SOP can be defined as the probability that the achievable secrecy rate is less than a predefined target secrecy rate, Rs, for cellular transmission, while the PNSC is the probability that the achievable secrecy capacity is greater than zero.

1.1.2 Device to Device Communications

Mobile wireless communication has experienced rapid development in data traffic due to the dramatic growth of smart devices. According to Cisco, the average number of mobiles per capita will be 3.6 by 2023 [14]. Thus, spectrum scarcity is a crucial issue in wireless networks. Device-to-Device (D2D) communication, which enables proximate user pairs to communicate directly rather than through the base station (BS), has received considerable attention as one of the main technologies in the fifth-generation (5G) and beyond cellular communications [15], [16]. The advantages of D2D communications are multi-fold and include increased spectrum efficiency, shortened transmission latency, increased cellular coverage, and increased energy efficiency [17]. D2D communication also offers new mobile service advantages for several proximity-based services such as multi-player gaming, social networking, and content sharing [18], [19].

According to the spectrum band utilization, D2D communication can be classified into two approaches; inband D2D and out-band D2D communications. In the first approach, the same spectrum band is shared between the cellular network and the D2D communication [17]. The inband D2D communication can further be classified into two categories, namely, underlay and overlay D2D communication. In underlay D2D communication, both D2D and cellular users share the same frequencies, resulting in enhanced spectral efficiency. By providing high spectral efficiency, the performance of cellular is improved [16]. Nevertheless, sharing the same spectrum band causes sereve interference between D2D and cellular users. Therefore, interference management is necessary. In overlay D2D communication, the cellular spectrum is split into non-overlapping frequency sets, where one set is allocated to D2D users, while the other is allocated to the cellular users. Since D2D and cellular communications occur in their spilled spectral bands, the interference issue is overcome. Therefore, interference management between D2D users and cellular users is not needed in overlay D2D communication. The significant deficiency of overlay D2D communication

is that the portion of cellular spectrum assigned for D2D communication might be utilized ineffectively, resulting in inadequate system throughput and resource utilization.

In the second approach, the D2D network utilizes the unlicensed spectrum band; usually ISM bands [20]. Since the D2D communications and cellular users operate in different spectrum bands, the outband communication effectively excludes the spectrum interference problem between D2D and cellular users. Nevertheless, outband D2D encounters problems in regulating communications over the unlicensed spectrum bands. To limit this drawback, two approaches have been proposed to tackle the regulating communications issue, namely controlled outband D2D and autonomous outband D2D [17]. In controlled outband D2D communication, the regulation between radio interfaces over the unlicensed spectrum bands is controlled by the cellular network. That is, the spectrum resources for the D2D users are preallocated; thus, the ISM band resources can be reasonably utilized. One obvious disadvantage of this approach is that the overhead signaling increases with increasing the network size. Consequently, the performance is declined. In the autonomous outband D2D communication, the devices communicating in D2D mode are responsible for controlling D2D communication, while the base station controls the cellular links. This approach considerably reduces the load of the cellular network [16].

More importantly, underlay D2D communications can play a primary role in improving cellular network security. In this case, the D2D users can be used as friendly jammers to enhance the secrecy performance of the cellular network, while the cellular network shares its spectrum with the D2D users in return.

1.1.3 Reconfigurable Intelligent Surfaces

Reconfigurable intelligent surface (RIS), which is a surface of electromagnetic (EM) material that consists of a large number of inexpensive passive reflecting elements controlled by a microcontroller, has received significant consideration as a leading technologies in the

sixth-generation (6G) wireless networks [21], [22]. There are many advantages of RIS such as the ability to control the transmission environment by directing the reflected signals in a specific direction and very low power consumption compared with relaying technology [23]. RIS has also been referred to as software-controlled metasurfaces [24] and intelligent reflecting surfaces [25].

1.2 Thesis Motivation

In this section, we discuss the main motivations that lead to this thesis's work and how they are important to the area of research in PLS in 5G and Beyond wireless networks enabling technologies.

With accelerated information and communication technologies, wireless communication services have become indispensable in daily life. Wireless communication services are tremendously growing due to the massive increase in smart wireless devices. Based on these, the surge in wireless data communication is essentially driven by the vast amount of smart mobile. The information is exchanged among authorized users; however, serious security risks arise due to the wireless broadcasting nature. Therefore, security techniques are utilized to protect wireless transmissions against eavesdropping attacks. Towards this end, the design of secure wireless communication systems for 5G and beyond wireless networks enabling technologies such as D2D communications, cognitive radio, and reconfigurable intelligent surfaces by utilizing PLS techniques is the core motivation for this thesis.

Motivated by the considerable importance of PLS mentioned above, the following research problems are investigated in this thesis:

- An efficient cooperative system, which consists of D2D communications and a cellular network, is proposed. Specifically, the spectrum sharing is advantageous for both D2D communications and cellular networks for reliability and robustness for

the former and the physical layer security enhancement for the latter.

- Applying full-duplex (FD) transmission and dual antenna selection to improve the security level of the cellular network while enhancing the D2D communication reliability is proposed. The practical scenario, where the eavesdropper is passive, is considered. The eavesdropper uses either selection combining or maximal ratio combining to combine the wiretapped signals of the cellular network.

- A full assessment of the above efficient system models is performed for perfect and outdated channel state information (CSI).

- An efficient secure system model is proposed by using relay selection techniques.

- Energy harvesting and dual-antenna selection are proposed to enhance the robustness and reliability of the CR network, while simultaneously improving the PLS of the primary network.

- A secure system model is proposed by using RIS technology.

- An active RIS is designed to overcome the double fading problem and improve the PLS.

1.3 Thesis Contributions

Motivated by the previous discussion, in this section, we describe the primary contributions of this dissertation.

1.3.1 Key Outcomes

The major outcomes of this dissertation can be summarized as follows:

1. We have designed a cooperative system, where a multiple-input multiple-output (MIMO) relay helps as a friendly jammer to enhance the security of the cellular network while transmitting the D2D data [26]. Consequently, a secure cellular network is achieved for perfect and outdated CSI scenarios.

2. We have proposed a new network-assisted inband underlay D2D communication system by applying FD transmission and dual antenna selection [27], [28]. The D2D relay node can simultaneously act as a friendly jammer to improve the secrecy performance of the cellular network while enhancing the D2D communication data transmission. This is an appealing and practical scheme where spectrum sharing benefits the D2D and cellular networks in terms of reliability enhancement and security provisioning, respectively. Furthermore, We have investigated the influence of outdated CSI on the PLS of the cellular network using the FD relay [29].

3. We have proposed secure inband underlay D2D communications by utilizing relay selection. For maximizing the secrecy capacity of D2D communications, two relay selection schemes have been investigated, namely, optimal relay selection (ORS) and suboptimal relay selection (SRS). Additionally, on the eavesdropper side, two practical combining approaches, maximum-ratio combining (MRC) and selection combining (SC), are examined [30], [31]. Furthermore, the PLS of underlay multihop D2D relaying has also been investigated [32].

4. We propose a secure underlay cognitive radio network with energy harvesting in the presence of a primary passive eavesdropper. Herein, a secondary multi-antenna full-duplex destination node acts as a jammer to the primary eavesdropper to improve the primary network's physical layer security [33].

5. We have proposed the use of the RIS technology to enhance the reliability and robustness of D2D communication and improve the security level of the cellular network

concurrently [34]. As compensation for spectrum sharing, the RIS serves as a friendly jammer to ensure a high-security level for the cellular network, thus enabling a win-win situation between the two networks, i.e., security provisioning for the cellular user and high reliability and robustness for the D2D users.

6. We have designed an active RIS to overcome the double fading problem in standard communication scenarios [35]. The essential characteristic of an active RIS is to amplify the reflected signal with extra power consumption. With this in mind, an active RIS has been investigated to enhance the robustness, reliability, and PLS of a wireless communication network.

7. We have proposed a secure RIS-aided underlay cognitive network to enhance the robustness and reliability of the secondary network (SN) communication while simultaneously improving the PLS of the primary network (PN) [36].

1.3.2 List of Publications

We have made significant contributions to the field PLS for the leading technologies in the 5G and 6G wireless networks. This dissertation has resulted in the following publications:

Journals Articles

1. **Majid H. Khoshafa**, T. M. Ngatched, and M. H. Ahmed, "Relay Selection for Improving Physical layer Security in D2D Underlay Communications," under second round of review for publication in *IEEE Transactions on Mobile Computing.*

2. **Majid H. Khoshafa**, T. M. Ngatched, and M. H. Ahmed, "Secure Underlay Cognitive Radio Networks Using Reconfigurable Intelligent Surface," under review for publication in *IEEE Transactions on Vehicular Technology.*

3. **Majid H. Khoshafa**, T. M. Ngatched, and M. H. Ahmed, "Active Reconfigurable Intelligent Surfaces-Aided Wireless Communication System," *IEEE Communications Letters*,vol. 25, no. 11, pp. 3699-3703, Nov. 2021

4. **Majid H. Khoshafa**, Jules M. Moualeu, T. M. Ngatched, and M. H. Ahmed, "On the Performance of Secure Underlay Cognitive Radio Networks with Energy Harvesting and Dual-Antenna Selection," *IEEE Communications Letters*, vol. 25, pp. 1815-1819, Jun. 2021.

5. **Majid H. Khoshafa**, T. M. Ngatched, and M. H. Ahmed, "Reconfigurable Intelligent Surfaces-Aided Physical Layer Security Enhancement in D2D Underlay Communications," *IEEE Communications Letters*, vol. 25, no. 5, pp. 1443–1447, May 2021.

6. **Majid H. Khoshafa**, T. M. Ngatched, M. H. Ahmed, and I. Ahmed, "Secure Transmission in Wiretap Channels Using Full-Duplex Relay-Aided D2D Communications with Outdated CSI," *IEEE Wireless Communications Letters*, vol. 9, pp. 1216–1220, Aug. 2020.

7. **Majid H. Khoshafa**, T. M. Ngatched, and M. H. Ahmed, "On the Physical Layer Security of Underlay Relay-Aided Device-to-Device Communications", *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 7609–7621, July 2020.

8. **Majid H. Khoshafa**, T. M. Ngatched, M. H. Ahmed, and I. Ahmed, "Improving Physical Layer Security of Cellular Networks Using Full-Duplex Jamming Relay-Aided D2D Communications," *IEEE Access*, vol. 8, pp. 53575–53586, Mar. 2020.

Conferences Papers

1. **Majid H. Khoshafa**, T. M. Ngatched, and M. H. Ahmed, "Secure Transmission in Underlay D2D Communications Using Optimal Relay Selection," *IEEE 92nd Vehic-*

ular Technology Conference (VTC2020-Fall), Victoria, BC, Canada, pp. 1–6, Aug. 2020.

2. **Majid H. Khoshafa**, T. M. Ngatched, M. H. Ahmed, and I. Ahmed, "Enhancing Physical Layer Security Using Underlay Full-Duplex Relay-Aided D2D Communications," *IEEE Wireless Communications and Networking Conference (WCNC)*, Seoul, South Korea, pp. 1–7, Mar. 2020.

3. **Majid H. Khoshafa**, T. M. Ngatched, and M. H. Ahmed, "On the Physical Layer Security of Underlay Multihop Device-to-Device Relaying," *IEEE Wireless Communications and Networking Conference (WCNC)*, Marrakesh, Morocco, pp. 1–6, Apr. 2019.

1.4 Thesis Organization

The remainder of this dissertation is organized as follows. In Chapter 2, We propose a cooperative scheme, whereby the D2D pair, in return of being allowed to share the spectrum band of the cellular network, serves as a friendly jammer, through its multiple-input multiple-output relay, to degrade the wiretapped signal at an eavesdropper. The perfect and outdated CSI are considered.

We propose to apply FD transmission and dual antenna selection at the D2D relay node in Chapter 3. The relay node can simultaneously act as a friendly jammer to improve the secrecy performance of the cellular network while enhancing the D2D communication data transmission. This is an appealing and practical scheme where spectrum sharing is beneficial for the D2D and cellular networks in terms of reliability enhancement and security provisioning, respectively. The perfect and outdated CSI are considered.

Chapter 4 investigates the PLS of inband underlay D2D communication, where the direct link between D2D users is not available. In this respect, optimal relay selection and

suboptimal relay selection are utilized to secure the D2D transmission. The eavesdropper uses either maximal-ratio combining or selection combining to increase the wiretapped signals. Moreover, the PLS of underlay multihop D2D relaying is also considered.

In Chapter 5, we propose a secure underlay cognitive radio network with energy harvesting in the presence of a primary passive eavesdropper. Herein, a secondary multi-antenna full-duplex destination node acts as a jammer to the primary eavesdropper to improve the primary network's physical layer security.

Chapter 6 investigates a RIS-aided wireless communication system in an inband underlay D2D communication, where the direct link between D2D users is unavailable. An RIS is used to adjust its reflecting elements to enhance the D2D communication data transmission while improving the cellular network's secrecy performance concurrently.

Chapter 7, we propose a secure RIS-aided underlay cognitive network, considering the interference produced by the SN and the RIS on the PN in Chapter.

Finally, we conclude the dissertation in Chapter 8 and discuss the possible extensions of this work.

References

[1] X. Chen, D. W. K. Ng, W. H. Gerstacker and H. Chen, "Survey on multiple-antenna techniques for physical layer security," *IEEE Commun, Surv. Tut.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart. 2017.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong and X. Gao, "A Survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[3] D. Wang, B. Bai, W. Zhao and Z. Han, "A Survey of optimization approaches for wireless physical layer security," *IEEE Commun, Surv. Tut.*, vol. 21, no. 2, pp. 1878–1911, 2nd quarter 2019.

[4] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun, Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, 2nd Quart. 2014.

[6] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[7] C. Jeong, I.-M. Kim, and D. I. Kim, “Joint secure beamforming design at the source and the relay for an Amplify-and-Forward MIMO untrusted relay system,” *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[8] H.-M. Wang, C. Wang, and D. W. K. Ng, “Artificial noise assisted secure transmission under training and feedback,” *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[9] A. Mukherjee and A. L. Swindlehurst, “Robust beamforming for security in MIMO wiretap channels with imperfect CSI,” *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[10] Y. Liu, J. Li, and A. P. Petropulu, “Destination assisted cooperative jamming for wireless physical-layer security,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[11] K.-H. Park, T. Wang, and M.-S. Alouini, “On the jamming power allocation for secure Amplify-and-Forward relaying via cooperative jamming,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.

[12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010

[13] L. Lai and H. El Gamal, “The relayâeavesdropper channel: Cooperation for secrecy,” *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[14] *Cisco Annual Internet Report (2018–2023) White Paper.*, “Available [Online]: http://goo.gl/ylTuVx, Mar. 2020.

[15] S. Zhang, J. Liu, H. Guo, M. Qi, and N. Kato, "Envisioning device-to-device communications in 6G," *IEEE Net.*, vol. 34, no. 3, pp. 86–91, Jun. 2020.

[16] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally and M. A. Javed, "A survey of device-to-Device communications: Research issues and challenges," *IEEE Commun, Surv. Tut.*, vol. 20, no. 3, pp. 2133-2168, 3rd Quart. 2018.

[17] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun, Surv. Tut.*, vol. 16, no. 4, pp. 1801-1819, 4th Quart. 2014.

[18] H. Wu, X. Gao, S. Xu, D. O. Wu, and P. Gong, "Proximate device discovery for d2d communication in lte advanced: Challenges and approaches," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 140–147, Aug. 2020.

[19] M. Ahmed, Y. Li, M. Waqas, M. Sheraz, D. Jin, and Z. Han, "A survey on socially aware device-to-device communications," *IEEE Commun, Surv. Tut.*, vol. 20, no. 3, pp. 2169-2197, 3rd Quart. 2018.

[20] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-device communication in LTE-advanced networks: A survey," *IEEE Commun, Surv. Tut.*, vol. 17, no. 4, pp. 1923-1940, 4th Quart. 2015.

[21] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, Jul. 2019.

[22] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. Di Renzo, and M. Debbah, "Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 118–125, Oct. 2020.

[23] Q. Wu and R. Zhang, “Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network,” *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[24] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, “A new wireless communication paradigm through softwarecontrolled metasurfaces,” *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162– 169, Sep. 2018.

[25] C. Huang, R. Mo, and C. Yuen, “Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning,” *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1839–1850, Aug. 2020.

[26] M. H. Khoshafa, T. Ngatched, and M. H. Ahmed, “On the physical layer security of underlay relay-aided device-to-device communications,” *IEEE Trans. Veh. Tech.*, vol. 69, no. 7, pp. 7609–7621, Jul. 2020.

[27] M. H. Khoshafa, T. Ngatched, M. H. Ahmed, and A. Ibrahim “Enhancing Physical Layer Security Using Underlay Full-Duplex Relay-Aided D2D Communications,” *IEEE Wireless Commun. Net. Conference (WCNC),* Seoul, South Korea, pp. 1–7, Mar. 2020.

[28] M. H. Khoshafa, T. Ngatched, M. H. Ahmed, and and A. Ibrahim, “Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications,” *IEEE Access*, vol. 8, pp. 53575–53586, Mar. 2020.

[29] M. H. Khoshafa, T. Ngatched, M. H. Ahmed, and A. Ibrahim, “Secure transmission in wiretap channels using full-duplex relay-aided D2D communications with outdated CSI,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 8, pp. 1216–1220, Aug. 2020.

[30] M. H. Khoshafa, T. Ngatched, and M. H. Ahmed, “Secure transmission in underlay D2D Communications using optimal relay selection,” *IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, Victoria, BC, Canada, pp. 1–6, Aug. 2020.

[31] M. H. Khoshafa, T. Ngatched, and M. H. Ahmed, “Relay selection for improving physical layer security in D2D underlay communications,” under second round of review for publication in *IEEE Trans. Mobile Computing.*

[32] M. H. Khoshafa, T. Ngatched, and M. H. Ahmed, “On the physical layer security of underlay multihop device-to-device relaying,” *IEEE Wireless Commun. Net. Conference (WCNC)*, Marrakesh, Morocco, pp. 1–6, Apr. 2019.

[33] M. H. Khoshafa, J. M. Moualeu, T. Ngatched, and M. H. Ahmed, “On the Performance of Secure Underlay Cognitive Radio Networks with Energy Harvesting and Dual-Antenna Selection,” *IEEE Commun. Lett.*, vol. 25, pp. 1815-1819, Jun. 2021.

[34] M. H. Khoshafa, T. Ngatched, and M. H. Ahmed, “Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications,” *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1443-1447, May 2021.

[35] M. H. Khoshafa, T. Ngatched, and M. H. Ahmed, “Active reconfigurable intelligent surfaces-aided wireless communication system,” *IEEE Commun. Lett,* vol. 25, no. 11, pp. 3699-3703, Nov. 2021.

[36] M. H. Khoshafa, T. Ngatched, and M. H. Ahmed, “Secure underlay cognitive radio networks using reconfigurable intelligent surface,” under review for publication in *IEEE Trans. Veh. Tech.*

Chapter 2

On the PLS of Underlay Relay-Aided Device-to-Device Communications

2.1 Abstract

In this chapter, we study the underlay relay-aided D2D communications to improve the PLS of the cellular network. We propose a cooperative scheme, whereby the D2D pair, in return of being allowed to share the spectrum band of the cellular network, serves as a friendly jammer, through its multiple-input multiple-output relay, to degrade the wiretapped signal at an eavesdropper. This chapter aims to show that spectrum sharing is advantageous for both D2D communications and cellular networks with respect to reliability and robustness for the former, and the PLS enhancement for the latter. To assess the proposed cooperative system model, closed-form expressions for the D2D outage probability, the secrecy outage probability, and the probability of non-zero secrecy capacity are derived. More importantly, the benefits due to the cooperation scheme are verified through numerical and simulation results.

2.2 Introduction

D2D communications is considered as one of the most important technologies for the 5G and beyond networks. In D2D communications, two close D2D users exchange information directly rather than relaying the information through the BS [1]. There are many advantages of D2D communications over the conventional cellular networks, for instance, low power consumption, high spectral efficiency, and short delay. It is worth noting that D2D communications have many significant applications like traffic offloading, disaster relief, content sharing, and file sharing [2].

As a result of the open wireless medium, security is considered as a critical issue in wireless networks. The PLS security, first explored by Wyner [3], is of great interest as an essential strategy to protect information. To this end, the natural randomness of communication channels and noise is utilized to reduce the wiretapped data. More specifically, the received signal by eavesdroppers is confounded with respect to the quality of service (QoS). More importantly, PLS is independent of the computational complexity as compared to the cryptography in the higher layers. As a result, eavesdroppers that have high powerful computational abilities do not affect the level of security. In addition, PLS approaches have a high scalability [4].

The advantages of cooperative communications, in the context of PLS, have been extensively studied. More specifically, both relaying and diversity techniques have been extensively utilized to increase the security level against eavesdropper attacks in the wireless transmission [5]. Moreover, cooperative jamming has also been comprehensively investigated to increase the secrecy capacity. To this end, a relay terminal is chosen to interfere with the wiretapping signal by transmitting a jamming signal [6], [7]. With this in mind, cooperative jamming and relaying [8], [9] have been considered as leading approaches to increase the security level efficiently.

As a matter of fact, MIMO relays are extensively utilized in PLS to increase the secrecy capacity of the cellular networks. The opportunities and challenges of MIMO relaying technologies in PLS were investigated in [10],[11]. Recently, MIMO relaying has been used to improve the PLS of mmWave band [12]. However, multiple radio frequency chains related to multiple antennas are expensive with respect to hardware, size, and power. To limit these drawbacks, antenna selection is an inexpensive low-complexity choice to achieve several of the benefits of MIMO systems. The secrecy performance of transmit antenna selection (TAS) was examined in the MIMO channels for selection combining [13] and maximum-ratio combining [14]. For the outdated CSI, the TAS technique was investigated in [15].

2.2.1 Related Work

As a result of spectrum sharing between D2D and cellular users, interference is considered as harmful. To limit this drawback, most current works on inband underlay D2D communications aim at mitigating and overcoming the interference between the cellular users and the D2D pairs [16]. However, from a PLS viewpoint, before-mentioned interference could be advantageous, since it could be used to confound the eavesdroppers [17]. Considering PLS in underlay D2D communications, some techniques are used to enhance the secrecy performance of the D2D communications. Two techniques for PLS, namely, guard zone and artificial noise (AN) were utilized to improve the security level of the D2D communications [18]. To guarantee a secure D2D link, the authors in [19] utilized the BS as a cooperative jammer to confound the eavesdropping signal by generating AN to interfere with the eavesdropper. However, the QoS of cellular users (CUs) should be taken into account when the BS generates AN. To do so, the jamming signal should be orthogonal to the null space of the main channels [20]. In [21], the PLS of D2D communications, multihop relaying scheme, was studied, only from the viewpoint of improving the security level of

D2D users only.

It is worth mentioning that a few works have studied the improvement of the PLS of cellular networks utilizing the potential of D2D links [22]. In [23], the use of the interference generated by the D2D links to confuse the eavesdroppers and thus enhance the security of the cellular network was studied. To enhance the security level of the CUs, the authors in [24] analyzed joint power control for the D2D users and CUs. By enhancing the resource sharing, spectral efficiency provisioning for D2D links and security improvement for CUs were obtained in [25][26].

All works mentioned above particularly study the case where the direct links are available between D2D nodes. However, in some scenarios, the distance and channel conditions may be unfavorable for direct communication. In these situations, the performance of the D2D communication can be improved by using network-assisted transmission through relays. Such a technique, relay-aided D2D communication, can provide more reliable QoS for connection between indirect D2D users. In practice, for smart cities, machine-to-machine communication is considered as a valuable application for relay-aided D2D communication [27]. In this case, inside a macro-cell for some city blocks, automated sensors are used when the proximity between devices and/or link conditions between nodes are unfavorable. To the best of our knowledge, no work has been reported in the open literature investigating the PLS of relay-aided underlay D2D communication.

2.2.2 Main Contributions

In this work, the PLS of the cellular network is examined. In the proposed scenario, the D2D communications are used to generate jamming signals to enhance the security level of the cellular network in return of sharing its spectrum. Unlike the existing work on the PLS of underlay D2D communication in the cellular network, we investigate the PLS of the cellular network where a MIMO relay serves the D2D pairs. To do so, the antenna selection

approach is utilized to simultaneously enhance the security level of the cellular network and improve the D2D data transmission. To confound the eavesdropper, the transmit antenna selection at the MIMO relay is used to generate jamming signals. Consequently, the secrecy capacity of the cellular network is increased. At the same time, the reliability and robustness of the D2D communications are improved as a result of utilizing the relay through antenna selection. By using antenna selection strategy at the relay, the high hardware complexity of multiple antennas is avoided, while its reliability and robustness advantages, and diversity are maintained.

The main contributions of this chapter are listed as follows:

- A cooperative system is introduced where the MIMO relay helps as a friendly jammer while transmitting the D2D data.
- An antenna selection strategy is employed to enhance the secrecy capacity of the cellular network by degrading the wiretapped signal at an eavesdropper and to improve the traffic capacity for D2D communication.
- Considering perfect and outdated CSI cases, the analysis is carried out to evaluate the secrecy performance of the cellular network with respect to the secrecy outage probability (SOP) and the probability of non-zero secrecy capacity (PNSC). Furthermore, the outage probability of D2D communication is also analyzed. Additionally, closed-form expressions are derived.
- Asymptotic analysis is carried out in high transmit power regime for the cellular network.
- Simulation results are presented where the derived expressions are evaluated and verified. The advantages due to the presence of D2D communications are highlighted.

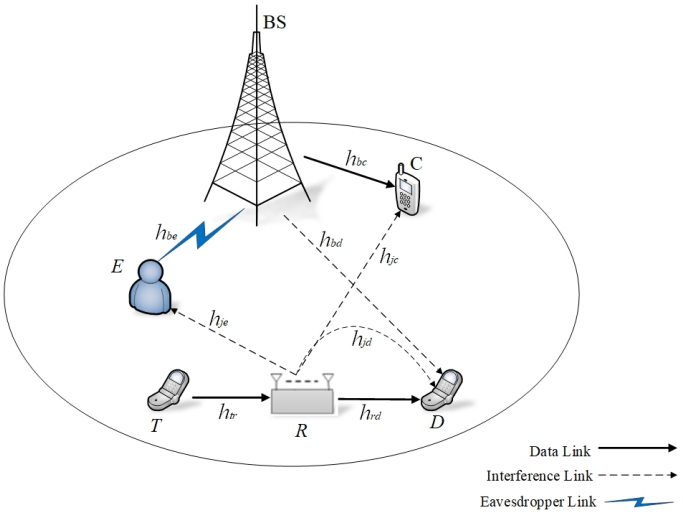


Fig. 2.1: System Model.

2.3 System Model

As depicted in Fig. 2.1, an underlay D2D network with MIMO relaying sharing the spectrum with the cellular network in a particular environment is considered. The cellular network consists of a base station BS as well as a cellular user, C, communicating in the presence of an eavesdropper, E, each equipped with a single antenna. The D2D communications consist of a D2D transmitter, T, a D2D receiver, D, and a MIMO amplify-and-forward (AF) relay, R, equipped with N_J antennas for sending jamming signals to confound E and N_D data antennas for receiving D2D signal at R and re-transmitting the signal to D. Besides, all the channels coefficients are modeled as to experience flat fading with Rayleigh distribution. Furthermore, the transmission of D2D users is set up during two phases, while the cellular transmissions occur once in one phase. To this end, cellular and D2D transmissions are considered to be fully synchronized for each phase. In the first phase, T transmits the D2D signal to R, while C remains silent to guarantee the cellular link security [28], [29]. In the second phase, at R, the amplified signal is re-transmitted to D. As compensation for security provisioning of the cellular network, the D2D pairs are permitted to share spectrum bandwidth; that is, high spectral efficiency is gained. There-

fore, for both networks, a win-win situation is enabled. To simplify matters, we indicate TR as the receiving antenna in the first phase, and RD as the transmitting antenna in the second phase. Similarly, RJ denotes the jamming antenna.

The channel coefficients for the $T \rightarrow$ TR, RD $\rightarrow D$, RJ $\rightarrow E$, RJ $\rightarrow C$, RJ $\rightarrow D$, BS $\rightarrow C$, BS $\rightarrow D$, and BS $\rightarrow E$ links are denoted as h_{tr}, h_{rd}, h_{je}, h_{jc}, h_{jd}, h_{bc}, h_{bd}, and h_{be}, respectively. Also, $|h_{ab}|^2$ represents the channel power gains, which are independent and exponentially distributed with a mean of $\lambda_{ab} = \mathbb{E}[|h_{ab}|^2]$,
where $ab \in \{bc, bd, tr, rd, be, je, jd, jc\}$. In addition, $\sigma_c^2, \sigma_r^2, \sigma_e^2$, and σ_d^2 represent the variances of the additive white Gaussian noise (AWGN) at C, R, E, and D, respectively. It is assumed that T and R have the same transmitted power, P. With this in mind, the received signal at TR, in the first phase, can be expressed as

$$y_R = \sqrt{P}\, h_{tr}\, x_d + n_r, \tag{2.1}$$

where x_d is the D2D transmitted signal, and n_r is the AWGN at R. The transmitting antenna RD, in the second phase, is chosen to maximize the instantaneous signal-to-noise ratio (SNR) at D. Then using the relaying gain $\mathcal{G}$, RD re-transmits the amplified signal to D. Thus, the received signal at D can be expressed as

$$y_D = \mathcal{G}\, h_{rd} \left(\sqrt{P}\, h_{tr}\, x_d + n_r \right) + \sqrt{P_B}\, h_{bd}\, x_b + \sqrt{P_J}\, h_{jd}\, x_j + n_d, \tag{2.2}$$

where x_b is the BS transmitted signal, P_B is the BS transmission power, P_J is the jamming transmitted power, x_j is the jamming signal, and n_d is the AWGN at D. It is assumed that the interference at D from RJ can be eliminated by using interference cancellation [30] since the coefficient h_{jd} and the jamming power P_J are presumed to be available at D. The

received signal at C, in the second phase, can be expressed as

$$y_C = \sqrt{P_B}\, h_{bc}\, x_b + \sqrt{P_J}\, h_{jc}\, x_j + n_c, \tag{2.3}$$

where n_c is the AWGN at C. Similarly, at E, the received signal, in the second phase, can be expressed by

$$y_E = \sqrt{P_B}\, h_{be}\, x_b + \sqrt{P_J}\, h_{je}\, x_j + n_e, \tag{2.4}$$

where n_e is the AWGN at the E. We assume that the received signals at C and E are not affected by the interference from T since T is located far away from both C and E, and transmits with low power [31]. It is noteworthy that since the data transmission power of RD is lower than the jamming transmission power of RJ, the interference at C, which is generated by RD, can be neglected. It is also notable that the D2D users are unlikely to be wiretapped as a result of their low transmit power as compared to cellular users. Therefore, as common in the literature (e.g., [32] and [33]), in this work, we only investigate the secrecy performance of the cellular network. More importantly, in this chapter, our main goal is to investigate the mutual benefit of the cooperation between the cellular and the D2D networks. In particular, the potential of the relay-aided D2D communication to enhance the security of the cellular network, while improving its reliability and spectral efficiency is studied. Towards this end, the relaying gain $\mathcal{G}$, for AF relaying scheme, is given by [34]

$$\mathcal{G} = \sqrt{\frac{P}{P\left|h_{tr}\right|^2 + \sigma_r^2}}. \tag{2.5}$$

For the end-to-end D2D link, the instantaneous signal-to-interference-and-noise ratio (SINR), γ_{D2D}, can be obtained by plugging (2.5) into (2.2) as

$$\gamma_{D2D} = \frac{\mathcal{G}^2 P \left|h_{tr}\right|^2 \left|h_{rd}\right|^2}{\mathcal{G}^2 \left|h_{rd}\right|^2 \sigma_r^2 + P_B \left|h_{bd}\right|^2 + \sigma_d^2}, \tag{2.6}$$

After some algebraic manipulations, one can get

$$\gamma_{D2D} = \frac{\gamma_R \, \gamma_D}{\gamma_R + \gamma_D + 1}, \tag{2.7}$$

where γ_R represents the SINR at R, which can be expressed as

$$\gamma_R = \frac{P}{\sigma_r^2} \left| h_{tr} \right|^2 = \bar{\gamma}_r \left| h_{tr} \right|^2, \tag{2.8}$$

and γ_D represents the SINR at D, which can be expressed as

$$\gamma_D = \frac{P \left| h_{rd} \right|^2}{\sigma_d^2 + P_B \left| h_{bd} \right|^2} = \frac{\gamma_{rd}}{1 + \gamma_{bd}}, \tag{2.9}$$

where $\gamma_{rd} = \bar{\gamma}_d \left| h_{rd} \right|^2$, $\gamma_{bd} = \bar{\gamma}_{bd} \left| h_{bd} \right|^2$, $\bar{\gamma}_d = \frac{P_d}{\sigma_d^2}$, and $\bar{\gamma}_{bd} = \frac{P_B}{\sigma_d^2}$. Let us define $\mu_1 = \bar{\gamma}_r \lambda_{tr}$, $\mu_2 = \bar{\gamma}_d \lambda_{rd}$, and $\mu_3 = \bar{\gamma}_{bd} \lambda_{bd}$. The receiving antenna at R is selected for the best data transmission performance in the D2D network. Moreover, the maximum channel gain can be determined by using

$$\left| h_{tr} \right|^2 = \max_{i=1,..N_D} \left| h_{ti} \right|^2, \tag{2.10}$$

and

$$\left| h_{rd} \right|^2 = \max_{i=1,..N_D} \left| h_{id} \right|^2, \tag{2.11}$$

The probability density function (PDF) of $\left| h_\upsilon \right|^2$ is given by

$$f_{|h_\upsilon|^2}(\gamma) = \frac{N_D}{\lambda_\upsilon} \exp\left(-\frac{\gamma}{\lambda_\upsilon}\right) \left(1 - \exp\left(-\frac{\gamma}{\lambda_\upsilon}\right)\right)^{N_D - 1}, \tag{2.12}$$

where $\upsilon \in \{tr, rd\}$.

2.4 Performance Analysis

In this section, a thorough analysis of the proposed system is performed. In particular, closed-form expressions of the main performance metrics, i.e., the D2D outage probability, the SOP, and the PNSC are provided. Moreover, the advantages of the proposed scheme are investigated. Furthermore, the asymptotic analysis is presented.

2.4.1 D2D Outage Probability

The outage probability of D2D communication, P_{out}, is given by

$$P_{out} = \Pr\left(\gamma_{D2D} \leq \varphi\right), \tag{2.13}$$

where $\varphi = 2^{\mathcal{R}_d} - 1$, and $\mathcal{R}_d$ is the data rate of the D2D communications. Since the expression in (2.7) is mathematically intractable, a tight upper bound, γ_{up}, is utilized to find the SINR of the D2D communications as [35]

$$\gamma_{D2D} \leq \gamma_{up} \stackrel{\triangle}{=} \min\left(\gamma_R, \gamma_D\right). \tag{2.14}$$

Hence, P_{out} can be expressed as

$$P_{out} = \Pr\left(\gamma_{up} \leq \varphi\right) = \Pr\left(\min\left(\gamma_R, \gamma_D\right) \leq \varphi\right). \tag{2.15}$$

P_{out} can be further expressed as [36]

$$P_{out} = F_{\gamma_R}(\varphi) + F_{\gamma_D}(\varphi) - F_{\gamma_R}(\varphi)F_{\gamma_D}(\varphi), \tag{2.16}$$

where $F_{\gamma_R}(.)$ and $F_{\gamma_D}(.)$ are the cumulative distribution functions (CDFs) of γ_R and γ_D, respectively. The PDF of γ_R in (2.12) can be expressed in terms of the binomial expansion as [37, eq. (1.111)]

$$f_{\gamma_R}(\gamma) = \frac{N_D}{\mu_1} \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D-1}{k} \exp\left(-\frac{\gamma\,(k+1)}{\mu_1}\right). \tag{2.17}$$

To derive $f_{\gamma_D}(\gamma)$, we use [36]

$$f_{\gamma_D}(\gamma) = \int_0^\infty (x+1) f_{\gamma_{rd}}(\gamma(x+1)) f_{\gamma_{bd}}(x)\, dx, \tag{2.18}$$

where $f_{\gamma_{rd}}(.)$ is given by

$$f_{\gamma_{rd}}(\gamma) = \frac{N_D}{\mu_2} \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D-1}{k} \exp\left(-\frac{\gamma\,(k+1)}{\mu_2}\right), \tag{2.19}$$

and $f_{\gamma_{bd}}(.)$ is given by

$$f_{\gamma_{bd}}(\gamma) = \frac{1}{\mu_3} \exp\left(-\frac{\gamma}{\mu_3}\right). \tag{2.20}$$

By plugging (2.19) and (2.20) into (2.18), the PDF of γ_D, after some algebraic manipulations, can be obtained as

$$f_{\gamma_D}(\gamma) = \frac{N_D}{\mu_2\mu_3} \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D-1}{k} \exp\left(-\frac{\gamma\,(k+1)}{\mu_2}\right) \left(\frac{1+\frac{\gamma(k+1)}{\mu_2}+\frac{1}{\mu_3}}{\left(\frac{\gamma(k+1)}{\mu_2}+\frac{1}{\mu_3}\right)^2}\right). \tag{2.21}$$

From (2.17) and (3.17), $F_{\gamma_R}(\gamma)$ and $F_{\gamma_D}(\gamma)$ are obtained as

$$F_{\gamma_R}(\gamma) = N_D \sum_{k=0}^{N_D-1} \frac{(-1)^k \binom{N_D-1}{k}}{(k+1)} \left(1 - \exp\left(-\frac{\gamma\,(k+1)}{\mu_1}\right)\right), \tag{2.22}$$

and

$$F_{\gamma_D}(\gamma) = N_D \sum_{k=0}^{N_D-1} \frac{(-1)^k \binom{N_D-1}{k}}{(k+1)} \left(1 - \frac{\exp\left(-\frac{\gamma\,(k+1)}{\mu_2}\right)}{\left(1+\frac{\gamma\,(k+1)\mu_3}{\mu_2}\right)}\right). \tag{2.23}$$

By substituting (2.22), (2.23) in (2.16), P_{out} can be obtained as

$$\begin{aligned} P_{out} =& N_D \sum_{k=0}^{N_D-1} \frac{(-1)^k \binom{N_D-1}{k}}{k+1} \left[\left(2 - \frac{1}{\exp\left(\frac{\varphi\,(k+1)}{\mu_1}\right)} - \frac{1}{\exp\left(\frac{\varphi\,(k+1)}{\mu_2}\right)\left(1+\frac{\varphi\,(k+1)\mu_3}{\mu_2}\right)}\right)\right. \\ & \left. - N_D \sum_{m=0}^{N_D-1} \frac{(-1)^m \binom{N_D-1}{m}}{m+1} \left(\left(1 - \frac{1}{\exp\left(\frac{\varphi\,(k+1)}{\mu_1}\right)}\right)\left(1 - \frac{\exp\left(-\frac{\varphi\,(m+1)}{\mu_2}\right)}{\left(1+\frac{\varphi\,(m+1)\mu_3}{\mu_2}\right)}\right)\right)\right]. \end{aligned} \tag{2.24}$$

2.4.2 Secrecy Outage Probability

The SOP can be defined as the probability that the achievable secrecy rate is less than a predefined target secrecy rate, $\mathcal{R}_s$, for the cellular transmission. Based on this, the SOP is given by [38]

$$\text{SOP} = \Pr\left(C_S < \mathcal{R}_s\right), \tag{2.25}$$

where $\mathcal{R}_s$ represents the target secrecy rate of cellular transmission and C_S is the secrecy capacity which can be expressed as

$$C_S = \begin{cases} C_C - C_E, & \gamma_C > \gamma_E, \\ 0, & \gamma_C \leq \gamma_E, \end{cases} \tag{2.26}$$

where C_C and C_E are the cellular and eavesdropper capacities, respectively. In this respect, C_C can be obtained by

$$C_C = \log_2(1+\gamma_C) = \log_2\left(1+\frac{\gamma_{bc}}{1+\gamma_{jc}}\right), \tag{2.27}$$

where $\gamma_{bc} = \bar{\gamma}_c |h_{bc}|^2$, $\gamma_{jc} = \bar{\gamma}_{jc} |h_{jc}|^2$, $\bar{\gamma}_c = \frac{P_B}{\sigma_c^2}$, and $\bar{\gamma}_{jc} = \frac{P_j}{\sigma_c^2}$. Let us define $\omega_1 = \bar{\gamma}_c \lambda_{bc}$, and $\omega_2 = \bar{\gamma}_{jc} \lambda_{jc}$. In addition, C_E can be obtained by

$$C_E = \log_2(1+\gamma_E) = \log_2\left(1+\frac{\gamma_{be}}{1+\gamma_{je}}\right), \tag{2.28}$$

where $\gamma_{be} = \bar{\gamma}_e |h_{be}|^2$, $\gamma_{je} = \bar{\gamma}_{je} |h_{be}|^2$, $\bar{\gamma}_e = \frac{P_B}{\sigma_e^2}$, and $\bar{\gamma}_{je} = \frac{P_j}{\sigma_e^2}$. Let us define $\omega_3 = \bar{\gamma}_e \lambda_{be}$, and $\omega_4 = \bar{\gamma}_{je} \lambda_{je}$.

2.4.2.1 Jamming Antenna Selection Approaches

According to the availability of the channel gains $R \rightarrow E$, we propose two approaches for the antenna jamming selection as follow.

Case I: For active E, where the channel gains of E are known, the criterion of jamming antenna selection is based on maximizing the interference to E. In this case, C will see a random jamming signal. In doing so, we use

$$|h_{je}|^2 = \max_{k=1,..N_J} |h_{ke}|^2 . \tag{2.29}$$

Henceforward, the expressions related to Case I and II are provided with subscripts I and II, respectively. The SOP_I can be further mathematically written as

$$\text{SOP}_\text{I} = \int_0^\infty F_{\gamma_{C_I}}(\beta\,\gamma+\alpha)\; f_{\gamma_{E_I}}(\gamma)\; d\gamma, \tag{2.30}$$

where $\beta = 2^{\mathcal{R}_s}$, and $\alpha = \beta - 1$and the CDF of γ_{C_I} can be derived as

$$F_{\gamma_{C_I}}(\gamma) = \left(1 - \frac{\exp\left(-\frac{\gamma}{\omega_1}\right)}{1 + \frac{\omega_2}{\omega_1}\gamma}\right). \tag{2.31}$$

and the PDF of γ_{E_I} can be derived as

$$f_{\gamma_{E_I}}(\gamma) = \frac{N_J}{\omega_3\omega_4}\sum_{k=0}^{N_J-1}(-1)^k\binom{N_J-1}{k}\exp\left(-\frac{\gamma}{\omega_3}\right)\left(\frac{1 + \frac{(k+1)}{\omega_4} + \frac{\gamma}{\omega_3}}{\left(\frac{(k+1)}{\omega_4} + \frac{\gamma}{\omega_3}\right)^2}\right). \tag{2.32}$$

By plugging (2.31) and (2.32) into (2.30), and with the help of partial fraction expansion, thereafter [37, eq. (3.352.4)] and [37, eq. (3.353.3)], SOP_I can be derived as

$$\begin{aligned}\text{SOP}_\text{I} = 1 - \frac{N_J\,\omega_1}{\omega_2\,\omega_4\,\beta}\sum_{k=0}^{N_J-1}\frac{(-1)^k\binom{N_J-1}{k}\exp\left(-\frac{\alpha}{\omega_1}\right)}{(\mathcal{A}_1 - \mathcal{A}_2)}\Bigg[\frac{(\mathcal{A}_3 - \mathcal{A}_1)}{(\mathcal{A}_1 - \mathcal{A}_2)}\Bigg(\frac{\text{Ei}\left[-\mathcal{A}_4\,\mathcal{A}_2\right]}{\exp\left(-\mathcal{A}_4\,\mathcal{A}_2\right)} \\ - \frac{\text{Ei}\left[-\mathcal{A}_4\,\mathcal{A}_1\right]}{\exp\left(-\mathcal{A}_4\,\mathcal{A}_1\right)}\Bigg) + (\mathcal{A}_3 - \mathcal{A}_2)\left(\frac{\mathcal{A}_4\,\text{Ei}\left[-\mathcal{A}_4\,\mathcal{A}_2\right]}{\exp\left(-\mathcal{A}_4\,\mathcal{A}_2\right)} + \frac{1}{\mathcal{A}_2}\right)\Bigg],\end{aligned} \tag{2.33}$$

where $\mathcal{A}_1 = \frac{1}{\beta}\left(\frac{\omega_1}{\omega_2} + \alpha\right)$, $\mathcal{A}_2 = \left(\frac{\omega_3\,(k+1)}{\omega_4}\right)$, $\mathcal{A}_3 = \omega_3\left(1 + \frac{k+1}{\omega_4}\right)$, $\mathcal{A}_4 = \left(\frac{\beta}{\omega_1} + \frac{1}{\omega_3}\right)$, $\text{Ei}(.)$ is the exponential integral function [37, eq. (8.21.1)].

Case II: For a passive E, where the channel gains of E are unknown, the criterion of jamming antenna selection is based on minimizing the interference towards C. In this case, E will see a random jamming signal. In doing so, we use

$$|h_{jc}|^2 = \min_{k=1,..N_J}|h_{kc}|^2. \tag{2.34}$$

The SOP_{II} can be further mathematically written as

$$\text{SOP}_{II} = \int_0^{\infty} F_{\gamma_{C_{II}}}(\beta\,\gamma + \alpha)\; f_{\gamma_{E_{II}}}(\gamma)\; d\gamma, \tag{2.35}$$

where the CDF of $\gamma_{C_{II}}$ can be derived as

$$F_{\gamma_{C_{II}}}(\gamma) = \left(1 - \frac{N_J \exp\left(-\frac{\gamma}{\omega_1}\right)}{N_J + \frac{\omega_2 \gamma}{\omega_1}}\right), \tag{2.36}$$

and the PDF of $\gamma_{E_{II}}$ can be derived as

$$f_{\gamma_{E_{II}}}(x) = \frac{\exp\left(-\frac{\gamma}{\omega_3}\right)}{\omega_3 \omega_4} \left(\frac{1 + \frac{1}{\omega_4} + \frac{x}{\omega_3}}{\left(\frac{1}{\omega_4} + \frac{x}{\omega_3}\right)^2}\right). \tag{2.37}$$

Using the same steps of the derivation of (2.33), the SOP for Case II, SOP_{II}, can be obtained as

$$\begin{aligned}\text{SOP}_{\text{II}} =& 1 - \frac{N_J\,\omega_1 \exp\left(-\frac{\alpha}{\omega_1}\right)}{\omega_2\,\omega_4\,\beta\left(\mathcal{B}_1 - \frac{\omega_3}{\omega_4}\right)} \left[\frac{(\mathcal{B}_2 - \mathcal{B}_1)}{\left(\mathcal{B}_1 - \frac{\omega_3}{\omega_4}\right)} \left(\frac{\text{Ei}\left[-\frac{\mathcal{B}_3\,\omega_3}{\omega_4}\right]}{\exp\left(-\frac{\mathcal{B}_3\,\omega_3}{\omega_4}\right)} - \frac{\text{Ei}\left[-\mathcal{B}_3\,\mathcal{B}_1\right]}{\exp\left(-\mathcal{B}_3\,\mathcal{B}_1\right)}\right)\right. \\ &\left. + \left(\mathcal{B}_2 - \frac{\omega_3}{\omega_4}\right) \left(\frac{\mathcal{B}_3\,\text{Ei}\left[-\frac{\mathcal{B}_3\,\omega_3}{\omega_4}\right]}{\exp\left(-\frac{\mathcal{B}_3\,\omega_3}{\omega_4}\right)} + \frac{\omega_4}{\omega_3}\right)\right],\end{aligned} \tag{2.38}$$

where $\mathcal{B}_1 = \frac{1}{\beta}\left(\frac{N_J\,\omega_1}{\omega_2} + \alpha\right)$, $\mathcal{B}_2 = \frac{1}{\omega_3}\left(1 + \frac{1}{\omega_4}\right)$, and $\mathcal{B}_3 = \left(\frac{\beta}{\omega_1} + \frac{1}{\omega_3}\right)$.

2.4.3 Asymptotic Secrecy Outage Analysis

Here, the secrecy performance at high SNR, i,e., when $\overline{\gamma}_c \to \infty$ is introduced to get better understanding of the proposed system behavior. In this scenario, we consider that $\overline{\gamma}_c >>$

$\overline{\gamma}_e$. As $\overline{\gamma}_c \to \infty$, the asymptotic expression of SOP can be expressed as

$$\text{SOP}^{\infty} = (G_a \overline{\gamma}_d)^{-G_d} + \mathcal{O}\left(\overline{\gamma}_d^{-G_d}\right), \tag{2.39}$$

where G_d and G_a denote the secrecy diversity order and the secrecy array gain, respectively. $\mathcal{O}(.)$ represents the higher order terms. To be more precise, G_d characterizes the SOP^{∞}, and G_a describes the SNR advantage of SOP^{∞} relative to the reference curve $(\overline{\gamma}_c)^{-G_d}$.

For Case I, to derive $\text{SOP}_{\text{I}}^{\infty}$, the exponential function and the polynomial in (2.31) are first expanded with the help of [37, eq. (1.211.1)] and [37, eq. (1.112.2)], respectively. Subsequently, we keep the first two terms, and the higher-order terms are ignored. Hence, the asymptotic CDF, $F_{\gamma_{C_I}}^{\infty}(.)$, is derived as

$$F_{\gamma_{C_I}}^{\infty}(\gamma) = \frac{1}{\omega_1}(\omega_2 + 1)x + \mathcal{O}\left(\frac{\gamma}{\omega_1}\right). \tag{2.40}$$

Now, the $\text{SOP}_{\text{I}}^{\infty}$ can be obtained using

$$\text{SOP}_{\text{I}}^{\infty} = \left(G_{a_I} \overline{\gamma}_c\right)^{-G_{d_I}} + \mathcal{O}\left(\overline{\gamma}_c^{-G_{d_I}}\right), \tag{2.41}$$

where G_{d_I} = 1 and G_{a_I} is given by

$$G_{a_I} = \left[\frac{(\omega_2 + 1)N_J}{\lambda_{bc}\,\omega_2\,\omega_4} \sum_{k=0}^{N_J - 1} (-1)^k \binom{N_J - 1}{k} \left[\exp\left(\frac{k+1}{\omega_4}\right) \omega_3\, \beta\, \Gamma\left(0, \frac{(k+1)}{\omega_4}\right) + \frac{\omega_4\, \alpha}{(k+1)}\right]\right]^{-1},$$

where $\Gamma(.,.)$ is the upper incomplete gamma function [37, eq. (8.350.2)].

For Case II, using the same steps for the derivation of (2.42), the asymptotic CDF, $F_{\gamma_C}^{\infty}(.)$, can be obtained as

$$F_{\gamma_{C_{II}}}^{\infty}(\gamma) = \frac{1}{\omega_1}\left(\frac{\omega_2}{N_J} + 1\right)\gamma + \mathcal{O}\left(\frac{\gamma}{\omega_1}\right). \tag{2.42}$$

Here, the $\text{SOP}_{\text{II}}^{\infty}$ can be obtained using

$$\text{SOP}_{\text{II}}^{\infty} = \left(G_{a_{II}}\overline{\gamma}_c\right)^{-G_{d_{II}}} + \mathcal{O}\left(\overline{\gamma}_c^{-G_{d_{II}}}\right), \tag{2.43}$$

where $G_{d_{II}}$ = 1, and $G_{a_{II}}$ is given by

$$G_{a_{II}} = \left[\frac{(N_J+\omega_2)}{N_J\,\lambda_{bc}}\left(\alpha + \frac{\beta\,\omega_3\,\exp\left(\frac{1}{\omega_4}\right)}{\omega_4}\Gamma\left(0,\frac{1}{\omega_4}\right)\right)\right]^{-1}.$$

2.4.4 Probability of Non-zero Secrecy Capacity

In this subsection, the requirement for the presence of the non-zero secrecy capacity is investigated. It is well known that a non-zero secrecy capacity is obtained when $\gamma_C > \gamma_E$. The PNSC can be formulated as

$$\text{PNSC} = \Pr\left(\frac{1+\gamma_C}{1+\gamma_E} > 1\right) = 1 - \Pr(\gamma_C < \gamma_E) = 1 - \int_0^{\infty} F_{\gamma_C}(\gamma)\, f_{\gamma_E}(\gamma)\, d\gamma. \tag{2.44}$$

By plugging (2.31) and (2.32) into (2.44), and with the help of partial fraction expansion, thereafter [37, eq. (3.352.4)] and [37, eq. (3.353.3)], PNSC_{I} can be derived as

$$\begin{aligned}\text{PNSC}_{\text{I}} =& \frac{N_J\,\omega_1}{\omega_2\,\omega_4}\sum_{k=0}^{N_J-1}\frac{(-1)^k\binom{N_J-1}{k}}{\left(\left(\frac{\omega_1}{\omega_2}\right)-\mathcal{A}_2\right)}\left[\frac{\left(\mathcal{A}_3-\left(\frac{\omega_1}{\omega_2}\right)\right)}{\left(\left(\frac{\omega_1}{\omega_2}\right)-\mathcal{A}_2\right)}\left(\frac{\text{Ei}\left[-\left(\frac{\omega_1+\omega_3}{\omega_1\,\omega_3}\right)\mathcal{A}_2\right]}{\exp\left(-\left(\frac{\omega_1+\omega_3}{\omega_1\,\omega_3}\right)\mathcal{A}_2\right)}\right.\right.\\ &\left.\left.-\frac{\text{Ei}\left[-\left(\frac{\omega_1+\omega_3}{\omega_2\,\omega_3}\right)\right]}{\exp\left(-\left(\frac{\omega_1+\omega_3}{\omega_2\,\omega_3}\right)\right)}\right)+(\mathcal{A}_3-\mathcal{A}_2)\left(\frac{\left(\frac{\omega_1+\omega_3}{\omega_1\,\omega_3}\right)\text{Ei}\left[-\left(\frac{\omega_1+\omega_3}{\omega_1\,\omega_3}\right)\mathcal{A}_2\right]}{\exp\left(-\left(\frac{\omega_1+\omega_3}{\omega_1\,\omega_3}\right)\mathcal{A}_2\right)}+\frac{1}{\mathcal{A}_2}\right)\right].\end{aligned} \tag{2.45}$$

By plugging (2.36) and (2.37) into (2.44), and using the same steps for the derivation of (2.45), PNSC_{II} can be derived as

$$\text{PNSC}_{\text{II}} = \frac{N_J\,\omega_1}{\omega_2\,\omega_4\left(\left(\frac{N_J\,\omega_1}{\omega_2}\right)-\frac{\omega_3}{\omega_4}\right)}\left[\frac{\left(\mathcal{B}_2-\left(\frac{N_J\,\omega_1}{\omega_2}\right)\right)}{\left(\left(\frac{N_J\,\omega_1}{\omega_2}\right)-\frac{\omega_3}{\omega_4}\right)}\left(\frac{\text{Ei}\left[-\left(\frac{\omega_1+\omega_3}{\omega_1\,\omega_4}\right)\right]}{\exp\left(-\left(\frac{\omega_1+\omega_3}{\omega_1\,\omega_4}\right)\right)}\right.\right.$$
$$\left.\left.-\frac{\text{Ei}\left[-\left(\frac{(\omega_1+\omega_3)\,N_J}{\omega_2\,\omega_3}\right)\right]}{\exp\left(-\left(\frac{(\omega_1+\omega_3)\,N_J}{\omega_2\,\omega_3}\right)\right)}\right)+\left(\mathcal{B}_2-\frac{\omega_3}{\omega_4}\right)\left(\frac{\left(\frac{\omega_1+\omega_3}{\omega_1\,\omega_3}\right)\text{Ei}\left[-\left(\frac{\omega_1+\omega_3}{\omega_1\,\omega_4}\right)\right]}{\exp\left(-\left(\frac{\omega_1+\omega_3}{\omega_1\,\omega_4}\right)\right)}+\frac{\omega_4}{\omega_3}\right)\right]. \tag{2.46}$$

2.5 Performance Analysis with Outdated CSI

As a result of some circumstances like the mobility and the delay of the feedback, the outdated CSI (indicated here as h_{ab}) may vary from the actual CSI denoted as $\widetilde{h}_{ab}$, giving by [39] $\widetilde{h}_{ab} = \rho_{ab}\,h_{ab} + \sqrt{1-\rho_{ab}}\,w_{ab}$, where ρ_{ab} is the correlation coefficient between $\widetilde{h}_{ab}$ and h_{ab}, w_{ab} is a circularly symmetric complex Gaussian random variable (RV) having the same variance as the RV h_{ab} where $ab \in \{tr, rd, je, jc\}$. Hence, the conditional PDF $f_{\widetilde{\gamma}_{ab}|\gamma_{ab}}(.)$ is given by

$$f_{\widetilde{\gamma}_{ab}|\gamma_{ab}}(\gamma/x) = \frac{1}{\Delta_{ab}}\exp\left(-\frac{(\gamma+\rho_{ab}^2\,x)}{\Delta_{ab}}\right)\,\mathcal{I}_0\left(\frac{2\rho_{bc}\sqrt{\gamma x}}{\Delta_{ab}}\right), \tag{2.47}$$

where $\widetilde{\gamma}_{ab}$ and γ_{ab} are the SINRs for the actual and outdated CSI for the ab channel, $\Delta_{ab} = (1-\rho_{ab}^2)\,\bar{\gamma}_{ab}$, and $\mathcal{I}_0(.)$ is the zero-order modified Bessel function of the first kind [37, eq. (8.445)].

2.5.1 D2D Outage Probability

In this section, the D2D outage probability for outdated CSI, $P_{o\bar{u}t}$, is investigated. To obtain the lower bound $P_{o\bar{u}t}$, we have

$$P_{o\bar{u}t} = F_{\widetilde{\gamma}_R}(\varphi) + F_{\widetilde{\gamma}_D}(\varphi) - F_{\widetilde{\gamma}_R}(\varphi) F_{\widetilde{\gamma}_D}(\varphi). \tag{2.48}$$

Lemma 1: The CDF of $\widetilde{\gamma}_R$ can be derived as

$$F_{\widetilde{\gamma}_R}(\gamma) = N_D \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D-1}{k} \left(\frac{1 - \exp\left(-\frac{(k+1)\gamma}{\Delta_{tr}\,(k+1) + \rho_{tr}^2\,\mu_1} \right)}{(k+1)} \right), \tag{2.49}$$

where $\Delta_{tr} = (1 - \rho_{tr}^2)\,\mu_1$.

Proof: See Appendix A. ■

Lemma 2: $F_{\widetilde{\gamma}_D}$ can be derived as

$$F_{\widetilde{\gamma}_D}(\gamma) = N_D \sum_{k=0}^{N_D-1} \frac{(-1)^k \binom{N_D-1}{k}}{k+1} \left(1 - \frac{\exp\left(-\frac{(k+1)\,\gamma}{\Delta_{rd}\,(k+1) + \rho_{rd}^2\,\mu_2} \right)}{1 + \frac{(k+1)\,\mu_3\,\gamma}{\Delta_{rd}\,(k+1) + \rho_{rd}^2\,\mu_2}} \right), \tag{2.50}$$

where $\Delta_{rd} = (1 - \rho_{rd}^2)\,\mu_2$.

Proof: See Appendix B. ■

By plugging (2.49) and (2.50) into (2.48), $P_{o\bar{u}t}$ can be obtained.

2.5.2 Secrecy Outage Probability

In this section, SOPs for outdated CSI, $\text{SOP}_{\bar{\text{I}}}$ and $\text{SOP}_{\overline{\text{II}}}$, are studied for both cases, respectively.

Lemma 3: For Case I, the PDF of $\widetilde{\gamma}_{E_I}$ can be derived as

$$f_{\widetilde{\gamma}_{E_I}}(\gamma) = N_J \sum_{k=0}^{N_J-1} \frac{(-1)^k \binom{N_J-1}{k} \exp\left(-\frac{\gamma}{\omega_3}\right)}{\omega_3 \left(\Delta_{je}(k+1) + \rho_{je}^2 \omega_4\right)} \left(\frac{1 + \frac{(k+1)}{\Delta_{je}(k+1)+\rho_{je}^2\omega_4} + \frac{\gamma}{\omega_3}}{\left(\frac{(k+1)}{\Delta_{je}(k+1)+\rho_{je}^2\omega_4} + \frac{\gamma}{\omega_3}\right)^2} \right). \tag{2.51}$$

Proof: See Appendix C. ■

The $\text{SOP}_{\bar{\text{I}}}$ can be derive using the following

$$\text{SOP}_{\bar{\text{I}}} = \int_0^\infty F_{\gamma_{C_I}}(\beta\gamma + \alpha)\, f_{\widetilde{\gamma}_{E_I}}(\gamma)\, d\gamma. \tag{2.52}$$

By plugging (2.31) and (2.51) into (2.52), and with the help of partial fraction expansion, thereafter [37, eq. (3.352.4)] and [37, eq. (3.353.3)], $\text{SOP}_{\bar{\text{I}}}$ can be derived as

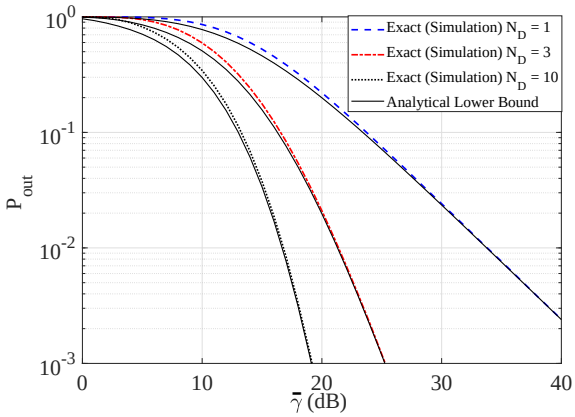
$$\begin{aligned}\text{SOP}_{\bar{\text{I}}} =& 1 - \frac{N_J\, \omega_1}{\omega_2\, \beta} \sum_{k=0}^{N_J-1} \frac{(-1)^k \binom{N_J-1}{k} \exp\left(-\frac{\alpha}{\omega_1}\right)}{\left(\Delta_{je}\,(k+1) + \rho_{je}^2\, \omega_4\right)\left(\mathcal{D}_1 - \mathcal{D}_2\right)} \left[\frac{\left(\mathcal{D}_3 - \mathcal{D}_1\right)}{\left(\mathcal{D}_1 - \mathcal{D}_2\right)} \right. \\ & \left. \left(\frac{\text{Ei}\left[-\mathcal{D}_2\, \mathcal{D}_4\right]}{\exp\left(-\mathcal{D}_2\, \mathcal{D}_4\right)} - \frac{\text{Ei}\left[-\mathcal{D}_1\, \mathcal{D}_4\right]}{\exp\left(-\mathcal{D}_1\, \mathcal{D}_4\right)} \right) + \left(\mathcal{D}_3 - \mathcal{D}_2\right) \left(\frac{\mathcal{D}_4\, \text{Ei}\left[-\mathcal{D}_2\, \mathcal{D}_4\right]}{\exp\left(-\mathcal{D}_2\, \mathcal{D}_4\right)} + \frac{1}{\mathcal{D}_2} \right) \right], \end{aligned} \tag{2.53}$$

where $\mathcal{D}_1 = \left(\frac{\omega_1 + \omega_2\, \alpha}{\beta\, \omega_2}\right)$, $\mathcal{D}_2 = \frac{\omega_3(k+1)}{\left(\Delta_{je}(k+1)+\rho_{je}^2\, \omega_4\right)}$, $\mathcal{D}_3 = \omega_3 \left(1 + \frac{\omega_3(k+1)}{\left(\Delta_{je}(k+1)+\rho_{je}^2\, \omega_4\right)}\right)$, and $\mathcal{D}_4 = \left(\frac{(\omega_1 + \omega_3\, \beta)}{\omega_1\, \omega_3}\right)$.

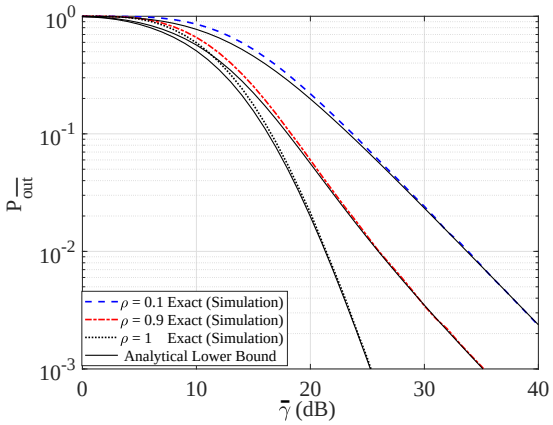
Lemma 4: The $\text{SOP}_{\bar{\text{II}}}$ can be derived as

$$\begin{aligned}\text{SOP}_{\bar{\text{II}}} =& 1 - \frac{N_J\, \omega_1 \exp\left(-\frac{\alpha}{\omega_1}\right)}{\left(N_J\, \Delta_{jc} + \rho_{jc}^2\, \omega_2\right)\, \omega_4\, \beta \left(\mathcal{H}_1 - \frac{\omega_3}{\omega_4}\right)} \left[\frac{\left(\mathcal{H}_2 - \mathcal{H}_1\right)}{\left(\mathcal{H}_1 - \frac{\omega_3}{\omega_4}\right)} \left(\frac{\text{Ei}\left[-\mathcal{H}_3\right]}{\exp\left(-\mathcal{H}_3\right)} \right. \right. \\ & \left. \left. - \frac{\text{Ei}\left[-\mathcal{H}_3\, \mathcal{H}_1\right]}{\exp\left(-\mathcal{H}_3\, \mathcal{H}_1\right)} \right) + \left(\mathcal{H}_2 - \frac{\omega_3}{\omega_4}\right) \left(\frac{\mathcal{H}_3\, \text{Ei}\left[-\mathcal{H}_3\right]}{\exp\left(-\mathcal{H}_3\right)} + \frac{\omega_4}{\omega_3} \right) \right], \end{aligned} \tag{2.54}$$

where $\mathcal{H}_1 = \frac{1}{\beta}\left(\alpha + \frac{N_J\, \omega_1}{\left(N_J\, \Delta_{jc} + \rho_{jc}^2\, \omega_2\right)}\right)$, $\mathcal{H}_2 = \left(\frac{\omega_4 + 1}{\omega_3\, \omega_4}\right)$, and $\mathcal{H}_3 = \left(\frac{\beta\, \omega_3 + \omega_1}{\omega_1 \omega_4}\right)$.



(a) The D2D outage probability, P_{out}, vs. SNR, $\bar{\gamma}$.



(b) The D2D outage probability, $P_{o\overline{u}t}$ vs. SNR, $\bar{\gamma}$.

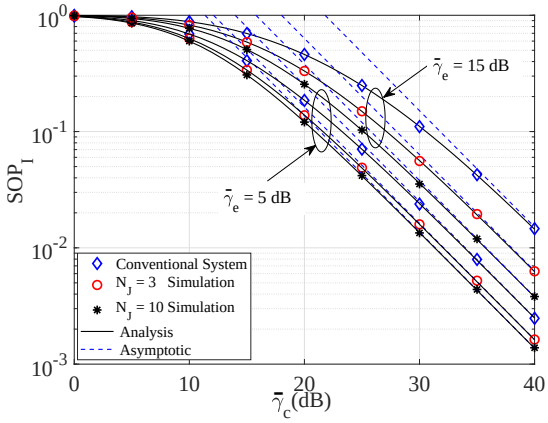
Fig. 2.2: The D2D outage probability for perfect and outaded CSI, P_{out}, where $\mathcal{R}_d = 1$ b/s/Hz.

Proof: See Appendix D. ■

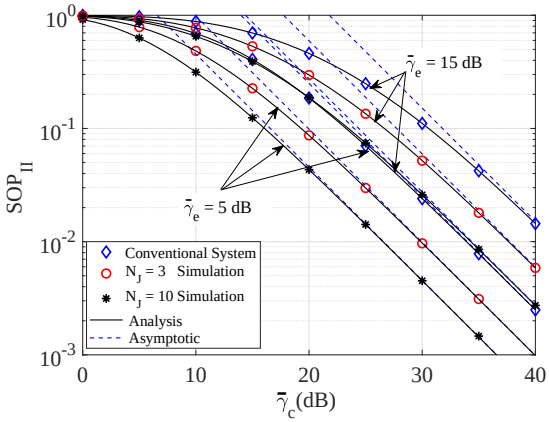
2.6 Results and Discussion

In this section, we present the numerical and simulation results to verify the analysis carried out in the above sections. Throughout the obtained results, the impact of the jamming power, the average SINRs, and the number of antenna at the jammer, N_J, on the secrecy performance of the cellular network are studied. Without loss of generality, the variances of the noise at all nodes are normalized to unity. Unless stated, $\mu_3 = 10$ dB , $\mathcal{R}_d = 1$ b/s/Hz, $\mathcal{R}_s = 1$ b/s/Hz , and ω_2 is 10 dB.

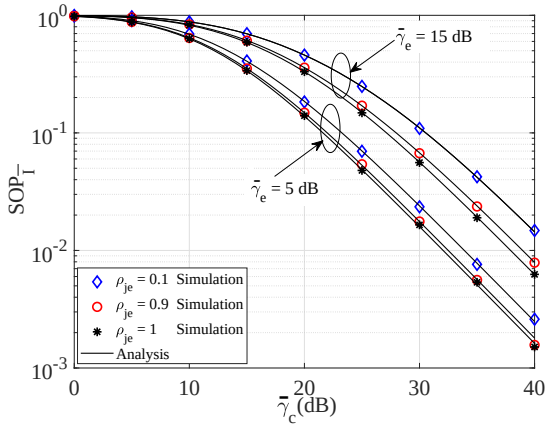
In Fig. 2.2a, the exact (simulation) and the lower bound (analysis) outage probability, P_{out}, for D2D communications is depicted versus $\bar{\gamma}$, where $\bar{\gamma} = \bar{\gamma}_r = \bar{\gamma}_d$. It turns out that P_{out} of the D2D link decreases as $\bar{\gamma}$ increases without any outage floor. In addition, we find that P_{out} improves significantly with increasing N_D. Moreover, the performance of D2D communications improves by using multiple antennas relay in comparison to a single antenna relay. It is also noteworthy that there is a perfect agreement, at high SNR,



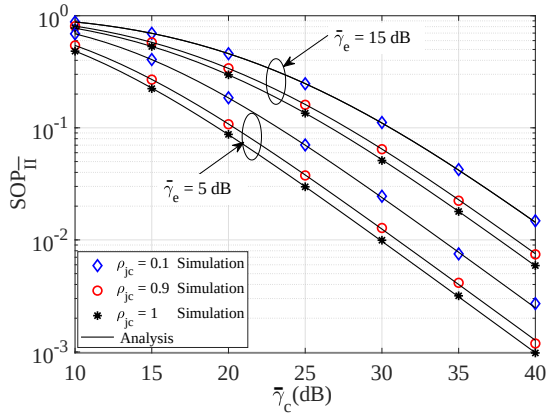
(a) The SOP for Case I



(b) The SOP for Case II



(c) The outdated SOP for Case I



(d) The outdated SOP for Case II

Fig. 2.3: The SOP for perfect and oudated CSI, where $\mathcal{R}_s$ = 1 b/s/Hz.

between the simulation and numerical results, verifying the preciseness of the analytical lower bound expression in (3.12). Regarding outdated CSI, Fig. 2.2b shows the exact (simulation) and lower bound (analysis) outage probability, $P_{o\bar{u}t}$, for different values of the correlation coefficient ρ where $\rho = \rho_{tr} = \rho_{rd}$ and $N_D = 3$. We note that as ρ increases to unity, the performance gain enhances substantially. Therefore, it can be concluded that the availability of the CSI is essential in enhancing the outage probability performance of the D2D communication. Furthermore, a good match between the exact (simulation) and lower bound (analysis) at high SNR can also be observed.

For Case I, SOP_I is depicted in Fig. 2.3a versus $\bar{\gamma}_c$. In this respect, the average SNR of the E, $\bar{\gamma}_e$, is set to 5 dB and 15 dB, and $\mathcal{R}_s$ is set to 1 b/s/Hz. With this in mind, it can be clearly observed that SOP_I decreases as N_J increases at the MIMO relay given the fact that the wiretapped signal is degraded. The generating jamming signals interfere with E, which means that secure data transmission is guaranteed. Moreover, SOP_I increases as $\bar{\gamma}_c$ decreases and $\bar{\gamma}_e$ increases, as expected. With respect to Case II, Fig. 2.3b shows SOP_II, versus $\bar{\gamma}_c$. It is clear that, for both $\bar{\gamma}_e$ = 5 and 15 dB, SOP_II increases with more jamming antennas as shown in Fig. 2.3b. Additionally, we can observe that SOP_II decreases as $\bar{\gamma}_c$ increases and $\bar{\gamma}_e$ decreases, as expected. Furthermore, for both cases, the asymptotic results are provided, where a perfect match with the exact results can be observed as $\overline{\gamma}_c \to \infty$. Again, there is a tight agreement between the simulation and numerical results, verifying the correctness of our analysis. It is worth mentioning that in both Cases I and II, the secrecy capacity of the cellular network increases as a result of using jamming antenna at R.

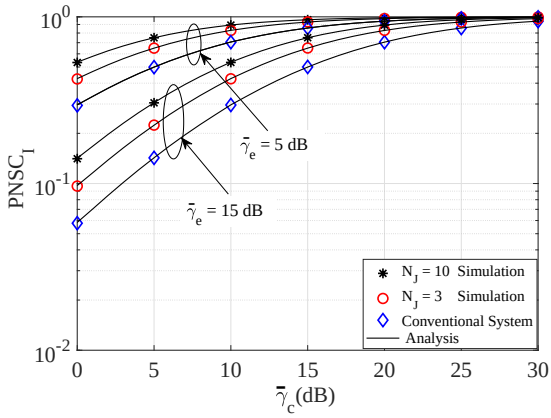
To support our contribution, Figs. 2.3a and 2.3b illustrate the security advantages that the cellular user can gain as compared to the conventional system model, where there is no relay. In the conventional system, there is no relay and T transmits directly to R. Each transmission from T to R occurs in one phase and the cellular transmits in the same phase. Equal transmit power in both schemes, i.e., the conventional one and the proposed one, is assumed to ensure a fair comparison. It is worth mentioning that, when $N_J = 1$, both schemes have the same performance. In this particular case, there is no advantage of the proposed scheme. However, it can be observed that the secrecy performance of the cellular network significantly improves as N_J increases. At $\text{SOP}_\text{II} = 10^{-3}$, we note a security improvement of 10 dB and 5 dB of the proposed scheme over the conventional one when $N_J = 10$ and $N_J = 3$, respectively. According to Fig. 2.3b, SOP_II decreases from 0.025 to 0.0045 at 30 dB as the number of jamming antenna increases from 1 to 10. With this in mind, it is worthy for the cellular system to be silent in the first phase to guarantee secure

data transmission in the second phase. In summary, the proposed system model has many advantages over the conventional system such as improving the secrecy performance of the cellular network, as shown in Figs. 2.3a and 2.3b and increasing the reliability and robustness of the D2D communications, as shown in Fig. 2.2a.

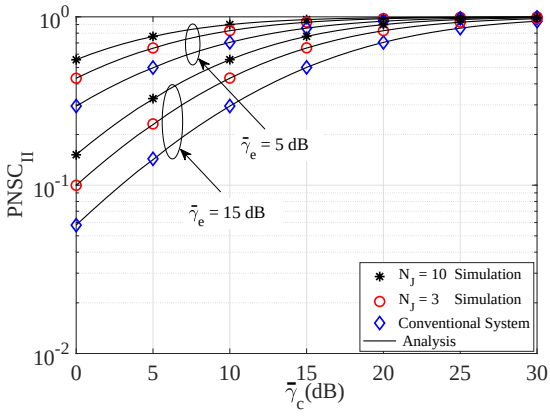
To study the influence of the outdated CSI case on the secrecy performance, Fig. 2.3c illustrates $\text{SOP}_{\bar{\text{I}}}$ for outdated CSI Case I versus SNR, $\bar{\gamma}_c$, for different values of $\bar{\gamma}_e$ and N_J set to 3. Without loss of generality, the correlation coefficient values ρ_{je} are set to 0.1, 0.9, and 1. From this figure, we can observe that $\text{SOP}_{\bar{\text{I}}}$ increases as $\bar{\gamma}_c$ decreases and $\bar{\gamma}_e$ increases. In addition, we can clearly note that $\text{SOP}_{\bar{\text{I}}}$ improves as ρ_{je} increases to 1 because the secrecy capacity impoves with perfect CSI.

Figure 2.3d illustrates $\text{SOP}_{\overline{\text{II}}}$ for outdated CSI Case II. As can be seen, for a fixed ρ_{jc}, namely, $\rho_{jc} \in \{0.1, 0.9, 1\}$, $\text{SOP}_{\overline{\text{II}}}$ improves as $\bar{\gamma}_c$ increases and ρ_{jc} increases to unity. This clearly suggests that the outdated CSI can have a harmful influence on the secrecy capacity for the cellular network. Therefore, Figs. 2.3c and 2.3d clearly show that, in both Cases I and II, the jamming antenna selection at the MIMO relay increases the secrecy capacity for the cellular network. Furthermore, in both cases, there is no outage floor. Moreover, the analytical results and the simulation results match perfectly.

Figure 2.4a shows the probability of non-zero secrecy capacity, PNSC_{I}, for Case I versus $\bar{\gamma}_c$. It is obvious that PNSC_{I} increases as $\bar{\gamma}_c$ increases for a fixed $\bar{\gamma}_e$. However, PNSC_{I} decreases with increasing $\bar{\gamma}_e$. Moreover, we note that PNSC_{I} decreases as N_J decreases. Simulation results are seen to conform with the analytical results, validating the analysis. Furthermore, Fig. 2.4b represents PNSC_{II} for Case II versus $\bar{\gamma}_c$. Both simulation and analytical results are shown, and match perfectly. It is clearly shown in Fig. 2.4b that, for both $\bar{\gamma}_e$ = 5 and 15 dB, PNSC_{II} increases with more jamming antennas.



(a) The PNSc vs. SNR, $\bar{\gamma}$, Case I



(b) The PNSC vs. SNR, $\bar{\gamma}$, Case II

Fig. 2.4: The PNSC for both cases where $\mathcal{R}_d = 1$ b/s/Hz.

2.7 Conclusion

In this chapter, a cooperative system model to simultaneously increase the D2D reliability and robustness, and enhance the secrecy capacity of the cellular network, in an inband underlay D2D cellular system, is introduced. Towards this end, a MIMO relay is utilized to confound the eavesdropper by transmitting jamming signals. A complete analysis, whereby closed-form expressions for the different performance metrics are provided for both perfect and outdated CSI cases. As revealed in the analysis and simulation, the D2D outage probability, the secrecy outage probability, and the probability of non-zero secrecy capacity are improved as a result of the cooperation. Obviously, the obtained results confirm the benefits of the cooperation system by enhancing the security level of the cellular link and the transmission rate for the D2D users, while utilizing the spectrum band of the cellular network. Furthermore, simulation results match entirely with numerical results, validating the analysis.

2.8 Appendices

2.8.1 Appendix A

Derivation of Lemma 1

The PDF of $\widetilde{\gamma}_R$ can be derived by using

$$f_{\widetilde{\gamma}_R}(y) = \int_0^\infty f_{\widetilde{\gamma}_R|\gamma_R}(y/x)\, f_{\gamma_R}(x)\, dx. \tag{2.55}$$

By substituting (2.47) and (2.17) in (2.55) and using [37, eq. (6.643.2)]and [37, eq. (9.220.2)], $f_{\widetilde{\gamma}_R}(y)$ can be derived as

$$f_{\widetilde{\gamma}_R}(\gamma) = N_D \sum_{k=0}^{N_r-1} (-1)^k \binom{N_r-1}{k} \left(\frac{\exp\left(-\frac{(k+1)\,\gamma}{\Delta_{tr}\,(k+1)+\rho_{tr}^2\,\mu_1}\right)}{\Delta_{tr}\,(k+1)+\rho_{tr}^2\,\mu_1} \right), \tag{2.56}$$

where $\Delta_{tr} = (1-\rho_{tr}^2)\,\mu_1$. Then the CDF of $\widetilde{\gamma}_R$ can be obtained as in (2.49).

2.8.2 Appendix B

Derivation of Lemma 2

The SINR at D for actual CSI can be expressed as

$$\widetilde{\gamma}_D = \frac{\widetilde{\gamma}_{rd}}{1+\gamma_{bd}}. \tag{2.57}$$

Now, we can determine the CDF of $\widetilde{\gamma}_D$ as

$$F_{\widetilde{\gamma}_D}(\gamma) = \int_0^\infty F_{\widetilde{\gamma}_{rd}}(\gamma(x+1)) f_{\gamma_{bd}}(x)\, dx. \tag{2.58}$$

Similarly, $F_{\widetilde{\gamma}_{rd}}(\gamma)$ can be derived following a similar procedure in the derivation of (2.49) and is obtained as

$$F_{\widetilde{\gamma}_{rd}}(\gamma) = N_D \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D-1}{k} \left(\frac{1 - \exp\left(-\frac{(k+1)\,\gamma}{\Delta_{rd}\,(k+1) + \rho_{rd}^2\,\mu_2} \right)}{k+1} \right), \tag{2.59}$$

where $\Delta_{rd} = (1-\rho_{rd}^2)\,\mu_2$. By substituting (2.20) and (2.59) in (2.58) and evaluating the integral, The CDF of $\widetilde{\gamma}_D$ can be obtained as in (2.50).

2.8.3 Appendix C

Derivation of Lemma 3

The SINR at E_I is given by

$$\widetilde{\gamma}_{E_I} = \frac{\gamma_{be}}{1 + \widetilde{\gamma}_{je}}. \tag{2.60}$$

The PDF of $\widetilde{\gamma}_E$ can be obtained by using

$$f_{\widetilde{\gamma}_{E_I}}(\gamma) = \int_0^\infty (x+1)\, f_{\gamma_{be}}(\gamma(x+1))\, f_{\widetilde{\gamma}_{je}}(x)\, dx, \tag{2.61}$$

where $f_{\gamma_{be}}$ is given by

$$f_{\gamma_{be}}(\gamma) = \frac{1}{\omega_3} \exp\left(-\frac{\gamma}{\omega_3} \right). \tag{2.62}$$

To derive the PDF of $\widetilde{\gamma}_{je}$, we use

$$f_{\widetilde{\gamma}_{je}}(y) = \int_0^\infty f_{\widetilde{\gamma}_{je}|\gamma_{jc}}(y/x)\, f_{\gamma_{je}}(x)\, dx, \tag{2.63}$$

where $f_{\gamma_{je}}(.)$ is given by

$$f_{\gamma_{je}}(\gamma) = \frac{N_J}{\omega_4} \sum_{k=0}^{N_J-1} (-1)^k \binom{N_J-1}{k} \exp\left(-\frac{\gamma\,(k+1)}{\omega_4} \right). \tag{2.64}$$

Similarly, $f_{\widetilde{\gamma}_{je}}(\gamma)$ can be derived following a similar procedure in the derivation of (2.56) and is obtained as

$$f_{\widetilde{\gamma}_{je}}(\gamma) = N_J \sum_{k=0}^{N_J-1} (-1)^k \binom{N_J-1}{k} \left(\frac{\exp\left(-\frac{(k+1)\gamma}{\Delta_{je}\,(k+1)+\rho_{je}^2\,\omega_4}\right)}{\Delta_{je}\,(k+1)+\rho_{je}^2\,\omega_4} \right). \tag{2.65}$$

By substituting (2.62) and (2.65) in (2.61), the PDF of $\widetilde{\gamma}_{E_I}$ can be obtained as in (2.51).

2.8.4 Appendix D

Derivation of Lemma 4

The SINR at C can be expressed as

$$\widetilde{\gamma}_{C_{II}} = \frac{\gamma_{bc}}{1+\min\left(\widetilde{\gamma}_{jc}\right)}. \tag{2.66}$$

The CDF of $\widetilde{\gamma}_C$ can be obtained using the following formula

$$F_{\widetilde{\gamma}_{C_{II}}}(\gamma) = \int_0^\infty F_{\gamma_{bc}}(\gamma(x+1))\; f_{\widetilde{\gamma}_{jc}}(x)\; dx, \tag{2.67}$$

where $F_{\gamma_{bc}}(.)$ is given by

$$F_{\gamma_{bc}}(\gamma) = 1 - \exp\left(-\frac{\gamma}{\omega_1}\right). \tag{2.68}$$

To derive $_{\widetilde{\gamma}_{jc}}(y)$, we use

$$f_{\widetilde{\gamma}_{jc}}(y) = \int_0^\infty f_{\widetilde{\gamma}_{jc}|\gamma_{jc}}(y/x) f_{\gamma_{jc}}(x)\; dx, \tag{2.69}$$

where $f_{\gamma_{jc}}(.)$ is given by

$$f_{\gamma_{jc}}(\gamma) = \frac{N_J}{\omega_2} \exp\left(-\frac{N_J\,\gamma}{\omega_2}\right). \tag{2.70}$$

Similarly, $f_{\widetilde{\gamma}_{jc}}(\gamma)$ can be derived following a similar procedure of derivation (2.56) and is obtained as

$$f_{\widetilde{\gamma}_{jc}}(\gamma) = \frac{N_J \exp\left(-\frac{N_J\,\gamma}{N_J\,\Delta_{jc}+\rho_{jc}^2\,\omega_2}\right)}{N_J\,\Delta_{jc}+\rho_{jc}^2\,\omega_2}. \tag{2.71}$$

By substituting (2.71) and (2.68) in (2.67), $F_{\widetilde{\gamma}_{C_{II}}}(\gamma)$ can be derived as

$$F_{\widetilde{\gamma}_{C_{II}}}(\gamma) = 1 - \frac{\omega_1 \exp\left(-\frac{\gamma}{\omega_1}\right)}{\omega_1 + \frac{\gamma\left(N_J\,\Delta_{jc}+\rho_{jc}^2\,\omega_2\right)}{N_J}}. \tag{2.72}$$

Now, $\text{SOP}_{\overline{\text{II}}}$ can be derive using the following

$$\text{SOP}_{\overline{\text{II}}} = \int_0^\infty F_{\widetilde{\gamma}_{C_{II}}}(\beta\gamma+\alpha)\, f_{\gamma_{E_{II}}}(\gamma)\, d\gamma. \tag{2.73}$$

By substituting (2.72) and (2.37) in (2.73), and using the same steps in the derivation of (2.53), $\text{SOP}_{\overline{\text{II}}}$ can be obtained as in (2.54).

References

[1] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, “Resource management for device-to-device communication: A physical layer security perspective” *IEEE J. Sel. Areas Commun*., vol. 36, no. 4, pp. 946–960, Apr. 2018

[2] A. Asadi, Q. Wang, and V. Mancuso, “A survey on device-to-device communication in cellular networks,” *IEEE Commun. Surv. Tut*., vol. 16, no. 4, pp. 1801–1819, 4th Quart. 2014.

[3] A. D. Wyner, “The wire-tap channel,” *Bell Sys. Tech. J*., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” *IEEE Commun. Surv. Tut*., vol. 21, no. 3, pp. 2734–2771, 3rd Quart. 2019.

[5] F. Jameel, S. Wyne, G. Kaddoum and T. Q. Duong, “A comprehensive survey on cooperative relaying and jamming strategies for physical layer security,” *IEEE Commun. Surv. Tut*., vol. 21, no. 3, pp. 2734–2771, 3rd Quart. 2019.

[6] Y. Liu, J. Li, and A. P. Petropulu, “Destination assisted cooperative jamming for wireless physical-layer security,” *IEEE Trans. Inf. Forensics Secur*., vol. 8, no. 4, pp. 682–694, Apr. 2013.

[7] J. M. Hamamreh, H. M. Furqan and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1773-1828, 2nd Quart. 2019.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[9] D. Wang, B. Bai, W. Zhao and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1878-1911, 2nd Quart. 2019.

[10] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[11] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, May 2015.

[12] XS. Gong, C. Xing, Z. Fei, and S. Ma, "Millimeter-wave secrecy beamforming designs for two-way amplify-and-forward MIMO relaying networks," *IEEE Trans. Veh. Tech.*, vol. 66, no. 3, pp. 2059–2071, Jun. 2016.

[13] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Oct. 2012.

[14] R. Zhao, H. Lin, Y.-C. He, D.-H. Chen, Y. Huang, and L. Yang, "Secrecy performance of transmit antenna selection for MIMO relay systems with outdated csi," *IEEE Trans Commun.*, vol. 66, no. 2, pp. 546–559, Aug. 2017.

[15] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, “Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI,” *IEEE Trans. Commun*., vol. 63, no. 8, pp. 2959–2971, Jun. 2015.

[16] K. Yang, S. Martin, C. Xing, J. Wu, and R. Fan, “Energy-efficient power control for device-to-device communications,” *IEEE J. Sel. Areas Commun*., vol. 34, no. 12, pp. 3208–3220, Nov. 2016.

[17] W. Wang, K. C. Teh, and K. H. Li, “Enhanced physical layer security in D2D spectrum sharing networks,” *IEEE Wireless Commun. Lett*., vol. 6, no. 1, pp. 106–109, Feb. 2017.

[18] M. A. Kishk and H. S. Dhillon, “Stochastic geometry-based comparison of secrecy enhancement techniques in D2D networks,” *IEEE Wireless Commun. Lett*., vol. 6, no. 3, pp. 394–397, Jun. 2017.

[19] Z. Chu, H. X. Nguyen, T. A. Le, M. Karamanoglu, E. Ever, and A. Yazici, “Secure wireless powered and cooperative jamming D2D communications,” *IEEE Trans. Green Commun. Netw*., vol. 2, no. 1, pp. 1–13, Mar. 2018.

[20] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, “Jamming strategies for physical layer security,” *IEEE Wireless Commun*., vol. 25, no. 1, pp. 148– 153, Feb. 2018.

[21] M. H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, “On the physical layer security of underlay multihop device-to-device relaying,” *in Proc. IEEE Wireless Commun. Netw. Conf*., Apr. 2019, pp. 1–6.

[22] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, “Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications,” *IEEE Access*, vol. 8, pp. 53 575–53 586, Mar. 2020.

[23] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, “Interference exploitation in D2D-enabled cellular networks: A secrecy perspective,” *IEEE Trans. Commun*, vol. 63, no. 1, pp. 229–242, Dec. 2014.

[24] R. Zhang, X. Cheng, and L. Yang, “Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks,” *IEEE Trans. Wireless Commun*, vol. 15, no. 8, pp. 5651–5663, May 2016.

[25] J. Wang, Q. Tang, C. Yang, R. Schober, and J. Li, “Security enhancement via device-to-device communication in cellular networks,” *IEEE Signal Process. Lett*, vol. 23, no. 11, pp. 1622–1626, Sep. 2016.

[26] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, “Resource management for device-to-device communication: A physical layer security perspective,” *IEEE J. Sel. Areas Commun*, vol. 36, no. 4, pp. 946–960, Apr. 2018

[27] N. K. Pratas and P. Popovski, “Low-rate machine-type communication via wireless device-to-device (D2D) links,” May 2013, *arXiv:1305.6783*

[28] T. Kim and M. Dong, “An iterative hungarian method to joint relay selection and resource allocation for D2D communications,” *IEEE Wireless Commun. Lett., vol.*, vol. 3, no. 6, pp. 625–628, Dec. 2014.

[29] J. M. Moualeu, T. M. Ngatched, and D. B. da Costa, “Sequential relay selection in D2D-enabled cellular networks with outdated csi over mixed fading channels,” *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 245–248, Sep. 2018.

[30] K. E. Kolodziej, B. T. Perry, and J. S. Herd, “In-band full-duplex technology: Techniques and systems survey,”*IEEE Trans. Microw. Theory Technol.*, vol. 67, no. 7, pp. 3025–3041, Jul. 2019.

[31] Lei, Hongjiang and Gao, Chao and Ansari, Imran Shafique and Guo, Yongcai and Zou, Yulong and Pan, Gaofeng and Qaraqe, Khalid A, "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237–2250, Mar. 2017.

[32] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5651–5663, May 2016.

[33] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 623–638, Jan. 2019.

[34] I. Krikidis, J. S. Thompson, S. McLaughlin, and N. Goertz, "Max-min relay selection for legacy amplify-and-forward systems with interference," *IEEE Trans. Wireless Commun.*,vol. 8, no. 6, pp. 3016–3027, Jun. 2009.

[35] S. S. Ikki and S. Aissa, "Performance analysis of two-way amplify-and-forward relaying in the presence of co-channel interferences," *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 933–939, Feb. 2012.

[36] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*, McGraw-Hill Education, 2002.

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

[38] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. on Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[39] J. L. Vicario, A. Bel, J. A. Lopez-Salcedo, and G. Seco, “Opportunistic relay selection with outdated CSI: outage probability and diversity analysis,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2872–2876, Jun. 2009.

Chapter 3

Improving PLS of Cellular Networks Using Full-Duplex Jamming Relay-Aided D2D Communications

3.1 Abstract

This chapter investigates the physical layer security and data transmission in cellular networks with inband underlay Device-to-Device (D2D) communications, where there is no direct link between D2D users. We propose to apply full-duplex (FD) transmission and dual antenna selection at the D2D relay node. The relay node can simultaneously act as a friendly jammer to improve the secrecy performance of the cellular network while enhancing the D2D communication data transmission. This is an appealing and practical scheme where spectrum sharing is beneficial for the D2D and cellular networks in terms of reliability enhancement and security provisioning, respectively. The practical scenario, where the eavesdropper is passive, is considered. The eavesdropper uses either selection combining or maximal ratio combining to combine the wiretapped signals of the cellular network. The

secrecy performance of the cellular network is analyzed, and closed-form expressions for the secrecy outage probability and the probability of non-zero secrecy capacity are derived. We show that increasing the number of FD jamming antennas enhances the secrecy performance of the cellular network. A closed-form expression of the D2D outage probability is also provided. Simulation and numerical results are provided to verify the efficiency of the proposed scheme and to validate the accuracy of the derived expressions.

3.2 Introduction

In cellular networks with inband underlay D2D communication, the interference generated by the spectrum sharing between cellular communications and D2D communication is considered as one of the most crucial problems. Such interference is traditionally considered as a drawback that leads to performance degradation of the cellular network. Thus, earlier works on D2D communication focused on decreasing the interference effects in cellular networks by interference management techniques. The underlying assumption in these works is that the interference generated as a result of the spectrum sharing is harmful, and needs to be mitigated, suppressed, or avoided by several techniques. However, as recently proposed in [1], from a PLS perspective, such interference could be beneficial as it can be utilized as artificial noise in CJ to paralyze malicious eavesdroppers and help the CUs prevent wiretapping. This is possible provided that the interference to the CUs is less severe than that to the eavesdroppers. In contrast to the friendly jammer, which consumes power merely to confound the eavesdroppers, D2D communication can further transmit the confidential signal simultaneously, achieving a win-win situation between the D2D users and the CUs. In [2], the influence of the resource allocation on the secrecy capacity is studied to achieve the minimum secrecy rate. Towards this end, the authors of [3] investigate the selection of the appropriate D2D pairs based on the distance between CUs and D2D pairs

to confuse the eavesdroppers.

On the other development, FD communications, which allow the concurrent transmission and reception on a specific spectrum band, has attracted lots of attention as a result of its potential to increase the spectrum efficiency compared to half-duplex communications. Due to the recent advances in the field of signal processing and antenna technology [4], FD transmission, which was previously considered impractical and difficult to implement because of the associated self-interference (SI), is now a convenient choice in various applications. Interestingly, this evolution on FD transmission presents new advantages in safeguarding wireless networks [5]. From a secrecy performance perspective, FD jamming receiver is investigated in [6]. Motivated by this observation, recent research works have studied the inband D2D communication from the PLS perspective [7], [8]. To enhance the PLS performance of cellular networks, these works study the potentials of inband D2D communication, but they only consider the case where there is a direct link between D2D users [9]. However, in some scenarios, the link condition and proximity may not be beneficial for direct communication. In such scenarios, the performance of D2D communication could be enhanced by employing network-assisted transmission through relays. This approach, referred to as relay-aided D2D communication, can efficiently provide a better quality of service between remote D2D pairs. The PLS of underlay multihop D2D relaying is investigated in [10], but from the perspective of enhancing the secrecy performance of D2D links only. It is important to note that, by adopting the FD operation for jamming, the cellular can have secure transmission during the two phases of the D2D transmission. This is in contrast with the work in [11] where, due to the absence of FD, the cellular user can only transmit during the second phase of the D2D transmission for improved secrecy, which negatively impact its spectral efficiency.

In this chapter, we study the PLS of FD relay-aided underlay D2D communication and propose a dual antenna selection to enhance the secrecy performance of the cellular network

and increase the reliability in the D2D communication concurrently. This is achieved by equipping the relay with FD MIMO antennas. Antenna selection approach is employed in this work to avoid the high hardware complexity while maintaining the diversity and reliability advantages from multiple antennas. In the proposed scheme, the data antenna selection at the relay is utilized to increase the reliability of D2D communications, whereas the jamming antenna selection is used to confound the eavesdropper. Thus, the secrecy capacity of the cellular network is maximized. Thanks to the FD dual antenna selection at the relay, the secrecy and data transmission performance are improved concomitantly. Compared to our earlier work in [12], in addition to the SC technique, the MRC technique is also investigated. To elaborate, MRC gives the lowest secrecy performance provided that the eavesdropper is not aware of the jamming signal. It is also noteworthy that, if the eavesdropper is aware of the jamming signal, then beamforming will give the worst secrecy performance. In this respect, the impact of the multiple antennas, at the base station and eavesdropper, on the secrecy performance of the cellular network is studied. In doing so, jamming antenna selection strategy is utilized in this work to maintain the reliability and diversity benefits from multiple antennas while avoiding the high hardware complexity and signaling overheads.

The main contributions of this chapter can be summarized as follows:

- A new network-assisted inband underlay D2D communication system is introduced, where an FD MIMO relay, in addition to its ability to improve data rate, is also used as a friendly jammer.

- A dual antenna selection at the FD MIMO relay is proposed to improve the data transmission of the D2D communication and enhance the secrecy capacity of the cellular network simultaneously.

- The secrecy performance of the cellular network is analyzed and closed-form expres-

sions of the SOP and the PNSC are derived. Additionally, the outage probability of the D2D communication is investigated, and an analytical expression is also obtained.

- Concise expressions for the asymptotic SOP for the cellular network are provided in the high transmit power regime. These expressions reveal that SC and MRC achieve the same secrecy diversity order.

- Monte-Carlo simulation results are presented and compared with the derived analytical expressions, verifying and confirming the correctness and accuracy of the latter.

3.3 System Model

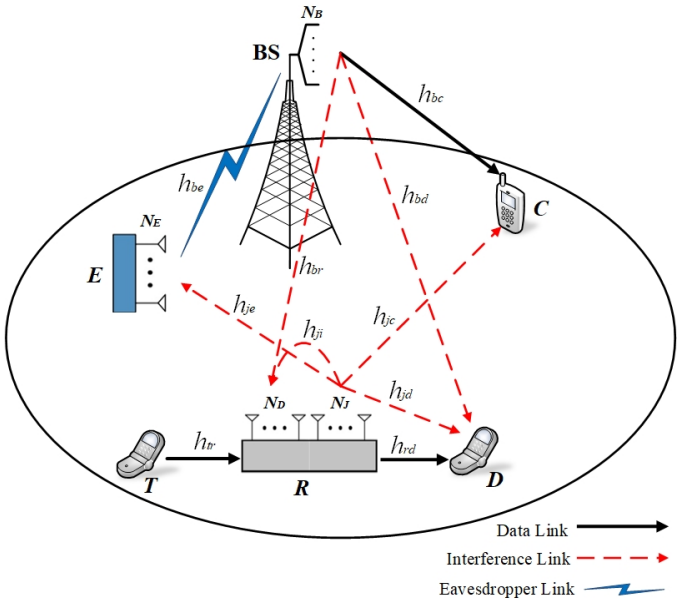


Fig. 3.1: **System Model**.

As shown in Fig. 3.1, a downlink transmission scenario in a relay-aided D2D communication underlying cellular network, where the cellular network enables the D2D users to transmit simultaneously in the same spectral band in a specific environment, is considered. We consider a cellular network consisting of a BS, equipped with N_B antennas,

communicating with a single-antenna cellular user, C, in the presence of a passive multi-antenna eavesdropper, E, equipped with N_E antennas. The D2D network consists of a single-antenna D2D transmitter, T, a multi-antenna relay, R, and a single-antenna D2D receiver, D. The AF relay, R, operates in the FD mode and is equipped with N_D antennas for receiving data from T and transmitting to D, and N_J antennas for transmitting jamming signals towards E. We assume that the CSI of the wiretap channel is available at E, and that of the cellular channel is known to C. All other nodes operate in the half-duplex mode. Furthermore, the D2D transmissions require two phases, one for each hop. In addition, all communication channels are assumed to undergo flat fading with Rayleigh distribution.

In the first phase, T transmits the D2D signal to R. Next, the received signal at R is amplified and re-transmitted to D in the second phase. In both phases, R transmits a jamming signal to E to improve the cellular link security. It should be noted that the BS transmits to the cellular user in both phases as well. Thus, as a compensation for spectrum sharing, the D2D MIMO relay serves as a friendly jammer to ensure high-security level for the cellular network, and thus enables a win-win situation between the two networks, i.e., security provisioning for the cellular user and high reliability for the D2D users. We indicate $\mathcal{U}_i^1$ and $\mathcal{U}_i^2$ as the i^{th} receiving and transmitting antennas in the first and second phases, respectively, where $i = 1, ..., N_D$. In a similar manner, R_j denotes the jamming antenna, where $j = 1, ..., N_J$, and BS$_l$ denotes the transmitting antenna in the BS, where $l = 1, ..., N_B$. The channel coefficients for the $T \rightarrow \mathcal{U}_i^1$, $\mathcal{U}_i^2 \rightarrow D$, BS$_l \rightarrow C$, BS$_l \rightarrow E$, BS$_l \rightarrow D$, $R_j \rightarrow E$, $R_j \rightarrow C$, $R_j \rightarrow \mathcal{U}_i^1$, and $R_j \rightarrow D$ links are denoted as h_{tr}, h_{rd}, h_{bc}, h_{be}, h_{bd}, h_{je}, h_{jc}, h_{ji}, and h_{jd}, respectively. In addition, the channel power gains are indicated by $|h_{ab}|^2$, which are independent and exponentially distributed random variables with a mean of $\lambda_{ab} = \mathbb{E}[|h_{ab}|^2]$, where $\mathbb{E}$ is the expectation operator and $ab \in \{tr, rd, bc, be, bd, je, jc, ji, jd\}$. Furthermore, the variances of the AWGN at R, D, C, and E are denoted by $\sigma_r^2, \sigma_d^2, \sigma_c^2$, and σ_e^2, respectively. It is as-

sumed that the wiretap channel gain is not available at the BS and R. It is also assumed that T and R are transmitting with equal power P.

During the first phase, the receiving antenna $\mathcal{U}_i^1$ is chosen to maximize the instantaneous SNR at R. As a result of using FD relaying, R receives data from T and transmits jamming signals to E at the same time. Since the modern technology can considerably suppress the self-interference to the noise level [13], it can be assumed that the residual self-interference is negligible. The received signal at the i^{th} receiving antenna, $\mathcal{U}_i^1$, is given by

$$y_R = \sqrt{P}\, h_{tr}\, x_d + \sqrt{P_B}\, h_{br}\, x_b + n_r, \tag{3.1}$$

where x_d and x_b are the D2D and BS transmission signals, respectively, P and P_B are the D2D and BS transmission power, respectively, and n_r is the AWGN at the MIMO relay. During the second phase, the transmitting antenna $\mathcal{U}_i^2$ is chosen to maximize the instantaneous SNR at D. Then $\mathcal{U}_i^2$ transmits an amplified version of the received signal to D after employing the relaying gain $\mathcal{G}$. Hence, the received signal at D is given by

$$y_D = \mathcal{G}\, h_{rd} \left(\sqrt{P}\, h_{tr}\, x_d + \sqrt{P_B}\, h_{br}\, x_b + n_r \right) + \sqrt{P_B}\, h_{bd}\, x_b + \sqrt{P_{Rj}}\, h_{jd}\, x_j + n_d, \tag{3.2}$$

where x_j is the jamming signal, P_{Rj} is the jamming transmitted power, and n_d is the AWGN at D. However, since the jamming power P_{Rj} and coefficient h_{jd} are assumed to be known at D, the interference at D generated by the jamming antenna can be eliminated through digital interference cancellation [13]. During each phase, the received signal at C is given by

$$y_C = \sqrt{P_B}\, h_{bc}\, x_b + \sqrt{P_{Rj}}\, h_{jc}\, x_j + n_c, \tag{3.3}$$

where n_c is the AWGN at C. In a similar manner, the received signal at E during each

phase is given by

$$y_E = \sqrt{P_B}\, h_{be}\, x_b + \sqrt{P_{Rj}}\, h_{je}\, x_j + n_e, \tag{3.4}$$

where n_e is the AWGN at the E. In (3.3) and (3.4), it is assumed that the interference from T is negligible. This widely used assumption can be justified by the fact that T is far away and transmits with low power [14]. As the jamming transmitted power from R_j is higher than the data transmitted power from $\mathcal{U}_i^2$, we assume that the interference from $\mathcal{U}_i^2$ towards C is negligible. This assumption is necessary to get mathematically tractable closed-form expressions. For AF relaying scheme, the relaying gain $\mathcal{G}$ is given by [15]

$$\mathcal{G} = \sqrt{\frac{P}{P\left|h_{tr}\right|^2 + P_B\left|h_{br}\right|^2 + \sigma_r^2}}. \tag{3.5}$$

Substituting (3.5) into (3.2), the SINR for the D2D link, γ_{D2D}, after some algebraic manipulations, can be derived as

$$\gamma_{D2D} = \frac{\mathcal{G}^2 P\left|h_{tr}\right|^2\left|h_{rd}\right|^2}{\mathcal{G}^2\left|h_{rd}\right|^2\left(P_B\left|h_{br}\right|^2 + \sigma_r^2\right) + P_B\left|h_{bd}\right|^2 + \sigma_d^2}, \tag{3.6}$$

which, after some algebraic manipulations, simplifies to

$$\gamma_{D2D} = \frac{\gamma_R\,\gamma_D}{\gamma_R + \gamma_D + 1}, \tag{3.7}$$

where γ_R and γ_D are the SINR at R and D, respectively. The SINR at R is given by

$$\gamma_R = \frac{P\left|h_{tr}\right|^2}{\sigma_r^2 + P_b\left|h_{br}\right|^2} = \frac{\gamma_{tr}}{1+\gamma_{br}}, \tag{3.8}$$

and the SINR at D is given by

$$\gamma_D = \frac{P\left|h_{rd}\right|^2}{\sigma_d^2 + P_b\left|h_{bd}\right|^2} = \frac{\gamma_{rd}}{1+\gamma_{bd}}, \tag{3.9}$$

where $\gamma_{tr} = \bar{\gamma}_{tr} |h_{tr}|^2$, $\gamma_{br} = \bar{\gamma}_{br} |h_{br}|^2$, $\bar{\gamma}_r = \frac{P}{\sigma_r^2}$, and $\bar{\gamma}_{br} = \frac{P_B}{\sigma_r^2}$. Similarity, $\gamma_{rd} = \bar{\gamma}_{rd} |h_{rd}|^2$, $\gamma_{bd} = \bar{\gamma}_{bd} |h_{bd}|^2$, $\bar{\gamma}_{rd} = \frac{P}{\sigma_d^2}$, and $\bar{\gamma}_{bd} = \frac{P_B}{\sigma_d^2}$. Let us define $\mu_1 = \bar{\gamma}_{tr}\lambda_{tr}$, $\mu_2 = \bar{\gamma}_{br}\lambda_{br}$, $\mu_3 = \bar{\gamma}_{rd}\lambda_{rd}$, and $\mu_4 = \bar{\gamma}_{bd}\lambda_{bd}$. The maximum D2D two-hop channel gain can be calculated as

$$|h_\upsilon|^2 = \max_{i=1,..N_D} |h_{\upsilon_i}|^2, \tag{3.10}$$

where $\upsilon \in \{tr, rd\}$.

3.4 Performance Analysis

In this section, a comprehensive performance analysis of the illustrated system model is presented. Specifically, closed-form expressions are derived for essential performance metrics, i.e., the D2D outage probability, the SOP, and the PNSC. Additionally, the benefits of the cooperative system model are examined. It is noteworthy that a passive eavesdropper is considered, where the eavesdropper channel states are not known to BS and R.

3.4.1 D2D Outage Probability

The outage probability of the D2D communication, P_{out}, can be expressed as

$$P_{out} = \Pr\left(\gamma_{D2D} \leq \varphi\right), \tag{3.11}$$

where $\varphi = 2^{2\mathcal{R}_d} - 1$, γ_{D2D} is the end-to-end SINR for the D2D link, and $\mathcal{R}_d$ is the D2D required data rate. However, the expression in (3.7) is not mathematically tractable. As a result, a tight upper bound γ_{up} is used to express the end-to-end SINR of the $T \rightarrow R \rightarrow D$ link as follows

$$\gamma_{D2D} \leq \gamma_{up} \stackrel{\triangle}{=} \min\left(\gamma_R, \gamma_D\right). \tag{3.12}$$

Thus, the lower bound P_{out} can be expressed as

$$P_{out} = \Pr\left(\gamma_{up} \leq \varphi\right) = \Pr\left(\min\left(\gamma_R, \gamma_D\right) \leq \varphi\right) = 1 - \left(1 - F_{\gamma_R}(\varphi)\right)\left(1 - F_{\gamma_D}(\varphi)\right), \tag{3.13}$$

where $F_{\gamma_R}(.)$ and $F_{\gamma_D}(.)$ are the cumulative distribution functions (CDFs) of γ_R and γ_D, respectively. We can determine the PDF of γ_R as

$$f_{\gamma_R}(\gamma) = \int_0^{\infty} (y+1) f_{\gamma_{tr}}(\gamma(y+1)) f_{\gamma_{br}}(y) dy, \tag{3.14}$$

where the PDF of γ_{tr} can be expressed in terms of the binomial expansion as

$$f_{\gamma_{tr}}(\gamma) = \frac{N_D}{\mu_1} \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D - 1}{k} e^{-\frac{\gamma\,(k+1)}{\mu_1}}, \tag{3.15}$$

and $f_{\gamma_{br}}(.)$ is given by

$$f_{\gamma_{br}}(x) = \frac{1}{\mu_2} e^{-\frac{x}{\mu_2}}. \tag{3.16}$$

By substituting (3.15) and (3.16) in (3.14), and after simple algebraic manipulations, the PDF of γ_R is derived as

$$f_{\gamma_R}(\gamma) = \frac{N_D}{\mu_1 \mu_2} \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D - 1}{k} e^{-\frac{\gamma\,(k+1)}{\mu_1}} \left(\frac{1 + \frac{\gamma(k+1)}{\mu_1} + \frac{1}{\mu_2}}{\left(\frac{\gamma(k+1)}{\mu_1} + \frac{1}{\mu_2}\right)^2} \right). \tag{3.17}$$

From (3.17), $F_{\gamma_R}(\gamma)$ can be easily obtained as

$$F_{\gamma_R}(\gamma) = N_D \sum_{k=0}^{N_D-1} (-1)^k \frac{\binom{N_D-1}{k}}{(k+1)} \left(1 - \frac{e^{-\frac{\gamma\,(k+1)}{\mu_1}}}{\left(1 + \frac{\gamma\,(k+1)\mu_2}{\mu_1}\right)} \right), \tag{3.18}$$

and

$$F_{\gamma_D}(\gamma) = N_D \sum_{k=0}^{N_D-1} \frac{(-1)^k \binom{N_D-1}{k}}{(k+1)} \left(1 - \frac{e^{-\frac{\gamma\,(k+1)}{\mu_3}}}{\left(1+\frac{\gamma\,(k+1)\mu_4}{\mu_3}\right)}\right). \tag{3.19}$$

By substituting (3.18) and (3.19) in (**??**), P_{out} can be obtained as

$$\begin{aligned} P_{out} =& N_D \sum_{k=0}^{N_D-1} \frac{(-1)^k \binom{N_D-1}{k}}{k+1} \left[\left(2 - \frac{\exp\left(-\frac{\varphi\,(k+1)}{\mu_1}\right)}{\left(1+\frac{\varphi\,(k+1)\mu_2}{\mu_1}\right)} - \frac{\exp\left(-\frac{\varphi\,(k+1)}{\mu_3}\right)}{\left(1+\frac{\varphi\,(k+1)\mu_4}{\mu_3}\right)}\right)\right. \\ & -N_D \sum_{m=0}^{N_D-1} \frac{(-1)^m}{m+1}\binom{N_D-1}{m} \left(\left(1 - \frac{\exp\left(-\frac{\varphi\,(k+1)}{\mu_1}\right)}{\left(1+\frac{\varphi\,(k+1)\mu_2}{\mu_1}\right)}\right)\right. \\ & \left.\left.\times \left(1 - \frac{\exp\left(-\frac{\varphi\,(m+1)}{\mu_3}\right)}{\left(1+\frac{\varphi\,(m+1)\mu_4}{\mu_3}\right)}\right)\right)\right]. \end{aligned} \tag{3.20}$$

3.4.2 Secrecy Outage Probability

The secrecy capacity, normalized to a unit bandwidth, C_S, is given

$$C_S = \left[C_C - C_E\right]^+, \tag{3.21}$$

wher $[x]^+ = \max(x, 0)$. With this in mind, γ_C and γ_E are the SINR at C and E, respectively. In this respect, C_C can be obtained by

$$C_C = \log_2\left(1+\gamma_C\right) = \log_2\left(1 + \frac{\gamma_{bc}}{1+\gamma_{jc}}\right), \tag{3.22}$$

where $\gamma_{bc} = \bar{\gamma}_c \left|h_{bc}\right|^2$, $\gamma_{jc} = \bar{\gamma}_{jc} \left|h_{jc}\right|^2$, $\bar{\gamma}_c = \frac{P_B}{\sigma_c^2}$, and $\bar{\gamma}_{jc} = \frac{P_j}{\sigma_c^2}$. Let us define $\omega_1 = \bar{\gamma}_c \lambda_{bc}$, and $\omega_2 = \bar{\gamma}_{jc}\lambda_{jc}$. In addition, C_E can be obtained by

$$C_E = \log_2\left(1+\gamma_E\right) = \log_2\left(1 + \frac{\gamma_{be}}{1+\gamma_{je}}\right), \tag{3.23}$$

where $\gamma_{be} = \bar{\gamma}_e |h_{be}|^2$, $\gamma_{je} = \bar{\gamma}_{je} |h_{je}|^2$, $\bar{\gamma}_e = \frac{P_B}{\sigma_e^2}$, and $\bar{\gamma}_{je} = \frac{P_j}{\sigma_e^2}$. Let us define $\omega_3 = \bar{\gamma}_e \lambda_{be}$, and $\omega_4 = \bar{\gamma}_{je} \lambda_{je}$.

Jamming Antenna Selection Approach: Because the channel gains between the jamming antennas, R_j, and the eavesdropper, E, are not available, the jamming antenna is selected based on the minimum interference generated towards C, since the channel gain between R_j and C is assumed to be known at R. In this case, the eavesdropper would see a random signal from the selected jamming antenna. Thus, the jamming antenna selection is chosen to satisfy $|h_{jc}|^2 = \min_{i=1,..N_J} |h_{jc_i}|^2$. On the other hand, E would see random channels h_{be} and h_{je}, from selected antennas at the BS and R, respectively. At E, two practical diversity combining techniques, SC and MRC, are investigated. It should be noted that the selected antenna R_j at R transmits a jamming signal to confuse E.

3.4.2.1 Eavesdropper's Channel with SC

In this technique, the signal with the highest instantaneous SNR is selected. The SOP for SC, SOP_{SC}, can be formulated as

$$\text{SOP}_{\text{SC}} = \int_0^\infty F_{\gamma_C}(\beta\gamma + \alpha) f_{\gamma_E}^{\text{SC}}(\gamma)\, d\gamma. \tag{3.24}$$

where $\beta = 2^{\mathcal{R}_s}$, $\alpha = \beta - 1$, $F_{\gamma_C}(\gamma)$ is the CDF of γ_C, and $f_{\gamma_E}^{\text{SC}}(\gamma)$ is the PDF of γ_E for SC. To derive the PDF of γ_C, we have [16]

$$F_{\gamma_C}(\gamma) = \int_0^\infty F_{\gamma_{bc}}(\gamma(\xi + 1)) f_{\gamma_{jc}}(\xi)\, d\xi, \tag{3.25}$$

where $F_{\gamma_{bc}}(.)$ is given by

$$F_{\gamma_{bc}}(\gamma) = N_B \sum_{k=0}^{N_B - 1} \frac{(-1)^k \binom{N_B - 1}{k}}{(k+1)} \left(1 - \exp\left(-\frac{\gamma\,(k+1)}{\omega_1}\right)\right). \tag{3.26}$$

The jamming antenna is selected based on the minimum interference generated from R_j towards C. Hence, $f_{\gamma_{jc}}(.)$ is given by

$$f_{\gamma_{jc}}(\gamma) = \frac{N_J}{\omega_2} \exp\left(-\frac{N_J\,\gamma}{\omega_2}\right). \tag{3.27}$$

Now, by plugging (3.26) and (3.27) into (3.25), and after simple algebraic manipulations, one can get

$$F_{\gamma_C}(\gamma) = N_B \sum_{k=0}^{N_B-1} \frac{(-1)^k \binom{N_B-1}{k}}{(k+1)} \left(1 - \frac{N_j\ \exp\left(-\frac{\gamma(k+1)}{\omega_1}\right)}{N_j + \frac{\omega_2\gamma(k+1)}{\omega_1}}\right). \tag{3.28}$$

Now, the PDF of γ_E can be derived using

$$f^{\text{SC}}_{\gamma_E}(x) = \int_0^\infty (y+1) f_{\gamma_{be}}(x(y+1)) f_{\gamma_{je}}(y) dy, \tag{3.29}$$

where $f_{\gamma_{be}}(.)$ is given by

$$f_{\gamma_{be}}(\gamma) = \frac{N_E}{\omega_3} \sum_{k=0}^{N_E-1} (-1)^k \binom{N_E-1}{k} e^{-\frac{\gamma\,(k+1)}{\omega_3}}. \tag{3.30}$$

and $f_{\gamma_{je}}(.)$ is given by

$$f_{\gamma_{je}}(\gamma) = \frac{1}{\omega_4} e^{-\frac{\gamma}{\omega_4}}. \tag{3.31}$$

By substituting (3.30) and (3.31) in (3.29), and after simple algebraic manipulations, $f^{\text{SC}}_{\gamma_E}(\gamma)$ is obtained as

$$f^{\text{SC}}_{\gamma_E}(\gamma) = \frac{N_E}{\omega_3\,\omega_4} \sum_{k=0}^{N_E-1} (-1)^k \binom{N_E-1}{k} \exp\left(-\frac{\gamma\,(k+1)}{\omega_3}\right) \left(\frac{1 + \frac{\gamma(k+1)}{\omega_3} + \frac{1}{\omega_4}}{\left(\frac{\gamma(k+1)}{\omega_3} + \frac{1}{\omega_4}\right)^2}\right). \tag{3.32}$$

By plugging (3.28) and (3.32) into (3.24), and utilizing partial fraction expansion, then [17, eq. (3.352.4)] and [17, eq. (3.353.3)], the SOP_{SC} can be derived as

$$\begin{aligned}\text{SOP}_{\text{SC}} =& \frac{N_E\, N_B}{\omega_3\, \omega_4} \sum_{k=0}^{N_E-1} \sum_{s=0}^{N_B-1} \frac{(-1)^k}{(k+1)} \binom{N_E-1}{k} \binom{N_B-1}{s} \left[\left(\frac{\omega_3\, \omega_4}{(k+1)} \right.\right. \\ & - \frac{N_J}{\exp\left(\frac{-(s+1)\,\alpha}{\omega_1}\right)} \left(\frac{1}{\mathcal{A}_4} \left(\frac{\omega_3\, \mathcal{A}_2\, \text{Ei}\left[-\mathcal{A}_2\, \mathcal{A}_3\right]}{(k+1)\exp\left(-\mathcal{A}_2\, \mathcal{A}_3\right)} + \left(\frac{\left(\frac{k+1}{\omega_3}\right)(N_J + \mathcal{A}_1\, \alpha)}{\mathcal{A}_4} \right.\right.\right. \\ & \left.\left.\left. - \frac{\mathcal{A}_1\, \beta \left(1 + \frac{1}{\omega_4}\right)}{\mathcal{A}_4} \right) \times \left(\frac{-\text{Ei}\left[-\mathcal{A}_2\, \mathcal{A}_3\right]}{\exp\left(-\mathcal{A}_2\, \mathcal{A}_3\right)} + \frac{\text{Ei}\left[-\frac{\mathcal{A}_2\,(N_J + \mathcal{A}_1\,\alpha)}{\mathcal{A}_1 \beta}\right]}{\exp\left(\frac{-\mathcal{A}_2\,(N_J+\mathcal{A}_1\,\alpha)}{\mathcal{A}_1\,\beta}\right)} \right) \right) \right) \right) \Bigg], \end{aligned} \tag{3.33}$$

where $\beta = 2^{\mathcal{R}_s}$, $\alpha = \beta - 1$, $\mathcal{A}_1 = \frac{\omega_2(s+1)}{\omega_1}$, $\mathcal{A}_2 = \frac{(s+1)\beta}{\omega_1} + \frac{k+1}{\omega_3}$, $\mathcal{A}_3 = \frac{\omega_3}{(k+1)\omega_4}$, $\mathcal{A}_4 = \frac{(k+1)}{\omega_3}(N_j + \mathcal{A}_1\alpha) - \frac{\mathcal{A}_1\beta}{\omega_4}$, and $\text{Ei}(.)$ is the exponential integral function [17, eq. (8.21.1)].

3.4.2.2 Eavesdropper's Channel with MRC

In this technique, the received signals are coherently combined. The SOP for MRC, SOP_{MRC}, is formulated as

$$\text{SOP}_{\text{MRC}} = \int_0^{\infty} F_{\gamma_C}(\beta\gamma + \alpha) f_{\gamma_E}^{\text{MRC}}(\gamma)\, dx, \tag{3.34}$$

where $f_{\gamma_E}^{\text{MRC}}(\gamma)$ is the PDF of γ_E for MRC which can be derived as

$$f_{\gamma_E}^{\text{MRC}}(x) = \int_0^{\infty} (y+1) f_{\gamma_{be}}(x(y+1)) f_{\gamma_{je}}(y) dy, \tag{3.35}$$

where $f_{\gamma_{be}}(.)$ is given by

$$f_{\gamma_{be}}(\gamma) = \frac{\gamma^{N_E-1}}{\Gamma(N_E)\, \omega_3^{N_E}}\, e^{\frac{-\gamma}{\omega_3}}, \tag{3.36}$$

where $\Gamma(.)$ is the gamma function, and $f_{\gamma_{je}}(.)$ is given by

$$f_{\gamma_{je}}(\gamma) = \frac{1}{\omega_4} e^{-\frac{\gamma}{\omega_4}}. \tag{3.37}$$

By substituting (3.36) and (3.37) in (3.35), and after simple algebraic manipulations, $f_{\gamma_E}^{\text{MRC}}(\gamma)$ is obtained as

$$f_{\gamma_E}^{\text{MRC}}(\gamma) = \frac{\gamma^{N_E-1}\, e^{\frac{-\gamma}{\omega_3}}}{\Gamma(N_E)\, \omega_3^{N_E} \omega_4} \sum_{k=0}^{N_E} \binom{N_E}{k} \frac{\Gamma(k+1)}{\left(\frac{\gamma}{\omega_3} + \frac{1}{\omega_4}\right)^{k+1}}. \tag{3.38}$$

By plugging (3.28) and (3.38) in (3.34), using partial fraction expansion, then with the help of [17, eq. (1.111)], [17, eq. (3.381.3)], and [17, eq. (3.383.10)], [17, eq. (3.383.4)], the SOP_{MRC} can be derived as

$$\begin{aligned}\text{SOP}_{\text{MRC}} =& \frac{N_B}{\Gamma(N_E)\, \omega_3^{N_E} \omega_4} \sum_{m=0}^{N_E} \sum_{q=0}^{N_B-1} \frac{(-1)^q \binom{N_E}{k} \binom{N_B-1}{q} \Gamma(m+1)}{(q+1)} \Bigg[\frac{\omega_3^{N_E}}{\exp\left(\frac{-1}{\omega_4}\right)} \sum_{p=0}^{N_E-1} \binom{N_E-1}{p} \\ &\times \frac{\Gamma\left(p-m, \frac{1}{\omega_4}\right)}{\left(\frac{-1}{\omega_4}\right)^{-(N_E-1-p)}} - \frac{N_J\, \omega_1\, \omega_3^{m+1}}{\omega_2\, (q+1)\, \beta \exp\left(\frac{(q+1)\,\alpha}{\omega_1}\right)} \left(\sum_{i=1}^{m+1} \frac{(-1)^{m+1-i} \exp\left(\frac{\mathcal{B}_1 \mathcal{B}_2}{2}\right)}{\left(\mathcal{B}_4 - \mathcal{B}_2\right)^{m+2-i}} \right. \\ &\left. \times \frac{\Gamma(N_E) \mathcal{W}_{\frac{1-i-N_E}{2}, \frac{i-N_E}{2}}\left(\mathcal{B}_1 \mathcal{B}_2\right)}{\mathcal{B}_1^{\left(\frac{N_E-i+1}{2}\right)} \mathcal{B}_2^{-\left(\frac{N_E-i-1}{2}\right)}} + \frac{\mathcal{B}_4^{N_E-1}\, \Gamma\left(N_E\right) \Gamma\left(1-N_E, \mathcal{B}_1 \mathcal{B}_4\right)}{\exp\left(-\mathcal{B}_1\, \mathcal{B}_4\right) \left(\mathcal{B}_2 - \mathcal{B}_4\right)^{m+1}} \right) \Bigg], \end{aligned} \tag{3.39}$$

where $\mathcal{B}_1 = \frac{\beta(q+1)}{\omega_1} + \frac{1}{\omega_3}$, $\mathcal{B}_2 = \frac{\omega_3(k+1)}{\omega_4}$, $\mathcal{B}_3 = \frac{1}{\beta}\left(\alpha + \frac{\omega_1}{\omega_2(q+1)}\right), \mathcal{B}_4 = \frac{1}{\beta}\left(\alpha + \frac{N_J\, \omega_1}{\omega_2(q+1)}\right)$, $\Gamma(.,.)$ is the upper incomplete gamma function [17, eq. (8.350.2)], and $\mathcal{W}_{a,b}(.)$ is the Whittaker function [17, eq. (9.220.4)].

3.4.3 Asymptotic Secrecy Outage Analysis

In this subsection, the SOP at high SNR, i.e., when $\overline{\gamma}_c \rightarrow \infty$, is presented to get more insights on the influence of the significant parameters of the proposed system on the performance of the SOP. Specifically, the secrecy diversity order, G_d, and the secrecy array gain, G_a, are investigated. In this case, it is considered that the locations of the BS and C are close. In this scenario, we consider that $\overline{\gamma}_c >> \overline{\gamma}_e$. As $\overline{\gamma}_c \rightarrow \infty$, the asymptotic expression of SOP$^{\infty}$ can be written as [18]

$$\text{SOP}^{\infty} = (G_a \overline{\gamma}_c)^{-G_d} + \mathcal{O}(\overline{\gamma}_c^{-G_d}), \tag{3.40}$$

where $\mathcal{O}(.)$ is the higher order terms. From this expression, it can be inferred that the SOP$^{\infty}$ curve is characterized by G_d, while the SNR gain of SOP$^{\infty}$ relative to the reference curve, $(\overline{\gamma}_c)^{-G_d}$, is characterized by G_a.

3.4.3.1 Eavesdropper's Channel with SC

To derive the asymptotic SOP for SC, SOP$_{\text{SC}}^{\infty}$, the exponential function in (3.28), given in the appendix, is expanded using Taylor series expansion in [17, eq. (1.211.1)]. Then, the first two terms in the expansion are kept, and the higher-order terms are neglected. Thus, the asymptotic CDF of γ_C, $F_{\gamma_C}^{\infty}(.)$, is given by

$$F_{\gamma_C}^{\infty}(\gamma) = \sum_{p=0}^{N_B} \frac{\binom{N_B}{p}\Gamma(p+1)}{\left(\frac{N_J}{\omega_2}\right)^p} \left(\frac{\gamma}{\omega_1}\right)^{N_B} + \mathcal{O}\left(\frac{\gamma}{\omega_1}\right). \tag{3.41}$$

Now, the SOP$_{\text{SC}}^{\infty}$ can be obtained using

$$\text{SOP}_{\text{SC}}^{\infty} = (G_{a_{\text{SC}}} \overline{\gamma}_c)^{-G_{d_{\text{SC}}}} + \mathcal{O}(\overline{\gamma}_c^{-G_{d_{\text{SC}}}}), \tag{3.42}$$

where $G_{d_{\text{SC}}} = N_B$ and $G_{a_{\text{SC}}}$ is given by

$$G_{a_{\text{SC}}} = \Bigg[\frac{N_E}{\omega_3 \omega_4} \sum_{p=0}^{N_B} \binom{N_B}{p} \left(\frac{\omega_2}{N_J}\right)^p \Gamma(p+1) \sum_{k=0}^{N_E-1} (-1)^k \binom{N_E-1}{m} \sum_{s=0}^{N_B} \binom{N_B}{s} \times \frac{\alpha^{N_B-s}\, \beta^s}{\exp\left(\frac{1}{2\omega_4}\right)} \left(\frac{\omega_3}{k+1}\right)^s \Gamma(s+1) \left(\left(\frac{1}{\omega_4}\right)^{\frac{s-2}{2}} \mathcal{W}_{\frac{-2-s}{2}, \frac{1-s}{2}} \left(\frac{1}{\omega_4}\right) \right) \Bigg]^{\frac{-1}{N_B}}. \tag{3.43}$$

3.4.3.2 Eavesdropper's Channel with MRC

Using the same approach and following the same steps as above, the asymptotic SOP for MRC, $\text{SOP}^{\infty}_{\text{MRC}}$, can also be written as

$$\text{SOP}^{\infty}_{\text{MRC}} = (G_{a_{\text{MRC}}} \overline{\gamma}_c)^{-G_{d_{\text{MRC}}}} + \mathcal{O}(\overline{\gamma}_c^{-G_{d_{\text{MRC}}}}), \tag{3.44}$$

where $G_{d_{\text{MRC}}} = N_B$ and $G_{a_{\text{MRC}}}$ is given by

$$G_{a_{\text{MRC}}} = \Bigg[\sum_{p=0}^{N_B} \binom{N_B}{p} \left(\frac{\omega_2}{N_J}\right)^p \Gamma(p+1) \sum_{m=0}^{N_E} \binom{N_E}{m} \frac{\Gamma(m+1)}{\omega_3^{N_E}\, \omega_4\, \Gamma(N_E)} \sum_{s=0}^{N_B} \binom{N_B}{s} \times \frac{\alpha^{N_B-s}\, \beta^s}{\exp\left(\frac{-1}{\omega_4}\right) \omega_3^{m+1}} \sum_{v=0}^{N_E+s-1} \binom{N_E+s-1}{v} \frac{\Gamma\left(v-m, \frac{1}{\omega_4}\right) \omega_3^{v-m}}{\left(\frac{-\omega_3}{\omega_4}\right)^{-(N_E+s-v-1)}} \Bigg]^{\frac{-1}{N_B}}. \tag{3.45}$$

3.4.4 Probability of Non-zero Secrecy Capacity

In this subsection, the requirement for the presence of the non-zero secrecy capacity is investigated. It is worth noting that the non-zero secrecy capacity is achieved when $\gamma_C > \gamma_E$. The PNSC is given by

$$\text{PNSC} = \Pr\left(\frac{1+\gamma_C}{1+\gamma_E} > 1\right) = 1 - \int_0^{\infty} F_{\gamma_C}(\gamma) f_{\gamma_E}(\gamma)\, d\gamma. \tag{3.46}$$

3.4.4.1 Eavesdropper's Channel with SC

By substituting (3.28) and (3.32) in (3.46), and using partial fraction expansion, then [17, eq. (3.352.4)] and [17, eq. (3.353.3)], the PNSC_{SC} can be obtained as

$$\begin{aligned}\text{PNSC}_{\text{SC}} = 1 - \frac{N_E\, N_B}{\omega_3\omega_4}\sum_{k=0}^{N_E-1}\sum_{s=0}^{N_B-1}\frac{(-1)^k}{(k+1)}\binom{N_E-1}{k}\binom{N_B-1}{s}\Bigg[\Bigg(\frac{\omega_3\omega_4}{(k+1)} - N_J \\ \times\left(\frac{1}{\frac{(k+1)}{\omega_3}N_j - \frac{\mathcal{A}_1}{\omega_4}}\left(\frac{\omega_3\mathcal{A}_2}{(k+1)}e^{\mathcal{A}_2\mathcal{A}_4}\text{Ei}\left[-\mathcal{A}_2\mathcal{A}_5\right] + \frac{1}{\mathcal{A}_4} + \frac{\left(\frac{k+1}{\omega_3}\right)(N_J) - \mathcal{A}_1\left(1+\frac{1}{\omega_4}\right)}{\left(\frac{k+1}{\omega_3}\right)N_j - \frac{\mathcal{A}_1}{\omega_4}}\right.\right. \\ \left.\left.\times\left(-\frac{\text{Ei}\left[-\mathcal{A}_2\mathcal{A}_5\right]}{e^{-\mathcal{A}_2\mathcal{A}_5}} + \frac{\text{Ei}\left[-\frac{\mathcal{A}_2 N_J}{\mathcal{A}_1}\right]}{e^{-\frac{\mathcal{A}_2 N_J}{\mathcal{A}_1}}}\right)\right)\right)\Bigg],\end{aligned} \tag{3.47}$$

where $\mathcal{A}_5 = \frac{s+1}{\omega_1} + \frac{k+1}{\omega_3}$.

3.4.4.2 Eavesdropper's Channel with MRC

Following the same steps of deriving (3.47), the PNSC_{MRC} can be obtained as

$$\begin{aligned}\text{PNSC}_{\text{MRC}} = 1 - \frac{N_B}{\Gamma(N_E)\,\omega_3^{N_E}\omega_4}\sum_{m=0}^{N_E}\sum_{q=0}^{N_B-1}\frac{(-1)^q\binom{N_E}{k}\binom{N_B-1}{q}\Gamma(m+1)}{(q+1)}\Bigg[\omega_3^{N_E}e^{\frac{1}{\omega_4}}\sum_{p=0}^{N_E-1} \\ \binom{N_E-1}{p}\left(\frac{-1}{\omega_4}\right)^{N_E-1-p}\Gamma\left(p-m,\frac{1}{\omega_4}\right) - \frac{N_J\,\omega_1\omega_3^{m+1}}{\omega_2(q+1)}\left(\sum_{i=1}^{m+1}(-1)^{m+1-i}\right. \\ \times\frac{e^{\frac{\vartheta_1\mathcal{B}_2}{2}}\vartheta_1^{-\left(\frac{N_E-i+1}{2}\right)}\vartheta_2^{\frac{N_E-i-1}{2}}\Gamma(N_E)}{(\vartheta_4-\vartheta_2)^{m+2-i}}\mathcal{W}_{\frac{1-i-N_E}{2},\frac{i-N_E}{2}}(\vartheta_1\vartheta_2) + \vartheta_4^{N_E-1}\,e^{\vartheta_1\,\vartheta_4} \\ \left.\times\frac{\Gamma(N_E)\Gamma\left(1-N_E,\vartheta_1\vartheta_4\right)}{(\vartheta_2-\vartheta_4)^{m+1}}\right)\Bigg],\end{aligned} \tag{3.48}$$

where $\vartheta_1 = \frac{q+1}{\omega_1} + \frac{1}{\omega_3}$, $\vartheta_2 = \frac{\omega_3(k+1)}{\omega_4}$, $\vartheta_3 = \frac{\omega_1}{\omega_2(q+1)}$, and $\vartheta_4 = \frac{N_J\,\omega_1}{\omega_2(q+1)}$.

3.5 Analysis with Outdated CSI

We study the influence of outdated CSI on the PLS of the cellular network using the FD relay. To do so, a dual antenna selection is introduced to increase the throughput in the D2D links while enhancing the security level of the cellular network simultaneously. To this end, we derive closed-form expressions for the SOP, and the outage probability of the D2D communication, assuming SC and MRC are utilized at the eavesdropper side. Additionally, for the high-SNR regime, tight asymptotic SOP expressions are derived for the cellular network. Furthermore, Monte-Carlo simulation is utilized to verify our analysis.

To find the maximum D2D two-hop channel gain, $|\mathcal{H}_\epsilon|^2$, we can use

$$|\mathcal{H}_\epsilon|^2 = \max_{i=1,..N_D} \left|\widetilde{h}_{\epsilon_i}\right|^2, \tag{3.49}$$

where $\epsilon \in \{tr, rd\}$. The SINR at R can be expressed as

$$\gamma_R = \frac{P\,|\mathcal{H}_{tr}|^2}{\sigma_r^2 + P_b\,|h_{br_i}|^2} = \frac{\gamma_{tr}}{1+\gamma_{br}}, \tag{3.50}$$

where $\gamma_{tr} = \bar{\gamma}_{tr}\,|\mathcal{H}_{tr}|^2$, $\gamma_{br} = \bar{\gamma}_{br}\,|h_{br_i}|^2$, $\bar{\gamma}_r = \frac{P}{\sigma_r^2}$, and $\bar{\gamma}_{br} = \frac{P_b}{\sigma_r^2}$. The SINR at D is given by

$$\gamma_D = \frac{P\,|h_{r_id}|^2}{\sigma_d^2 + P_b\,|h_{bd}|^2} = \frac{\gamma_{rd}}{1+\gamma_{bd}}, \tag{3.51}$$

where $\gamma_{rd} = \bar{\gamma}_{rd}\,|\mathcal{H}_{rd}|^2$, $\gamma_{bd} = \bar{\gamma}_{bd}\,|h_{bd}|^2$, $\bar{\gamma}_{rd} = \frac{P}{\sigma_d^2}$, and $\bar{\gamma}_{bd} = \frac{P_b}{\sigma_d^2}$. Let us define $\mathcal{E}_1 = \bar{\gamma}_{tr}\lambda_{tr}$, $\mathcal{E}_2 = \bar{\gamma}_{br}\lambda_{br}$, $\mathcal{E}_3 = \bar{\gamma}_{rd}\lambda_{rd}$, and $\mathcal{E}_4 = \bar{\gamma}_{bd}\lambda_{bd}$.

It is also noteworthy that the CSI for all D2D links are outdated, while it is perfect for the cellular network. As a result of some circumstances such as the delay of the feedback and the mobility, the outdated CSI $\widetilde{h}_\upsilon$ may vary from the actual CSI denoted as h_υ, giving by [19] $h_\upsilon = \rho_\upsilon\,\widetilde{h}_\upsilon + \sqrt{1-\rho_\upsilon}\,w_\upsilon$, where ρ_υ is the correlation coefficient between h_υ and $\widetilde{h}_\upsilon$, and w_υ is a circularly symmetric complex Gaussian RV having equal variance as the

RV h_υ. Hence, the conditional PDF $f_{\gamma_\upsilon|\widetilde{\gamma}_\upsilon}(.)$ is given by

$$f_{\gamma_\upsilon|\widetilde{\gamma}_\upsilon}(\gamma/x) = \frac{1}{\Delta_\upsilon} e^{-\frac{\left(\gamma+\rho_\upsilon^2\, x\right)}{\Delta_\upsilon}}\, \mathcal{I}_o\left(2\,\frac{\rho_\upsilon\sqrt{\gamma\, x}}{\Delta_\upsilon}\right), \tag{3.52}$$

where γ_υ and $\widetilde{\gamma}_\upsilon$ are the SINRs for the actual and outdated CSI for the υ channel, $\Delta_\upsilon = (1-\rho_\upsilon^2)\,\bar{\gamma}_\upsilon$, and $\mathcal{I}_o(.)$ is the zero-order modified Bessel function of the first kind [17, eq. (8.445)]. The PDF of γ_υ is given by

$$f_{\gamma_\upsilon}(\gamma) = \int_0^\infty f_{\gamma_\upsilon|\widetilde{\gamma}_\upsilon}(\gamma/x) f_{\widetilde{\gamma}_\upsilon}(x)\, dx. \tag{3.53}$$

3.5.1 Performance Analysis

3.5.1.1 D2D Outage Probability

In this section, the D2D outage probability, P_{out}, is investigated. To obtain P_{out}, we have

$$P_{out} = \Pr\left(\gamma_{up} \leq \varphi\right) = F_{\gamma_R}(\gamma_{th}) + F_{\gamma_D}(\gamma_{th}) - F_{\gamma_R}(\gamma_{th}) F_{\gamma_D}(\gamma_{th}). \tag{3.54}$$

Lemma 3: The CDF of γ_R can be derived as

$$F_{\gamma_R}(\gamma) = N_D \sum_{k=0}^{N_D-1} \frac{(-1)^k \binom{N_D-1}{k}}{k+1} \left(1 - \frac{\exp\Big(-\Xi_1\,\gamma\Big)}{1+\mathcal{E}_2\,\Xi_1\,\gamma}\right), \tag{3.55}$$

where $\Xi_1 = \frac{(k+1)}{\Delta_{tr}(k+1)+\rho_{tr}^2\mathcal{E}_1}$ with $\Delta_{tr} = (1-\rho_{tr}^2)\,\mathcal{E}_1$.

Proof: See Appendix A. ■

Following the same steps, F_{γ_D} can by expressed as

$$F_{\gamma_D}(\gamma) = N_D \sum_{m=0}^{N_D-1} \frac{(-1)^m \binom{N_D-1}{m}}{m+1} \left(1 - \frac{\exp\Big(-\Xi_2\,\gamma\Big)}{1+\mathcal{E}_4\,\Xi_2\,\gamma}\right), \tag{3.56}$$

where $\Xi_2 = \frac{(m+1)}{\Delta_{rd}(m+1)+\rho_{rd}^2\mathcal{E}_3}$ with $\Delta_{rd} = (1-\rho_{rd}^2)\,\mathcal{E}_3$. By plugging (3.55) and (3.56) into (3.54), P_{out} can be obtained.

3.5.1.2 Secrecy Outage Probability

In this section, the SOP is analyzed. The secrecy capacity, C_S, is given by

$$C_S = [C_C - C_E]^+, \tag{3.57}$$

where C_C and C_E are the cellular and eavesdropper normalized capacities, respectively, and $[x]^+ = max\,(x, 0)$. Moreover, the best antenna at BS is chosen based on the following criterion $|\mathcal{H}_{bc}|^2 = \max\limits_{l=1,..N_B} |h_{b_l c}|^2$. In this respect, C_C is given by

$$C_C = \log_2(1+\gamma_C) = \log_2\left(1+\frac{\gamma_{bc}}{1+\gamma_{jc}}\right), \tag{3.58}$$

where $\gamma_{bc} = \bar{\gamma}_c\,|\mathcal{H}_{bc}|^2$, $\gamma_{jc} = \bar{\gamma}_{jc}\,|h_{jc}|^2$, $\bar{\gamma}_c = \frac{P_b}{\sigma_c^2}$, and $\bar{\gamma}_{jc} = \frac{P_j}{\sigma_c^2}$. Let us define $\mathcal{Z}_1 = \bar{\gamma}_c\lambda_{bc}$, and $\mathcal{Z}_2 = \bar{\gamma}_{jc}\lambda_{jc}$. In addition, C_E is given by

$$C_E = \log_2(1+\gamma_E) = \log_2\left(1+\frac{\gamma_{be}}{1+\gamma_{je}}\right), \tag{3.59}$$

where $\gamma_{be} = \bar{\gamma}_e\,|h_{be}|^2$, $\gamma_{je} = \bar{\gamma}_{je}\,|h_{be}|^2$, $\bar{\gamma}_e = \frac{P_b}{\sigma_e^2}$, and $\bar{\gamma}_{je} = \frac{P_j}{\sigma_e^2}$. Let us define $\mathcal{Z}_3 = \bar{\gamma}_e\lambda_{be}$, and $\mathcal{Z}_4 = \bar{\gamma}_{je}\lambda_{je}$.

Jamming Antenna Selection Approach: The jamming antenna, which produces the minimum interference generated towards C, is selected to satisfy $|h_{jc}|^2 = \min\limits_{j=1,..N_J} \left|\widetilde{h}_{jc}\right|^2$.

Lemma 2: The CDF of $\widetilde{\gamma}_{C_I}$ can be derived as

$$F_{\gamma_C(\gamma)} = \frac{N_B N_J}{\varphi_3}\sum_{q=0}^{N_B-1}\frac{(-1)^q\binom{N_B-1}{q}}{(q+1)}\left(\frac{1}{\varphi_2}-\frac{\exp\Big(-\varphi_1\gamma\Big)}{\varphi_2+\varphi_1\gamma}\right), \tag{3.60}$$

where $\varphi_1 = \frac{q+1}{\mathcal{Z}_1}$, $\varphi_2 = \frac{N_J}{N_J\Delta_{jc}+\rho_{jc}^2\mathcal{Z}_2}$, $\varphi_3 = N_J\Delta_{jc} + \rho_{jc}^2\mathcal{Z}_2$, and, $\Delta_{jc} = \left(1-\rho_{jc}^2\right)\mathcal{Z}_1$.

Proof: See Appendix B. ■

Now, the SOP can be derived as

$$\text{SOP}_{\xi} = \int_0^{\infty} F_{\gamma_C}(\gamma)(\beta x+\alpha) f_{\gamma_E}^{\xi}(\gamma)\, d\gamma, \tag{3.61}$$

where $\xi \in \{\text{SC}, \text{MRC}\}$. The $f_{\gamma_E}^{\text{SC}}(\gamma)$ can be derived as

$$f_{\gamma_E}^{\text{SC}}(\gamma) = \frac{N_E}{\mathcal{Z}_3\mathcal{Z}_4}\sum_{k=0}^{N_E-1}(-1)^k\binom{N_E-1}{k}\exp\Big(-\frac{\gamma(k+1)}{\mathcal{Z}_3}\Big)\left(\frac{1+\frac{\gamma(k+1)}{\mathcal{Z}_3}+\frac{1}{\mathcal{Z}_4}}{\left(\frac{\gamma(k+1)}{\mathcal{Z}_3}+\frac{1}{\mathcal{Z}_4}\right)^2}\right). \tag{3.62}$$

By substituting (3.60) and (3.62) in (3.61), and with help of partial fraction expansion, then using [17, eq. (3.353.3)] and [17, eq. (3.352.4)], the SOP_{SC} can be derived as

$$\begin{aligned}\text{SOP}_{\text{SC}} =& \frac{N_B N_J N_E}{\varphi_4\mathcal{Z}_3\,\mathcal{Z}_4}\sum_{q=0}^{N_B-1}\sum_{k=0}^{N_E-1}\frac{(-1)^{q+k}\binom{N_B-1}{q}\binom{N_E-1}{k}}{(q+1)}\left[\frac{\mathcal{Z}_3\,\mathcal{Z}_4}{(k+1)\,\varphi_2}-\frac{\mathcal{Z}_3\,\zeta_1\exp\Big(-\varphi_1\alpha\Big)}{(k+1)}\right.\\ &\times\left(\frac{\left(\varphi_1\beta+\frac{(k+1)}{\mathcal{Z}_3}\right)\text{Ei}\Big[-\zeta_2\zeta_4\Big]}{\exp\Big(-\zeta_2\,\zeta_4\Big)}+\frac{1}{\zeta_4}\right)+\zeta_3\left(\frac{\varphi_2+\varphi_1\alpha}{\varphi_1\beta}\right)\left(\frac{\text{Ei}\left[-\zeta_2\left(\frac{\varphi_2+\varphi_1\alpha}{\varphi_1\beta}\right)\right]}{\exp\Big(-\zeta_2\Big)}\right.\\ &\left.\left.-\frac{\text{Ei}\Big[-\zeta_2\zeta_4\Big]}{\exp\Big(-\zeta_2\,\zeta_4\Big)}\right)\right],\end{aligned} \tag{3.63}$$

where

$\zeta_1 = \frac{\mathcal{Z}_3\,\mathcal{Z}_4}{(k+1)(\mathcal{Z}_4(\varphi_2+\varphi_1\alpha)-\mathcal{Z}_3\varphi_1\beta)}$, $\zeta_2 = \left(\varphi_1\beta+\frac{(k+1)}{\mathcal{Z}_3}\right)$,

$\zeta_3 = \zeta_1\left(\frac{\varphi_2(k+1)}{\mathcal{Z}_3}-\varphi_1\left(\beta\left(1+\frac{1}{\mathcal{Z}_4}\right)-\frac{(k+1)\alpha}{\mathcal{Z}_3}\right)\right)$, and $\zeta_4 = \frac{\mathcal{Z}_3}{\mathcal{Z}_4(k+1)}$.

For MRC, $f_{\gamma_E}^{\text{MRC}}(\gamma)$ can be derived as

$$f_{\gamma_E}^{\text{MRC}}(\gamma) = \frac{\gamma^{N_E-1}\, e^{\frac{-\gamma}{\mathcal{Z}_3}}}{\Gamma(N_E)\, \mathcal{Z}_3^{N_E}\, \mathcal{Z}_4} \sum_{k=0}^{N_E} \frac{\binom{N_E}{k}\Gamma(k+1)}{\left(\frac{\gamma}{\mathcal{Z}_3}+\frac{1}{\mathcal{Z}_4}\right)^{k+1}}. \tag{3.64}$$

By plugging (3.60) and (3.38) into (3.61), and with the help of the partial fraction expansion, then using [17, eq. (1.111)],[17, eq. (3.383.4)], and [17, eq. (3.383.10)], the SOP_{MRC} can be derived as

$$\begin{aligned}\text{SOP}_{\text{MRC}} =& \frac{N_B N_J}{\varphi_3 \mathcal{Z}_3^{N_E}\, \mathcal{Z}_4} \sum_{k=0}^{N_E} \sum_{q=0}^{N_B-1} \frac{(-1)^q \binom{N_E}{m}\binom{N_B-1}{q}\Gamma(m+1)}{(q+1)} \Bigg[\frac{\mathcal{Z}_3^{2N_E+k} \exp\left(\frac{1}{2\mathcal{Z}_4}\right)}{\varphi_2\, \mathcal{Z}_4^{\frac{N_E-k-2}{2}}} \\ &\times \mathcal{W}_{\frac{-k-N_E}{2},\frac{1-N_E+k}{2}}\left(\frac{1}{\mathcal{Z}_4}\right) - \frac{\mathcal{Z}_3^{k+1}}{\exp\left(\varphi_1\alpha\right)\varphi_1\,\beta} \left(\sum_{i=1}^{k+1} \frac{(-1)^{k+1-i}\exp\left(\frac{\delta_1\delta_2}{2}\right)}{(\delta_3-\delta_2)^{k+2-i}} \right. \\ &\left. \times \frac{\delta_1^{-\left(\frac{N_E-i+1}{2}\right)}}{\delta_2^{-\left(\frac{N_E-i-1}{2}\right)}} \mathcal{W}_{\frac{1-i-N_E}{2},\frac{i-N_E}{2}}\left(\delta_1\delta_2\right) + \frac{\delta_3^{N_E-1}\Gamma\left(1-N_E,\delta_1\delta_3\right)}{\exp\left(-\delta_1\delta_3\right)(\delta_2-\delta_3)^{k+1}} \right) \Bigg], \end{aligned} \tag{3.65}$$

where $\delta_1 = \beta\varphi_1 + \frac{1}{\mathcal{Z}_3}$, $\delta_2 = \frac{\mathcal{Z}_3}{\mathcal{Z}_4}$, and $\delta_3 = \frac{\varphi_2+\varphi_1\alpha}{\beta\varphi_1}$.

3.5.1.3 Asymptotic Secrecy Outage Analysis

The asymptotic, SOP^{∞}, can be expressed as $\text{SOP}^{\infty} = (G_{a_\xi}\overline{\gamma}_c)^{-G_d} + \mathcal{O}(\overline{\gamma}_c^{-G_{d_\xi}})$. Mathematically speaking, the asymptotic CDF, $F_{\gamma_C}^{\infty}(.)$, can be expressed as

$$F_{\gamma_C}^{\infty}(\gamma) = \sum_{p=0}^{N_B} \frac{\binom{N_B}{p}\Gamma(p+1)}{\varphi_2^p} \left(\frac{\gamma}{\mathcal{Z}_1}\right)^{N_B} + \mathcal{O}\left(\frac{\gamma}{\mathcal{Z}_1}\right). \tag{3.66}$$

Now, $\text{SOP}_{\text{SC}}^{\infty}$ can be obtained by substituting (3.66) in (3.61). After performing some algebraic manipulations, $G_{d_{\text{SC}}} = N_B$ and the $G_{a_{\text{SC}}}$ is given by

$$G_{a_{\text{SC}}} = \Bigg[\frac{N_E}{\mathcal{Z}_3 \mathcal{Z}_4} \sum_{p=0}^{N_B} \frac{\binom{N_B}{p} \Gamma(p+1)}{\varphi_2^p} \sum_{k=0}^{N_E-1} (-1)^k \binom{N_E-1}{m} \sum_{s=0}^{N_B} \binom{N_B}{s} \frac{\alpha^{N_B-s} \Gamma(s+1)}{\left(\frac{k+1}{w_3}\right)^s \beta^{-s} \exp\left(\frac{1}{2\mathcal{Z}_4}\right)} \left(\frac{1}{\mathcal{Z}_4}\right)^{\frac{s-1}{2}} \left(\left(\frac{1}{\mathcal{Z}_4}\right)^{\frac{-1}{2}} \mathcal{W}_{\frac{-2-s}{2}, \frac{1-s}{2}} \left(\frac{1}{\mathcal{Z}_4}\right) \right) \Bigg]^{\frac{-1}{N_B}}.$$

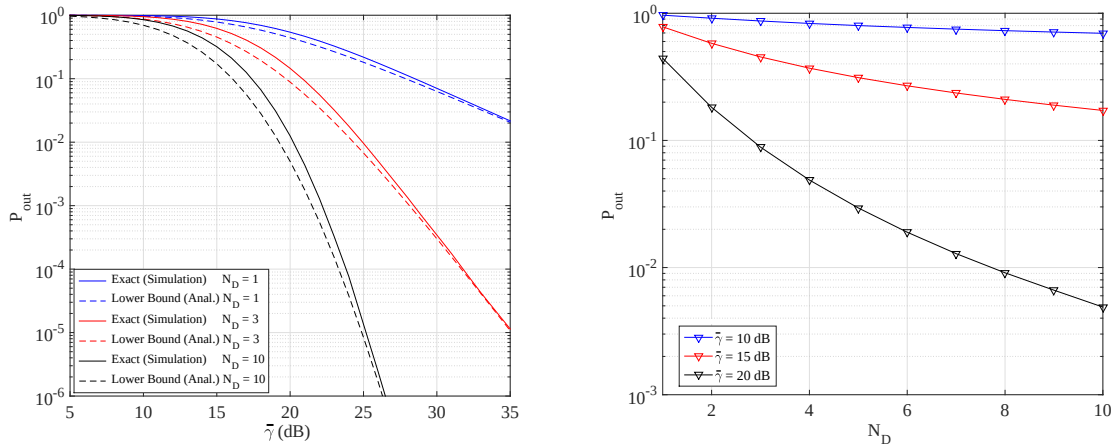
For MRC, $G_{d_{\text{MRC}}} = N_B$ and $G_{a_{\text{MRC}}}$ is given by

$$G_{a_{\text{MRC}}} = \Bigg[\sum_{p=0}^{N_B} \frac{\binom{N_B}{p} \Gamma(p+1)}{\varphi_2^p} \sum_{m=0}^{N_E} \binom{N_E}{m} \frac{\Gamma(m+1)}{\mathcal{Z}_3^{N_E} \mathcal{Z}_4 \Gamma(N_E)} \sum_{s=0}^{N_B} \binom{N_B}{s} \frac{\alpha^{N_B-s} \mathcal{Z}_3^{m+1}}{\beta^{-s} \exp\left(\frac{-1}{\mathcal{Z}_4}\right)} \sum_{v=0}^{N_E+s-1} \binom{N_E+s-1}{v} \left(\frac{-\mathcal{Z}_3}{\mathcal{Z}_4}\right)^{N_E+s-v-1} \Gamma\left(v-m, \frac{1}{\mathcal{Z}_4}\right) \mathcal{Z}_3^{v-m} \Bigg]^{\frac{-1}{N_B}}.$$

3.6 Results and Discussions

In this section, the analytical results of the D2D outage probability, the SOP, and the PNSC are presented and compared with those obtained by Monte-Carlo simulations. Regarding the described system model, the secrecy performance of the cellular network is analyzed, and the impact of the FD relay is investigated. Without loss of generality, we normalize the variances of the noise at R, D, C, and E to unity. Unless stated, μ_2 = μ_4 = 10 dB, $\mathcal{R}_s = 1$ b/s/Hz , $\omega_2 = \omega_3 = 10$ dB, and $\mathcal{R}_s = 1$ b/s/Hz.

Fig. 3.2a plots the analytical lower bound and exact (simulation) outage probability, P_{out}, for D2D communication versus $\bar{\gamma}$, where $\bar{\gamma} = \bar{\gamma}_{tr} = \bar{\gamma}_{rd}$, for different values of N_D at the FD relay. It can be seen that P_{out} of the D2D link decreases monotonically as $\bar{\gamma}$ increases, and there is no any outage floor. Notably, P_{out} improves significantly with increasing N_D. Thus, the data transmission of D2D communication improves as a result of



(a) The D2D outage probability, P_{out}, vs. SNR, $\bar{\gamma}$.

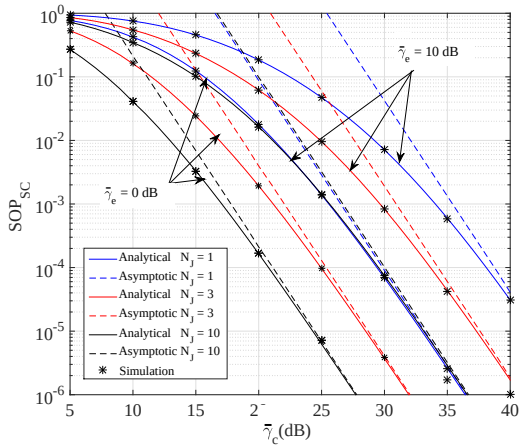
(b) The D2D outage probability, P_{out}, vs. N_D

Fig. 3.2: The D2D outage probability, P_{out}, where μ_2 = μ_4 = 10 dB, and $\mathcal{R}_d = 1$ b/s/Hz.

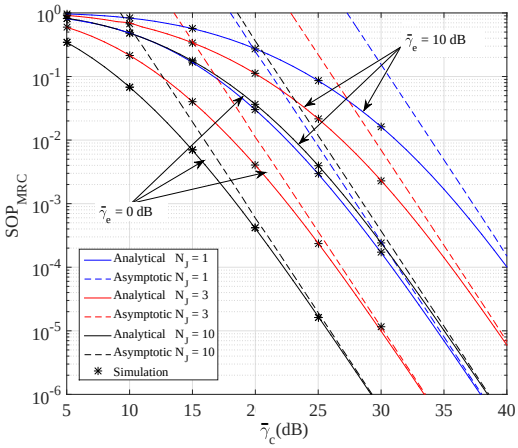
utilizing the MIMO relay as compared to a single relay. Furthermore, it can be observed that simulation and numerical results match at high SNR, confirming the tightness of the lower bound in this regime.

To evaluate the impact of the MIMO relay on the reliability in the D2D communication, Fig. 3.2b presents P_{out} versus N_D, for different values of $\bar{\gamma}$. As such, the effect of N_D on the D2D performance is examined, where P_{out} is seen to improve continuously with increasing N_D and $\bar{\gamma}$ as expected.

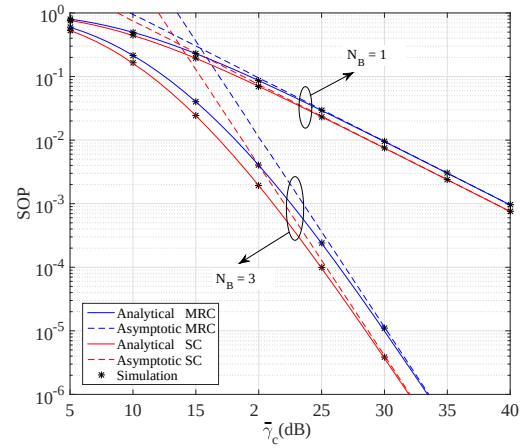
The SOP for selection combining, SOP_{SC}, of the cellular network is plotted in Fig. 3.3a versus $\bar{\gamma}_c$, for different $\bar{\gamma}_e$ and N_J. The SNR at E, $\bar{\gamma}_e$, takes two possible values: 0 dB and 10 dB while $\mathcal{R}_s$ is set at 1 b/s/Hz and $N_B = N_E = 3$. It can be noted that the SOP_{SC} decreases as N_J increases, illustrating the impact of the jamming signals on E. As a result, secure data transmission is guaranteed. Additionally, the SOP_{SC} increases as $\bar{\gamma}_c$ decreases, and $\bar{\gamma}_e$ increases. Besides, the asymptotic curves are depicted, and a very good match with the exact analysis is seen as $\overline{\gamma}_c \rightarrow \infty$. Most noteworthy in the asymptotic curves is the fact that they precisely predict G_a and G_d. Furthermore, the numerical and the simulation results match perfectly, verifying the accuracy of our analysis. Interesting, the SOP_{SC} of



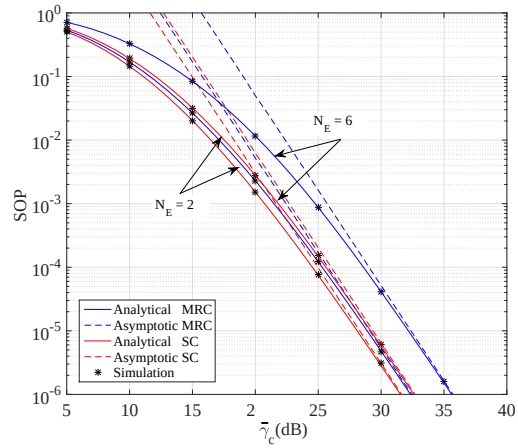
(a) The SOP for SC



(b) The SOP for MRC



(c) The SOP vs. SNR, $\bar{\gamma}_c$, for different N_B

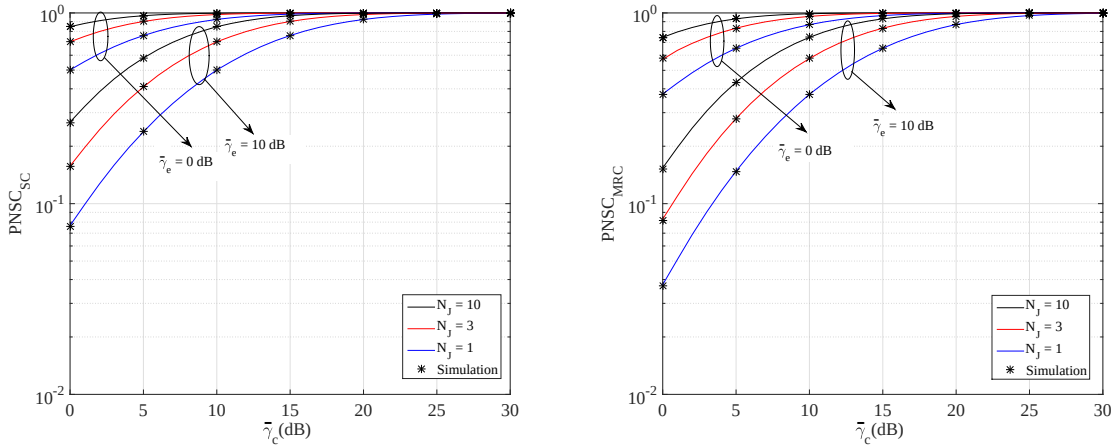


(d) The SOP vs. SNR, $\bar{\gamma}_c$, for different N_E

Fig. 3.3: The SOP, where $\omega_2 = \omega_4 = 10$ dB, $N_B = N_E = 3$, and $\mathcal{R}_s = 1$ b/s/Hz.

the cellular network decreases as a result of using the FD jamming MIMO relay.

In Fig. 3.3b, the secrecy outage probability for maximum ratio combining, SOP_{MRC}, of the cellular network is plotted using the same parameters as in Fig. 3.3a. It can be seen that SOP_{MRC} decreases with increasing N_J, implying an improvement in the security level of the cellular network. From Figs. 3.3a and 3.3b, we can note that the secrecy performance of the cellular network is lower when E employs the MRC as compared to the SC technique. This can be described by the fact that the MRC provides the best SNR gain at E over the



(a) PNSC_{SC}, vs. SNR, $\bar{\gamma}_c$, for different N_B.

(b) The PNSC_{MRC}, vs. SNR, $\bar{\gamma}_c$.

Fig. 3.4: The PNSC, where $\omega_2 = \omega_4 = 10$ dB, $N_B = N_E = 3$, and $\mathcal{R}_s = 1$ b/s/Hz.

SC scheme.

Figures 3.3c and 3.3d show the SOP versus $\bar{\gamma}_c$. Additionally, the asymptotic SOP results for both SC and MRC are also presented. In Fig. 3.3c, there is an increase in the SOP for both SC and MRC with decreasing N_B because the cellular capacity, C_C, increases with increasing N_B. This can be explained by the fact that G_a increases with N_B. In Fig. 3.3d, there is an increase in the SOP for both SC and MRC with increasing N_E. Since the diversity order is not influenced by N_E, the increase in the SOP is due to the array gain. From Figs. 3.3c and 3.3d, it can be confirmed that the SOP for both SC and MRC has the same secrecy diversity orders, N_B.

Figures 3.4a and 3.4b plot the PNSC versus $\bar{\gamma}_c$. From these figures, it is obvious that the PNSC increases as $\bar{\gamma}_c$ increases for a fixed $\bar{\gamma}_e$. Additionally, the PNSC increases with decreasing $\bar{\gamma}_e$. Moreover, it can also be noted that the PNSC increases as N_J increases. It is worth mentioning that even when the average SNR of the main channel, $\bar{\gamma}_c$, is lower than that of the eavesdropper's channel, $\bar{\gamma}_e$, the PNSC exists. Interestingly, for the SC technique, the PNSC is higher than that of the MRC technique. Analytical results are also found to match the simulation results, validating the correctness of our analysis.

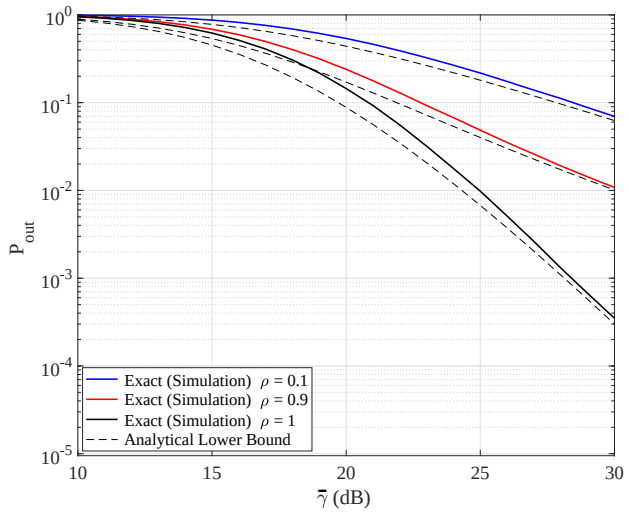
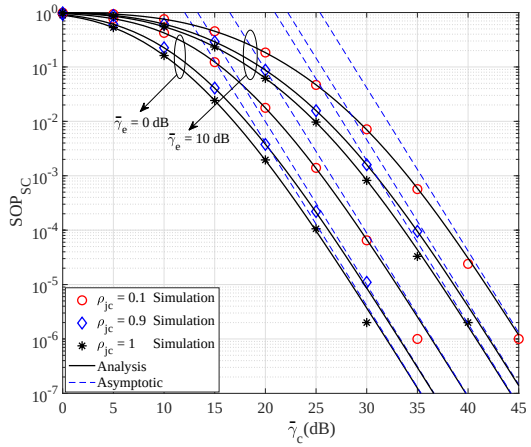


Fig. 3.5: The outage probability, P_{out}, vs SNR, $\bar{\gamma}$, for different ρ, where $\rho = \rho_{tr} = \rho_{rd}$, $\mathcal{E}_2 = \mathcal{E}_4$ = 10 dB, N_D = 3, and R_d = 1 b/s/Hz.

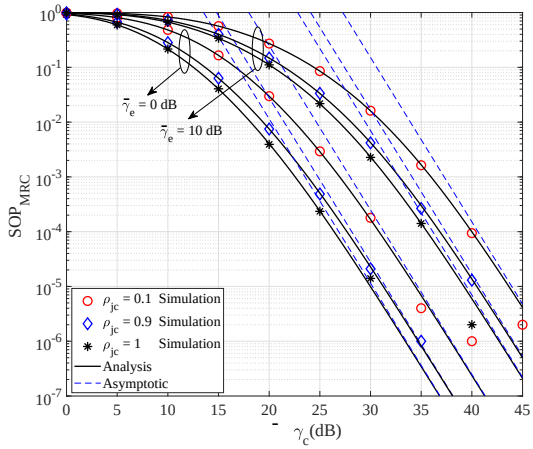
As shown in Fig. 3.5, the exact (simulation) and the analytical lower bound outage probability, P_{out}, for D2D communications is depicted versus $\bar{\gamma}$, where $\bar{\gamma} = \bar{\gamma}_d = \bar{\gamma}_r$. for different values of ρ, where $\rho = \rho_{tr} = \rho_{rd}$. We can observe that as ρ increases, there is a significant performance gain. Therefore, it can be concluded that the availability of CSI substantially impacts the outage probability performance of D2D communications. Furthermore, the match between the exact (simulation) and lower bound (analysis) at high SNR can also be seen, validating the analysis.

Figures 3.6a and 3.6b illustrate the SOP versus $\bar{\gamma}_c$, for different values of ρ_{jc} and $\bar{\gamma}_e$. The values, 0 dB and 10 dB, are set for the SNR, $\bar{\gamma}_e$, at E. R_s takes a value of 1 b/s/Hz, and $N_J = N_B = N_E = 3$. It can be noted that the SOP_{SC} and SOP_{MRC} decrease as ρ_{jc} increases, demonstrating the effect of the outdated CSI on the performance of the cellular network. Also, the SOP decreases as $\bar{\gamma}_c$ increases and $\bar{\gamma}_e$ decreases. Besides, the asymptotic results are illustrated, and an excellent agreement with the exact results can be observed as $\bar{\gamma}_c \to \infty$. From asymptotic curves, G_a and G_d are accurately predicted.

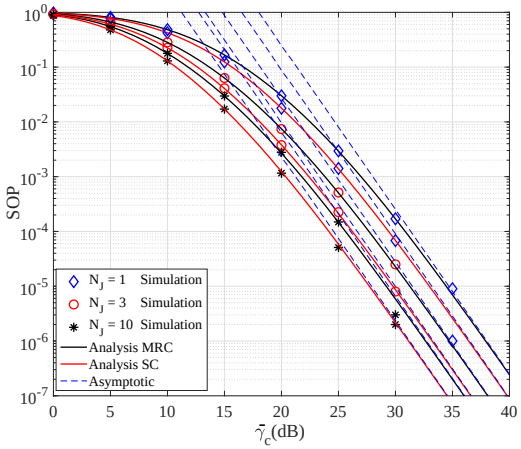
The SOP for SC and MRC, SOP_{SC} and SOP_{MRC}, are illustrated in Fig. 3.6c versus



(a) The secrecy outage probability, SOP_{SC}, vs SNR, $\bar{\gamma}_c$.



(b) The secrecy outage probability, SOP_{MRC}, vs SNR, $\bar{\gamma}_c$.



(c) The secrecy outage probability, SOP, vs SNR, $\bar{\gamma}_c$.

Fig. 3.6: The secrecy outage probability, SOP_{SC} and SOP_{MRC}, vs SNR, $\bar{\gamma}_c$, for different $\bar{\gamma}_e$, where ρ_{jc} = 0.9, $\mathcal{Z}_2$ = $\mathcal{Z}_4$ = 10 dB, N_B = N_J = N_E = 3, and R_s = 1 b/s/Hz.

$\bar{\gamma}_c$. To illustrate the influence of the jamming signals, the SOP increases as N_J decreases. Hence, the cellular transmission is secured. Also, the SOP decreases as $\bar{\gamma}_c$ increases and $\bar{\gamma}_e$ decreases. Besides, an accurate match between the asymptotic curves and the exact results can also be seen as $\bar{\gamma}_c \to \infty$. More importantly, the SOP is higher when the MRC is utilized by E in comparison to the SC approach. This is because the MRC provides higher SNR gain at E than the SC approach.

3.7 Conclusion

In this chapter, a cooperative scheme is proposed to improve the secrecy performance of the cellular network and the reliability of the D2D communications simultaneously. To this end, an FD MIMO relay is employed to confuse the eavesdropper by generating jamming signals, while ensuring improved transmission performance for the D2D system. At E, two practical combining techniques, SC or MRC, are utilized to combine the wiretapped signals. Considering a practical scenario in which the CSI of the eavesdropper's channel is unknown, a dual antenna selection scheme at the relay is proposed. A comprehensive analysis is undertaken to evaluate the performance of the proposed system model, and new closed-form expressions for the D2D outage probability, the cellular SOP, and the cellular PNSC are derived. To gain more insights into the effect of the various system parameters on the SOP, an asymptotic analysis is carried out. This analysis reveals that the same diversity order of N_B is achieved for both SC and MC techniques. It is also observed that the diversity order is not influenced by N_E. Moreover, we confirmed that, under these combining techniques, increasing N_J and N_B enhances the secrecy performance of the cellular network. Furthermore, the effect of outdated CSI on a practical cellular network with in-band underlay relay-aided D2D communication, where an FD relay is used to confound a passive eavesdropper while guaranteeing enhanced data transmission for the D2D link, is investigated. Practical combining approaches, SC or MRC, are employed to increase the eavesdropped signals. To this end, new closed-form expressions are provided. Moreover, it is verified that a win-win situation is enabled for both networks, i.e., high spectral efficiency for the D2D users and security provisioning for the cellular user. Finally, numerical results are found to agree very well with simulation results, confirming our analysis. As revealed by the analytical and simulation results, the SOP and the D2D outage probability are simultaneously improved, confirming the benefits of the cooperation.

3.8 Appendices

3.8.1 Appendix A

Derivation of Lemma 1

The SINR at R for actual CSI is given by $\gamma_R = \frac{\gamma_{tr}}{1+\gamma_{br}}$. Now, we can determine the CDF of γ_R as [16]

$$F_{\gamma_R}(x) = \int_0^\infty F_{\gamma_{tr}}(x(y+1)) f_{\gamma_{br}}(y)\, dy, \tag{3.67}$$

where

$$f_{\gamma_{br}}(\gamma) = \frac{1}{\mathcal{E}_2} \exp\left(-\frac{1}{\mathcal{E}_2}\right). \tag{3.68}$$

To derive the PDF of $\widetilde{\gamma}_{tr}$, one can get

$$f_{\widetilde{\gamma}_{tr_i}}(\gamma) = \frac{N_D}{\mathcal{E}_1} \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D-1}{k} \exp\left(-\frac{\gamma\,(k+1)}{\mathcal{E}_1}\right). \tag{3.69}$$

By substituting (3.52) and (3.69) in (3.53) and using [17, eq. (6.643.2)] and [17, eq. (9.220.2)], the PDF of γ_{tr} can be obtained. Then, the CDF of γ_{tr} can be derived as

$$F_{\gamma_{tr}}(\gamma) = N_D \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D-1}{k} \left(\frac{1-\exp\left(-\frac{(k+1)\gamma}{\Delta_{tr}(k+1)+\rho_{tr}^2\mathcal{E}_1}\right)}{k+1}\right). \tag{3.70}$$

By substituting $f_{\gamma_{br}}(\gamma)$ and $F_{\gamma_{tr}}(\gamma)$ in (3.67) and evaluating the integral, the CDF of γ_R can be obtained as in (3.55).

3.8.2 Appendix B

Derivation of Lemma 2

The SINR at C is given by

$$\gamma_C = \frac{\gamma_{bc}}{1 + \min\left(\gamma_{jc}\right)}. \tag{3.71}$$

The CDF of γ_C can be obtained using

$$F_{\gamma_C}(\gamma) = \int_0^\infty F_{\gamma_{bc}}(\gamma(y+1)) f_{\gamma_{jc}}(y)\, dy, \tag{3.72}$$

where

$$F_{\gamma_{bc}}(\gamma) = N_B \sum_{k=0}^{N_B-1} \frac{(-1)^k \binom{N_B-1}{k}}{(k+1)} \left(1 - \exp\left(-\frac{\gamma\,(k+1)}{\mathcal{Z}_1}\right)\right), \tag{3.73}$$

and

$$f_{\tilde{\gamma}_{jc}}(\gamma) = \frac{N_j}{\mathcal{Z}_2} \exp\left(-\frac{N_j\,\gamma}{\mathcal{Z}_2}\right). \tag{3.74}$$

By substituting (3.52) and (3.74) in (3.53) and using [17, eq. (6.643.2)] and [17, eq. (9.220.2)], the $f_{\gamma_{jc}}(\gamma)$ can be obtained as

$$f_{\gamma_{jc}}(\gamma) = \frac{N_j\ \exp\left(-\frac{N_j\,\gamma}{N_j\,\Delta_{jc} + \rho_{jc}^2\,\mathcal{Z}_2}\right)}{N_j\,\Delta_{jc} + \rho_{jc}^2\,\mathcal{Z}_2}. \tag{3.75}$$

By substituting $F_{\gamma_{bc}}(\gamma)$ and $f_{\gamma_{jc}}(\gamma)$ in (3.72), the CDF of γ_C can be obtained as in (3.60).

References

[1] J. Yue, C. Ma, H. Yu, and W. Zhou, “Secrecy-based access control for device-to-device communication underlaying cellular networks,” *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.

[2] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, “Resource management for Device-to-Device communication: A physical layer security perspective,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 946–960, Apr. 2018.

[3] W. Wang, K. C. Teh, and K. H. Li, “Enhanced physical layer security in D2D spectrum sharing networks,” *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 106–109, Feb. 2017.

[4] F. Alavi, N. M. Yamchi, M. R. Javan, and K. Cumanan, “Limited feedback scheme for device-to-device communications in 5G cellular networks with reliability and cellular secrecy outage constraints,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8072–8085, Sep. 2017.

[5] L. Wang, J. Liu, M. Chen, G. Gui, and H. Sari, “Optimization-based access assignment scheme for physical-layer security in D2D communications underlaying a cellular network,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5766–5777, Jul. 2018.

[6] Z. Mobini, M. Mohammadi and C. Tellambura, “Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications,” *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 3, pp. 621–634, Mar. 2019.

[7] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, “Safeguarding decentralized wireless networks using full-duplex jamming receivers,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.

[8] G. Chen, J. P. Coon, and M. Di Renzo, “Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers,” *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 5, pp. 1195–1206, May 2017.

[9] H.-M. Wang, B.-Q. Zhao, and T.-X. Zheng, “Adaptive full-duplex jamming receiver for secure D2D links in random networks,” *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1254–1267, Feb. 2019.

[10] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, “Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective,” *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 623–638, Jan. 2019.

[11] M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, “On the physical layer security of underlay multihop Device-to-Device relaying,” *in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6.

[12] J. M. Moualeu, T. M. N. Ngatched, and D. B. da Costa, “Sequential relay selection in D2D-enabled cellular networks with outdated CSI over mixed fading channels,” *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 245–248, Feb. 2019.

[13] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, “Enhancing physical layer security using underlay full-duplex relay-aided D2D communications,” *in Proc. IEEE Wireless Commun. NetW. Conf. (WCNC)*, Apr. 2020, pp. 1–7.

[14] Ren, Chao and Zhang, Haijun and Wen, Jinming and Chen, Jian and Tellambura, Chintha, “Successive two-way relaying for full-duplex users with generalized selfinterference mitigation,” *IEEE Trans. on Wireless Commun.*, vol. 18, no. 1, pp. 63–76, Jan. 2019.

[15] H. Lei et al., “Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237–2250, Mar. 2017.

[16] I. Krikidis, J. S. Thompson, S. McLaughlin, and N. Goertz, “Max-min relay selection for legacy amplify-and-forward systems with interference,” *IEEE Trans. Wireless Commun.*,vol. 8, no. 6,pp. 3016–3027, Jun. 2009.

[17] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*, McGraw-Hill Education, 2002.

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

[19] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, “Transmit antenna selection for security enhancement in mimo wiretap channels,” *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[20] J. L. Vicario, A. Bel, J. A. Lopez-Salcedo, and G. Seco, “Opportunistic relay selection with outdated CSI: Outage probability and diversity analysis,” *IEEE Trans. Wireless Commun*, vol. 8, no. 6, pp. 2872–2876, Jun. 2009.

Chapter 4

Relay Selection for Improving PLS in D2D Underlay Communications

4.1 Abstract

This chapter investigates the physical layer security of inband underlay D2D communication, where the direct link between D2D users is not available. In this respect, optimal relay selection and suboptimal relay selection are utilized to secure the D2D transmission. The eavesdropper uses either maximal-ratio combining or selection combining to increase the wiretapped signals. The D2D secrecy performance analysis is performed regarding the SOP and the PNSC, where closed-form expressions are provided for both relay selection approaches and verified using Monte-Carlo simulation. From the numerical results, it is shown that increasing the number of D2D relays enhances the secrecy performance of D2D communications. Moreover, the exact asymptotic analysis of the SOP is provided. It turns out that the diversity order of both relay selection approaches is the same.

4.2 Introduction

Mobile wireless communication has experienced rapid development in data traffic due to the dramatic growth of smart devices. According to Cisco, the average number of mobiles per capita will be 3.6 by 2023 [1]. Thus, spectrum scarcity is a crucial issue in wireless networks. Device-to-Device (D2D) communication, which allows nearby pairs to communicate directly rather than routing into a base station (BS), has received important consideration as a leading technology in future cellular communications to increase spectrum efficiency. Signal relaying has also been considerably used to increase the quality of service in cellular networks. Relaying techniques provide many advantages, including extended coverage and higher data rate. The benefits of cooperative communications, in the context of PLS, have been widely investigated. Specifically, in the wireless transmission, diversity and relaying strategies have been widely employed to enhance the D2D security.

4.2.1 Related Work

The trade-off of the security vs reliability was studied for wireless communications in [2] where an opportunistic relay selection approach was introduced to increase the secrecy capacity of the cellular network. In this regard, the relay selection of a cooperative scenario was analyzed in [3] to guarantee a secure transmission for the cellular network. Towards this end, relay selection approach was proposed for guarding wireless transmissions against eavesdropping attack.

The benefits of using D2D relays over the direct D2D communications have been investigated in [4], [5] especially when there is a long distance between D2D users or poor link quality. As a result of sharing the same spectrum band, interference is a serious issue for both D2D and cellular users. Thus, interference management is necessary to mitigate the effects of interference [6]. However, the interference can be utilized to increase the secrecy

level for cellular and D2D communications by confounding the eavesdropped signal [7], [8]. To maximize the wiretapped signal quality, the eavesdropper can utilize either MRC or SC [9]. For the PLS in underlay D2D communications, many approaches can be used to increase the security level of D2D communications. More specifically, artificial noise and guard zone were used to guarantee a secure transmission for the D2D communications [10]. To secure D2D transmission, the BS was used as a friendly jammer to confuse the wiretapper by producing artificial noise [11]. Nevertheless, the quality of service of cellular users should be taken into consideration. In order to improve the PLS, spectrum partition and mode selection for D2D inband communications were investigated in [12]. To compensate for sharing the spectrum, the D2D relay guarantees a high-security cellular transmission by sending jamming signals towards an eavesdropper. As a result, the benefits for cellular and D2D users are achieved, i.e., security enhancement for the former and high reliability and robustness for the latter [13].

4.2.2 Motivation and Contributions

Although the works mentioned above have presented some techniques to enhance the security of the direct inband underlay D2D communications from the PLS perspective, they only focus on enhancing the security of the cellular network. It is worth noting that, as a result of the restricted computational potential of user equipment, the transmissions of the D2D communications are also vulnerable to eavesdropping attacks. Consequently, the security enhancement of D2D relaying is worth studying as well. However, this aspect has not been considered in the literature. Driven by this observation, in this chapter, the secrecy capacity of the D2D relaying is investigated, where the D2D pairs utilize decode-and-forward (DF) relays to overcome the far distance and increase the quality of the D2D links. Taking into account the interference produced by the BS, the impact of the D2D relaying on the D2D security is evaluated. Two combining techniques at the eavesdropper are investigated. Our

main contributions are as follows:

- The D2D SOP and the D2D PNSC are investigated, and closed-form expressions are derived. Moreover, for maximizing the secrecy capacity of D2D communications, two relay selection schemes are utilized, namely, optimal relay selection (ORS) and suboptimal relay selection (SRS).

- The impact of D2D relays on the D2D secrecy performance is investigated. Additionally, at the eavesdropper side, two practical combining approaches, MRC and SC, are examined.

- From the numerical results, it is shown that increasing the number of D2D relays enhances the secrecy performance of D2D communications. Moreover, the D2D secrecy performance is enhanced by using the ORS scheme as compared with the SRS scheme.

- Accurate expressions for the asymptotic SOP for the D2D communications are derived in the high-SNR regime. The upshot is that the secrecy diversity order is the same for both combining techniques as well as for the relay selection schemes.

- The provided analytical expressions are verified and confirmed using Monte-Carlo simulations.

4.3 System Model

We consider a downlink transmission scenario in D2D relay communication as illustrated in Fig. 4.1, where the cellular network shares its spectral band with the D2D network in a particular environment. The D2D network consists of a D2D transmitter, T, N_R decode-and-forward (DF) D2D relays ($R_k|\ k = 1, ..., N_R$), a D2D receiver, D, each equipped

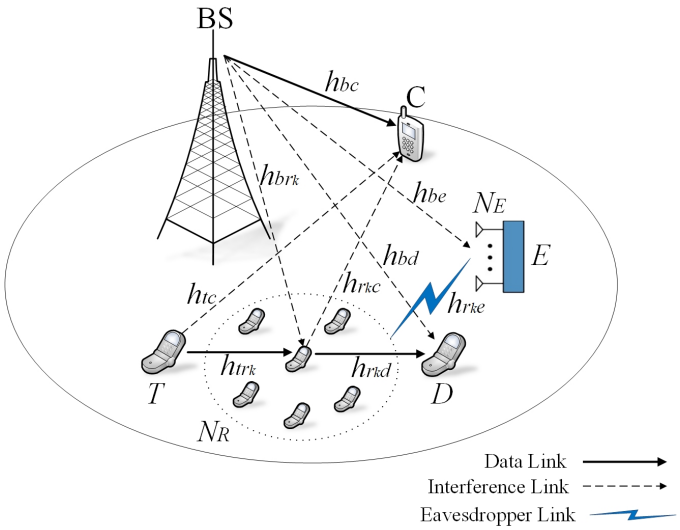


Fig. 4.1: System Model.

with a single antenna, and a multi-antenna eavesdropper, E, equipped with N_E antennas. We consider a cellular network consisting of a BS, equipped with a single antenna, communicating with a single antenna cellular user, C. It is worth mentioning that, as a result of severe shadowing, the direct link between the D2D pairs is unavailable in the proposed scenario. Thus, communication from T to D can be set only through relays. Thus, the D2D transmissions require two phases. In the first phase, the received signals from T are fully decoded by the D2D relays. In the second phase, based on the highest secrecy capacity, the best D2D relay, R_k, is chosen from the D2D relays set to forward the decoded signal to D. During this phase E may wiretap the transmission of R_k. The BS transmits in both phases. Furthermore, we assume that all communication channels experience flat fading with a Rayleigh distribution.

The channel coefficients for the $T \rightarrow R_k$, $T \rightarrow C$, BS $\rightarrow C$, BS $\rightarrow E$, $R_k \rightarrow E$, BS $\rightarrow R_k$, BS $\rightarrow D$, and $R_k \rightarrow D$ links are denoted as h_{tr_k}, h_{tc}, h_{bc}, h_{be}, h_{r_ke}, h_{br_k}, h_{bd}, and h_{r_kd}, respectively. In addition, the channel power gains are indicated by $|h_{ab}|^2$, which are independent and exponentially distributed random variables with a mean of λ_{ab}, where $ab \in \{tr_k, tc, bc, be, r_ke, br_k, bd, r_kd\}$. Additionally, the Euclidean distance is denoted as

d_{ab}. Also, the variances of the AWGN at R_k, D, C, and E are denoted by $\sigma^2_{r_k}, \sigma^2_d, \sigma^2_c$, and σ^2_e, respectively. We assume that the D2D nodes, T and R_k, transmit with equal power P. In the first phase, the received signal at R_k is given by

$$y_{R_k} = \sqrt{P}\left(\frac{d_{tr_k}}{d_o}\right)^{-\frac{\eta}{2}} h_{tr_k}\, x_d + \sqrt{P_b}\left(\frac{d_{br_k}}{d_o}\right)^{-\frac{\eta}{2}} h_{br_k}\, x_b + n_{r_k}, \tag{4.1}$$

where d_o is a reference distance, η denotes the path loss exponent, P and P_b are the D2D and BS transmitted power, respectively, x_b and x_d are the BS and D2D signals, respectively, and n_{r_k} is the AWGN at R_k. In the second phase, a D2D relay, R_k, is chosen to maximize the secrecy capacity of the D2D link. The received signal at D is given by

$$y_D = \sqrt{P}\left(\frac{d_{r_k d}}{d_o}\right)^{-\frac{\eta}{2}} h_{r_k d}\, x_d + \sqrt{P_b}\left(\frac{d_{bd}}{d_o}\right)^{-\frac{\eta}{2}} h_{bd}\, x_b + n_d, \tag{4.2}$$

where n_d is the AWGN at D. The eavesdropped signal, in the second phase, can be expressed as

$$y_E = \sqrt{P}\left(\frac{d_{r_k e}}{d_o}\right)^{-\frac{\eta}{2}} h_{r_k e}\, x_d + \sqrt{P_b}\left(\frac{d_{be}}{d_o}\right)^{-\frac{\eta}{2}} h_{be}\, x_b + n_e, \tag{4.3}$$

where n_e is the AWGN at E. It is worth mentioning that, due to the powerful resources that are available at the BS where advanced security techniques such as beamforming can be implemented to secure the cellular transmission, we assume in this work that the cellular user is unlikely to be wiretapped. However, D2D transmission is more likely to be eavesdropped as a result of the low resources at the D2D communications side. Consequently, we only investigate the PLS of D2D communications. The instantaneous SINR at R_k, in the first phase, is given by

$$\gamma_{TR_k} = \frac{P\left(\frac{d_{tr_k}}{d_o}\right)^{-\eta} |h_{tr_k}|^2}{\sigma^2_{r_k} + P_b\left(\frac{d_{br_k}}{d_o}\right)^{-\eta} |h_{br_k}|^2} = \frac{\gamma_{tr_k}}{1+\gamma_{br_k}}, \tag{4.4}$$

where

$\gamma_{tr_k} = \bar{\gamma}_{r_k} \left(\frac{d_{tr_k}}{d_o}\right)^{-\eta} |h_{tr_k}|^2$, $\gamma_{br_k} = \bar{\gamma}_{br_k} \left(\frac{d_{br_k}}{d_o}\right)^{-\eta} |h_{br_k}|^2$, $\bar{\gamma}_{r_k} = \frac{P}{\sigma^2_{r_k}}$, and $\bar{\gamma}_{br_k} = \frac{P_b}{\sigma^2_{r_k}}$. The channel capacity of the $T \rightarrow R_k$ link is given by $C_{TR_k} = \frac{1}{2}\log_2\left(1 + \gamma_{TR_k}\right)$. The SINR at D, in the second phase, is given by

$$\gamma_{R_k D} = \frac{P\left(\frac{d_{r_k d}}{d_o}\right)^{-\eta} |h_{r_k d}|^2}{\sigma_d^2 + P_b\left(\frac{d_{bd}}{d_o}\right)^{-\eta} |h_{bd}|^2} = \frac{\gamma_{r_k d}}{1 + \gamma_{bd}}, \tag{4.5}$$

where

$\gamma_{r_k d} = \bar{\gamma}_d \left(\frac{d_{r_k d}}{d_o}\right)^{-\eta} |h_{r_k d}|^2$, $\gamma_{bd} = \bar{\gamma}_{bd} \left(\frac{d_{bd}}{d_o}\right)^{-\eta} |h_{bd}|^2$, $\bar{\gamma}_d = \frac{P}{\sigma^2_d}$, and $\bar{\gamma}_{bd} = \frac{P_b}{\sigma^2_d}$. Let us define $\omega_1 = \bar{\gamma}_d \left(\frac{d_{r_k d}}{d_o}\right)^{-\eta} \lambda_{r_k d}$, and $\omega_2 = \bar{\gamma}_{bd} \left(\frac{d_{bd}}{d_o}\right)^{-\eta} \lambda_{bd}$. Additionally, the SINR at E is given by

$$\gamma_{R_k E} = \frac{P\left(\frac{d_{r_k e}}{d_o}\right)^{-\eta} |h_{r_k e}|^2}{\sigma_e^2 + P_b\left(\frac{d_{be}}{d_o}\right)^{-\eta} |h_{be}|^2} = \frac{\gamma_{r_k e}}{1 + \gamma_{be}}, \tag{4.6}$$

where

$\gamma_{r_k e} = \bar{\gamma}_e \left(\frac{d_{r_k e}}{d_o}\right)^{-\eta} |h_{r_k e}|^2$, $\gamma_{be} = \bar{\gamma}_{be} \left(\frac{d_{be}}{d_o}\right)^{-\eta} |h_{be}|^2$, $\bar{\gamma}_e = \frac{P}{\sigma^2_e}$, and $\bar{\gamma}_{be} = \frac{P_b}{\sigma^2_e}$. Similarly, we define $\omega_3 = \bar{\gamma}_e \left(\frac{d_{r_k e}}{d_o}\right)^{-\eta} \lambda_{r_k e}$, and $\omega_4 = \bar{\gamma}_{be} \left(\frac{d_{be}}{d_o}\right)^{-\eta} \lambda_{be}$. The channel capacities of the $R_k \rightarrow D$ and $R_k \rightarrow E$ links are given by $C_{R_k D} = \frac{1}{2}\log_2\left(1 + \gamma_{R_k D}\right)$ and $C_{R_k E} = \frac{1}{2}\log_2\left(1 + \gamma_{R_k E}\right)$ respectively. At the E side, two combining techniques are utilized to maximize the SNR at E, namely, MRC and SC.

4.4 Secrecy Outage Probability

To examine the D2D secrecy capacity, C_S, the SOP is investigated in this subsection.

4.4.1 Optimal Relay Selection

The ORS is achieved when the relay selection is based on the particular D2D relay having the highest secrecy capacity [14], [15]. For the main and wiretap links, the CSI is assumed to be known. Practically, the CSI of the wiretapped link can be estimated by observing the transmissions of the eavesdropper. For the ORS, the criterion of the relay selection is given by [2],

$$\theta = \arg \max_{k \in N_R} \left[C_{R_k D} - C_{R_k E}\right]^+, \tag{4.7}$$

where θ signifies the selected antenna and $[x]^+ = \max(x, 0)$. Mathematically speaking, the secrecy capacity, C_S^{ORS}, can be expressed as

$$C_S^{\text{ORS}} = \max_{k \in N_R} \left[C_{R_k D} - C_{R_k E}\right]^+. \tag{4.8}$$

Using (4.8), the SOP can be expressed as

$$\begin{aligned} \text{SOP}_{\upsilon}^{\text{ORS}} &= \Pr\left(C_S^{\text{ORS}} \leq \mathcal{R}_s\right) = \Pr\left(\max_{k \in N_R} \left[C_{R_k D} - C_{R_k E}\right]^+ \leq \mathcal{R}_s\right) \\ &= \prod_{k \in N_R} \underbrace{\Pr\left(\frac{1+\gamma_{R_k D}}{1+\gamma_{R_k E}} \leq \vartheta_s\right)}_{\mathcal{P}_k^{\upsilon}}, \end{aligned} \tag{4.9}$$

where $\mathcal{R}_s$ represents the target secrecy rate of the D2D communication, $\upsilon \in \{\text{MRC}, \text{SC}\}$ and $\vartheta_s = 2^{2\mathcal{R}_s}$. The cumulative distribution function (CDF) of the $R_k \rightarrow D$ link, $F_{\gamma_{R_k D}}(.)$, can be obtained as

$$F_{\gamma_{R_k D}}(\gamma) = 1 - \frac{\exp\left(-\frac{\gamma}{\omega_1}\right)}{1 + \frac{\omega_2}{\omega_1}\gamma}. \tag{4.10}$$

4.4.1.1 Eavesdropper Channel with MRC

In this approach, the received signals are coherently combined. Hence, the the channel gain between the selected relay and E can be obtained as

$$|h_{r_k e}|^2 = \sum_{m=1}^{N_E} |h_{r_k m}|^2 . \tag{4.11}$$

Lemma 1: The expression $\mathcal{P}_k^{\text{MRC}}$ can be derived as

$$\begin{aligned}\mathcal{P}_k^{\text{MRC}} =& 1 - \frac{\omega_2 \exp\left(-\frac{\alpha}{\omega_1}\right)}{\omega_3^{N_E}\, \omega_4\, \beta} \sum_{m=0}^{N_E} \binom{N_E}{m} \Gamma(m+1)\, \omega_3^{m+1} \left[\sum_{i=1}^{m+1} \frac{(-1)^{m+1-i} \exp\left(\frac{\mathcal{A}_1 \mathcal{A}_2}{2}\right)}{(\mathcal{A}_3 - \mathcal{A}_2)^{m+2-i}} \right. \\ & \left. \times \frac{\mathcal{A}_2^{\left(\frac{N_E-i-1}{2}\right)}}{\mathcal{A}_1^{\left(\frac{N_E-i+1}{2}\right)}} \mathcal{W}_{\frac{1-i-N_E}{2}, \frac{i-N_E}{2}}\left(\mathcal{A}_1 \mathcal{A}_2\right) + \frac{\mathcal{A}_3^{N_E-1}\, \Gamma\left(1-N_E, \mathcal{A}_1 \mathcal{A}_3\right)}{\exp\left(-\mathcal{A}_1\, \mathcal{A}_3\right) \left(\mathcal{A}_2 - \mathcal{A}_3\right)^{m+1}} \right],\end{aligned} \tag{4.12}$$

where $\beta = 2^{\mathcal{R}_s}$ and $\alpha = \beta - 1$, $\text{A}_1 = \frac{\beta}{\omega_1} + \frac{1}{\omega_3}$, $\mathcal{A}_2 = \frac{\omega_3}{\omega_4}$, $\mathcal{A}_3 = \frac{1}{\beta}\left(\alpha + \frac{\omega_1}{\omega_2}\right)$, $\Gamma(.,.)$ is the upper incomplete gamma function [16, eq. (8.350.2)], and $\mathcal{W}_{a,b}(.)$ is the Whittaker function [16, eq. (9.220.4)]. Now, the $\text{SOP}_{\text{MRC}}^{\text{ORS}}$ can be obtained by plugging (4.12) into (4.9).

Proof: See Appendix A. ■

4.4.1.2 Eavesdropper Channel with SC

In this approach, the signal with the highest instantaneous SNR is selected. Thus, the channel gain between the selected relay and E can be obtained as

$$|h_{r_k e}|^2 = \max_{1 \le m \le N_E} |h_{r_k m}|^2 . \tag{4.13}$$

Lemma 2: The expression $\mathcal{P}_k^{\text{SC}}$ can be derived as

$$\begin{aligned}\mathcal{P}_k^{\text{SC}} =& 1 - \frac{N_E \exp\left(\frac{\alpha}{\omega_1}\right)}{\omega_3\,\omega_4\,\mathcal{B}_1} \sum_{m=0}^{N_E-1} (-1)^m \binom{N_E-1}{m} \left[\frac{\mathcal{B}_2\,\text{Ei}\left[-\mathcal{B}_2\mathcal{B}_3\right]}{\exp\left(-\mathcal{B}_2\mathcal{B}_3\right)} + \frac{1}{\mathcal{B}_3} + \frac{\mathcal{B}_4}{\mathcal{B}_1}\right. \\ & \left. \times \left(-\frac{\text{Ei}\left[-\mathcal{B}_2\mathcal{B}_3\right]}{\exp\left(-\mathcal{B}_2\mathcal{B}_3\right)} + \exp\left(\frac{\mathcal{B}_2}{\beta}\left(\frac{\omega_k}{\omega_2}+\alpha\right)\right)\text{Ei}\left[-\frac{\mathcal{B}_2}{\beta}\left(\frac{\omega_k}{\omega_2}+\alpha\right)\right]\right)\right],\end{aligned} \tag{4.14}$$

where $\mathcal{B}_1 = \frac{(m+1)}{\omega_3}\left(\frac{(m+1)}{\omega_3}\left(1+\frac{\omega_2\alpha}{\omega_1}\right) - \frac{\omega_2\beta}{\omega_1\omega_4}\right)$, $\mathcal{B}_2 = \frac{m+1}{\omega_3} + \frac{\beta}{\omega_1}$, $\mathcal{B}_3 = \frac{\omega_3}{(m+1)\omega_4}$, $\mathcal{B}_4 = \frac{(m+1)}{\omega_3}\left(1+\frac{\omega_2\alpha}{\omega_1}\right) - \left(1+\frac{1}{\omega_4}\right)\frac{\omega_2\beta}{\omega_1}$, and $\text{Ei}(.)$ is the exponential integral function [16, eq. (8.21.1)]. Now, the $\text{SOP}_{\text{SC}}^{\text{ORS}}$ can be obtained by plugging (4.14) into (4.9).

Proof: See Appendix B. ■

4.4.2 Suboptimal Relay Selection Scheme

In practice, the CSI of the eavesdropper is not available when it is passive. In this case, the relay selection is based on the best relay that maximizes the reliability of the D2D link in the second phase. That is, the relay selection is given by [2]

$$\theta = \arg\max_{k\in N_R} C_{R_kD}. \tag{4.15}$$

Mathematically speaking, the secrecy capacity, C_S, can be expressed as

$$C_S^{\text{SRS}} = \left[\max_{k\in N} C_{R_kD} - C_{RE}\right]^+ = \left[\frac{1}{2}\log_2\left(1+\gamma_{SRS}\right) - \frac{1}{2}\log_2\left(1+\gamma_{R_\theta E}\right)\right]^+, \tag{4.16}$$

where $\gamma_{\text{SRS}} = \max_{k\in N} \gamma_{R_kD}$. Using (4.16), the SOP_υ can be expressed as

$$\begin{aligned}\text{SOP}_{\upsilon}^{\text{SRS}} &= \Pr\left(C_S \leq \mathcal{R}_s\right) = \Pr\left(\left[\max_{k\in N} C_{R_k D} - C_{RE}\right]^{+} \leq \mathcal{R}_s\right) \\ &= \Pr\left(\frac{1+\gamma_{\text{SRS}}}{1+\gamma_{R_\theta E}} \leq \vartheta_s\right).\end{aligned} \tag{4.17}$$

The CDF of the $R_k \rightarrow D$ link, $F_{\gamma_{\text{SRS}}}(.)$, can be obtained as

$$F_{\gamma_{\text{SRS}}}(\gamma) = N_R \sum_{k=0}^{N_R-1} \frac{(-1)^k \binom{N_R-1}{k}}{(k+1)} \left(1 - \frac{\exp\left(\frac{-\gamma\,(k+1)}{\omega_1}\right)}{\left(1+\frac{\gamma\,(k+1)\,\omega_2}{\omega_1}\right)}\right). \tag{4.18}$$

4.4.2.1 Eavesdropper Channel with MRC

In this subsection, the $\text{SOP}_{\text{MRC}}^{\text{SRS}}$ will be derived for the SRS scheme. The $\text{SOP}_{\text{MRC}}^{\text{SRS}}$ can be obtained by

$$\text{SOP}_{\text{MRC}}^{\text{SRS}} = \int_0^{\infty} F_{\gamma_{\text{SRS}}}(\beta\gamma+\alpha)\, f_{\gamma_{R_\theta E}}^{\text{MRC}}(\gamma)\, d\gamma, \tag{4.19}$$

where $f_{\gamma_{R_\theta E}}(\cdot)$ is the probability density function (PDF) of the $R_\theta \rightarrow E$ link.

Lemma 3: The $\text{SOP}_{\text{MRC}}^{\text{SRS}}$ can be derived as

$$\begin{aligned}\text{SOP}_{\text{MRC}}^{\text{SRS}} =& N_R \sum_{k=0}^{N_R-1} \frac{(-1)^k \binom{N_R-1}{k}}{(k+1)} \Bigg[1 - \sum_{m=0}^{N_E} \frac{\binom{N_E}{m}\Gamma(m+1)\,\omega_1 \exp\left(-\frac{(k+1)\,\alpha}{\omega_1}\right)}{\omega_3^{N_E-(m+1)}\,\omega_2\,\omega_4\,\beta\,(k+1)} \\ &\times \Bigg\{\sum_{j=1}^{m+1} \frac{(-1)^{m+1-j}}{\exp\left(-\frac{\mathcal{H}_1\mathcal{H}_2}{2}\right)} \frac{\mathcal{H}_1^{-\left(\frac{N_E-j+1}{2}\right)} \mathcal{H}_2^{\left(\frac{N_E-j-1}{2}\right)}}{(\mathcal{H}_3-\mathcal{H}_2)^{m+2-j}} \mathcal{W}_{\frac{1-j-N_E}{2},\frac{j-N_E}{2}}(\mathcal{H}_1\mathcal{H}_2) \\ &+ \frac{\mathcal{H}_3^{N_E-1}\,\Gamma\left(1-N_E, \mathcal{H}_1\mathcal{H}_3\right)}{\exp\left(-\mathcal{H}_1\,\mathcal{H}_3\right)(\mathcal{H}_2-\mathcal{H}_3)^{m+1}}\Bigg\}\Bigg],\end{aligned} \tag{4.20}$$

where $\mathcal{H}_1 = \frac{\beta(k+1)}{\omega_1} + \frac{1}{\omega_3}$, $\mathcal{H}_2 = \frac{\omega_3}{\omega_4}$, and $\mathcal{H}_3 = \frac{1}{\beta}\left(\alpha + \frac{\omega_1}{\omega_2(k+1)}\right)$.

Proof: See Appendix C. ■

4.4.2.2 Eavesdropper Channel with SC

In this subsection, the $\text{SOP}_{\text{SC}}^{\text{SRS}}$ is derived for the SRS scheme. The $\text{SOP}_{\text{SC}}^{\text{SRS}}$ can be obtained by

$$\text{SOP}_{\text{SC}}^{\text{SRS}} = \int_0^{\infty} F_{\gamma_{\text{SRS}}}\left(\beta\gamma + \alpha\right) f_{\gamma_{R_\theta E}}^{\text{SC}}(\gamma)\, d\gamma. \tag{4.21}$$

Lemma 4: The $\text{SOP}_{\text{SC}}^{\text{SRS}}$ can be derived as

$$\begin{aligned}\text{SOP}_{\text{SC}}^{\text{SRS}} =& N_R \sum_{k=0}^{N_R-1} \frac{(-1)^k \binom{N_R-1}{k}}{(k+1)} \Bigg[1 - \frac{N_E\, \omega_1 \exp\left(-\frac{(k+1)\,\alpha}{\omega_1}\right)}{\beta\, \omega_2\, \omega_4\, (k+1)} \sum_{m=0}^{N_E-1} \frac{(-1)^m \binom{N_E-1}{m}}{(m+1)} \\ &\times \Bigg\{ \frac{(\mathcal{Z}_2 - \mathcal{Z}_3)}{(\mathcal{Z}_3 - \mathcal{Z}_4)^2} \left(\frac{\text{Ei}\left[-\mathcal{Z}_1\, \mathcal{Z}_4\right]}{\exp\left(-\mathcal{Z}_1\, \mathcal{Z}_4 \gamma\right)} - \frac{\text{Ei}\left[-\mathcal{Z}_1\, \mathcal{Z}_3\right]}{\exp\left(-\mathcal{Z}_1\, \mathcal{Z}_3 \gamma\right)} \right) + \frac{(\mathcal{Z}_2 - \mathcal{Z}_4)}{(\mathcal{Z}_3 - \mathcal{Z}_4)} \\ &\times \left(\frac{\mathcal{Z}_1\, \text{Ei}\left[-\mathcal{Z}_1\, \mathcal{Z}_4\right]}{\exp\left(-\mathcal{Z}_1\, \mathcal{Z}_4 \gamma\right)} + \frac{1}{\mathcal{Z}_4} \right) \Bigg\} \Bigg],\end{aligned} \tag{4.22}$$

where

$\mathcal{Z}_1 = \frac{(k+1)\,\beta}{\omega_1}$, $\mathcal{Z}_2 = \frac{\omega_3}{(m+1)} \left(1 + \frac{1}{\omega_4}\right)$, $\mathcal{Z}_3 = \frac{1}{\beta} \left(\frac{\omega_1}{(k+1)\,\omega_2} + \alpha\right)$, and $\mathcal{Z}_4 = \frac{\omega_3}{(m+1)\,\omega_4}$.

Proof: See Appendix D. ■

4.4.3 Asymptotic Secrecy Outage Analysis

Now, the SOP of the D2D communications at high SNR, i.e., when $\overline{\gamma}_d \to \infty$, is investigated to gain more insight into the impact of the essential parameters of the system model. In this scenario, we consider that $\omega_1 >> \omega_3$. As $\omega_1 \to \infty$, the asymptotic expression of the SOP

can be expressed by [17]

$$\text{SOP}^{\infty} = (\mathcal{G}_a\, \omega_1)^{-\mathcal{G}_d} + \mathcal{O}(\omega_1^{-\mathcal{G}_d}), \tag{4.23}$$

where $\mathcal{G}_d$ is the secrecy diversity order, $\mathcal{G}_a$ is the secrecy array gain, and $\mathcal{O}(.)$ is the higher order terms. To elaborate, one can conclude that the curve of SOP^{∞} is defined by $\mathcal{G}_d$, and the SNR improvement of SOP^{∞} related to the reference curve $\omega_1^{-\mathcal{G}_d}$ is described by $\mathcal{G}_a$.

4.4.3.1 Eavesdropper Channel with MRC in the ORS scheme

To derive the asymptotic SOP for MRC, $\text{SOP}^{\infty}_{\text{MRC}}$, we first expand the exponential function and the polynomial in (4.10) with the help of [16, eq. (1.112.2)] and [16, eq. (1.211.1)], respectively. Then, we neglect the higher order terms. Now, the $\text{SOP}^{\infty}_{\text{MRC, ORS}}$ can be obtained using

$$\text{SOP}^{\infty}_{\text{MRC, ORS}} = \left(\mathcal{G}^{\text{ORS}}_{a_{\text{MRC}}}\omega_1\right)^{-\mathcal{G}^{\text{ORS}}_{d_{\text{MRC}}}} + \mathcal{O}(\omega_1^{-\mathcal{G}^{\text{ORS}}_{d_{\text{MRC}}}}), \tag{4.24}$$

where $\mathcal{G}^{\text{ORS}}_{d_{\text{MRC}}} = N_R$ and $\mathcal{G}^{\text{ORS}}_{a_{\text{MRC}}}$ can be derived as

$$\begin{aligned} G^{\text{ORS}}_{a_{\text{MRC}}} = \Bigg[\prod_{k=1}^{N_R}(\omega_2+1)\Bigg(\alpha + \frac{N_E\,\omega_3\,\beta}{\omega_4\exp\left(\frac{-1}{2\omega_4}\right)}\sum_{m=0}^{N_E}\binom{N_E}{m}\Gamma(m+1)\left(\frac{1}{\omega_4}\right)^{\frac{N_E-m-1}{2}} \\ \times\mathcal{W}_{\frac{-N_E-m-1}{2},\frac{-N_E+m}{2}}\left(\frac{1}{\omega_4}\right)\Bigg)\Bigg]^{-\frac{1}{N_R}}. \end{aligned} \tag{4.25}$$

4.4.3.2 Eavesdropper Channel with SC in the ORS scheme

Similarly, the asymptotic SOP for SC, $\text{SOP}^{\infty}_{\text{SC, ORS}}$, can be derived following a similar procedure to that given above as

$$\text{SOP}^{\infty}_{\text{SC, ORS}} = \left(\mathcal{G}^{\text{ORS}}_{a_{\text{SC}}}\omega_1\right)^{-\mathcal{G}^{\text{ORS}}_{d_{\text{SC}}}} + \mathcal{O}(\omega_1^{-\mathcal{G}^{\text{ORS}}_{d_{\text{SC}}}}), \tag{4.26}$$

where $\mathcal{G}_{d_{\text{SC}}}^{\text{ORS}} = N_R$ and $\mathcal{G}_{a_{\text{SC}}}^{\text{ORS}}$ is given by

$$G_{a_{\text{SC}}}^{\text{ORS}} = \left[\prod_{k=1}^{N_R}(\omega_2+1)\left(\alpha + \frac{N_E}{\omega_3\,\omega_4}\sum_{m=0}^{N_E-1}\binom{N_E-1}{m}\frac{(-1)^m\beta\,\omega_3^2}{(m+1)\exp\left(\frac{1}{\omega_4}\right)}\left(-\text{Ei}\left[-\frac{1}{\omega_4}\right]\right)\right)\right]^{-\frac{1}{N_R}}. \tag{4.27}$$

4.4.3.3 Eavesdropper Channel with MRC in the SRS scheme

The asymptotic SOP for MRC, $\text{SOP}_{\text{MRC, SRS}}^{\infty}$, can be obtained with the help of [16, eq. (1.112.2)] and [16, eq. (1.211.1)], and neglecting the higher order terms. Now, the $\text{SOP}_{\text{MRC, SRS}}^{\infty}$ can be obtained using

$$\text{SOP}_{\text{MRC, SRS}}^{\infty} = \left(\mathcal{G}_{a_{\text{MRC}}}^{\text{SRS}}\omega_1\right)^{-\mathcal{G}_{d_{\text{MRC}}}^{\text{SRS}}} + \mathcal{O}(\omega_1^{-\mathcal{G}_{d_{\text{MRC}}}^{\text{SRS}}}), \tag{4.28}$$

where $\mathcal{G}_{d_{\text{MRC}}}^{\text{SRS}} = N_R$ and $\mathcal{G}_{a_{\text{MRC}}}^{\text{SRS}}$ can be derived as

$$G_{a_{\text{MRC}}}^{\text{SRS}} = \left[\sum_{p=0}^{N_R}\binom{N_R}{p}\frac{\omega_2^p\,\Gamma(p+1)}{\Gamma(N_E)}\sum_{m=0}^{N_E}\binom{N_E}{m}\frac{\Gamma(m+1)}{\omega_3^{N_E}\,\omega_4}\sum_{s=0}^{N_R}\binom{N_R}{s}\alpha^{N_R-s}\beta^s\exp\left(\frac{1}{\omega_4}\right)\right.$$
$$\left.\times\omega_3^{m+1}\sum_{v=0}^{N_E+s-1}\binom{N_E+s-1}{v}\left(\frac{-\omega_3}{\omega_4}\right)^{N_E+s-v-1}\Gamma\left(v-m,\frac{1}{\omega_4}\right)\omega_3^{v-m}\right]^{\frac{-1}{N_R}}. \tag{4.29}$$

4.4.3.4 Eavesdropper Channel with SC in the SRS scheme

The asymptotic SOP for SC, $\text{SOP}_{\text{SC, SRS}}^{\infty}$, can be obtained with the help of [16, eq. (1.112.2)] and [16, eq. (1.211.1)], respectively, and neglecting the higher order terms. Now, the $\text{SOP}_{\text{SC, SRS}}^{\infty}$ can be obtained using

$$\text{SOP}_{\text{SC, SRS}}^{\infty} = \left(\mathcal{G}_{a_{\text{SC}}}^{\text{SRS}}\omega_1\right)^{-\mathcal{G}_{d_{\text{MRC}}}^{\text{SRS}}} + \mathcal{O}(\omega_1^{-\mathcal{G}_{d_{\text{SC}}}^{\text{SRS}}}), \tag{4.30}$$

where $\mathcal{G}_{d_{\text{SC}}}^{\text{SRS}} = N_R$ and $\mathcal{G}_{a_{\text{SC}}}^{\text{SRS}}$ can be derived as

$$G_{a_{\text{SC}}}^{\text{SRS}} = \Bigg[\frac{N_E}{\omega_3\,\omega_2} \sum_{p=0}^{N_R} \binom{N_R}{p} \omega_2^p\, \Gamma(p+1) \sum_{k=0}^{N_E-1} (-1)^k \binom{N_E-1}{m} \sum_{s=0}^{N_R} \binom{N_R}{s} \alpha^{N_R-s} \beta^s \times \exp\left(-\frac{1}{2\,\omega_4}\right) \left(\frac{\omega_3}{k+1}\right)^s \Gamma(s+1) \left(\left(\frac{1}{\omega_4}\right)^{\frac{s-2}{2}} \mathcal{W}_{\frac{-2-s}{2},\frac{1-s}{2}}\left(\frac{1}{\omega_4}\right)\right)\Bigg]^{\frac{-1}{N_R}}. \tag{4.31}$$

4.5 Probability of Non-zero Secrecy Capacity

Considering the PNSC, non-zero secrecy capacity is achieved if $\gamma_{R_k D} > \gamma_{R_k E}$.

4.5.1 The ORS scheme

From (5.11), the PNSC for the ORS, $\text{PNSC}_v^{\text{ORS}}$, is given by

$$\text{PNSC}_v^{\text{ORS}} = \Pr\left(C_S > 0\right) = 1 - \Pr\left(C_S \leq 0\right) = 1 - \prod_{k \in N} \underbrace{\Pr\left(\frac{1+\gamma_{R_k D}}{1+\gamma_{R_k E}} \leq 1\right)}_{\mathcal{D}_k^v}. \tag{4.32}$$

Following the same steps of the derivation of (4.12) and (4.14), $\mathcal{D}_k^v$ can be derived as

$$\mathcal{D}_k^{\text{MRC}} = 1 - \frac{\omega_2}{\omega_3^{N_E}\,\omega_4\,\beta} \sum_{m=0}^{N_E} \binom{N_E}{m} \Gamma(m+1)\,\omega_3^{m+1} \Bigg[\sum_{i=1}^{m+1} (-1)^{m+1-i}\, \mathcal{W}_{\frac{1-i-N_E}{2},\frac{i-N_E}{2}}\left(\mathcal{A}_4\mathcal{A}_2\right) \times \frac{\mathcal{A}_4^{-\left(\frac{N_E-i+1}{2}\right)} \mathcal{A}_2^{\left(\frac{N_E-i-1}{2}\right)}}{\exp\left(\frac{-\mathcal{A}_4\mathcal{A}_2}{2}\right)\left(\mathcal{A}_5-\mathcal{A}_2\right)^{m+2-i}} + \frac{\mathcal{A}_5^{N_E-1}\,\Gamma\left(1-N_E, \mathcal{A}_4\mathcal{A}_5\right)}{\exp\left(-\mathcal{A}_1\,\mathcal{A}_5\right)\left(\mathcal{A}_2-\mathcal{A}_5\right)^{m+1}} \Bigg], \tag{4.33}$$

and

$$\mathcal{D}_k^{\text{SC}} = 1 - \frac{N_E}{\omega_3\,\omega_4\,\mathcal{B}_5}\sum_{m=0}^{N_E-1}(-1)^m\binom{N_E-1}{m}\left[\frac{\mathcal{B}_6\,\text{Ei}\left[-\mathcal{B}_6\,\mathcal{B}_3\right]}{\exp\left(-\mathcal{B}_6\,\mathcal{B}_3\right)} + \frac{1}{\mathcal{B}_3} + \frac{\mathcal{B}_7}{\mathcal{B}_5}\left(-\frac{\text{Ei}\left[-\mathcal{B}_6\,\mathcal{B}_3\right]}{\exp\left(-\mathcal{B}_6\,\mathcal{B}_3\right)}\right.\right.$$
$$\left.\left.+\exp\left(\mathcal{B}_6\left(\frac{\omega_1}{\omega_2}\right)\right)\text{Ei}\left[-\mathcal{B}_6\left(\frac{\omega_1}{\omega_2}\right)\right]\right)\right], \tag{4.34}$$

respectively, where $\mathcal{A}_4 = \frac{1}{\omega_1}+\frac{1}{\omega_3}$, $\mathcal{A}_5 = \frac{\omega_1}{\omega_2}$, $\mathcal{B}_5 = \frac{(m+1)}{\omega_3}\left(\frac{(m+1)}{\omega_3} - \frac{\omega_2}{\omega_1\omega_4}\right)$, $\mathcal{B}_6 = \frac{m+1}{\omega_3}+\frac{1}{\omega_1}$, and $\mathcal{B}_7 = \frac{(m+1)}{\omega_3} - \left(1+\frac{1}{\omega_4}\right)\frac{\omega_2}{\omega_1}$.

4.5.2 The SRS scheme

From (4.17), the PNSC for the ORS, $\text{PNSC}_v^{\text{SRS}}$, can be formulated as

$$\text{PNSC}_v^{\text{SRS}} = \Pr\left(\frac{1+\gamma_{\text{SRS}}}{1+\gamma_{RE}} > 1\right) = 1 - \int_0^\infty F_{\gamma_{\text{SRS}}}(\gamma) f_{\gamma_{\text{RE}}}(\gamma)\,d\gamma. \tag{4.35}$$

Following the same steps of the derivation of (4.20) and (4.22), the $\text{PNSC}_v^{\text{SRS}}$ can be derived as

$$\text{PNSC}_{\text{MRC}}^{\text{SRS}} = 1 - N_R\sum_{k=0}^{N_R-1}\frac{(-1)^k\binom{N_R-1}{k}}{(k+1)}\left[1 - \sum_{m=0}^{N_E}\frac{\binom{N_E}{m}\,\Gamma(m+1)\,\omega_1}{\omega_3^{N_E-(m+1)}\,\omega_2\,\omega_4\,(k+1)}\right.$$
$$\times\left\{\sum_{j=1}^{m+1}\frac{(-1)^{m+1-j}\exp\left(\frac{\mathcal{H}_4\mathcal{H}_2}{2}\right)}{\left(\mathcal{H}_5-\mathcal{H}_2\right)^{m+2-j}}\mathcal{H}_4^{-\left(\frac{N_E-j+1}{2}\right)}\mathcal{H}_2^{\left(\frac{N_E-j-1}{2}\right)}\mathcal{W}_{\frac{1-j-N_E}{2},\frac{j-N_E}{2}}\left(\mathcal{H}_4\mathcal{H}_2\right)\right.$$
$$\left.\left.+\frac{\mathcal{H}_5^{N_E-1}\,\Gamma\left(1-N_E,\mathcal{H}_4\mathcal{H}_5\right)}{\exp\left(-\mathcal{H}_4\,\mathcal{H}_5\right)\left(\mathcal{H}_2-\mathcal{H}_5\right)^{m+1}}\right\}\right], \tag{4.36}$$

and

$$\begin{aligned}\text{PNSC}_{\text{SC}}^{\text{SRS}} =& 1 - N_R \sum_{k=0}^{N_R-1} \frac{(-1)^k \binom{N_R-1}{k}}{(k+1)} \left[1 - \frac{N_E\, \omega_1}{\omega_2\, \omega_4\, (k+1)} \sum_{m=0}^{N_E-1} \frac{(-1)^m \binom{N_E-1}{m}}{(m+1)} \right. \\ & \times \left\{ \frac{(\mathcal{Z}_2 - \mathcal{Z}_6)}{(\mathcal{Z}_6 - \mathcal{Z}_4)^2} \left(\frac{\text{Ei}\left[-\mathcal{Z}_5\, \mathcal{Z}_4\right]}{\exp\left(-\mathcal{Z}_5\, \mathcal{Z}_4\right)} - \frac{\text{Ei}\left[-\mathcal{Z}_5\, \mathcal{Z}_6\right]}{\exp\left(-\mathcal{Z}_5\, \mathcal{Z}_6\right)} \right) + \frac{(\mathcal{Z}_2 - \mathcal{Z}_4)}{(\mathcal{Z}_6 - \mathcal{Z}_4)} \right. \\ & \left. \left. \times \left(\frac{\mathcal{Z}_5\, \text{Ei}\left[-\mathcal{Z}_5\, \mathcal{Z}_4\right]}{\exp\left(-\mathcal{Z}_5\, \mathcal{Z}_4\right)} + \frac{1}{\mathcal{Z}_4} \right) \right\} \right], \end{aligned} \tag{4.37}$$

respectively, where $\mathcal{H}_4 = \frac{(k+1)}{\omega_1} + \frac{1}{\omega_3}$, $\mathcal{H}_5 = \frac{\omega_1}{\omega_2(k+1)}$, $\mathcal{Z}_5 = \frac{(k+1)}{\omega_1} + \frac{(m+1)}{\omega_3}$, and $\mathcal{Z}_6 = \frac{\omega_1}{\omega_2(k+1)}$.

4.6 Underlay Multihop Device-to-Device Relaying

Multi-hop relaying has gained more attention to improve QoS of cellular networks. The two main approaches for wireless relay networks are DF and AF [20]. In this respect, it is worth mentioning that there are many advantages of multihop relaying such as a higher data rate and coverage. In [21], a thorough analysis of the data routing approaches is provided for multihop D2D networks. Considering the traffic offloading from the cellular network, the multihop D2D scheme was utilized in [22]. The authors of [23] showed that using D2D relays is more efficient than direct D2D communication, particularly in case of poor link quality or long distance between D2D users. The PLS of underlay D2D communications was studied in [24]. Due to sharing the spectrum band, D2D and cellular users interfere with each other. In this respect, the secrecy level for cellular communications can be improved by exploiting the interference. Consequently, the signal-to-interference-and-noise ratio (SINR) of the eavesdropper is degraded. The authors of [25] studied the benefits of the interference produced by D2D pairs to increase the secrecy capacity of the cellular network. The authors of [26] investigated the D2D radio resource management to increase the security level of the cellular network by utilizing the underlay D2D users as friendly jammers.

Although the above-mentioned works have shown the benefits of D2D in terms of se-

curity provisioning for the cellular networks, few studies have investigated the PLS of the D2D relaying. It should be noted that due to the limited computational capacity of mobile devices and the semi/fully autonomous security management, the D2D links are more vulnerable to security threats. Therefore, the security improvement of D2D links deserves to be investigated. Motivated by this, in this work, we investigate the PLS for the D2D multihop relaying, where the D2D users are used as multihop relays to cope with the proximity and link condition issues in D2D communications. In this respect, the effect of multihop relays on the performance of the D2D communications is assessed, taking into account the interference generated by the cellular network. The main contributions of this section are summarized as follows:

- The secrecy performance of the D2D communications in terms of SOP and the PNSC is analyzed and closed-form expressions are derived. Furthermore, the outage probability of the D2D communication is analyzed, and a closed-form expression on its lower bound is provided.
- The impact of the number of multihop relays on the secrecy performance of D2D communications is evaluated.
- The asymptotic result is investigated in the high transmit power regime for the D2D communications.
- Simulation results are provided to validated and confirm the derived analytical expressions.

4.6.1 System Model

As illustrated in Fig. 4.2, an underlay D2D network is considered with multihop D2D relaying where the cellular system and D2D system share the same spectral band in a specific

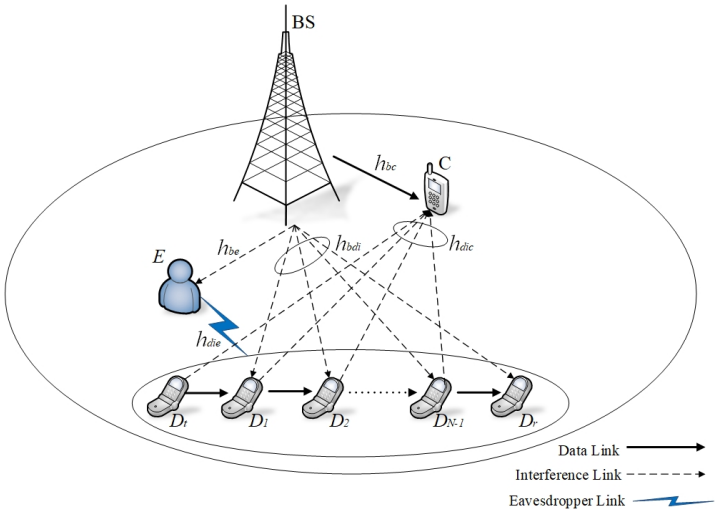


Fig. 4.2: System Model.

environment. The cellular network consists of a BS and a cellular user, C, each equipped with a single antenna. A D2D transmitter, D_t, is communicating with a D2D receiver, D_r, via (N-1) D2D users, D_i, $i = 1.....N-1$, in the presence of an eavesdropper, E, and where the D2D users are acting as DF relaying. In the proposed scenario, there is no direct link between D_t and D_r. Hence, the whole transmission time is allocated equally to each D_i during the D2D multihop link. Moreover, only one D_i is assumed to transmit in each time slot. All communication channels are supposed to experience flat fading with Rayleigh distribution. Let h_{di} indicate the main channel coefficient for the i^{th} D2D link, h_{dic}, the interference channel from D2D link to C, h_{bdi}, the interference channel from BS link to D2D users, and h_{d_ie} the eavesdropper channel coefficient. In addition, the channel power gain $|h_{ab}|^2$ is independent and exponentially distributed with a mean of λ_{ab} = E$[|h_{ab}|^2]$ where $ab \in \{d_id_{i+1}, bd_i, bc, be, d_ie\}$. Moreover, the variances of the AWGN at D_i and E are given by $\sigma_{d_i}^2$ and σ_e^2, respectively. Furthermore, it is assumed that all D2D nodes transmit with the same power P_d. The received signals at the i^{th} D2D relay, y_{d_i}, can be expressed as

$$y_{d_i} = \sqrt{P_d}\, h_{d_i}\, x_d + \sqrt{P_b}\, h_{bd_i}\, x_b + n_d, \tag{4.38}$$

where x_d and x_b are the D2D and BS transmitted signals, respectively. Moreover, n_d is the AWGN at the the i^{th} D2D hop, P_d and P_b are the transmitted power from D2D users and BS, respectively. In addition, the received signal at E is given by

$$y_{e_i} = \sqrt{P_d}\, h_{d_i e}\, x_d + \sqrt{P_b}\, h_{be}\, x_b + n_e, \tag{4.39}$$

where n_e is the AWGN at E. The SINR at the i^{th} D2D hop, γ_{D_i}, is given by

$$\gamma_{D_i} = \frac{P_d \left|h_{d_i}\right|^2}{\sigma_d^2 + P_b \left|h_{bd_i}\right|^2} = \frac{\gamma_{d_i}}{1 + \gamma_{bd_i}}, \tag{4.40}$$

where $\gamma_{d_i} = \bar{\gamma}_{di} \left|h_{d_i}\right|^2$, $\gamma_{bd_i} = \bar{\gamma}_{bd_i} \left|h_{d_2}\right|^2$, $\bar{\gamma}_{d_i} = \frac{P_d}{\sigma_d^2}$, and $\bar{\gamma}_{bd_i} = \frac{P_b}{\sigma_d^2}$. Let us denote $\mu_1 = \bar{\gamma}_{di}\lambda_{d_i}$ and $\mu_2 = \bar{\gamma}_{bdi}\lambda_{bd_i}$.

4.6.2 Performance Analysis

In this subsection, the performance analysis of the described system model is carried out where the outage probability, the SOP, and the PNSC for the D2D communications are investigated.

4.6.2.1 D2D Outage Probability

In multihop D2D relaying, an outage event happens in the end-to-end D2D communication if the capacity of at least one of the multihop relays falls below the predefined required data rate R_d. The outage probability of underlay multihop D2D relaying, P_{out}, can be defined as

$$P_{out} = \Pr\left(\gamma_{e2e} \leq 2^{R_d} - 1\right). \tag{4.41}$$

A tight upper bound, γ_{up}, is utilized to express γ_{e2e} at D_r as

$$\gamma_{e2e} \leq \gamma_{up} = \min\ \left(\gamma_{D_1}, \gamma_{D_2}, ...\gamma_{D_N}\right). \tag{4.42}$$

The CDF of γ_{up} is given by [27]

$$F_{\gamma_{up}}(\gamma) = 1 - \prod_{i=1}^{N} \left(1 - F_{\gamma_{Di}}(\gamma)\right), \tag{4.43}$$

where $F_{\gamma_{D_i}}(.)$ is the CDF of γ_{D_i} at the i^{th} relay link. To derive the PDF of γ_{D_i}, the following formula can be used [18]

$$f_{\gamma_{D_i}}(x) = \int_0^{\infty} (y+1) f_{\gamma_{di}}(x(y+1)) f_{\gamma_{bdi}}(y) dy, \tag{4.44}$$

where $f_{\gamma_{di}}(.)$ is given by

$$f_{\gamma_{di}}(\gamma) = \frac{1}{\mu_1} \exp\left(-\frac{\gamma}{\mu_1}\right), \tag{4.45}$$

and $f_{\gamma_{bdi}}(.)$ is given by

$$f_{\gamma_{bdi}}(\gamma) = \frac{1}{\mu_2} \exp\left(-\frac{\gamma}{\mu_2}\right). \tag{4.46}$$

By substituting (4.45) and (4.46) in (4.44), the PDF of γ_{D_i} can be derived as

$$f_{\gamma_{D_i}}(\gamma) = \frac{1}{\mu_1 \mu_2}\ \exp\left(-\frac{\gamma}{\mu_1}\right) \left(\frac{1 + \frac{\gamma}{\mu_1} + \frac{1}{\mu_2}}{\left(\frac{\gamma}{\mu_1} + \frac{1}{\mu_2}\right)^2}\right). \tag{4.47}$$

From (4.47), the CDF of γ_{D_i} can be obtained as

$$F_{\gamma_{D_i}}(\gamma) = \int_0^{\gamma} f_{\gamma_{D_i}}(\zeta)\, d\zeta = \left(1 - \frac{\frac{1}{\mu_2} \exp\left(-\frac{\gamma}{\mu_1}\right)}{\left(\frac{\gamma}{\mu_1} + \frac{1}{\mu_2}\right)}\right). \tag{4.48}$$

By plugging (4.48) into (4.43), $F_{\gamma_{up}}(\gamma)$ becomes straightforward. Now, P_{out}, can be expressed as

$$P_{out} = \Pr\left(\gamma_{up} < \gamma_{th}\right) = F_{\gamma_{up}}(\gamma_{th}), \tag{4.49}$$

where $\gamma_{th} = 2^{NR_d} - 1$ and R_d is the D2D required data rate. By plugging (4.48) into (4.49), P_{out} can be obtained as

$$P_{out} = 1 - \prod_{i=1}^{N} \left(\frac{\frac{1}{\mu_2} \exp\left(-\frac{\gamma_{th}}{\mu_1}\right)}{\left(\frac{\gamma_{th}}{\mu_1} + \frac{1}{\mu_2}\right)} \right). \tag{4.50}$$

4.6.2.2 Secrecy Outage Probability

In this subsection, the secrecy outage probability, SOP, is investigated for the underlay multihop D2D relaying scheme where the closed-form expression is derived. The secrecy capacity, C_{s_i}, for the proposed scheme at the i^{th} D2D hop is given by

$$C_{s_i} = \begin{cases} C_{D_i} - C_{Ei}, & \gamma_{D_i} > \gamma_{E_i} \\ 0, & \gamma_{D_i} \leq \gamma_{E_i} \end{cases}, \tag{4.51}$$

where the capacity of the i^{th} D2D relay, C_{D_i}, is given by

$$C_{D_i} = \log_2\left(1 + \gamma_{D_i}\right) = \log_2\left(1 + \frac{\gamma_{d_i}}{1 + \gamma_{bd_i}}\right), \tag{4.52}$$

and the eavesdropper's capacity, C_{Ei}, is given by

$$C_{Ei} = \log_2\left(1 + \gamma_{E_i}\right) = \log_2\left(1 + \frac{\gamma_{d_i e}}{1 + \gamma_{be}}\right), \tag{4.53}$$

where γ_{E_i} is the SINR at E, $\gamma_{d_ie} = \bar{\gamma}_{ei} |h_{d_ie}|^2$, $\gamma_{be} = \bar{\gamma}_{be} |h_{be}|^2$, $\bar{\gamma}_{e_i} = \frac{P_d}{\sigma_e^2}$, and $\bar{\gamma}_{be} = \frac{P_b}{\sigma_e^2}$. Let us denote $\omega_1 = \bar{\gamma}_{ei}\lambda_{d_ie}$ and $\omega_2 = \bar{\gamma}_{be}\lambda_{be}$. By plugging (4.52) and (4.53) into (4.51), C_{s_i} simplifies to

$$C_{s_i} = \left[\log_2\left(\frac{1+\gamma_{D_i}}{1+\gamma_{E_i}}\right)\right]^+, \tag{4.54}$$

where $[x]^+ = \max\{0, x\}$. Let us define $\gamma_i = \left(\frac{1+\gamma_{D_i}}{1+\gamma_{E_i}}\right)$. The SOP is the probability that at least one of secrecy capacities, C_{s_i}, falls below the predefined secrecy rate R_s. Therefore, the SOP of the underlay multihop D2D relaying is given by [26]

$$\begin{aligned}\text{SOP} &= \Pr\left(\frac{1}{N}\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right) < R_s\right) = \Pr\left(\min_i \gamma_i < 2^{NR_s}\right) \\ &= 1 - \Pr\left(\min_i \gamma_i > 2^{N\,R_s}\right) = 1 - \prod_{i=1}^{N}\Pr\left(\gamma_i > 2^{N\,R_s}\right) = 1 - \prod_{i=1}^{N}\left(1 - F_{\gamma_i}(\beta)\right),\end{aligned} \tag{4.55}$$

where $F_{\gamma_i}(.)$ is the CDF of γ_i and $\beta = 2^{NR_s}$. The factor $1/N$ in (4.55) accounts for the N multihop relays where the end-to-end D2D transmission is divided into N phases. The CDF of γ_i can be expressed as

$$F_{\gamma_i}(\gamma) = \int_0^\infty F_{\gamma_{D_i}}(\beta\gamma + \alpha) f_{\gamma_{E_i}}(\gamma)\, d\gamma, \tag{4.56}$$

where $\alpha = \beta - 1$. The SINR at E, γ_{E_i}, is given by

$$\gamma_{E_i} = \frac{P_d |h_{d_ie}|^2}{\sigma_e^2 + P_b |h_{be}|^2} = \frac{\gamma_{d_ie}}{1+\gamma_{be}}. \tag{4.57}$$

To derive the PDF of γ_{E_i}, the following formula can be used [18]

$$f_{\gamma_{E_i}}(x) = \int_0^\infty (y+1) f_{\gamma_{d_ie}}(x(y+1)) f_{\gamma_{be}}(y) dy, \tag{4.58}$$

where $f_{\gamma_{d_i e}}(\cdot)$ is given by

$$f_{\gamma_{d_i e}}(\gamma) = \frac{1}{\omega_1} \exp\left(-\frac{\gamma}{\omega_1}\right), \tag{4.59}$$

and $f_{\gamma_{be}}(\cdot)$ is given by

$$f_{\gamma_{be}}(\gamma) = \frac{1}{\omega_2} \exp\left(-\frac{\gamma}{\omega_2}\right). \tag{4.60}$$

By substituting (4.59) and (4.60) in (4.58), the PDF of γ_{E_i} can be obtained as

$$f_{\gamma_{E_i}}(\gamma) = \frac{\exp\left(-\frac{\gamma}{\omega_1}\right)}{\omega_1 \omega_2} \left(\frac{1 + \frac{\gamma}{\omega_1} + \frac{1}{\omega_2}}{\left(\frac{\gamma}{\omega_1} + \frac{1}{\omega_2}\right)^2}\right). \tag{4.61}$$

By substituting (4.48) and (4.61) in (4.56), and using partial fraction expansion, then [16, eq. (3.352.4)] and [16, eq. (3.353.3)], the CDF of γ_i, $F_{\gamma_i}(\cdot)$, can be obtained as

$$\begin{aligned} F_{\gamma_i}(\beta) = 1 - \frac{\exp\left(-\frac{\alpha}{\mu_1}\right)}{\mu_2\, \omega_1\, \omega_2} \Bigg(\frac{\omega_1}{\Xi_1} \left(\left(\frac{\beta}{\mu_1} + \frac{1}{\omega_1}\right) \frac{\mathrm{Ei}\left[-\Xi_2\right]}{\exp\left(-\Xi_2\right)} + \left(\frac{\omega_2}{\omega_1}\right)\right) - \frac{\Xi_3}{\Xi_1^2} \left(\frac{\mathrm{Ei}\left[-\Xi_2\right]}{\exp\left(-\Xi_2\right)}\right) \\ + \frac{\Xi_3}{\Xi_1^2} \left(\frac{\mathrm{Ei}\left[-\Xi_4\right]}{\exp\left(-\Xi_4\right)}\right)\Bigg), \end{aligned} \tag{4.62}$$

where $\Xi_1 = \left(\frac{1}{\omega_1}\left(\frac{\alpha}{\mu_1} + \frac{1}{\mu_2}\right) - \frac{\beta}{\mu_1 \omega_2}\right)$, $\Xi_2 = \left(\frac{\beta}{\mu_1} + \frac{1}{\omega_1}\right)\left(\frac{\omega_1}{\omega_2}\right)$, $\Xi_3 = \frac{1}{\omega_1}\left(\frac{\alpha}{\mu_1} + \frac{1}{\mu_2}\right) - \frac{\beta}{\mu_1}\left(\frac{1}{\omega_2} + 1\right)$, $\Xi_4 = \left(\frac{\beta}{\mu_1} + \frac{1}{\omega_1}\right)\left(\frac{\mu_1}{\beta}\left(\frac{\alpha}{\mu_1} + \frac{1}{\mu_2}\right)\right)$, and $\mathrm{Ei}(\cdot)$ is the exponential integral function [16, eq. (8.21.1)]. By substituting (4.62) in (4.55), the expression of SOP becomes straightforward.

4.6.2.3 Asymptotic Secrecy Outage Analysis

In this subsection, the outage performance at high SNR, i.e., $\overline{\gamma}_{d_i} \to \infty$ is provided to get more insights on the impact of key parameters on the performance of the proposed system.

As $\overline{\gamma}_{d_i} \to \infty$, the asymptotic expression of the i^{th} hop, SOP_i^{∞}, can be expressed as

$$\text{SOP}_i^{\infty} = (\mathcal{G}_{a_i}\overline{\gamma}_{d_i})^{-\mathcal{G}_{d_i}} + \mathcal{O}(\overline{\gamma}_{d_i})^{-\mathcal{G}_{di}}, \tag{4.63}$$

where $\mathcal{G}_{d_i}$ and $\mathcal{G}_{a_i}$ denote the diversity order and the coding gain, respectively. In this respect, the SOP_i^{∞} curve is described by $\mathcal{G}_{d_i}$ while the SNR advantage of SOP_i^{∞} relative to the reference curve $(\overline{\gamma}_{d_i})^{-\mathcal{G}_{d_i}}$ is characterized by $\mathcal{G}_{a_i}$. To derive SOP_i^{∞}, the exponential function and the polynomials in (4.48) are first expanded using the series expansion in [16, eq. (1.211.1)], [16, eq. (1.112.2)], respectively. After that, the first two terms in the expansion are kept and the higher order terms are neglected. As a result, the asymptotic CDF, $F_{\gamma_{D_i}}^{\infty}(.)$, is expressed as

$$F_{\gamma_{D_i}}^{\infty}(\gamma) = \frac{1}{\mu_1}(\mu_2 + 1)\gamma + \mathcal{O}\left(\frac{\gamma}{\mu_1}\right). \tag{4.64}$$

Now, $F_{\gamma_i}^{\infty}(.)$ can be obtained as follows

$$F_{\gamma_i}^{\infty}(\gamma) = \int_0^{\infty} F_{\gamma_{D_i}}^{\infty}(\gamma) f_{\gamma_E}(\gamma)\, d\gamma. \tag{4.65}$$

By using (4.64) and (4.61) in (4.65), and after simple algebraic manipulations and using [16, eq. (3.351.4)], the asymptotic SOP in the i^{th} D2D hop, SOP_i^{∞}, can be derived as

$$\text{SOP}_i^{\infty} = \left(\frac{\mu_2 + 1}{\mu_1}\right)\left(\alpha - \frac{\omega_1\beta \exp\left(\frac{1}{\omega_2}\right)\ \text{Ei}\left[\frac{-1}{\omega_2}\right]}{\omega_2}\right) + \mathcal{O}\left(\frac{\gamma}{\mu_1}\right), \tag{4.66}$$

where $\Gamma(\cdot,\cdot)$ is the upper incomplete gamma function [16, eq. (8.350.2)]. By comparing (4.66) and (4.63), we have $\mathcal{G}_{d_i}$ = 1 and $\mathcal{G}_{a_i}$ is given by

$$\mathcal{G}_{a_i} = \left[(\mu_2 + 1) \left(\alpha - \frac{\omega_1 \beta \exp\left(\frac{1}{\omega_2}\right) \text{Ei}\left[\frac{-1}{\omega_2}\right]}{\omega_2} \right) \right]^{-1}.$$

After simple algebraic manipulations, the end-to-end $P^{\infty}_{s,out}$ expression becomes straightforward by plugging (4.66) into (4.55) as

$$\begin{aligned} \text{SOP}^{\infty} &= 1 - \prod_{i=1}^{N} \left(1 - \text{SOP}_i^{\infty}\right) \\ &= \sum_{k=1}^{N} \binom{N}{k} (-1)^{k+1} \left(\left(\frac{\mu_2 + 1}{\mu_1} \right) \left(\frac{\omega_1 \beta \exp\left(\frac{1}{\omega_2}\right) \text{Ei}\left[\frac{-1}{\omega_2}\right]}{\omega_2} + \alpha \right) + \mathcal{O}\left(\frac{\gamma}{\mu_1}\right) \right)^{k}. \end{aligned} \tag{4.67}$$

4.6.2.4 Probability of Non-zero Secrecy Capacity

A positive secrecy is achieved when $\gamma_{Di} > \gamma_{Ei}$. Hence, the probability of non-zero secrecy capacity, PNSC, is formulated as

$$\begin{aligned} \text{PNSC} &= \Pr\left(\frac{1}{N} \log_2 \left(\frac{1 + \gamma_D}{1 + \gamma_E} \right) > 0 \right) = \Pr\left(\min_i \gamma_i > 1 \right) \\ &= \prod_{i=1}^{N} \Pr\left(\gamma_i > 1\right) = \prod_{i=1}^{N} \left(1 - F_{\gamma_i}\left(1\right)\right). \end{aligned} \tag{4.68}$$

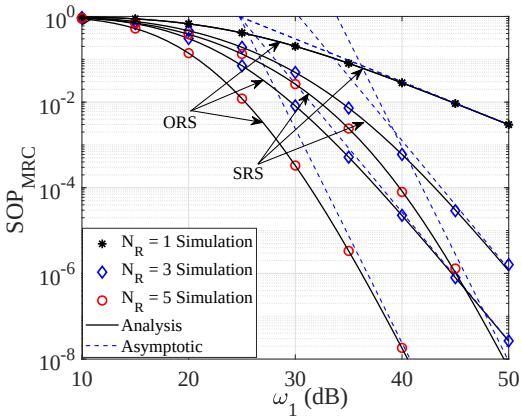
After simple algebraic manipulations, we can get PNSC by plugging (4.62) into (4.68) when $\beta = 1$.

4.7 Results and Discussion

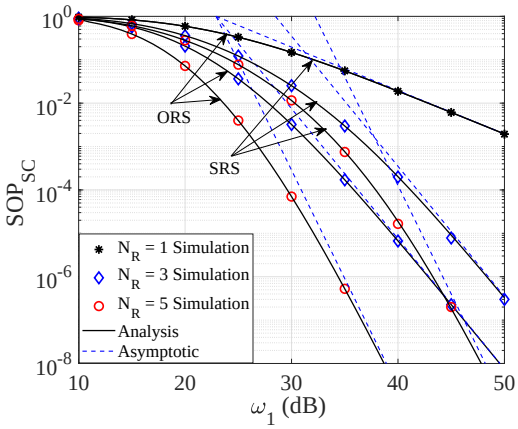
4.7.1 D2D Relay Selection

In this subsection, the analysis of the SOP and the PNSC for both combining techniques, MRC and SC, are presented and validated through Monte-Carlo simulations. From the obtained results, the impact of D2D relays and the number of eavesdropper's antennas for both MRC and SC are investigated. For simplicity, the noise variances of all nodes are normalized to unity. Unless stated, $\mathcal{R}_s = 1$ b/s/Hz , $\omega_2 = \omega_3 = \omega_4 = 10$ dB, and $\mathcal{R}_s = 1$ b/s/Hz.

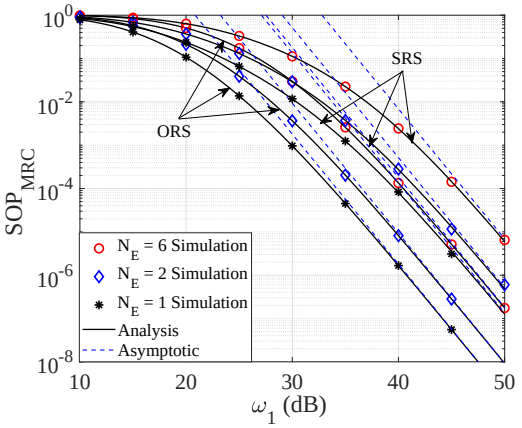
The SOP for MRC, SOP_{MRC}, of the D2D communications, is illustrated in Fig. 4.3a versus ω_1 for different values of N_R for both relay selection schemes, namely, ORS and SRS. $\mathcal{R}_s$ is 1 b/s/Hz, and $N_E = 3$. It can be observed that SOP_{MRC} decreases as N_R increases, showing the influence of the cooperative communications for enhancing the D2D secrecy performance. It is worth mentioning that the SOP_{MRC} increases as ω_1 decreases. At $\text{SOP}_{\text{MRC}} = 10^{-4}$, a security enhancement of 6 dB and 9 dB of the ORS scheme over the SRS one at N_R = 3 and N_R = 5, respectively, can be noticed. In Fig. 4.3a, SOP_{MRC} decreases from 0.008 to 0.0002 at 30 dB when the OSR scheme is used as compared to the SRS scheme. The results in Fig. 4.3a show that both schemes are close to each other at low SNR; however, the gap increases as the SNR increases. It can be inferred that the ORS guarantees the optimal secrecy performance for the D2D link. However, the CSI of the wiretapped link should be available to utilize the ORS scheme, which is not always the case in a practical scenario. Additionally, the asymptotic SOP is plotted, and a perfect agreement with the exact result is noted as $\omega_1 \to \infty$. From the asymptotic curves, it is noteworthy that G_a and G_d can be accurately predicted. It is also observed that G_d is not affected by N_E. These asymptotic results reveal that the SOP under both ORS and SRS has the same G_d for both combining techniques at E. Furthermore, the theoretical results and



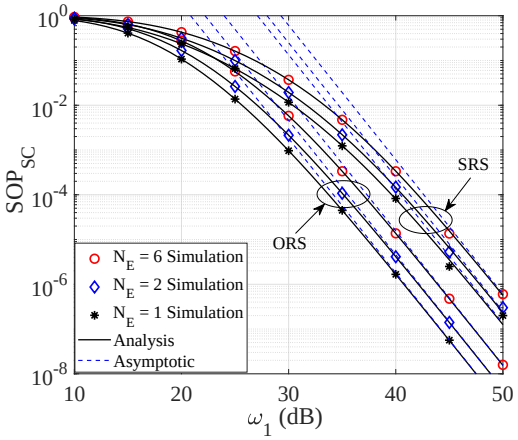
(a) The SOP_{MRC} vs. SNR, ω_1 for different N_R.



(b) The SOP_{SC} vs. SNR, ω_1 for different N_R.



(c) The SOP_{MRC} vs. SNR, ω_1 for different N_E.



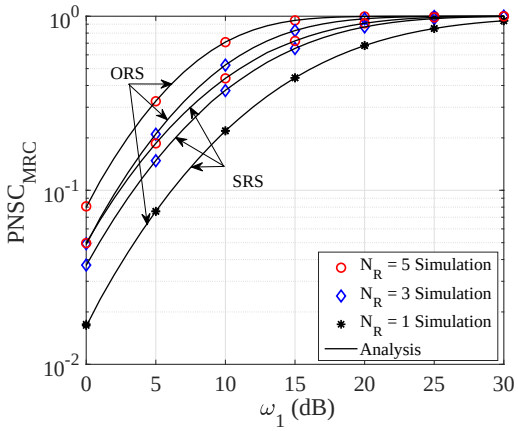
(d) The SOP_{SC} vs. SNR, ω_1 for different N_E.

Fig. 4.3: The SOP for ORS and SRS schemes, where $\omega_2 = \omega_4 = 10$ dB, and $\mathcal{R}_s = 1$ b/s/Hz.

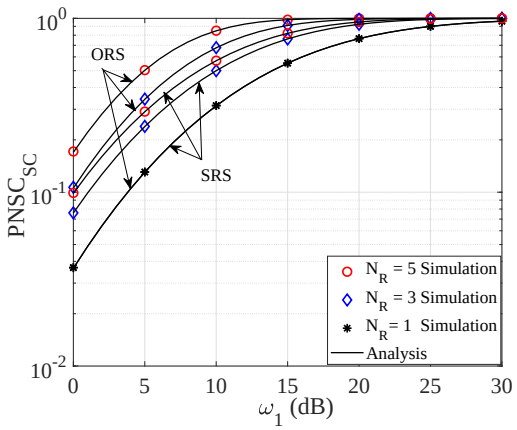
the simulation results agree exactly, confirming the correctness of the derived expressions.

In Fig. 4.3b, the SOP_{SC} of the D2D communications is illustrated for the ORS and SRS schemes, where $N_E = 3$. It can be seen that the SOP_{SC} increases with decreasing N_R, implying an improvement in the D2D secrecy performance. From Figs. 4.3a and 4.3b, one can observe that the high-security level for D2D communications is obtained when E employs SC in comparison to the MRC approach. This is because the MRC gives higher SNR gain at E as compared to the SC approach.

Figures 4.3c and 4.3d show the influnce of N_E on the SOP for both selections combining



(a) The PNSC_{MRC}, vs. SNR, ω_1, for different N_R



(b) The PNSC_{SC}, vs. SNR, ω_1, for different N_R

Fig. 4.4: The PNSC for ORS and SRS schemes, where ω_2 = ω_4 = 10 dB, N_E = 3, and $\mathcal{R}_s$ = 1 b/s/Hz.

versus ω_1 for OSC and SRS schemes, where $N_R = 3$. In addition, the asymptotic curves for both combining approaches and relay selection schemes are also illustrated. In Fig. 4.3c, for MRC, SOP for both ORS and SRS schemes decreases with decreasing N_E because the eavesdropper capacity, C_E, decreases with decreasing N_E. In Fig. 4.3d, for SC, there is also a decrease in the SOP for both ORS and SRS schemes with decreasing N_E. As N_E does not influence the diversity order, the array gain is responsible for increasing the SOP. From the results above, it can be verified that SOP for both combining approaches and relay selection schemes have the same secrecy diversity orders N_R. Again, numerical results are also seen to agree with the simulation results, confirming the accuracy of the analysis carried out.

Figures 4.4a and 4.4b plot the PNSC versus ω_1 for both selections combining techniques and both relay selection schemes. From these figures, one can see that the PNSC improves as ω_1 increases. Further, it is also remarkable that the PNSC decreases as N_R decreases. Thus, for the MRC approach, the PNSC is lower than that of the SC approach because the MRC gives higher SNR gain at E. Finally, it is worth emphasizing that the ORS scheme always outperforms the SRS scheme. Numerical results are also found to match the simulation results, verifying our analysis.

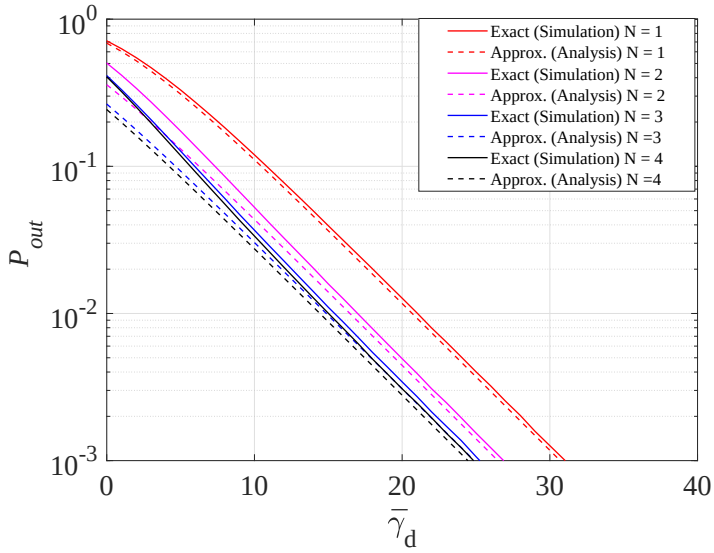


Fig. 4.5: The exact (simulation) and approximation (analysis) plots for the P_{out} vs $\bar{\gamma}_d$ for different N where $\bar{\gamma}_{bd}$ = 10 dB, and $R_d = 1$ b/s/Hz.

4.7.2 D2D Multihop Relaying

In this subsection, the analytical results of the outage probability, the SOP, and the probability of non-zero secrecy capacity are presented and verified through Monte-Carlo simulations. In this context, the effect of the proposed multihop D2D relaying on the secrecy performance of the D2D communications is studied. We assume that the distance between D_t and D_r is normalized to unity where the distances between different D2D relays are identical, $\frac{1}{N}$. In addition, we assume that BS is located at (0.5, 2), E at (0.5, 1), D_t at the origin (0, 0), and D_r at (0, 1). Therefore, λ_{ab} = d_{ab}^{-4} where d_{ab} is the Euclidean distance between terminals a and b. Without losing generality, the variances of the noise at D_i, C, and E are normalized to unity and $\overline{\gamma}_{d_i}$ = $\overline{\gamma}_d$. Unless mentioned otherwise, $\bar{\gamma}_{bd}$ is set to 5 dB.

Figure 4.5 shows the exact (simulation) and approximate (analysis) outage probability, P_{out}, for D2D communications versus $\bar{\gamma}_d$ for different values of N. In this figure, it can be seen that the exact and approximate outage probabilities match, particularly at high $\bar{\gamma}_d$ values. Additionally, from Fig. 4.5, we can see that P_{out} decreases monotonically as $\bar{\gamma}_d$

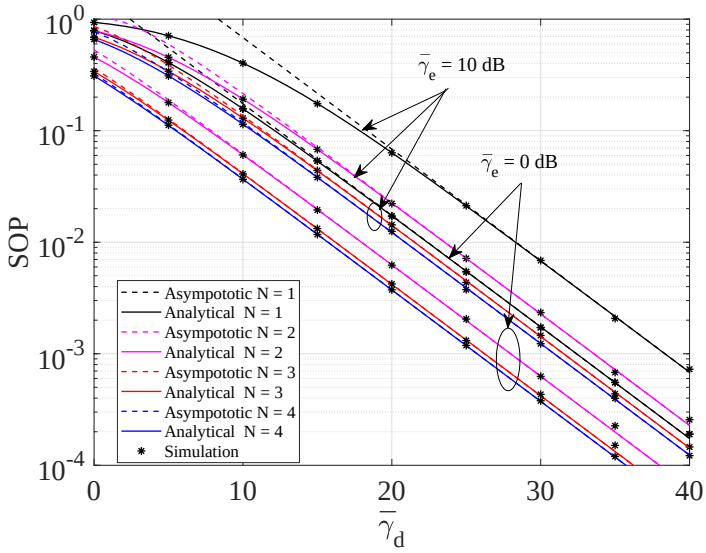


Fig. 4.6: The analytical and Monte-Carlo simulation for the SOP vs $\bar{\gamma}_d$ for different N where $R_s = 1$ b/s/Hz.

decreases without any outage floor. Another interesting point is that P_{out} decreases with increasing number of relays. Furthermore, the direct link scenario (N = 1) is depicted for comparison purposes and clearly shows the advantage of using relays.

To evaluate the effect of the multihop D2D relaying scenario on the secrecy performance of the D2D communications, Fig. 4.6 presents SOP versus $\bar{\gamma}_d$, for different values of $\bar{\gamma}_e$ and N. Without loss of generality, $\bar{\gamma}_e$ is set to 10 dB and 0 dB and we set R_s at 1 b/s/Hz. It can be noticed from this figure that SOP decreases as $\bar{\gamma}_d$ increases and $\bar{\gamma}_e$ decreases, as expected. Additionally, it can clearly be observed that SOP increases as N decreases given the fact that the secrecy capacity is improved with increasing N. Moreover, the asymptotic curves are plotted where a very tight agreement with the exact analysis is observed at high $\overline{\gamma}_d$. Again, perfect match between the analytical and the simulation results is observed, validating the accuracy of our analysis.

Finally, to evaluate the probability of non-zero secrecy capacity, PNSC, under the proposed underlay multihop D2D relaying scheme, Fig. 4.7 shows PNSC versus $\bar{\gamma}_d$. As can be noticed from this figure, the PNSC increases with increasing $\bar{\gamma}_d$ for a fixed $\bar{\gamma}_e$. Nevertheless,

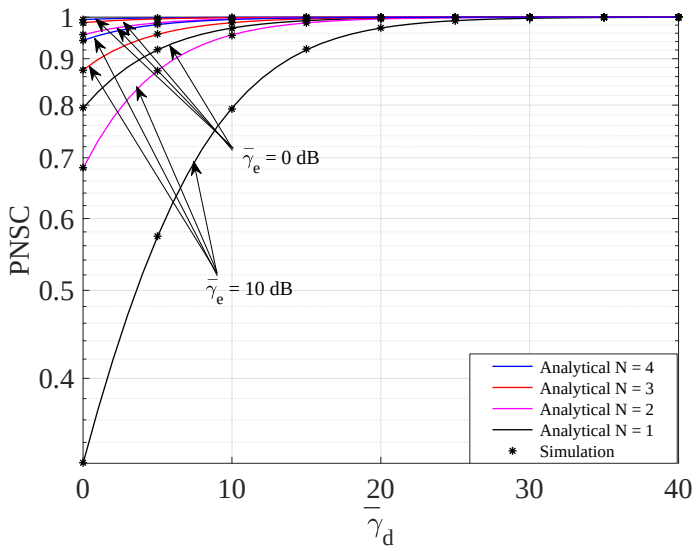


Fig. 4.7: The analytical and Monte-Carlo simulation plots for the PNSC vs $\bar{\gamma}_d$ for different N where $\bar{\gamma}_b$= 5 dB.

the PNSC decreases with decreasing $\bar{\gamma}_e$. It is worth mentioning that even when $\bar{\gamma}_d < \bar{\gamma}_e$, a secrecy capacity exists. Additionally, we also observe that the PNSC increases as N increases. Numerical results are observed to match the simulation results, corroborating once more our analysis.

4.8 Conclusion

In this chapter, the ORS and SRS schemes are utilized to enhance the inband underlay D2D secrecy performance. Two practical combining approaches, MRC and SC, are used to increase the eavesdropped signals. For combining techniques as well as relay selection schemes, new closed-form expressions for the D2D SOP and the PNSC are derived. Most noteworthy in the obtained results is the fact that the ORS scheme always outperforms the SRS scheme, assuming that the CSI of the wiretapped link is available. That is, the ORS guarantees the optimal secrecy performance for D2D communications. Additionally, the impact of D2D relays is investigated. It is observed, under these combining techniques,

that increasing N_R enhances the D2D secrecy performance. The asymptotic results, which give a better understanding of the influence of the main system parameters on the SOP, are provided. As revealed in our analysis and confirmed through simulations, the diversity order is equal to N_R for both combining approaches and relay selection schemes. These results also show that N_E does not influence the diversity order. Moreover, we verified that, under both ORS and SRS schemes, increasing N_E degrades the secrecy performance of D2D communications. Furthermore, the various Monte-Carlo simulations corroborate the provided analysis, validating the later.

The secrecy performance of underlay multihop D2D relaying is studied where closed-form expressions for the outage probability, the SOP and the probability of non-zero secrecy capacity are derived. Simulation results, validating the derived analytical expressions, are provided. The results revealed the effect of the different number of D2D multihop relays on the security level of the D2D communications.

4.9 Appendices

4.9.1 Appendix A

Derivation of Lemma 1

The expression $\mathcal{P}_k^{\upsilon}$ can be obtained by

$$\mathcal{P}_k^{\upsilon} = \int_0^{\infty} F_{\gamma_{R_k D}}\left(\beta\,\gamma + \alpha\right)\, f_{\gamma_{R_k E}}^{\upsilon}(\gamma)\, d\gamma, \tag{4.69}$$

where $\beta = 2^{\mathcal{R}_s}$ and $\alpha = \beta - 1$. The PDF of $\gamma_{R_k E}$ for MRC can be derived using [18] as

$$f_{\gamma_{R_k E}}^{\text{MRC}}(\gamma) = \int_0^{\infty} (\zeta + 1)\, f_{\gamma_e}^{\text{MRC}}(\gamma(\zeta + 1))\, f_{\gamma_{be}}(\zeta)\, d\zeta, \tag{4.70}$$

where $f_{\gamma_e}^{\text{MRC}}(.)$ is given by

$$f_{\gamma_e}^{\text{MRC}}(\gamma) = \frac{\gamma^{N_E - 1}}{\Gamma(N_E)\,\omega_3^{N_E}} \exp\left(\frac{-\gamma}{\omega_3}\right), \tag{4.71}$$

and $f_{\gamma_{be}}(.)$ is given by

$$f_{\gamma_{be}}(\gamma) = \frac{1}{\omega_4} \exp\left(-\frac{\gamma}{\omega_4}\right). \tag{4.72}$$

By plugging (4.71) and (4.72) into (4.70), $f_{\gamma_{R_k E}}^{\text{MRC}}(\gamma)$ is obtained as

$$f_{\gamma_{R_k E}}^{\text{MRC}}(\gamma) = \frac{\gamma^{N_E - 1} \exp\left(-\frac{\gamma}{\omega_3}\right)}{\Gamma(N_E)\,\omega_3^{N_E}\omega_4} \sum_{m=0}^{N_E} \binom{N_E}{k} \frac{\Gamma(m+1)}{\left(\frac{\gamma}{\omega_3} + \frac{1}{\omega_4}\right)^{m+1}}. \tag{4.73}$$

By substituting (4.10) and (4.73) in (4.69), with the help of the partial fraction expansion, then using [16, eq. (1.111)], [16, eq. (3.383.4)], [16, eq. (3.383.10)], and [16, eq. (3.381.3)], $\mathcal{P}_k^{\text{MRC}}$ can be derived as in (4.12).

4.9.2 Appendix B

Derivation of Lemma 2

The PDF of $\gamma_{R_k E}$, $f^{\text{SC}}_{\gamma_{R_k E}}(\gamma)$, can be derived using [18] as

$$f^{\text{SC}}_{\gamma_{R_k E}}(\gamma) = \int_0^{\infty} (\zeta + 1)\, f^{\text{SC}}_{\gamma_e}(\gamma\,(\zeta + 1))\, f_{\gamma_{be}}(\zeta)\, d\zeta, \tag{4.74}$$

where $f^{\text{SC}}_{\gamma_e}(.)$ is given by

$$f^{\text{SC}}_{\gamma_e}(\gamma) = \frac{N_E}{\omega_3} \sum_{m=0}^{N_E-1} (-1)^m \binom{N_E - 1}{m} \exp\left(-\frac{\gamma\,(m+1)}{\omega_3}\right). \tag{4.75}$$

By plugging (4.75) and (4.72) into (4.74), we get $f^{\text{SC}}_{\gamma_{R_k E}}(\gamma)$ as

$$f^{\text{SC}}_{\gamma_{R_k E}}(\gamma) = \frac{N_E}{\omega_3\,\omega_4} \sum_{m=0}^{N_E-1} (-1)^m \binom{N_E - 1}{m} \frac{\exp\left(-\frac{\gamma\,(m+1)}{\omega_3}\right)\left(1 + \frac{\gamma(m+1)}{\omega_3} + \frac{1}{\omega_4}\right)}{\left(\frac{\gamma(m+1)}{\omega_3} + \frac{1}{\omega_4}\right)^2}. \tag{4.76}$$

By plugging (4.10) and (4.76) into (4.69), and with the help of the partial fraction expansion, then with the help of [16, eq. (3.353.3)], and [16, eq. (3.352.4)], $\mathcal{P}^{\text{SC}}_k$ can be obtained as in (4.14).

4.9.3 Appendix C

Derivation of Lemma 3

The $\text{SOP}^{\text{SRS}}_{\text{MRC}}$ can be obtained by plugging (4.73) and (4.18) in (4.19), and after simple

algebraic manipulations, it can be expressed as

$$\text{SOP}_{\text{MRC}}^{\text{SRS}} = N_R \sum_{k=0}^{N_R-1} \frac{(-1)^k \binom{N_R-1}{k}}{(k+1)} \left[1 - \sum_{m=0}^{N_E} \frac{\binom{N_E}{m} \Gamma(m+1)\, \omega_1 \exp\left(-\frac{(k+1)\,\alpha}{\omega_1}\right)}{\Gamma(N_E)\, \omega_3^{N_E-(m+1)}\, \omega_2\, \omega_4\, \beta\, (k+1)} \left\{ \underbrace{\int_0^{\infty} \frac{\gamma^{N_E-1} \exp\left(-\mathcal{H}_1 \gamma\right)}{\left(\mathcal{H}_2+\gamma\right)^{m+1} \left(\mathcal{H}_3+\gamma\right)} d\gamma}_{\mathcal{I}} \right\} \right], \tag{4.77}$$

where $\mathcal{H}_1 = \frac{\beta(k+1)}{\omega_1} + \frac{1}{\omega_3}$, $\mathcal{H}_2 = \frac{\omega_3}{\omega_4}$, and $\mathcal{H}_3 = \frac{1}{\beta}\left(\alpha + \frac{\omega_1}{\omega_2(k+1)}\right)$. In what follows, the integral in (4.77), $\mathcal{I}$, is evaluated. First, $\mathcal{I}$ can be rewritten in a more general form as

$$\mathcal{I} = \int_0^{\infty} \frac{\gamma^{N_E-1}}{\exp\left(\mathcal{H}_1 \gamma\right)} \underbrace{\frac{1}{\left(\mathcal{H}_2+\gamma\right)^s \left(\mathcal{H}_3+\gamma\right)^z}}_{\Delta} d\gamma. \tag{4.78}$$

The partial fraction expansion is utilized in (4.78) to obtain

$$\Delta = \sum_{i=1}^{s} \frac{\mathcal{Q}_i}{\left(\mathcal{H}_2+\gamma\right)^i} + \sum_{j=1}^{z} \frac{\mathcal{U}_j}{\left(\mathcal{H}_3+\gamma\right)^j}, \tag{4.79}$$

where

$$\mathcal{Q}_i = \frac{(-1)^z}{\left(\mathcal{H}_2-\mathcal{H}_3\right)^{s+z-i}} \left[(1-\zeta_1) + \zeta_1 \sum_{p_n=1}^{s+1-i} \cdots \sum_{p_1=1}^{p_2} (1) \right],$$

where $n = z-1$, and

$$\zeta_1 = \begin{cases} 0, & z = 1, \\ 1, & \text{elsewhere,} \end{cases}$$

and

$$\mathcal{U}_j = \frac{(-1)^{z-j}}{\left(\mathcal{H}_2-\mathcal{H}_3\right)^{s+z-j}} \left[(1-\zeta_2) + \zeta_2 \sum_{p_q=1}^{c+1-j} \cdots \sum_{p_1=1}^{p_2} (1) \right],$$

where $q = s - 1$, and

$$\zeta_2 = \begin{cases} 0, & s = 1, \\ 1, & \text{elsewhere.} \end{cases}$$

By plugging (4.79) into (4.78), we get

$$\mathcal{I} = \int_0^{\infty} \frac{\gamma^{N_E - 1}}{\exp\left(\mathcal{H}_1 \gamma\right)} \left(\sum_{i=1}^{s} \frac{\mathcal{Q}_i}{\left(\mathcal{H}_2 + \gamma\right)^i} + \sum_{j=1}^{z} \frac{\mathcal{U}_j}{\left(\mathcal{H}_3 + \gamma\right)^j} \right) d\gamma. \tag{4.80}$$

From (4.78), we have $s = m + 1$ and $z = 1$. With the help of [16, eq. (3.383.4)], $\mathcal{I}$ can be obtained. Then, by plugging the result of $\mathcal{I}$ into (4.77), and after simple algebraic manipulations, $\text{SOP}_{\text{MRC}}^{\text{SRS}}$ can be derived as in (4.20).

4.9.4 Appendix D

Derivation of Lemma 4

The $\text{SOP}_{\text{SC}}^{\text{SRS}}$ can be obtained by substituting (4.76) and (4.18) in (4.21), and following a similar procedure in the derivation of Lemma 3, then using [16, eq. (3.353.3)] and [16, eq. (3.352.4)], $\text{SOP}_{\text{SC}}^{\text{SRS}}$ can be obtained as in (4.22).

References

[1] *Cisco Annual Internet Report (2018–2023) White Paper.*, "Available [Online]: http://goo.gl/ylTuVx, Mar. 2020.

[2] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Nov. 2013.

[3] J. Zhu, Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Security reliability trade-off analysis of multirelay-aided decode-and-forward cooperation systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5825–5831, Jul. 2015.

[4] R. Ma, N. Xia, H.-H. Chen, C.-Y. Chiu, and C.-S. Yang, "Mode selection, radio resource allocation, and power coordination in D2D communications," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 112–121, Feb. 2017.

[5] R. Ma, Y.-J. Chang, H.-H. Chen, and C.-Y. Chiu, "On relay selection schemes for relay-assisted D2D communications in LTE-A systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8303–8314, Sep. 2017.

[6] M. Hasan, E. Hossain, and D. I. Kim, "Resource allocation under channel uncertainties for relay-aided device-to-device communication underlaying lte-a cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2322–2338, Apr. 2014.

[7] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, “Resource management for device-to-device communication: A physical layer security perspective,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 946–960, Apr. 2018.

[8] W. Wang, K. C. Teh, and K. H. Li, “Enhanced physical layer security in D2D spectrum sharing networks,” *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 106–109, Dec. 2016.

[9] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, “Secure transmission in wiretap channels using full-duplex relay-aided D2D communications with outdated CSI,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 8, pp. 1216–1220, Aug. 2020.

[10] R. Zhao, H. Lin, Y.-C. He, D.-H. Chen, Y. Huang, and L. Yang, “Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI,” *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 546–559, Feb. 2018.

[11] M. A. Kishk and H. S. Dhillon, “Stochastic geometry-based comparison of secrecy enhancement techniques in D2D networks,” *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 394–397, Jun. 2017.

[12] Z. Chu, H. X. Nguyen, T. A. Le, M. Karamanoglu, E. Ever, and A. Yazici, “Secure wireless powered and cooperative jamming d2d communications,” *IEEE Trans. Green Commun. Netw.*,vol. 2, no. 1, pp. 1–13, Mar. 2018.

[13] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, “Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective,” *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 623–638, Jan. 2019.

[14] M. H. Khoshafa, T. Ngatched, and M. H. Ahmed, “On the physical layer security of underlay relay-aided device-to-device communications,” *IEEE Trans. Veh. Tech.*,vol. 69, pp. 7609–7621, Jul. 2020.

[15] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, “Relay-selection improves the security-reliability trade-off in cognitive radio systems,” *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Dec. 2014.

[16] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, “Secrecy outage performance of transmit antenna selection for mimo underlay cognitive radio systems over Nakagami-m channels,” *IEEE Trans. Veh. Technol.*,vol. 66, no. 3, pp. 2237–2250, Mar. 2017.

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

[18] 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, Nov. 2014.

[19] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*, McGraw-Hill Education, 2002.

[20] G. Kramer, M. Gastpar, and P. Gupta, “Cooperative strategies and capacity theorems for relay networks,” *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3037–3063, Sep. 2005.

[21] F. S. Shaikh and R. Wismuller, “Routing in multi-hop cellular device-todevice (d2d) networks: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 3, no. 1, pp. 120–154, Jun. 2018.

[22] D. Ebrahimi, H. Elbiaze, and W. Ajib, “Device-to-device data transfer through multi-hop relay links underlaying cellular networks,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9669–9680, Oct. 2018

[23] R. Ma, N. Xia, H.-H. Chen, C.-Y. Chiu, and C.-S. Yang, “Mode selection, radio resource allocation, and power coordination in D2D communications,” *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 112–121, Jun. 2017.

[24] W. Wang, K. C. Teh, and K. H. Li, “Enhanced physical layer security in D2D spectrum sharing networks,” *IEEE Wireless Commun. Lett*, vol. 6, no. 1, pp. 106–109, Feb. 2017.

[25] J. Yue, C. Ma, H. Yu, and W. Zhou, “Secrecy-based access control for device-to-device communication underlaying cellular networks,” *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.

[26] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, “Resource management for device-to-device communication: A physical layer security perspective,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 946–960, April 2018.

[27] S. S. Ikki and S. Aissa, “Multihop wireless relaying systems in the presence of cochannel interferences: Performance analysis and design optimization,” *IEEE Trans. Veh. Technol.*, vol. 61, no. 2, pp. 566–573, Feb. 2012.

[28] V. N. Q. Bao, T. Q. Duong, and C. Tellambura, “On the performance of cognitive underlay multihop networks with imperfect channel state information,” *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4864–4873, Dec. 2013.

Chapter 5

Secure Underlay CR Networks with EH and Dual-Antenna Selection

5.1 Abstract

In this chapter, we consider a secure underlay cognitive radio network consisting of a secondary source-destination pair and a primary transmitter-receiver pair in the presence of a primary passive eavesdropper. Herein, a secondary multi-antenna full-duplex destination node acts as a jammer to the primary eavesdropper in an effort to improve the physical layer security of the primary network. In return for this favor, the energy constrained secondary source gets access to the primary network to transmit its own information so long as the interference to the latter is below a certain level. In light of the aforementioned, we evaluate the system performance in terms of the outage probability for the secondary network, the secrecy outage probability, and the probability of non-zero secrecy capacity for the primary network. Numerical results are provided to verify the correctness of the proposed analytical framework.

5.2 Introduction

In recent years, energy harvesting (EH) and cognitive radio (CR) concepts have attracted considerable attention in the research community, for providing perpetual power supply and improving the spectrum utilization efficiency, respectively. In the CR concept, there exist three main paradigms, viz. underlay, overlay and interweave. Among the above-cited ways of accessing the licensed spectrum, the underlay scheme is the most popular due to its simplicity and practical implementation. Based on the advantages of these two technologies, the use of EH in the context of underlay CR networks has recently been investigated in [1], [2], [3], [4]. Besides the aggregated advantages of EH in CR networks, achieving secure communications of the secondary network or primary network via information theoretic-based PLS has been the focus in [1], [2], [3], [4]. Particularly, cooperation between the primary system and energy-constrained secondary network is studied in [1]. The authors aim at improving the security of the information in the primary network when the secondary users (SUs) act as potential eavesdroppers. In [2], the authors propose an optimal antenna selection to improve the secrecy performance of the secondary network. The secrecy energy efficiency optimization problem for a multiple-input single-output (MISO) underlay CR network with an EH receiver is studied in [3]. In [4], a full-duplex transmission and dual-antenna selection in the secondary network is proposed in an effort to improve its data transmission as well as the secrecy performance of the primary network. This work provides a win-win situation for the secondary and primary networks in the sense that it yields data transmission improvement for the former and security provisioning for the latter. However, EH is not considered in [4] which can render the system impractical in commonly seen situations wherein the secondary source is an energy-constrained device (e.g., a wireless sensor node). Moreover, the constraint on the secondary transmit power assumed in [4] is rather simplistic as it does not take into account the effect of the maximum

transmit power (see [5] and the references therein).

Motivated by the preceding discussion, we investigate a secure underlay CR network with energy harvesting over Rayleigh fading channels. Specifically, we consider a scenario wherein EH and dual-antenna selection are employed to enhance the robustness and reliability of the CR network, while simultaneously improving the PLS of the primary network by confounding the eavesdropper. In this respect, we derive novel closed-form expressions of the outage probability for the CR network, the SOP and the PNSC for the primary network. Moreover, the asymptotic analysis is provided to get more insights into the impact of the significant parameters of the proposed system on the performance of the SOP for the primary network. The accuracy of our analysis is verified through extensive Monte-Carlo simulations.

5.3 System Model

As shown in Fig. 5.1, we consider an underlay cognitive network which shares the licensed spectrum of the primary user, PR, and consists of a source node, S, and a destination node, D. In the primary network, a primary transmitter, denoted by PT, communicates with a primary receiver, PR, under malicious attempt of an eavesdropper, E. All the nodes are equipped with a single antenna except D, which operates in a full-duplex and is equipped with N_R receive antennas and N_T transmit antennas. We consider a scenario where S is an energy-constrained device, i.e., the transmission can be achieved using power harvested from the power beacon (PB). Furthermore, we indicate D_i as the i^{th} receiving antenna of D, where $i = 1, ..., N_R$. In a similar manner, D_j denotes the j^{th} jamming antenna of D, where $j = 1, ..., N_T$. All the channels are assumed to undergo Rayleigh fading. The channels PB$\rightarrow$S, S$\rightarrow\mathrm{D}_i$, $\mathrm{D_j}\rightarrow$E, $\mathrm{D_j}\rightarrow$PR, S$\rightarrow$PR, $\mathrm{D}_i\rightarrow\mathrm{D_j}$, PT$\rightarrow$PR, S$\rightarrow$E, and PT$\rightarrow$E are assumed to consist of path loss and an independent fading effect as h_{S},

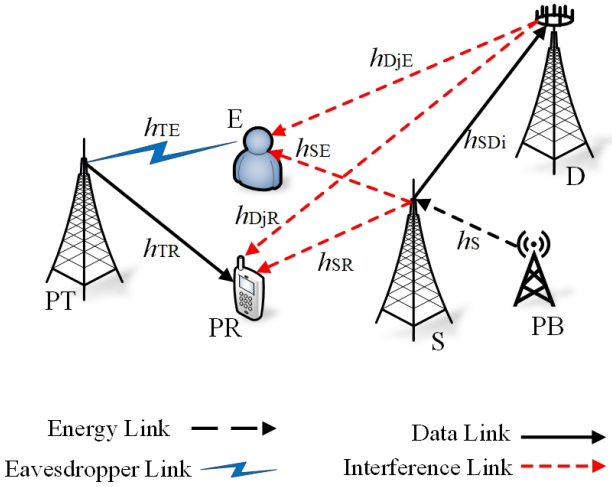


Fig. 5.1: Underlay Cognitive Radio Network.

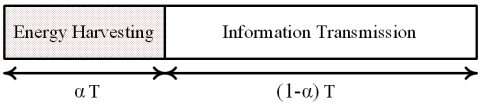


Fig. 5.2: TS-based EH protocol.

h_{SD_i}, $h_{\mathrm{D_jE}}$, $h_{\mathrm{D_jR}}$, h_{SR}, $h_{\mathrm{D}_i\mathrm{D_j}}$, h_{TR}, h_{SE}, and h_{TE}, respectively. In this respect, $h_\upsilon = \chi_\upsilon\, d_\upsilon^{-\frac{\eta}{2}}$, $\upsilon \in \{\mathrm{S}, \mathrm{SD}_i, \mathrm{D_jR}, \mathrm{D_jE}, \mathrm{SR}, \mathrm{D}_i\mathrm{D_j}, \mathrm{TR}, \mathrm{SE}, \text{and } \mathrm{TE}\}$, where d and η denote the Euclidean distances between two nodes and the pathloss exponent, respectively, and χ_υ is the fading coefficient which is a complex Gaussian random variable with unit variance. Also, $Y_\upsilon = |h_\upsilon|^2$ represents the channel power gains, which are independent and exponentially distributed with a mean $\lambda_\upsilon = \mathbb{E}[|h_\upsilon|^2] = d_\upsilon^{-\eta}$. Moreover, n_ξ is the AWGN, where $\xi \in \{\mathrm{D}_i, \mathrm{PR}, \mathrm{E}\}$, with a zero mean and variance σ_ξ^2. As shown in Fig. 5.4, a time-switching (TS) protocol [6] is considered in this work, where the time durations for the EH and information transmission (IT) phases are given by α and $(1-\alpha)$, respectively, with $0 \leq \alpha \leq 1$.

5.4 Secondary Transmission

5.4.1 Energy harvesting

It is assumed that the PB operates on a frequency band which is different from the communication band where the primary and secondary transmissions take place [7]. Hence, the power transmitted by the PB does not interfere with the primary and secondary transmissions. In the EH phase, S harvests energy from the radio frequency (RF) signal received from the PB, and the harvested energy can be written as

$$E_{\mathrm{S}} = \zeta \alpha \, T \, P_{\mathrm{PB}} Y_{\mathrm{S}}, \tag{5.1}$$

where ζ is the EH efficiency, T is the dedicated time slot, P_{PB} is the transmit power at PB, $Y_{\mathrm{S}} = |h_{\mathrm{S}}|^2$ is the channel fading coefficient of the PB$\rightarrow$S link. The PDF and CDF of Y_{υ} can be presented, respectively, as

$$f_{Y_{\upsilon}}(\gamma) = \frac{1}{\lambda_{\upsilon}} \exp\Big(- \frac{\gamma}{\lambda_{\upsilon}}\Big), \tag{5.2}$$

$$F_{Y_{\upsilon}}(\gamma) = 1 - \exp\Big(- \frac{\gamma}{\lambda_{\upsilon}}\Big). \tag{5.3}$$

The maximal transmit power at S is given by

$$P_{\max} = \frac{\zeta \, \alpha \, P_{\mathrm{PB}} Y_{\mathrm{S}}}{(1-\alpha)}. \tag{5.4}$$

5.4.2 Information Transmission

In the IT phase (for secondary transmissions), S transmits to D under interference power constraints and the transmit power is given by

$$P_{\mathrm{S}} = \min\left(P_{\max}, \frac{\mathcal{Q}}{Y_{\mathrm{SR}}}\right), \tag{5.5}$$

where $P_{\max}$ represents the maximum allowable transmit power at the source node, and $\mathcal{Q}$ is the interference temperature limit, which represents the maximum tolerated interference power at PR. In the secondary network, the communication takes place between S and the best receiving antenna chosen among the N_R antennas of D. Consider a communication taking place between S and the i^{th} receive antenna of D. Hence, the received signal at D is given by

$$y_{\mathrm{SD}_i} = \sqrt{P_{\mathrm{S}}}\, h_{\mathrm{SD}_i}\, x_{\mathrm{S}} + \underbrace{\sqrt{P_{\mathrm{D}_j}}\, h_{\mathrm{D}_j\mathrm{D}_i} x_{\mathrm{D}}}_{\text{residual self-interference}} + n_{\mathrm{D}i}, \tag{5.6}$$

where P_{S} and P_{D_j} are the transmit powers at S and the j^{th} antenna of D, respectively. Moreover, x_{S} and x_{D} are the signals transmitted from S and the j^{th} transmit antenna of D, respectively. At D, it is assumed that the interference from PT to D is negligible. This widely used assumption can be justified because the PT is far away [8], [9]. The capacity for receiving the data at the i^{th} receive antenna of D is given by

$$C_{\mathrm{SD}_i} = \log_2\left(1 + \frac{P_{\mathrm{S}} Y_{\mathrm{SD}_i}}{P_{\mathrm{D_j}} Y_{\mathrm{D}_i\mathrm{D_j}} + \sigma^2_{\mathrm{D}_i}}\right). \tag{5.7}$$

It is possible to suppress the self-interference (SI) to the noise level [10], and the residual SI term can be neglected [11]. Hence, C_{SD_i} can be approximated by

$$C_{\mathrm{SD}_i} \approx \log_2\left(1 + \frac{P_{\mathrm{S}} Y_{\mathrm{SD}_i}}{\sigma^2_{\mathrm{D}_i}}\right). \tag{5.8}$$

The best receive antenna is selected according to the following criterion

$$i^* = \arg \max_{i=1,\ldots,N_R} C_{\mathrm{SD}_i} = \arg \max_{i=1,\ldots,N_R} Y_{\mathrm{SD}_i}. \tag{5.9}$$

5.4.3 CR Outage Probability

The CR outage probability, P_{out}, is defined by

$$P_{out} = \Pr\left(\max_{i=1..N_R} C_{\mathrm{SD}_i} \leq \mathcal{R}_b\right) = \prod_{i=1}^{N_R} \underbrace{\Pr\left(\frac{P_{\mathrm{S}} Y_{\mathrm{SD}_i}}{\sigma^2_{\mathrm{D}_i}} \leq \vartheta_b\right)}_{\mathcal{P}_i}, \tag{5.10}$$

where $\mathcal{R}_b$ is the data rate, and $\vartheta_b = 2^{\mathcal{R}_b} - 1$. Now, $\mathcal{P}_i$ can be expressed as

$$\begin{aligned}
\mathcal{P}_i &= \Pr\left(Y_{\mathrm{SD}_i} \leq \frac{\vartheta_b\, \sigma^2_{\mathrm{D}_i}}{P_{\mathrm{S}}}, P_{\mathrm{S}} = P_{\max}\right) + \Pr\left(Y_{\mathrm{SD}_i} \leq \frac{\vartheta_b\, \sigma^2_{\mathrm{D}_i}}{P_{\mathrm{S}}}, P_{\mathrm{S}} = \frac{\mathcal{Q}}{Y_{\mathrm{SR}}}\right) \\
&= \Pr\left(Y_{\mathrm{SD}_i} \leq \frac{\vartheta_b\, \sigma^2_{\mathrm{D}_i}}{P_{\max}}, Y_{\mathrm{SR}} \leq \frac{\mathcal{Q}}{P_{\max}}\right) + \Pr\left(Y_{\mathrm{SD}_i} \leq \frac{\vartheta_b\, \sigma^2_{\mathrm{D}_i}\, Y_{\mathrm{SR}}}{\mathcal{Q}}, Y_{\mathrm{SR}} > \frac{\mathcal{Q}}{P_{\max}}\right) \\
&= \underbrace{\Pr\left(Y_{\mathrm{SD}_i} \leq \frac{\varphi_1}{Y_{\mathrm{S}}}, Y_{\mathrm{SR}} \leq \frac{\varphi_2}{Y_{\mathrm{S}}}\right)}_{\mathcal{I}_1} + \underbrace{\Pr\left(Y_{\mathrm{SD}_i} \leq \varphi_3\, Y_{\mathrm{SR}}, Y_{\mathrm{S}} > \frac{\varphi_2}{Y_{\mathrm{SR}}}\right)}_{\mathcal{I}_2},
\end{aligned} \tag{5.11}$$

where $\varphi_1 = \frac{\vartheta_b\, \sigma^2_{\mathrm{D}_i}\, (1-\alpha)}{\zeta\, \alpha\, P_{\mathrm{PB}}}$, $\varphi_2 = \frac{\mathcal{Q}\,(1-\alpha)}{\zeta\, \alpha\, P_{\mathrm{PB}}}$, and $\varphi_3 = \frac{\vartheta_b\, \sigma^2_{\mathrm{D}_i}}{\mathcal{Q}}$. From (5.11), $\mathcal{I}_1$ can be rewritten as

$$\mathcal{I}_1 = \int_0^\infty F_{Y_{\mathrm{SR}}}\left(\frac{\varphi_2}{\gamma}\right) F_{Y_{\mathrm{SD}_i}}\left(\frac{\varphi_1}{\gamma}\right) f_{Y_{\mathrm{S}}}(\gamma)\, d\gamma. \tag{5.12}$$

By plugging (5.2) and (5.3) into (5.12) with the help of [12, eq. (3.324.1)], $\mathcal{I}_1$ can be derived as

$$\begin{aligned}
\mathcal{I}_1 = \frac{1}{\sqrt{\lambda_{\mathrm{S}}}} \Bigg[&\sqrt{\lambda_{\mathrm{S}}} - 2\sqrt{\frac{\varphi_1}{\lambda_{\mathrm{SD_i}}}}\, K_1\left(2\sqrt{\frac{\varphi_1}{\lambda_{\mathrm{S}}\lambda_{\mathrm{SD_i}}}}\right) \\
&-2\sqrt{\frac{\varphi_2}{\lambda_{\mathrm{SR}}}}\, K_1\left(2\sqrt{\frac{\varphi_2}{\lambda_{\mathrm{S}}\lambda_{\mathrm{SR}}}}\right) + 2\sqrt{\mathcal{Z}_1}\, K_1\left(2\sqrt{\frac{\mathcal{Z}_1}{\lambda_{\mathrm{S}}}}\right) \Bigg],
\end{aligned} \tag{5.13}$$

where $\mathcal{Z}_1 = \left(\frac{\varphi_1}{\lambda_{\mathrm{SD}_i}} + \frac{\varphi_2}{\lambda_{\mathrm{SR}}}\right)$, and $K_1(.)$ is the modified Bessel function of the second kind [12, eq. (8.446)]. From (5.11), $\mathcal{I}_1$ can be rewritten as

$$\mathcal{I}_2 = \int_0^\infty \left(1 - F_{Y_{\mathrm{S}}}\left(\frac{\varphi_2}{\gamma}\right)\right) F_{Y_{\mathrm{SD}_i}}\left(\varphi_3\,\gamma\right) f_{Y_{\mathrm{SR}}}\left(\gamma\right)\, d\gamma. \tag{5.14}$$

By plugging (5.2) and (5.3) into (5.14), and with the help of [12, eq. (3.324.1)], $\mathcal{I}_2$ can be derived as

$$\begin{aligned}\mathcal{I}_2 = \frac{2}{\mathcal{Z}_2}\sqrt{\frac{\varphi_2}{\lambda_{\mathrm{S}}}}\Bigg[\frac{\mathcal{Z}_2}{\sqrt{\lambda_{\mathrm{SR}}}}\, K_1\left(2\sqrt{\frac{\varphi_2}{\lambda_{\mathrm{S}}\lambda_{\mathrm{SR}}}}\right) - \lambda_{\mathrm{SD}_i}\sqrt{\left(\frac{\varphi_3}{\lambda_{\mathrm{SD}_i}} + \frac{1}{\lambda_{\mathrm{SR}}}\right)} \\ \times K_1\left(2\sqrt{\frac{\varphi_2}{\lambda_{\mathrm{S}}}\left(\frac{\varphi_3}{\lambda_{\mathrm{SD}_i}} + \frac{1}{\lambda_{\mathrm{SR}}}\right)}\right)\Bigg],\end{aligned} \tag{5.15}$$

where $\mathcal{Z}_2 = \left(\varphi_3\lambda_{\mathrm{SR}} + \lambda_{\mathrm{SD}_i}\right)$. Now, $\mathcal{P}_i$ is obtained by substituting (5.13) and (5.15) into (5.11). Thus, P_{out} can be obtained by plugging $\mathcal{P}_i$ into (5.10).

5.5 Primary Network

In the primary network, PT communicates with PR in the presence of E. Hence, the received signal at PR is given by

$$y_{\mathrm{PR}} = \sqrt{P_{\mathrm{PT}}}\, h_{\mathrm{TR}}\, x_{\mathrm{P}} + \sqrt{P_{\mathrm{D_j}}}\, h_{\mathrm{D_jR}}\, x_{\mathrm{D}} + \sqrt{P_{\mathrm{S}}}\, h_{\mathrm{SR}}\, x_{\mathrm{S}} + n_{\mathrm{PR}}, \tag{5.16}$$

where P_{PT} and x_{P} are the transmitted power and signal from PT, respectively. In the meantime, the eavesdropper overhears the primary transmissions and the best transmit antenna among the N_T antennas of D can confound the activities of E. The received signal at E

affected by the j^{th} antenna of D is given by

$$y_{\text{E}} = \sqrt{P_{\text{PT}}}\, h_{\text{TE}}\, x_{\text{P}} + \sqrt{P_{\text{D}_\text{j}}}\, h_{\text{D}_\text{j}\text{E}}\, x_{\text{D}} + \sqrt{P_{\text{S}}}\, h_{\text{SE}}\, x_{\text{S}} + n_{\text{E}}. \tag{5.17}$$

However, we assume that the S $\rightarrow$ E link is strong and thus E can first decode x_{S}. At this stage, the PT $\rightarrow$ E transmission is considered as interference. After that, E subtracts x_{S} term from its received signal at E, y_{E}, and decodes x_{P}. Thus, the received signal at E reduces to

$$y_{\text{E}} = \sqrt{P_{\text{PT}}}\, h_{\text{TE}}\, x_{\text{P}} + \sqrt{P_{\text{D}_\text{j}}}\, h_{\text{D}_\text{j}\text{E}}\, x_{D} + n_{\text{E}}. \tag{5.18}$$

The secrecy capacity, C_{S_j}, in the primary network when the j^{th} antenna of D is jamming E, is written as

$$C_{S_\text{j}} = \max\left[\log_2\left(1+\gamma_{\text{PRj}}\right) - \log_2\left(1+\gamma_{\text{Ej}}\right), 0\right], \tag{5.19}$$

where γ_{PRj} is given by

$$\gamma_{\text{PR}_\text{j}} = \frac{P_{\text{PT}} Y_{\text{TR}}}{P_{\text{D}_\text{j}} Y_{\text{D}_\text{j}\text{R}} + P_{\text{S}} Y_{\text{SR}} + \sigma^2_{\text{PR}}}. \tag{5.20}$$

In addition, $\gamma_{\text{E}_\text{j}}$ is given by

$$\gamma_{\text{E}_\text{j}} = \frac{P_{\text{PT}} Y_{\text{TE}}}{P_{\text{D}_\text{j}} Y_{\text{D}_\text{j}\text{E}} + \sigma^2_{\text{E}}}. \tag{5.21}$$

In the underlay CR system, the transmitted power from the secondary jamming antenna, P_{D_j}, must be under a certain level of interference. With this in mind, P_{D_j} and P_{S} can be constrained as $P_{\text{D}_\text{j}}\, Y_{\text{D}_\text{j}\text{R}} \leq \mathcal{Q}$ and $P_{\text{S}}\, Y_{\text{SR}} \leq \mathcal{Q}$, respectively. From the primary user perspective, setting $P_{\text{S}} = \frac{\mathcal{Q}}{Y_{\text{SR}}}$ is the worst case scenario which still guarantees its reliable operation. It is true that when $P_{\text{max}} < \frac{\mathcal{Q}}{Y_{\text{SR}}}$, P_{S} would be equal to P_{max}. But this would not affect the reliable operation of the primary user. In this sense, our expression can be viewed as an upper bound for the primary SOP and lower bound for the primary PNSC. Having said that it is important to note that, in practice, $P_{\text{max}} > \frac{\mathcal{Q}}{Y_{\text{SR}}}$ most of the time. Moreover, the exact analysis including the effect of P_{max} is not mathematically tractable. Then, replacing P_{D_j}

and P_{S} with $\frac{\mathcal{Q}}{Y_{\mathrm{D_jR}}}$ and $\frac{\mathcal{Q}}{Y_{\mathrm{SR}}}$, respectively, gives

$$\gamma_{\mathrm{PR_j}} = \frac{\omega_p \, Y_{\mathrm{TR}}}{2\mathcal{Q}_1 + 1}, \tag{5.22}$$

and

$$\gamma_{\mathrm{E_j}} = \frac{\omega_e \, Y_{\mathrm{TE}}}{\mathcal{Q}_2 \left(\frac{Y_{\mathrm{D_jE}}}{Y_{\mathrm{D_jR}}}\right) + 1}, \tag{5.23}$$

where $\omega_p = \frac{P_{\mathrm{PT}}}{\sigma^2_{\mathrm{PR}}}$, $\omega_e = \frac{P_{\mathrm{PT}}}{\sigma^2_{\mathrm{E}}}$, $\mathcal{Q}_1 = \frac{\mathcal{Q}}{\sigma^2_{\mathrm{PR}}}$, and $\mathcal{Q}_2 = \frac{\mathcal{Q}}{\sigma^2_{\mathrm{E}}}$. Let us define $\mathcal{A} = \frac{(2\mathcal{Q}_1+1)}{\omega_p}$. Considering the optimal antenna selection approach, in which the global CSI knowledge is known [13], [14], the selection criterion for the best transmit antenna at D is given by

$$j^* = \arg \max_{j=1,\ldots,N_T} C_{S_{\mathrm{j}}} = \arg \max_{j=1,\ldots,N_T} \left(\frac{Y_{\mathrm{D_jE}}}{Y_{\mathrm{D_jR}}}\right). \tag{5.24}$$

5.5.1 Secrecy Outage Probability

The SOP can be defined as the probability that the achievable secrecy rate is less than a predefined target secrecy rate, $\mathcal{R}_s$, for the cellular transmission, and is given by

$$\mathrm{SOP} = \Pr\left(C_{S_{\mathrm{j}}} \leq \mathcal{R}_s\right) = \Pr\left(\frac{1+\gamma_{\mathrm{PR_j}}}{1+\gamma_{\mathrm{E_j}}} \leq \vartheta_s\right), \tag{10}$$

where $\vartheta_s = 2^{\mathcal{R}_s}$. The CDF of $\gamma_{\mathrm{PR_j}}$, $F_{\gamma_{\mathrm{PR_j}}}(\gamma)$, is given by

$$F_{\gamma_{\mathrm{PR_j}}}(\gamma) = \left(1 - \exp\left(-\mathcal{A}\,\gamma/\lambda_{\mathrm{TR}}\right)\right). \tag{5.25}$$

The instantaneous end-to-end SINR at E can be rewritten as

$$\gamma_{\mathrm{E}_j} = \frac{X}{W+1}, \tag{5.26}$$

where $X = \omega_e\, Y_{\text{TE}}$ and

$$W = \mathcal{Q}_2 \max_{j=1,\ldots,N_T} \left(\frac{Y_{\text{D}_j\text{E}}}{Y_{\text{D}_j\text{R}}} \right), \tag{5.27}$$

where $f_W(\gamma)$ can be derived as

$$f_W(\gamma) = \frac{N_T\, \mathcal{Q}_2\, \lambda_{\text{D}_j\text{E}}\, \gamma^{N_T-1}}{\lambda_{\text{D}_j\text{R}} \left(\frac{\mathcal{Q}_2\, \lambda_{\text{D}_j\text{E}}}{\lambda_{\text{D}_j\text{R}}} + \gamma \right)^{N_T+1}}, \tag{5.28}$$

and $f_X(\gamma)$ is given by

$$f_X(\gamma) = \frac{1}{\lambda_{\text{TE}}\, \omega_e} \exp\left(-\frac{\gamma}{\lambda_{\text{TE}}\, \omega_e} \right). \tag{5.29}$$

The PDF of γ_{E_j}, $f_{\gamma_{\text{E}_j}}(\gamma)$, can be derived by using

$$f_{\gamma_{\text{E}_j}}(\gamma) = \int_0^\infty (\varsigma + 1)\; f_X(\gamma\,(\varsigma+1))\, f_W(\varsigma)\, d\varsigma. \tag{5.30}$$

By substituting (5.28) and (5.29) in (5.30), then evaluating the integration, $f_{\gamma_{\text{E}_j}}(\gamma)$ can be derived as

$$\begin{aligned} f_{\gamma_{\text{E}_j}}(\gamma) = \frac{N_T \exp\left(-\frac{\gamma}{\lambda_{\text{TE}}\, \omega_e} \right) \Gamma(N_T)}{\lambda_{\text{TE}}\, \omega_e} \Bigg[U\left(N_T, 0, \frac{\mathcal{Q}_2\, \lambda_{\text{D}_j\text{E}}\, \gamma}{\omega_e\, \lambda_{\text{TE}}\, \lambda_{\text{D}_j\text{R}}} \right) + \frac{N_T \mathcal{Q}_2\, \lambda_{\text{D}_j\text{E}}}{\lambda_{\text{D}_j\text{R}}} \\ \times U\left(N_T + 1, 1, \frac{\mathcal{Q}_2\, \lambda_{\text{D}_j\text{E}}\, \gamma}{\omega_e\, \lambda_{\text{TE}}\, \lambda_{\text{D}_j\text{R}}} \right) \Bigg], \end{aligned} \tag{5.31}$$

where $\Gamma(.)$ is the gamma function [12, eq. (8.310.1)] and $U(a, b, c)$ is the Tricomi confluent hypergeometric function [15, eq. (07.33.02.0001.01)], which can be represented in terms of the Meijer function as [15, eq. (07.33.26.0004.01)]

$$U(a, b, c) = \frac{1}{\Gamma(a)\, \Gamma(a - b + 1)}\, G_{1,2}^{2,1}\left(c \,\middle|\, \begin{matrix} 1-a \\ 0,\; 1-b \end{matrix} \right), \tag{5.32}$$

where $G_{p,q}^{m,n}(.)$ represents the Meijer *G*-function [12, eq. (9.301)]. The SOP is formulated

as

$$\text{SOP} = \int_0^{\infty} F_{\gamma_{\text{PR}_\text{j}}}(\beta\gamma + \delta)\, f_{\gamma_{\text{E}_\text{j}}}(\gamma)\, d\gamma, \tag{5.33}$$

where $\beta = 2^{\mathcal{R}_s}$, $\delta = \beta - 1$. By using (5.25) and (5.31), and with the help of [12, eq. (7.813.1)], the upper bound of SOP can be derived as

$$\begin{aligned}\text{SOP} = 1 - &\frac{N_T \exp\Big(-\frac{\mathcal{A}\,\delta}{\lambda_{\text{TR}}}\Big)\,\lambda_{\text{TR}}}{\Big(\mathcal{A}\,\beta\,\lambda_{\text{TE}}\,\omega_e + \lambda_{\text{TR}}\Big)\Gamma\Big(N_T+1\Big)}\left[G_{2,2}^{2,2}\left(\Xi \,\middle|\, \begin{matrix} 0,\, 1-N_T \\ 0,\, 1 \end{matrix}\right)\right. \\ &\left. + \frac{N_T\,\mathcal{Q}_2\,\lambda_{\text{D}_\text{j}\text{E}}\,\Gamma\Big(N_T\Big)}{\Gamma\Big(N_T+1\Big)\lambda_{\text{D}_\text{j}\text{R}}}\, G_{2,2}^{2,2}\left(\Xi \,\middle|\, \begin{matrix} 0,\, -N_T \\ 0,\, 0 \end{matrix}\right)\right],\end{aligned} \tag{5.34}$$

where $\Xi = \frac{\mathcal{Q}_2\,\lambda_{\text{D}_\text{j}\text{E}}\,\lambda_{\text{TR}}}{(\mathcal{A}\,\beta\,\lambda_{\text{TE}}\,\omega_e + \lambda_{\text{TR}})\lambda_{\text{D}_\text{j}\text{R}}}$.

5.5.2 Asymptotic Secrecy Outage Analysis

To acquire more insights on the system design, the asymptotic SOP, SOP$^{\infty}$, is examined as $\omega_p \to \infty$. SOP$^{\infty}$ can be written as

$$\text{SOP}^{\infty} = (\mathcal{G}_a \overline{\gamma}_d)^{-\mathcal{G}_d} + \mathcal{O}(\overline{\gamma}_d^{-\mathcal{G}_d}), \tag{5.35}$$

where $\mathcal{G}_d$ is the secrecy diversity order, $\mathcal{G}_a$ is the secrecy array gain, and $\mathcal{O}(.)$ is the higher order terms. Mathematically speaking, to derive the SOP$^{\infty}$, the asymptotic CDF, $F^{\infty}_{\gamma_{\text{PR}_\text{j}}}(\gamma)$, can be derived by following the same steps in the derivation of [17, eq. (42)]. By using $F^{\infty}_{\gamma_{\text{PR}_\text{j}}}(\gamma)$, and with the help of [18, eq. (07.34.16.0001.01)], and [12, eq. (7.813.1)], after

performing some algebraic manipulations, it turns out that $\mathcal{G}_d$ = 1 and $\mathcal{G}_a$ is given by

$$\mathcal{G}_a = \left[\Psi_1 \left(\Delta \left(\frac{1}{\Gamma\Big(N_T\Big)} G_{2,2}^{2,2}\left(\Psi_2 \,\middle|\, \begin{matrix} 0,\, 2-N_T \\ 1,\, 2 \end{matrix}\right) + \Psi_3\, G_{2,2}^{2,2}\left(\Psi_2 \,\middle|\, \begin{matrix} 0,\, 2-N_T \\ 1,\, 1 \end{matrix}\right)\right) + \delta\right)\right]^{-1}, \tag{5.36}$$

where $\Delta = \frac{N_T\,\beta\,\Gamma(N_T)\,\lambda_{\mathrm{D_jR}}\,\lambda_{\mathrm{TE}}\,\omega_e}{\mathcal{Q}_2\;\lambda_{\mathrm{D_jE}}\,\Gamma(N_T+1)}$, $\Psi_1 = \frac{(2\mathcal{Q}_1+1)}{\lambda_{\mathrm{TR}}}$, $\Psi_2 = \frac{\mathcal{Q}_2\,\lambda_{\mathrm{D_jE}}}{\lambda_{\mathrm{D_jR}}}$, and $\Psi_3 = \frac{N_T\,\mathcal{Q}_2\,\lambda_{\mathrm{D_jE}}}{\Gamma(N_T+1)\lambda_{\mathrm{D_jR}}}$.

5.5.3 Probability of Non-zero Secrecy Capacity

In this subsection, the requirement for the presence of the non-zero secrecy capacity is investigated. The non-zero secrecy capacity is obtained when $\gamma_{\mathrm{PR_j}} > \gamma_{\mathrm{E_j}}$. From (10), the PNSC is given by

$$\text{PNSC} = \Pr\left(\frac{1+\gamma_{\mathrm{PR_j}}}{1+\gamma_{\mathrm{E_j}}} > 1\right) = \Pr\left[\gamma_{\mathrm{PR_j}} > \gamma_{\mathrm{E_j}}\right] = 1 - \int_0^\infty F_{\gamma_{\mathrm{PR_j}}}(\gamma) f_{\gamma_{\mathrm{E_j}}}(\gamma)\, d\gamma. \tag{5.37}$$

By substituting $\beta = 1$ in (5.34), then plugging the result into PNSC, the lower bound PNSC can be obtained as

$$\text{PNSC} = \frac{N_T\,\Gamma\left(N_T\right)}{\Big(\mathcal{A}\,\omega_e + 1\Big)\Gamma\left(N_T+1\right)} \left[\frac{1}{\Gamma\left(N_T\right)} G_{2,2}^{2,2}\left(\Xi \,\middle|\, \begin{matrix} 0,\, 1-N_T \\ 0,\, 1 \end{matrix}\right) + \frac{N_T\,\mathcal{Q}}{\Gamma\Big(N_T+1\Big)} G_{2,2}^{2,2}\left(\Xi \,\middle|\, \begin{matrix} 0,\, -N_T \\ 0,\, 0 \end{matrix}\right)\right]. \tag{5.38}$$

5.6 Results and Discussions

In this section, the numerical results of the CR outage probability, the primary SOP, and the primary PNSC are presented and compared with those obtained through Monte-Carlo simulations. Unless otherwise stated, the numerical and simulation results are obtained

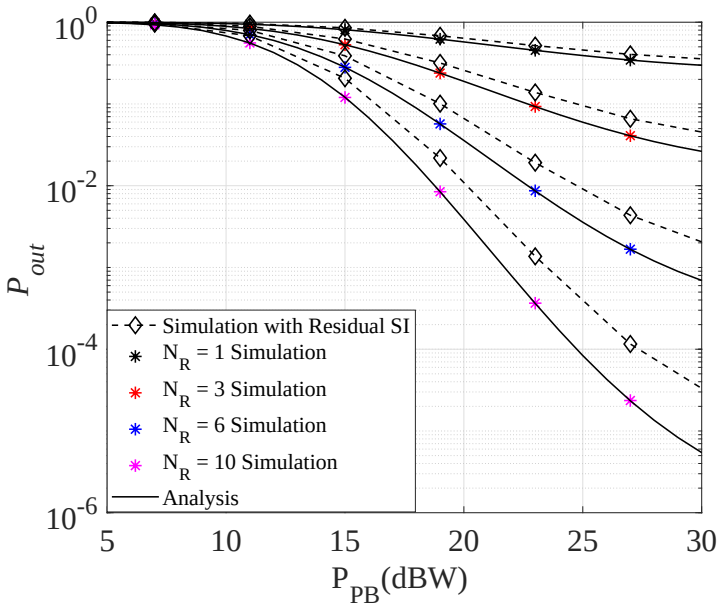


Fig. 5.3: The outage probability of secondary network, P_{out}, versus P_{PB}, where $\mathcal{Q}$ = 5 dBW, $\zeta = 0.8$, $\alpha = 0.3$, and $\mathcal{R}_b$ = 1 b/s/Hz.

considering the following parameters: $\mathcal{Q}$ = 5 dBW, $\zeta = 0.8$, $\sigma_v^2 = 1$, $\eta = 4$, $\alpha = 0.3$, $\mathcal{R}_b$ = 1 b/s/Hz, and $\mathcal{R}_s$ = 1 b/s/Hz. We assume that PT is located at the origin [0; 0], PR at [0.5; 0], E at [0.5; 0.2], S at [0.7; 0], D at [0.7; 0.2], and the PB at [0.8; 0], where the distances are normalized to be in the range [0, 1] [8].

Figure 5.3 plots the exact outage probability, P_{out}, for the CR network versus the transmitted power, P_{PB}, for different values of N_R at the CR receiver, D. It can be noticed that P_{out} of the CR link decreases as P_{PB} increases. That is, the CR transmitter, S, transmits with high power. It is worth mentioning that an outage floor exists in the high P_{PB} region, which implies that the reliability and robustness of the CR cannot be enhanced infinitely by increasing the power at S. Interestingly, P_{out} improves significantly with increasing N_R. Consequently, the CR network's reliability and robustness are enhanced as a result of utilizing multiple antennas at D compared to a single one. As an illustration, P_{out} decreases from 6.94×10^{-4} to 5.44×10^{-6} at 30 dB as the number of receiving antenna, N_R, increases from 6 to 10. To show the performance loss caused by the residual self-interference (SI), we

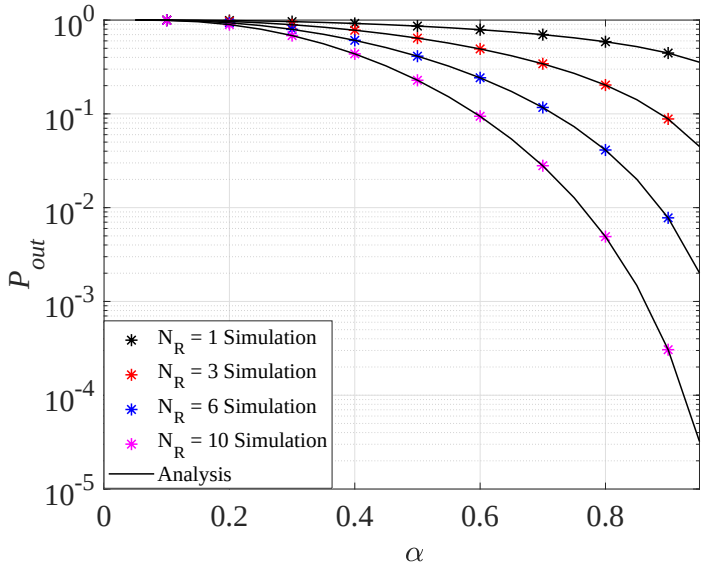


Fig. 5.4: The outage probability of secondary network, P_{out}, versus α, where $\mathcal{Q}$ = 5 dBW, $\zeta = 0.8$, P_{PB} = 10 dBW, and $\mathcal{R}_b$ = 1 b/s/Hz.

provide simulation results with the effect of the residual SI, where the transmitted power at D, P_{D_j} = 0 dBW. It can be seen that as N_R increases, P_{out} improves. This is due to the fact that if the received antenna with the best channel is selected, then the effect of the residual SI is attenuated. In Fig. 5.4, P_{out} is plotted versus α and N_R. In this respect, the impact of both α and N_R on the CR performance is evaluated. It can be seen that P_{out} improves with increasing α and N_R. This can be justified by the fact that, as α approaches 1, more EH at S can be achieved and less time devoted for the IT phase. Most noteworthy in the CR performance is the fact that, as α increases, S transmits with high power. Simultaneously, the CR network's reliability decreases because most TS-based EH protocol is allocated to harvest energy. The numerical and simulation results match perfectly, verifying the accuracy of our analysis.

In Fig. 5.5, the exact (simulation) and the upper bound (analysis) SOP for the primary network is depicted versus ω_p and N_T, where ω_e takes two possible values, 0 dB and 15 dB, while $\mathcal{Q}$ = 0 dBW, and P_{PB} = 0 dBW. It can be noted that the SOP improves as N_T in-

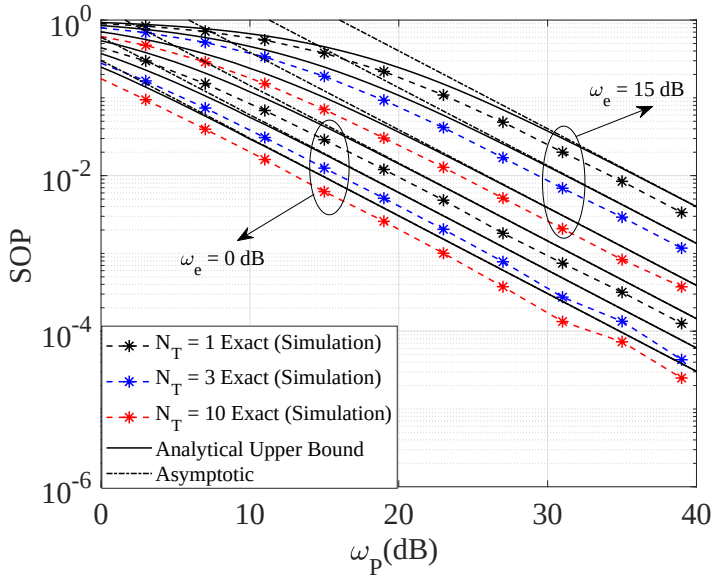


Fig. 5.5: The SOP of primary network versus ω_p, where $\mathcal{Q}$ = 0 dBW.

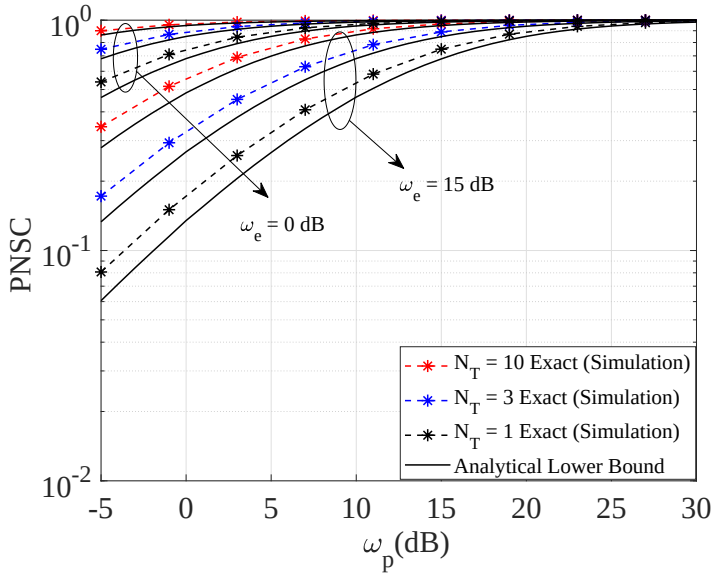


Fig. 5.6: The PNSC of primary network versus ω_p, where $\mathcal{Q}$ = 0 dBW.

creases, demonstrating the influence of using jamming antennas at D. Consequently, secure data transmission is guaranteed for the primary user. It is worthwhile to observe that the SOP improves as ω_p increases and ω_e decreases. It is important to emphasize that the jamming antenna selection at D leads to security improvement for the primary network, while

decreasing the interference at PR. As an example, ω_p can be decreased by approximately 14 dB, using jamming antennas at D with N_T = 10 compared with N_T = 1 to achieve an SOP of 10^{-2}. According to Fig. 5.5, the SOP decreases from 0.025 to 0.0025 at 30 dB as the number of jamming antennas, N_T, increases from 1 to 10, when ω_e = 15 dB. Furthermore, the asymptotic curves are presented, and a perfect match with the exact analysis is seen as $\omega_p \to \infty$. It is significant to remark that the asymptotic curves accurately predict $\mathcal{G}_a$ and $\mathcal{G}_d$. Figure 5.6 illustrates the exact (simulation) and the lower bound (analysis) of the primary PNSC versus ω_p for the same parameters given in Fig. 5.5. Noteworthy, the PNSC improves as N_T increases, showing the benefits of using jamming antennas at D. Additionally, as ω_p increases and ω_e decreases, the PNSC increases.

5.7 Conclusion

In this chapter, EH technology and dual-antenna selection are employed in the underlying system to enhance the reliability and robustness of the CR network and improve the security level of the primary network concurrently. To this end, multiple antennas N_R and N_T are employed at D to enhance the CR network's reliability and robustness and confuse the eavesdropper by generating jamming signals, respectively. New analytical expressions are derived for the CR outage probability, primary SOP, and primary PNSC. In addition, asymptotic analysis is provided to get insight into the parameters of the proposed system model. The accuracy of these expressions is verified through the Monte-Carlo simulation.

References

[1] L. Jiang, H. Tian, C. Qin, S. Gjessing, and Y. Zhang, “Secure beamforming in wireless-powered cooperative cognitive radio networks,” *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 522–525, Mar. 2016.

[2] H. Lei, et al., “On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection,” *IEEE Trans. Green Commun. Net.*, vol. 1, no. 2, pp. 192–203, Jun. 2017.

[3] M. Zhang, et al., “Energy efficiency optimization for secure transmission in miso cognitive radio network with energy harvesting,” *IEEE Access*, vol. 7, pp. 126 234–126 252, Sep. 2019.

[4] G. Chen, Y. Gong, P. Xiao and J. A. Chambers, “Dual antenna selection in secure cognitive radio networks,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7993–8002, Oct. 2016.

[5] J. M. Moualeu, W. Hamouda and F. Takawira, “Cognitive coded cooperation in underlay spectrum-sharing networks under interference power constraints,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2099–2113, Mar. 2017

[6] Z. Hadzi-Velkov, I. Nikoloska, G. K. Karagiannidis and T. Q. Duong, “Wireless networks with energy harvesting and power transfer: Joint power and time allocation,” *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 50–54, Jan. 2016.

[7] Y. Liu, L. Wang, S. A. Raza Zaidi, M. Elkashlan and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan. 2016

[8] J. Lee, H. Wang, J. G. Andrews, and D. Hong, "Outage probability of cognitive relay networks with interference constraints," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 390–395, Feb. 2011.

[9] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels," *IEEE Trans. Veh. Technol.*,vol. 66, no. 3, pp. 2237–2250, Mar. 2017.

[10] C. Ren, H. Zhang, J. Wen, J. Chen and C. Tellambura, "Successive two-way relaying for full-duplex users with generalized self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, pp. 63–76, Jan. 2019.

[11] M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed and A. Ibrahim, "Secure transmission in wiretap channels using full-duplex relay-aided D2D communications with outdated CSI," *IEEE Wireless Commun. Lett.*, vol. 9, no. 8, pp. 1216–1220, Aug. 2020.

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

[13] 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, Nov. 2014.

[14] J. Zhu, Y. Zou, G. Wang, Y. Yao and G. K. Karagiannidis, “On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 214–225, Jan. 2016

[15] *The Wolfram Functions Site*, “Wolfram Research. (Oct. 2001). [Online]. Available: http://functions.wolfram.com/07.33.02.0001.01

[16] *The Wolfram Functions Site*, “Wolfram Research. (Oct. 2001). [Online]. Available: http://functions.wolfram.com/07.33.26.0004.01

[17] M. H. Khoshafa, T. M. N. Ngatched and M. H. Ahmed, “On the physical layer security of underlay relay-aided device-to-device communications,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7609–7621, July 2020

[18] *The Wolfram Functions Site*, “Wolfram Research. (Oct. 2001). [Online]. Available: http://functions.wolfram.com/07.34.16.0001.01

Chapter 6

Reconfigurable Intelligent Surfaces Aided PLS Enhancement

6.1 Introduction

Reconfigurable Intelligent Surface (RIS) has recently developed as a promising new technology to achieve intelligent and reconfigurable wireless channels propagation environment for 6G wireless communication systems [1], [2], [3]. Specifically, RIS is a planar surface containing a large number of passive reflecting units, each reflecting the incident wireless signal with an adjustable phase shift [4], [5]. On the other development, originally investigated by Wyner [6], PLS has been developed as an appealing technique for enhancing cellular network security against eavesdropping attacks. Towards this end, PLS uses the natural properties and characteristics of wireless communication channels and noise to secure the data transmission by limiting the amount of data that can be leaked at the bit level by eavesdroppers. Thanks to their unique properties, which allows them the ability to control the transmission environment, RIS can be used for interference suppression and signal enhancement without the use of active transmitters. In this respect, RIS technology was

recently investigated to improve the PLS of wireless communication system [7], [8], [9]. For channel estimation in RIS technology, efficient strategies were proposed in [10], [11].

D2D communication is of great interest as a pioneering technology in future cellular communications to overcome the spectrum scarcity problem. In scenarios where direct links are unfavorable for the D2D nodes, the relay-aided transmission plays an essential role in enhancing D2D communication's performance. For the relay-aided underlay D2D communication, the PLS was recently studied in [12], [13]. It was shown that multi-antenna relays can be used to enhance the reliability of the D2D transmission and the PLS of the cellular network concurrently. However, as lately demonstrated in [14], improving the data rate and reducing the implementation complexity can be achieved by utilizing RIS, which outperform the relay-aided communications. To the best of our knowledge, no work has been reported in the literature investigating the use of RIS to enhance the PLS of the cellular network and improve the D2D transmission link concurrently. The main contributions of this chapter are listed as follows:

- The RIS is used to enhance the robustness and reliability of D2D communication, while simultaneously improving the PLS of the cellular network by generating jamming signals towards the eavesdropper.

- As compensation for spectrum sharing, the RIS serves as a friendly jammer to ensure a high-security level for the cellular network, thus enabling a win-win situation between the two networks, i.e., security provisioning for the cellular user and high reliability and robustness for the D2D users.

- The outage probability of D2D communication is investigated, and an analytical expression is obtained. Moreover, the cellular network's secrecy performance is analyzed, and closed-form expressions of the SOP and the PNSC are also derived.

- Asymptotic analysis is provided to get more insights into the impact of the significant

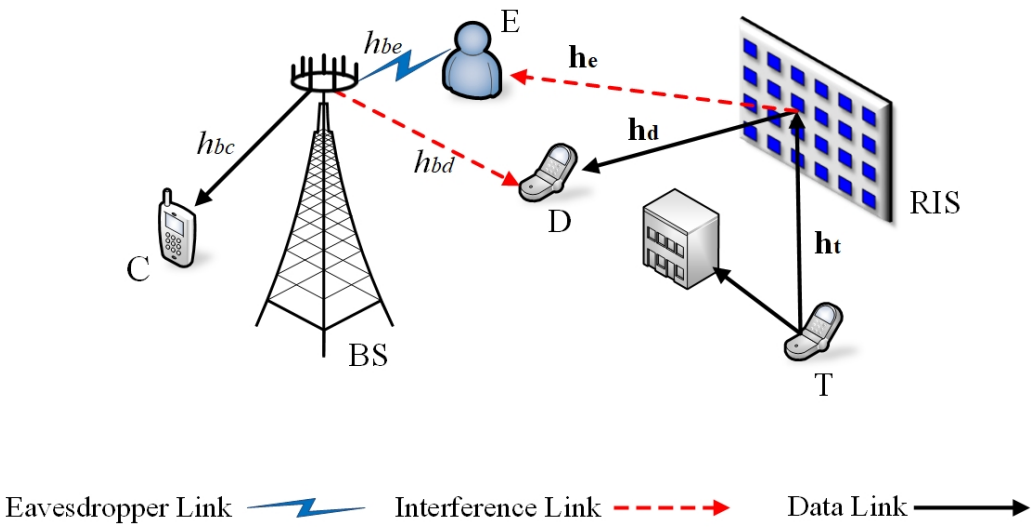


Fig. 6.1: The System Model.

parameters of the proposed system on the performance of the SOP.

- The accuracy of our analyses is verified through intensive Monte-Carlo simulations.

6.2 System Model

In this chapter, we consider a D2D communication, including a single-antenna D2D transmitter, T, and a single-antenna D2D receiver, D, as illustrated in Fig. 6.3. The D2D communication is underlying a cellular network consisting of a BS, equipped with N_B antennas, communicating with a single-antenna cellular user, C, in the presence of a single-antenna eavesdropper, E. The direct path between T and D is not available due to severe shadowing caused by obstacles. Thus, the direct communication links between D2D users suffer high signal attenuation [15], [16]. An RIS is deployed on a surrounding building's facade to assist the D2D transmitter in overcoming the disadvantageous propagation conditions by giving high-quality virtual link from T to D, while serving as a jammer to E, resulting in an enhanced secrecy rate for the cellular user. The RIS is made of N reflecting elements.

All communication channels are assumed to be independent, identical, slowly varying, flat, and their envelope follows Rayleigh distributions with a scale parameter equal to 1. Furthermore, we assume that the CSI of all channels, including E's channel, is perfectly available at the RIS for transmitting/reflecting data and jamming signals [7], [17], [18].

The channel coefficients for the $T \rightarrow$ RIS, RIS $\rightarrow D$, RIS $\rightarrow E$, BS $\rightarrow C$, BS $\rightarrow D$, and BS $\rightarrow E$ links are denoted as $\mathbf{h}_t$[1] , $\mathbf{h}_d$, $\mathbf{h}_e$, h_{bc}, h_{bd}, and h_{be}, respectively. In addition, the Euclidean distances between $T \rightarrow$ RIS, RIS $\rightarrow D$, RIS $\rightarrow E$, BS $\rightarrow C$, BS $\rightarrow D$, and BS $\rightarrow E$ links are denoted as d_{tr}, d_{rd}, d_{re}, d_{bc}, d_{bd}, and d_{be}, respectively. The signals reflected by the RIS two or more times are neglected due to severe path loss. Thus, the received signal at D can be expressed as

$$y_D = \sqrt{P_d}\left(\frac{d_{tr}\, d_{rd}}{d_o^2}\right)^{-\frac{\eta}{2}}\left[\sum_{i=1}^{N} h_{t_i}\, g_i\, h_{d_i}\, x_d\right] + \sqrt{P_b}\left(\frac{d_{bd}}{d_o}\right)^{-\frac{\eta}{2}} h_{bd}\, x_b + n_d, \tag{6.1}$$

where d_o is a reference distance, P_d is the D2D transmission power, P_b is the BS transmission power, x_d and x_b are the D2D and BS transmitted signals, respectively, and n_d is the AWGN at D. The variable g_i denotes the i^{th} reflecting meta-surfaces response of the RIS, and η denotes the path loss exponent. In addition, h_{t_i}, g_i, and h_{d_i} are complex Gaussian random variables with a zero mean and unit variance, where $g_i = |g_i|\ \exp(j\theta_i)$. Moreover, the phases of the channels h_{t_i} and h_{d_i} are assumed to be completely available at the RIS[2]. Hence, the RIS element select the optimal phase shift as [1] $\theta_i = -(\phi_i + \varphi_i)$, where ϕ_i and φ_i are respectively the phases of h_{t_i} and h_{d_i}. Furthermore, we assume that the reflected gain of the i^{th} metasurface is equal to 1. The received signal at C can be expressed as

$$y_C = \sqrt{P_b}\left(\frac{d_{bc}}{d_o}\right)^{-\frac{\eta}{2}} h_{bc}\, x_b + n_c, \tag{6.2}$$

[1]The bold font is used to indicate vectors.

[2]Since this is an ideal situation, the results obtained represent an upper bound on the performance gain that can be achieved by the RIS.

where n_c is the AWGN at C. In this respect, we assume that the received signals at C is not affected by the interference from T since it is located far away from C, and transmits with low power. Now, the received signal at E is given by

$$y_E = \sqrt{P_b}\left(\frac{d_{be}}{d_o}\right)^{-\frac{\eta}{2}} h_{be}\, x_b + \sqrt{P_d}\left(\frac{d_{tr}\, d_{re}}{d_o^2}\right)^{-\frac{\eta}{2}} \left[\sum_{i=1}^{N} h_{t_i}\, g_i\, h_{e_i}\, x_d\right] + n_e,$$

(6.3)

where h_{e_i} is the channel coefficient between the i^{th} element of the RIS and E, and n_e is the AWGN at E.

6.3 Performance Analysis

6.3.1 D2D Outage Probability

For the D2D communication, the outage probability, P_{out}, is defined by

$$P_{out} = \Pr\left(\gamma_D \leq \varphi\right) = F_{\gamma_D}(\varphi), \tag{6.4}$$

where $\varphi = 2^{\mathcal{R}_d} - 1$, $\mathcal{R}_d$ is the data rate of D2D transmission, and γ_D is the instantaneous end-to-end SINR for the D2D link, γ_D, which is given by

$$\gamma_D = \frac{P_d \left(\frac{d_{tr}\, d_{rd}}{d_o^2}\right)^{-\eta} \left(\sum_{i=1}^{N} |h_{t_i}|\, |h_{d_i}|\right)^2}{\sigma_d^2 + P_b \left(\frac{d_{bd}}{d_o}\right)^{-\eta} |h_{bd}|^2} = \frac{\gamma_{td}}{1 + \gamma_{bd}}, \tag{6.5}$$

where $\gamma_{td} = \bar{\gamma}_{td} \left(\frac{d_{tr}\, d_{rd}}{d_o^2}\right)^{-\eta} \left(\sum_{i=1}^{N} |h_{t_i}|\, |h_{d_i}|\right)^2$, $\gamma_{bd} = \bar{\gamma}_{bd} \left(\frac{d_{bd}}{d_o}\right)^{-\eta} |h_{bd}|^2$, $\bar{\gamma}_{td} = \frac{P_d}{\sigma_d^2}$, and $\bar{\gamma}_{bd} = \frac{P_b}{\sigma_d^2}$. Let us define $\omega_1 = \bar{\gamma}_{td} \left(\frac{d_{tr}\, d_{rd}}{d_o^2}\right)^{-\eta}$ and $\omega_2 = \bar{\gamma}_{bd} \left(\frac{d_{bd}}{d_o}\right)^{-\eta}$. The CDF of γ_D can

be obtained using [19]

$$F_{\gamma_D}(\gamma) = \int_0^{\infty} F_{\gamma_{td}}(\gamma\,(\zeta+1))\, f_{\gamma_{bd}}(\zeta)\, d\zeta, \tag{6.6}$$

where $F_{\gamma_{td}}(.)$ is given by [14]

$$F_{\gamma_{td}}(\gamma) = \frac{\Upsilon\left(\xi+1, \mu\sqrt{\frac{\gamma}{\omega_1}}\right)}{\Gamma\left(\xi+1\right)}, \tag{6.7}$$

where $\xi = \frac{N\pi^2}{(16-\pi^2)} - 1$, $\mu = \frac{2\pi}{(16-\pi^2)}$, $\Gamma(.)$ is the gamma function [20, eq. (8.310.1)], and $\Upsilon\left(a,x\right) = \int_0^x t^{a-1}\exp\left(-t\right)\, dt$ is the lower incomplete gamma function defined by [20, eq. (8.350.1)]. On the other hand, $f_{\gamma_{bd}}(.)$ is given by $f_{\gamma_{bd}}(\gamma) = \frac{1}{\omega_2}\exp\left(-\frac{\gamma}{\omega_2}\right)$. By plugging (6.7) and $f_{\gamma_{bd}}(.)$ into (6.6), using series expansion in [20, eq. (8.354.1)], then with the help of [20, eq. (3.382.4)], $F_{\gamma_D}(\gamma)$ can be obtained as

$$\begin{aligned} F_{\gamma_D}(\gamma) =& \frac{1}{\Gamma\left(\xi+1\right)\omega_2} \sum_{n=0}^{\infty} \frac{(-1)^n \left(\mu\sqrt{\frac{\gamma}{\omega_1}}\right)^{\xi+n+1} \exp\left(\frac{1}{\omega_2}\right)}{n!\left(\xi+n+1\right)\,\omega_2^{-\left(\frac{\xi+n+3}{2}\right)}} \\ & \times \Gamma\left(\frac{\xi+n+3}{2}, \frac{1}{\omega_2}\right), \end{aligned} \tag{6.8}$$

where $\Gamma(.,.)$ is the upper incomplete gamma [20, eq. (8.350.2)]. By plugging (6.8) into (6.4), P_{out} can be obtained.

6.3.2 Secrecy Outage Probability

The SOP can be expressed as [21]

$$\text{SOP} = \Pr\left(C_S < \mathcal{R}_s\right), \tag{6.9}$$

where C_S is the secrecy capacity, that is given by [22]

$$C_S = \begin{cases} C_C - C_E, & \gamma_C > \gamma_E, \\ 0, & \gamma_C \leq \gamma_E, \end{cases} \tag{6.10}$$

where C_C and C_E denote the cellular and eavesdropper capacities, respectively, and γ_C and γ_E are the SINR at C and E, respectively. In this regard, C_C is given by

$$C_C = \log_2 (1 + \gamma_C), \tag{6.11}$$

where γ_C is given by

$$\gamma_C = \frac{P_b \left(\frac{d_{bc}}{d_o}\right)^{-\eta} |h_{bc}|^2}{\sigma_c^2} = \gamma_{bc}, \tag{6.12}$$

where $\gamma_{bc} = \bar{\gamma}_{bc} \left(\frac{d_{bc}}{d_o}\right)^{-\eta} |h_{bc}|^2$ and $\bar{\gamma}_{bc} = \frac{P_b}{\sigma_c^2}$. Let us define $\omega_3 = \bar{\gamma}_{bc} \left(\frac{d_{bc}}{d_o}\right)^{-\eta}$. In addition, C_E can be obtained by

$$C_E = \log_2 (1 + \gamma_E), \tag{6.13}$$

where γ_E is given by

$$\begin{aligned} \gamma_E &= \frac{P_b \left(\frac{d_{be}}{d_o}\right)^{-\eta} |h_{be}|^2}{\sigma_e^2 + P_d \left(\frac{d_{tr}\, d_{re}}{d_o^2}\right)^{-\eta} \left(\sum_{i=1}^{N} |h_{t_i}|\, |h_{e_i}|\right)^2} \\ &= \frac{\gamma_{be}}{1 + \gamma_e}, \end{aligned} \tag{6.14}$$

where $\gamma_e = \bar{\gamma}_e \left(\frac{d_{tr}\, d_{re}}{d_o^2}\right)^{-\eta} \left(\sum_{i=1}^{N} |h_{t_i}|\, |h_{e_i}|\right)^2$, $\gamma_{be} = \bar{\gamma}_{be} \left(\frac{d_{be}}{d_o}\right)^{-\eta} |h_{be}|^2$, $\bar{\gamma}_{be} = \frac{P_b}{\sigma_e^2}$, and $\bar{\gamma}_e = \frac{P_d}{\sigma_e^2}$. Let us define $\omega_4 = \bar{\gamma}_{be} \left(\frac{d_{be}}{d_o}\right)^{-\eta}$, and $\omega_5 = \bar{\gamma}_e \left(\frac{d_{tr}\, d_{re}}{d_o^2}\right)^{-\eta}$.

To maximize the cellular capacity, the best transmit antenna at the BS is chosen based

on the following criterion

$$k^* = \arg \max_{k=1,\ldots,N_B} C_{C_k} = \arg \max_{k=1,\ldots,N_B} \gamma_{C_k}. \tag{6.15}$$

The SOP is formulated as

$$\text{SOP} = \int_0^\infty F_{\gamma_C}(\beta\gamma + \alpha)\, f_{\gamma_E}(\gamma)\, d\gamma, \tag{6.16}$$

where $\beta = 2^{\mathcal{R}_s}$, $\alpha = \beta - 1$, and $F_{\gamma_C}(.)$ is given by

$$F_{\gamma_C}(\gamma) = N_B \sum_{k=0}^{N_B-1} \frac{(-1)^k \binom{N_B-1}{k}}{(k+1)} \left(1 - \exp\left(-\frac{\gamma\,(k+1)}{\omega_3}\right)\right). \tag{6.17}$$

The PDF of γ_E can be derived using

$$f_{\gamma_E}(\gamma) = \int_0^\infty (x+1)\, f_{\gamma_{be}}(\gamma\,(x+1))\, f_{\gamma_e}(x)\, dx, \tag{6.18}$$

where $f_{\gamma_{be}}(.)$ is given by

$$f_{\gamma_{be}}(\gamma) = \frac{1}{\omega_4} \exp\left(-\frac{\gamma}{\omega_4}\right), \tag{6.19}$$

and $f_{\gamma_e}(.)$ is given by [14]

$$f_{\gamma_e}(\gamma) = \frac{\mu^{\xi+1}}{2\,\Gamma(\xi+1)\,\omega_5^{\frac{\xi+1}{2}}}\, \gamma^{\frac{\xi-1}{2}} \exp\left(-\mu\sqrt{\frac{\gamma}{\omega_5}}\right). \tag{6.20}$$

By substituting (6.19) and (6.20) in (6.18), and utilizing [23, eq. (07.34.03.0606.01)] and [24, eq. (07.34.03.0228.01)], then [20, eq. (7.811.1)], $f_{\gamma_E}(\gamma)$ can be obtained as

$$f_{\gamma_E}(\gamma) = \frac{\Delta}{\exp\left(\frac{\gamma}{\omega_4}\right)} \left[\frac{1}{\gamma}\, G_{2,1}^{1,2}\left(\frac{\gamma}{\omega_4\,\mathcal{Q}_1^2}\,\middle|\, \begin{matrix} \frac{-\xi+1}{2}, \frac{-\xi}{2} \\ 1 \end{matrix}\right) + \frac{1}{\omega_4} G_{2,1}^{1,2}\left(\frac{\gamma}{\omega_4\,\mathcal{Q}_1^2}\,\middle|\, \begin{matrix} \frac{-\xi+1}{2}, \frac{-\xi}{2} \\ 0 \end{matrix}\right)\right], \tag{6.21}$$

where $\Delta = \frac{\mu^{\xi+1}\,\mathcal{Q}_1^{-(\xi+1)}}{2\sqrt{\pi}\,\Gamma(\xi+1)\,\omega_5^{\left(\frac{\xi+1}{2}\right)}}$, $\mathcal{Q}_1 = \left(\frac{\mu}{2\sqrt{\omega_5}}\right)$, and $G_{p,q}^{m,n}\left(x \,\middle|\, \begin{matrix} a_p \\ b_q \end{matrix}\right)$ represents the Meijer G-function [20, eq. (9.301)]. Now, the SOP can be derived by plugging (6.17) and (6.21) into (6.16), and utilizing [24, eq. (07.34.03.0228.01)], then [20, eq. (7.811.1)], as

$$\begin{aligned}\text{SOP} =& N_B \sum_{k=0}^{N_B-1} \frac{(-1)^k \binom{N_B-1}{k}}{(k+1)} \Bigg[1 - \Bigg(\frac{\Delta}{\mathcal{Q}_1^{-2}} \exp\left(-\frac{(k+1)\,\alpha}{\omega_3}\right) \\ &\times \Bigg[\mathcal{Q}_2\,\omega_4\, G_{1,3}^{3,1}\left(\mathcal{Q}_1^2\,\mathcal{Q}_2\,\omega_4 \,\middle|\, \begin{matrix} -1 \\ -1\,,\,\frac{\xi-1}{2}\,,\,\frac{\xi}{2} \end{matrix}\right) + G_{1,3}^{3,1}\left(\mathcal{Q}_1^2\,\mathcal{Q}_2\,\omega_4 \,\middle|\, \begin{matrix} 0 \\ 0\,,\,\frac{\xi-1}{2}\,,\,\frac{\xi}{2} \end{matrix}\right)\Bigg]\Bigg)\Bigg],\end{aligned} \tag{6.22}$$

where $\mathcal{Q}_2 = \left(\frac{1}{\omega_4} + \frac{(k+1)\beta}{\omega_3}\right)$.

6.3.3 Asymptotic Secrecy Outage Analysis

To acquire more insights on the system design, the asymptotic SOP, SOP$^\infty$, is examined. SOP$^\infty$ can be written as

$$\text{SOP}^\infty = (\mathcal{G}_a \overline{\gamma}_d)^{-\mathcal{G}_d} + \mathcal{O}(\overline{\gamma}_d^{-\mathcal{G}_d}), \tag{6.23}$$

where $\mathcal{G}_d$ and $\mathcal{G}_a$ are the secrecy diversity order and the secrecy array gain, respectively. Mathematically speaking, to derive the SOP$^\infty$, the asymptotic CDF, $F_{\gamma_C}^{\infty}(.)$, is derived and then plugging into (6.16), and using [20, eq. (7.813.1)]. After performing some algebraic manipulations, it turns out that $\mathcal{G}_d$ = N_B and $\mathcal{G}_a$ is given by

$$\mathcal{G}_a = \left[\Delta\,\alpha^{N_B} \sum_{k=0}^{N_B} \binom{N_B}{k} \left(\frac{\omega_4\,\beta}{\alpha}\right)^k G_{3,1}^{1,3}\left(\frac{1}{\mathcal{Q}_1^2} \,\middle|\, \begin{matrix} 1-k\,,\,\frac{-\xi+1}{2}\,,\,\frac{-\xi}{2} \\ 1 \end{matrix}\right)\right]^{\frac{-1}{N_B}}.$$

6.3.4 Probability of Non-zero Secrecy Capacity

The non-zero secrecy capacity is obtained when $\gamma_C > \gamma_E$. The PNSC is given by

$$\text{PNSC} = \Pr\left(\frac{1+\gamma_C}{1+\gamma_E} > 1\right) = 1 - \int_0^\infty F_{\gamma_C}(\gamma) f_{\gamma_E}(\gamma)\, d\gamma. \tag{6.24}$$

By plugging (6.17) and (6.21) into (6.24), and following the same procedure as in the derivation of (6.22), the PNSC can be derived as

$$\text{PNSC} = 1 - N_B \sum_{k=0}^{N_B-1} \frac{(-1)^k \binom{N_B-1}{k}}{(k+1)} \left[1 - \left(\frac{\Delta}{\mathcal{Q}_1^{-2}} \left[\mathcal{Q}_3\, \omega_4\, G_{1,3}^{3,1}\left(\mathcal{Q}_1^2\, \mathcal{Q}_3\, \omega_4 \,\middle|\, \begin{matrix} -1 \\ -1\,,\, \frac{\xi-1}{2}\,,\, \frac{\xi}{2} \end{matrix}\right)\right.\right.$$
$$\left.\left. + G_{1,3}^{3,1}\left(\mathcal{Q}_1^2\, \mathcal{Q}_3\, \omega_4 \,\middle|\, \begin{matrix} 0 \\ 0\,,\, \frac{\xi-1}{2}\,,\, \frac{\xi}{2} \end{matrix}\right)\right]\right], \tag{6.25}$$

where $\mathcal{Q}_3 = \left(\frac{1}{\omega_4} + \frac{(k+1)}{\omega_3}\right)$.

6.4 Active Reconfigurable Intelligent Surfaces-Aided Wireless Communication

Despite its many advantages, the practical implementation of RIS-aided wireless communications may face a couple of challenges. One of them is the double-fading problem. More specifically, the signal that goes through the RIS module experiences a double fading attenuation due to the product of path losses on both links, i.e., source-RIS and RIS-destination links. Moreover, the RIS module might generate some noise. The combination of all these may result in a significant decrease of the achievable gain expected from the RIS module [25]. The double fading problem has been traditionally tackled by increasing the number of passive RIS elements [26], [27]. However, this approach results in an increase of the

physical size of the RIS module, which might not be practical in some scenarios. The use of active elements in the RIS was recently proposed in [28], [29] to overcome this problem. In this section we investigate the secrecy performance of an RIS-aided wireless communication system, where the RIS module is made of active elements. Moreover, a practical design for the active RIS is proposed.

6.4.1 System Model

As shown in Fig.6.2, we consider a wireless network which consists of a single-antenna transmitter, S, and a single-antenna receiver, D, which are communicating in the presence of a single-antenna eavesdropper, E. It is worth mentioning that the direct links from S to D, and E are considered. An RIS with active elements is deployed to assist S and enhance the propagation conditions by providing a high-quality virtual link from S to D, while improving the secrecy performance simultaneously. The RIS consists of N reflecting elements. In the proposed system model, each element in the RIS module is equipped with a power amplifier to strengthen the reflected signal. In such a scenario, the significant path loss of the RIS-aided link can be compensated, thus overcoming the double fading. In this work, the CSI of S is perfectly obtained at the RIS to maximize the received SNR at D. However, the E is considered as passive, and thus its CSI is not available at both the transmitter and the RIS.

All the channels are assumed to undergo Rayleigh fading. The channel coefficients for the S $\rightarrow$ D, S $\rightarrow$ RIS, RIS $\rightarrow$ D, S $\rightarrow$ E, and RIS $\rightarrow$ E links are denoted as h_{sd}, $\mathbf{h_S}$[3], $\mathbf{h_D}$, h_{se}, and $\mathbf{h_E}$, respectively. The Euclidean distances for the above links are denoted as $d_{sd}, d_{sr}, d_{rd}, d_{se}$, and d_{re}, respectively. At D, the received signal can be expressed

[3] The bold font is used to indicate vectors.

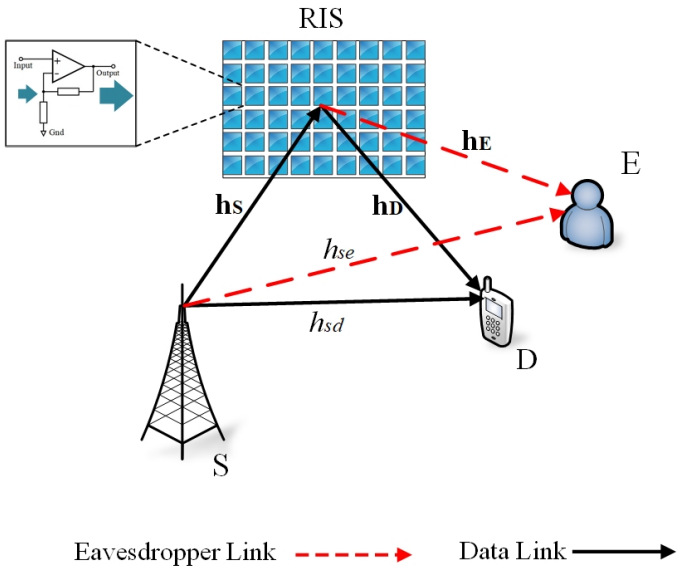


Fig. 6.2: System Model.

as

$$y_D = \sqrt{P_s}\, x_s \left[\left(\frac{d_{sr}\, d_{rd}}{d_o^2} \right)^{-\frac{\eta}{2}} \sum_{i=1}^{N} h_{s_i}\, \rho\, h_{d_i}\, e^{j\phi_i} + h_{sd} \left(\frac{d_{sd}}{d_o} \right)^{-\frac{\eta}{2}} \right] + \rho\, n_r + n_d, \qquad (6.26)$$

where ρ is the amplification gain of each RIS element, d_o is a reference distance, η denotes the path loss exponent, P_s is the transmission power, x_s is the transmitted signal, h_{s_i} and h_{d_i} are complex Gaussian RVs with a zero mean and unit variance, i.e., $\mathcal{CN}\,(0, 1)$, and n_r, and n_d are the AWGN at the RIS and D, which are distributed as $\mathcal{CN}\,(0, \sigma_{rd}^2)$ and $\mathcal{CN}\,(0, \sigma_d^2)$, respectively. In addition, ϕ_i is the adjustable phase applied to the i^{th} RIS reflecting element. At the E, the received signal can be expressed as

$$y_E = \sqrt{P_s}\, x_s \left[\left(\frac{d_{sr}\, d_{re}}{d_o^2} \right)^{-\frac{\eta}{2}} \sum_{i=1}^{N} h_{s_i}\, \rho\, h_{e_i}\, e^{j\phi_i} + \left(\frac{d_{se}}{d_o} \right)^{-\frac{\eta}{2}} h_{se} \right] + \rho\, n_r + n_e, \qquad (6.27)$$

where h_{e_i} is the channel coefficient between the i^{th} RIS element and the E, and n_e is the AWGN at the E.

6.4.2 Performance Analysis

In this section, the outage probability, P_{out}, and the SOP are investigated.

6.4.3 Outage Probability

The outage probability, P_{out}, is defined by $P_{out} = \Pr(\gamma_D \leq \vartheta_b) = F_{\gamma_D}(\vartheta_b)$, where γ_D is the instantaneous SNR at D and $\vartheta_b = 2^{\mathcal{R}_d} - 1$, $\mathcal{R}_d$ being the data transmission rate. In this regards, γ_D can be expressed as

$$\begin{aligned}\gamma_D &= \frac{P_s}{\sigma_{rd}^2}\left|\left(\frac{d_{sr}\,d_{rd}}{d_o^2}\right)^{-\frac{\eta}{2}}\sum_{i=1}^{N} h_{s_i}\,\rho\,h_{d_i}\,e^{j\phi_i} + \left(\frac{d_{sd}}{d_o}\right)^{-\frac{\eta}{2}} h_{sd}\right|^2 \\ &= \left|\Omega_1\sum_{i=1}^{N} h_{s_i}\,h_{d_i}\,e^{j\phi_i} + \Omega_2\,h_{sp}\right|^2,\end{aligned} \tag{6.28}$$

where $\sigma_{rd}^2 = \sigma_d^2 + \rho^2\sigma_r^2$, $\Omega_1 = \sqrt{\bar{\gamma}_d}\,\rho\left(\frac{d_{sr}\,d_{rp}}{d_o^2}\right)^{-\frac{\eta}{2}}$, and $\Omega_2 = \sqrt{\bar{\gamma}_d}\left(\frac{d_{sp}}{d_o}\right)^{-\frac{\eta}{2}}$, $\bar{\gamma}_d = \frac{P_s}{\sigma_{rd}^2}$. According to the central limit theorem, $\chi_1 = \sum_{i=1}^{N}|h_{s_i}|\,|h_{d_i}|$ can be approximated as a Gaussian RV with a mean value $\mu = \frac{N\pi}{4}$ and variance $\sigma^2 = N\left(1 - \frac{\pi}{16}\right)$ [1]. Moreover, $\chi_2 = |h_{sd}|$ is a Rayleigh-distributed RV with a parameter λ_D. Thus, γ_D can be expressed as $\gamma_D = \Big(\Omega_1\chi_1 + \Omega_2\,\chi_2\Big)^2$, leading to the CDF given by [9]

$$\begin{aligned}F_{\gamma_D}(\gamma) = \frac{1}{2}&\left[\text{erf}\left(\frac{(\vartheta_1/\vartheta_2)\sqrt{\gamma}-\mu}{\sqrt{2\sigma^2}}\right) + \text{erf}\left(\frac{\mu}{\sqrt{2\sigma^2}}\right)\right] \\ &- \frac{\sqrt{\lambda_D}}{2\zeta_1}\exp\left(\frac{-\left(\vartheta_1\sqrt{\gamma}-\vartheta_2\mu\right)^2}{2\zeta_1^2}\right)\text{erf}\left(\frac{\zeta_4\sqrt{\gamma}-\zeta_5}{\zeta_1\zeta_2}\right) \\ &- \frac{\sqrt{\lambda_D}}{2\zeta_1}\exp\left(\frac{-\left(\vartheta_1\sqrt{\gamma}-\vartheta_2\mu\right)^2}{2\zeta_1^2}\right)\text{erf}\left(\frac{\zeta_3\sqrt{\gamma}+\zeta_5}{\zeta_1\zeta_2}\right),\end{aligned} \tag{6.29}$$

where $\vartheta_1 = \frac{1}{\Omega_2}$, $\vartheta_2 = \frac{\Omega_1}{\Omega_2}$, $\zeta_1 = \sqrt{\sigma^2\vartheta_2 + \lambda_D}$, $\zeta_2 = \sqrt{2\sigma^2\lambda_D}$, $\zeta_3 = \sigma^2\vartheta_1\vartheta_2$, $\zeta_4 = \frac{\lambda_D\vartheta_1}{\vartheta_2}$, $\zeta_5 = \lambda_D\mu$, and $\text{erf}(\cdot)$ is the error function [20, eq. (8.250.1)].

6.4.4 Secrecy Outage Probability

The SOP can be defined as the probability that the achievable secrecy rate is less than a predefined target secrecy rate, $\mathcal{R}_s$, for the cellular transmission system. Based on the definition, the SOP is given by $\text{SOP} = \Pr\left(C_S < \mathcal{R}_s\right)$, where $\mathcal{R}_s$ is the secrecy rate, and C_S is the secrecy capacity, which is given by $C_S = \left[C_D - C_E, 0\right]^+$, where C_D and C_E are the cellular and eavesdropper capacities, respectively, and $[x, 0]^+ = \max(x, 0)$. In this regard, C_D and C_E are given by $C_D = \log_2\left(1 + \gamma_D\right)$, and $C_E = \log_2\left(1 + \gamma_E\right)$, where γ_D and γ_E are the SNR at D and E, respectively. γ_D is defined in (6.28), and γ_E is given by

$$\begin{aligned}\gamma_E &= \frac{P_s}{\sigma_{re}^2}\left|\left(\frac{d_{sr}\, d_{re}}{d_o^2}\right)^{-\frac{\eta}{2}} \sum_{i=1}^{N} h_{s_i}\, \rho\, h_{e_i}\, e^{j\phi_i} + \left(\frac{d_{se}}{d_o}\right)^{-\frac{\eta}{2}} h_{se}\right|^2 \\ &= \left|\mathcal{E}_1 \sum_{i=1}^{N} h_{s_i}\, h_{e_i}\, e^{j\phi_i} + \mathcal{E}_2\, h_{sp}\right|^2,\end{aligned} \tag{6.30}$$

where $\sigma_{re}^2 = \sigma_e^2 + \rho^2\sigma_r^2$, $\mathcal{E}_1 = \sqrt{\bar{\gamma}_e}\,\rho\left(\frac{d_{sr}\, d_{re}}{d_o^2}\right)^{-\frac{\eta}{2}}$, $\bar{\gamma}_e = \frac{P_s}{\sigma_{re}^2}$, and $\mathcal{E}_2 = \sqrt{\bar{\gamma}_e}\left(\frac{d_{se}}{d_o}\right)^{-\frac{\eta}{2}}$. γ_E can be approximated using an exponential random variable with parameter $\lambda_{\text{E}} = N\,\mathcal{E}_1^2 + \mathcal{E}_2^2$. Hence, the PDF of γ_E can be expressed as

$$f_{Y_E}(\gamma) = \frac{1}{\lambda_E}\,\exp\left(-\frac{\gamma}{\lambda_E}\right). \tag{6.31}$$

Generally, the SOP can be formulated as [30]

$$\text{SOP} = \int_0^{\infty} F_{\gamma_D}(\beta\,\gamma + \alpha)\, f_{\gamma_E}(\gamma)\, d\gamma, \tag{6.32}$$

where $\beta = 2^{\mathcal{R}_s}$, and $\alpha = \beta - 1$. However, using the expression in (6.29) to evaluate the SOP is not mathematically tractable. Thus, the following alternative expression for the

error function [31]

$$\text{erf}\,(x) \approx \begin{cases} 1 - \sum_{i=1}^{4} \Psi_i \exp\left(-\Delta_i\, x^2\right) & x \geq 0 \\ -1 + \sum_{i=1}^{4} \Psi_i \exp\left(-\Delta_i\, x^2\right) & x < 0, \end{cases} \tag{6.33}$$

where $\Psi = [1/8, 1/4, 1/4, 1/4]$ and $\Delta = [1, 2, 20/3, 20/17]$, can be utilized. By plugging (6.29) and (6.31) into (6.32) with the help of (6.33) and [20, eq. (2.33.1)], the SOP can be derived as

$$\text{SOP} = \mathcal{I}_1 - \mathcal{I}_2 - \mathcal{I}_3, \tag{6.34}$$

where $\mathcal{I}_1$, $\mathcal{I}_2$, and $\mathcal{I}_3$ can be derived as

$$\begin{aligned} \mathcal{I}_1 = &\exp\left(\frac{\alpha}{\lambda_E \beta}\right)\left(\exp\left(\frac{b_2^2}{b_1^2 \lambda_E \beta}\right) + \frac{1}{2}\left(\text{erf}\left(\frac{\mu}{\sqrt{2\sigma^2}}\right) - 1\right)\right) + \sum_{i=1}^{4} \frac{\Psi_i \exp\left(\frac{\alpha}{\lambda_E \beta} - a_3\right)}{4\sqrt{a_1^3}\, b_1^2 \lambda_E \beta} \\ &\Bigg[(a_2 - 2a_1 b_1) \exp\left(\frac{a_2^2}{4a_1}\right)\sqrt{\pi}\,\text{erfc}\left(\frac{a_2}{2\sqrt{a_1}}\right) - 2\sqrt{a_1} + \exp\left(-\mathcal{A}_1 \Lambda_1\right)\left((a_2 - 2a_1 b_2)\right. \\ &\left.\sqrt{\pi}\exp\left(\frac{\Lambda_2^2}{4a_1}\right)\left(\text{erf}\left(\frac{\Lambda_2}{2\sqrt{a_1}}\right) - \text{erf}\left(\frac{a_2}{2\sqrt{a_1}}\right)\right) - 2\sqrt{a_1}\left(\exp\left(-\mathcal{A}_1 \Lambda_1\right) - 1\right)\right)\Bigg], \end{aligned} \tag{6.35}$$

where $b_1 = \frac{(\vartheta_1/\vartheta_2)}{\sqrt{2\sigma^2}}$, $b_2 = \frac{\mu}{\sqrt{2\sigma^2}}$, $\mathcal{A}_1 = \sqrt{\alpha}\, b_1 - b_2$, $a_1 = \frac{1}{\lambda_E \beta b_1^2} + \Delta_i$, $a_2 = \frac{2b_2}{\lambda_E \beta b_1^2}$, $\Lambda_1 = \mathcal{A}_1 a_1 + a_2$, $\Lambda_2 = 2\mathcal{A}_1 a_1 + a_2$.

$$
\begin{aligned}
\mathcal{I}_2 =& \Xi_1 \left[\frac{1}{\sqrt{c_1^3}} \left(2\sqrt{c_1} + \exp\left(-\mathcal{A}_2\, \Xi_2\right) \left(2\sqrt{c_1}\left(\exp\left(-\mathcal{A}_2\, \Xi_2\right) - 1\right) + \left(c_2 - 2c_1 d_5\right) \exp\left(\frac{\Xi_3^2}{4c_1}\right) \right.\right.\right. \\
& \left. \sqrt{\pi} \left(\text{erf}\left(\frac{c_2}{2\sqrt{c_1}}\right) - \text{erf}\left(\frac{\Xi_3}{2}\right)\right) - \left(c_2 - 2c_1 \left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)\right) \exp\left(\frac{c_2^2}{4c_1}\right) \sqrt{\pi}\, \text{erfc}\left(\frac{c_2}{2\sqrt{c_1}}\right)\right)\right) \\
& + \sum_{i=1}^{4} \frac{\Psi_i}{\sqrt{c_4^3}} \left(-2\sqrt{c_4} + \exp\left(-\mathcal{A}_2\, \Xi_4\right) \left(-2\sqrt{c_4}\left(\exp\left(-\mathcal{A}_2\, \Xi_4\right) - 1\right) + \left(c_2 - 2c_4 \left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)\right)\right.\right. \\
& \exp\left(\frac{\Xi_5^2}{4c_4}\right) \sqrt{\pi} \left(\text{erf}\left(\frac{\Xi_5}{2\sqrt{c_4}}\right) - \text{erf}\left(\frac{c_2}{2\sqrt{c_4}}\right)\right) - \left(c_2 - 2c_4 d_5\right) \exp\left(\frac{c_2^2}{4c_4}\right) \\
& \left.\left.\left. \sqrt{\pi}\, \text{erfc}\left(\frac{c_2}{2\sqrt{c_4}}\right)\right)\right)\right],
\end{aligned}
\tag{6.36}
$$

where $c_1 = \frac{\vartheta_1^2\zeta_2^2}{2\zeta_4^2} + \frac{\zeta_1^2\zeta_2^2}{\lambda_E\beta\zeta_4^2\gamma}$, $c_2 = \frac{\zeta_2}{\zeta_1\zeta_4^2}\left(\vartheta_1\left(\vartheta_1\zeta_5 - \vartheta_2\mu\zeta_4\right) + \frac{2\zeta_1^2\zeta_5}{\lambda_E\beta}\right)$, $\Xi_1 = \frac{d_1}{2d_4^2\lambda_E\beta}\exp\left(\frac{\alpha}{\lambda_E\beta} - c_3\right)$, $c_3 = \frac{\zeta_5^2}{\lambda_E\beta\zeta_4^2} + \frac{1}{2\zeta_1^2}\left(\frac{\vartheta_1\zeta_5}{\zeta_4} - \vartheta_2\mu\right)^2$, $c_4 = c_1 + \Delta_i$, $\mathcal{A}_2 = \sqrt{\alpha}\left(\frac{\zeta_4}{\zeta_1\zeta_2}\right) - \frac{\zeta_5}{\zeta_1\zeta_2}$, $\Xi_2 = \mathcal{A}_2 c_1 + c_2$, $\Xi_3 = 2\mathcal{A}_2 c_1 + c_2$, $\Xi_4 = \mathcal{A}_2 c_4 + c_2$, $\Xi_5 = 2\mathcal{A}_2 c_4 + c_2$.

$$
\begin{aligned}
\mathcal{I}_3 =& \Phi_1 \left(\frac{1}{\sqrt{\upsilon_1^3}} \exp\left(-\mathcal{A}_3\Phi_2\right) \left(2\sqrt{\upsilon_1} - \exp\left(\frac{\Phi_3^2}{4\upsilon_1}\right) \left(2\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)\upsilon_1 + \upsilon_2\right)\sqrt{\pi}\, \text{erfc}\left[\frac{\Phi_3}{2\sqrt{\upsilon_1}}\right]\right)\right. \\
& + \sum_{i=1}^{4} \frac{\Psi_i}{\sqrt{\upsilon_4^3}} \exp\left(-\mathcal{A}_3\, \Phi_4\right) \left(-2\sqrt{\upsilon_4} + \exp\left(\frac{\Phi_5^2}{4\upsilon_4}\right) \left(\upsilon_2 + 2\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)\upsilon_4\right)\right. \\
& \left.\left. \times\sqrt{\pi}\, \text{erfc}\left[\frac{\Phi_5}{2\sqrt{\upsilon_4}}\right]\right)\right),
\end{aligned}
\tag{6.37}
$$

where $\upsilon_1 = \frac{\vartheta_1^2\zeta_2^2\gamma}{2\zeta_3^2} + \frac{\zeta_1^2\zeta_2^2}{\lambda_P\zeta_3^2}$ $\upsilon_2 = \frac{\zeta_2}{\zeta_1\zeta_3^2}\left(\vartheta_1\left(\vartheta_1\zeta_5 + \vartheta_2\mu\zeta_3\right) + \frac{2\zeta_1^2\zeta_5}{\lambda_E\beta}\right)$, $\Phi_1 = \frac{d_1}{2d_8^2\lambda_E\beta}\exp\left(\frac{\alpha}{\lambda_E\beta} - \upsilon_3\right)$, $\upsilon_3 = \frac{\zeta_5^2}{\lambda_E\beta\zeta_3^2} + \frac{1}{2\zeta_1^2}\left(\frac{\vartheta_1\zeta_5}{\zeta_3} + \vartheta_2\mu\right)^2$, $\upsilon_4 = \upsilon_1 + \Delta_i$, $\mathcal{A}_3 = \sqrt{\alpha}\left(\frac{\zeta_3}{\zeta_1\zeta_2}\right) + \frac{\zeta_5}{\zeta_1\zeta_2}$, $\Phi_2 = \mathcal{A}_3\upsilon_1 + \upsilon_2$, $\Phi_3 = 2\mathcal{A}_3\upsilon_1 + \upsilon_2$ $\Phi_4 = \mathcal{A}_3\upsilon_4 + \upsilon_2$, $\Phi_5 = 2\mathcal{A}_3\upsilon_4 + \upsilon_2$.

Finally, the SOP can be obtained by plugging (6.35), (6.36), and (6.37) into (6.34).

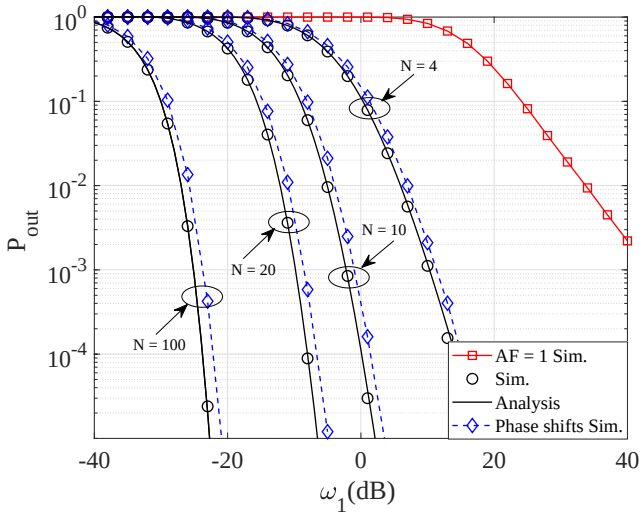


Fig. 6.3: The D2D outage probability, where $\mathcal{R}_b$ = 1 b/s/Hz .

6.5 Results and Discussions

6.5.1 Passive RIS

In this section, we present the numerical results of the D2D outage probability, the SOP of the cellular network, and the PNSC to validate the analytical analysis. In this respect, the cellular network's secrecy performance is analyzed, and the influence of the RIS is examined. The main parameters utilized to obtain the numerical and simulation results are set as ω_4 = 20 dB, ω_5 = 0 dB, N_B = 4 , $\mathcal{R}_b$ = 1 b/s/Hz, $\mathcal{R}_s$ = 1 b/s/Hz, and $\sigma_\upsilon^2 = 1$, where $\upsilon \in \{d, c, e\}$.

Figure 6.3 plots the analytical and simulation results of the outage probability of the RIS-assisted D2D P_{out}, versus ω_1, for different values of N at the RIS. For comparison purposes, the outage probability of a single AF-relaying D2D communication is presented. As shown, P_{out} of the D2D link decreases dramatically when ω_1 increases. Interestingly, as the number of elements at the RIS, N, increases, P_{out} improves significantly. Consequently, the reliability of D2D communication increases. As a result, it can be inferred that for a given D2D outage probability requirement, the RIS's energy efficiency can be enhanced by

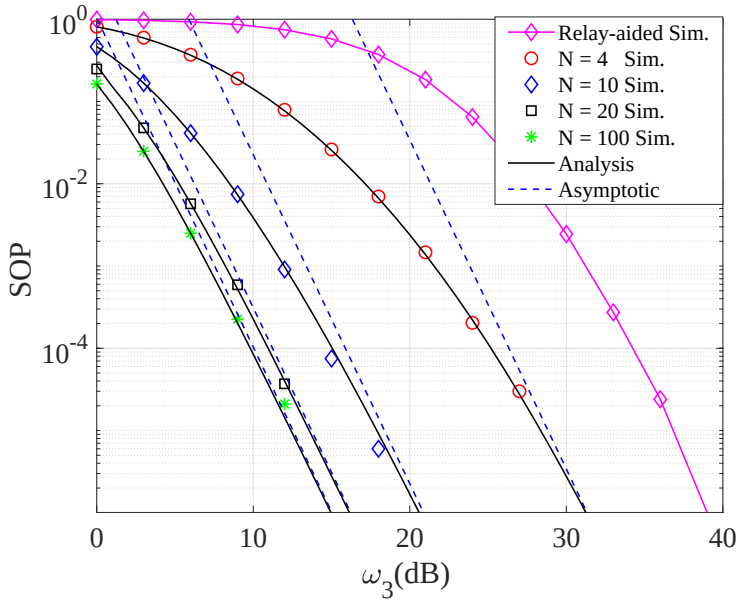


Fig. 6.4: The SOP of cellular network, where ω_4 = 20 dB, ω_5 = 0 dB, N_B = 4, and $\mathcal{R}_s$ = 1 b/s/Hz.

increasing N. To illustrate, ω_1 can be decreased by approximately 15 dB, using an RIS with N = 10 compared with N = 4 to achieve the D2D outage probability of 10^{-4}. It is worth mentioning that RIS-assisted system outperforms the AF-relaying system. To show the performance loss caused by discrete phase shifts, we provide simulation results with the phase error of each reflector uniformly distributed in $\left\{-\frac{\pi}{4}, \frac{\pi}{4}\right\}$ [32]. Furthermore, the simulation and numerical results agree perfectly, confirming the accuracy of our results.

The SOP is shown in Fig. 6.4 versus ω_3 for different values of N. Notably, the SOP decreases as N increases, demonstrating the influence of the jamming signals from RIS on E. Therefore, the security of the data transmission is enhanced. Moreover, the SOP decreases as ω_3 increases. To illustrate, ω_3 can be decreased by approximately 10 dB, using an RIS with N = 10 compared with N = 4 to achieve an SOP of 10^{-4}. As a benchmark, the SOP of the AF-relaying D2D communication [33] is provided. As revealed in our analysis and simulation, improved secrecy performance can be achieved using RIS compared to the relay-aided scenario. This is due to the fact that the eavesdropping signal is degraded at E

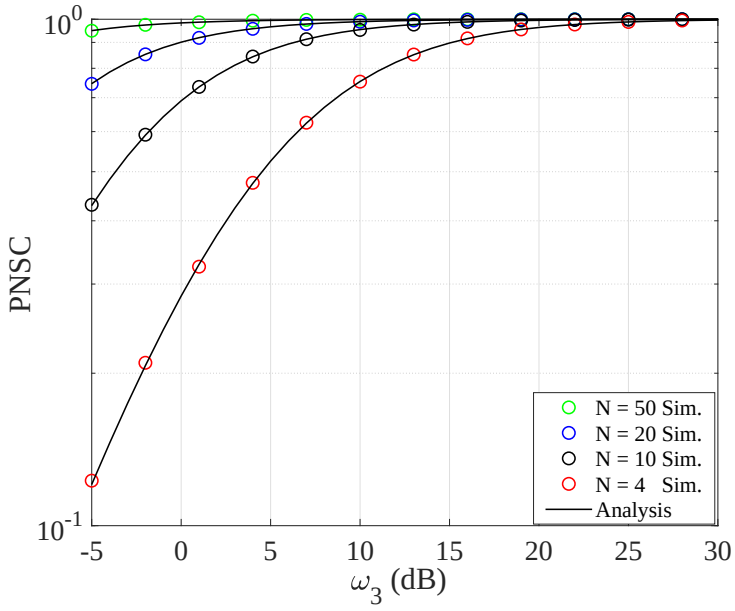


Fig. 6.5: The PNSC of cellular network, where ω_4 = 20 dB, ω_5 = 0 dB, and $\mathcal{R}_s$ = 1 b/s/Hz.

due to the jamming signals produced by RIS, which in turn results in more secure cellular transmission. To illustrate, ω_3 can be decreased by approximately 15 dB, using an RIS with N = 10 compared with relay-aided scenario to achieve an SOP of 10^{-4}. With this in mind, the asymptotic results are also presented, and an excellent match with the exact ones can be observed as $\omega_3 \to \infty$. This also confirms the accuracy of the expressions of $\mathcal{G}_a$ and $\mathcal{G}_d$.

Figure 6.5 illustrates the cellular PNSC versus ω_3, where the analytical result is provided by (6.25). Interestingly, the PNSC improves as N increases, showing the benefits of RIS. Additionally, as ω_3 increases, the PNSC increases, implying an improvement in the security level of the cellular network. It is worth mentioning that the non-zero secrecy capacity exists even when the eavesdropper's channel has a higher average SNR as compared to main channel i.e., $\gamma_E > \gamma_C$. Simulation results are shown to conform with the analytical results, validating the analysis.

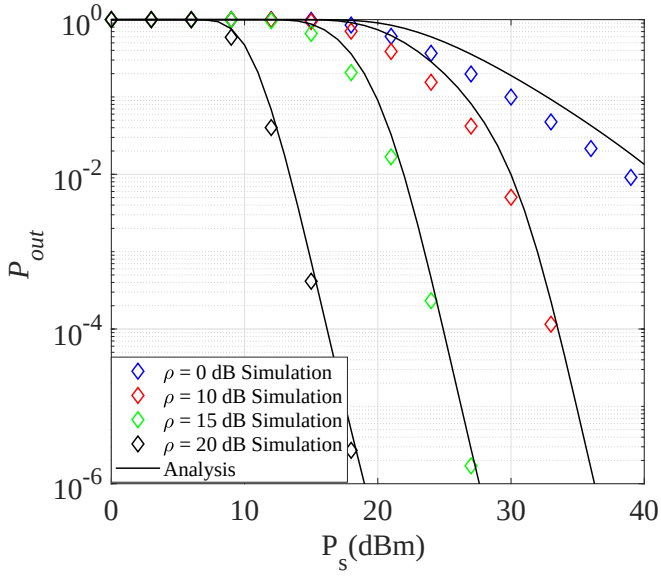


Fig. 6.6: The outage probability, P_{out}, vs. P_s, for different amplification gain values, ρ, where $N = 30$.

6.5.2 Active RIS

In this subsection, numerical results validated by Monte-Carlo simulations are presented. Specifically, the proposed active RIS-aided communication performance is evaluated in terms of the outage probability and SOP. Unless otherwise stated, the numerical and simulation results are obtained considering the following parameters: ϑ_b = 0.0001, β = 1.0007, $\eta = 3.5$, $\sigma_d^2 = 0$ dBm, $\sigma_e^2 = 0$ dBm, and $\sigma_r^2 = -80$ dBm. Considering a two-dimensional Cartesian coordinate for the simulation setup of the active RIS-aided system, we assume that S is located at the origin (0, 0), the RIS at (40m, 10m), E at (50m, 10m), and D at (100m, 0m).

In Fig. 6.6, the amplification impact on the received SNR at D is investigated. In this regard, the analytical and simulation results of the outage probability of the active RIS-aided communication, P_{out}, versus P_s, for different values of ρ at the RIS, where $N = 30$, is shown. It can be observed that P_{out} improves as ρ increases. That is, the transmission reliability increases. As an illustration, P_s can be reduced by about 18 dBm, employing an

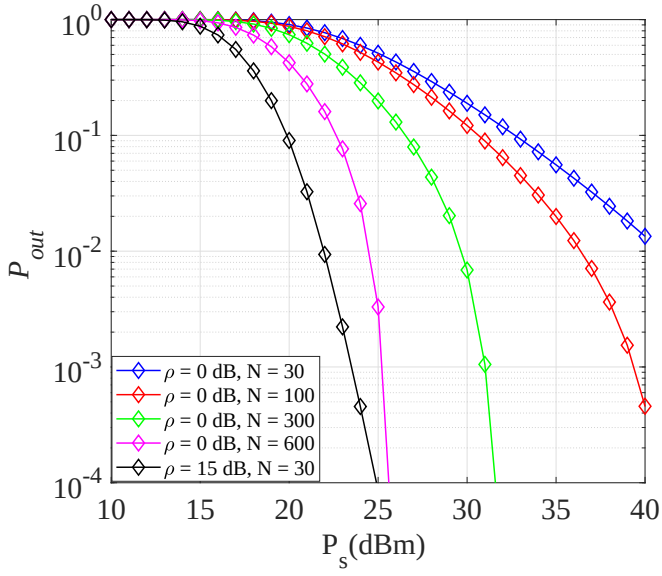


Fig. 6.7: The outage probability, P_{out}, vs. P_s, for different amplification gain values, ρ and N.

active RIS with ρ = 15 dB compared with passive RIS (ρ = 0 dB) to achieve $P_{out} = 10^{-2}$. To evaluate the influence of the active RIS on the reliability in the RIS-aided communication compared to a passive RIS, Fig. 6.7 presents P_{out}, versus P_s, for different values of N at the RIS. It can be seen that passive RIS requires more than N = 600 to achieve the same performance of active RIS with only N = 30 and ρ = 15 dB. Clearly using active RIS results in a significant decrease in the number of elements required to achieve a given performance. This reduction in the number of elements implies a decrease in the size of the RIS and the cost. A cost-effective design of the active RIS is proposed in the next section. The obtained results reveal that the double fading impact is overcome due to using active RIS compared to the passive RIS. Furthermore, simulation and numerical results agree well, confirming the accuracy of our analysis.

The SOP versus P_s is shown in Fig. 6.8 for different values of ρ, where $N = 30$, and $\bar{\gamma}_e = 10$ dB. It is evident that the SOP decreases as ρ increases, demonstrating the influence of the amplification at the active RIS, leading to the secrecy performance enhancement. In

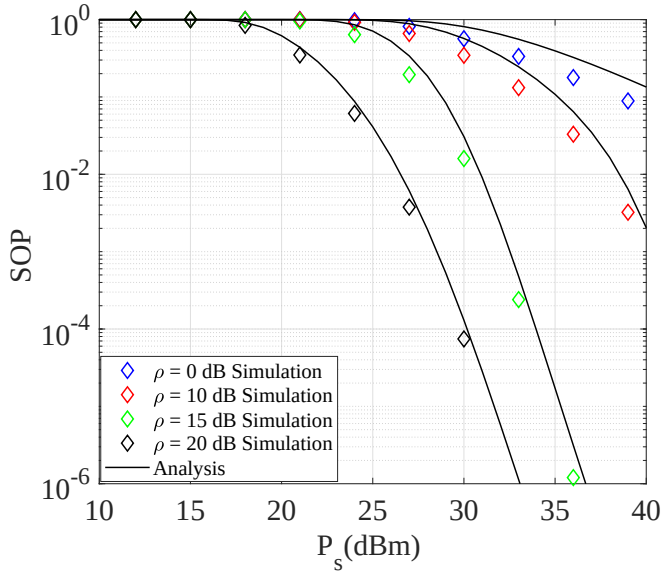


Fig. 6.8: The secrecy outage probability, SOP, vs. P_s, for different amplification gain, ρ, where $N = 30$, and $\bar{\gamma}_e = 10$ dB.

Fig. 6.9, the SOP is plotted versus the location of D, distance L(m), for the active aided communication. It can be observed that the SOP is significantly improved by using active RIS. It is also noteworthy that active RIS can potentially overcome the double fading problem by producing higher amplification gain and guaranteeing secure transmission. Furthermore, the SOP initially decreases to the lowest values at L = 40 m and then increases to 1. This can be explained by the fact that at L = 40 m, minimum distance between S and D, the fading on the RIS-D link is minimized. As a result, the SOP is lower.

Although active RIS consumes additional power to amplify the reflected signals, the significant decrease in the number of required elements considerably reduces the circuit power consumption. Thus, the benefit provided by active RIS over its passive counterpart can be achieved with the same power budget. It is also important to note that active RIS exploits the electromagnetic scattering principles to amplify the signals in the air without reception, and thus do not need complex and power-hungry radio-frequency chain components as in relays.

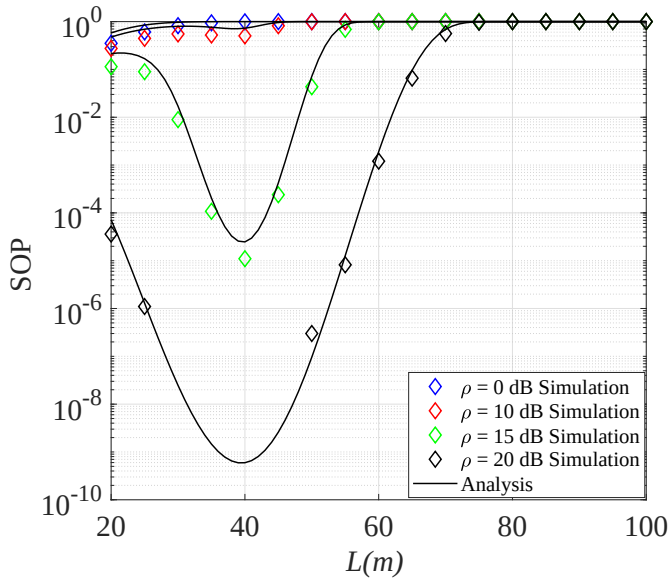


Fig. 6.9: The secrecy outage probability, SOP, vs. $L(m)$, for different amplification gain, ρ, where $N = 30$, $P_s = 40$ dBm, and $\bar{\gamma}_e = 10$ dB.

6.6 Design of an Active RIS for Smart Radio Environments

In the past, several designs have been proposed for reflect-arrays, which are the ancestors of RIS. For example, a 6" square offset beam reflect-array operating at 28 GHz with a 28.4 dB and 31.3 dB gains for square and parabolic modules, respectively [34]. We also have liquid crystal, graphene, terahertz arrays, and arrays of lenses for optical frequencies [35]. To obtain an intelligent radio environment, with these modules, their design must involve reconfigurable parameters. This improvement led to the design of reconfigurable reflect-arrays, liquid-crystal-based reconfigurable, and metal-only reflect-arrays [36], an electronically reconfigurable dual-frequency reflect-array with 1600 elements for X/Ku-band [37], to mention only a few. An overhead-aware RIS design has recently been proposed for an intelligent radio environment [38]. Here we propose an active RIS for smart radio environment, which has reflection and amplification capabilities.

Figure 6.10 depicts the structure of the proposed multi-layer active RIS module. It combines two feeds, two delay-lines, and a variable-gain amplifier. The RF-in feed detects the

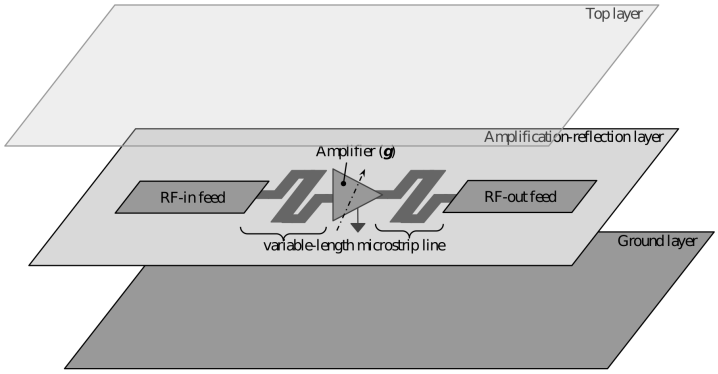


Fig. 6.10: Active RIS for an intelligent radio environment.

incoming signal, while the RF-out feed radiates the reflected and amplified signal towards the receiver. The two feeds are connected through an RF-amplifier. The ground layer represents the RIS module's connection to the ground and maybe slotted to reduce the amount of material used. The top layer represents the top cover of the module, and the middle layer represents the patch/RIS layer, which contains the feeds, the amplifier, and the two microstrip lines.

The incident wave couples into the input feed (RF-in feed), travels through the first variable length microstrip line, and undergoes the variable-gain amplification. The resulting signal goes through the second microstrip line before reaching the output feed (RF-out feed) for radiation towards the receiver. The most prominent way to design variable microstrip lines is by creating an insulated wire microstrip transmission line with a defined impedance. In our case, the line is to be printed in the form of a printed circuit board (PCB) trace of appropriate geometry. Two PCB traces are placed symmetrically to a specific axis to obtain the two microstrip lines, which are connected to the variable-gain amplifier. The amplifier in the RIS module, which includes an electronically tunable phase shifter, can be designed using ERA-1 [39], which requires about 3.4 V and 4 mA to introduce an angle retardation, ϕ, and a magnification coefficient, ρ. A Class-E wideband monolithic amplifier with a high dynamic frequency range can be used. In practice, it can be enclosed in a package using

transistors in the Darlington configuration, and their fabrication may use the InGaP doping technology.

6.7 Conclusion

In this chapter, RIS technology is investigated to enhance the reliability and robustness of D2D communication and improve the security level of the cellular network concurrently. New analytical expressions are derived for the cellular SOP and PNSC, and the D2D outage probability. Moreover, an active RIS-aided communication system is investigated in terms of robustness, reliability, and PLS. The performance of the system is evaluated . As revealed by our analysis and simulation, active RIS can overcome the double fading problem introduced by the cascaded channel due to the S-RIS and RIS-D links. Finally, a practical and cost-effective design of active RIS elements is proposed. Furthermore, the accuracy of these expressions are verified through Monte-Carlo simulations.

References

[1] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, Jul. 2019.

[2] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. Di Renzo, and M. Debbah, "Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 118–125, Oct. 2020.

[3] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[4] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162– 169, Sep. 2018.

[5] C. Huang, R. Mo, and C. Yuen, "Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1839–1850, Aug. 2020.

[6] A. D. Wyner, "The wire-tap channel," *Bell sys. tech. j.*, vol. 54, no. 8, pp. 1355â1387, Oct. 1975.

[7] X. Guan, Q. Wu, and R. Zhang, “Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[8] Z. Chu, W. Hao, P. Xiao, and J. Shi, “Intelligent reflecting surface aided multi-antenna secure transmission,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Jan. 2020.

[9] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis and M. D. Renzo, “Secrecy performance analysis of RIS-aided wireless communication systems,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12296–12300, Oct. 2020.

[10] B. Zheng, C. You, and R. Zhang, “Intelligent reflecting surface assisted multi-user OFDMA: Channel estimation and training design,” *IEEE Trans. on Wireless Commun.*, vol. 19, no. 12, pp. 8315–8329, Dec. 2020.

[11] B. Zheng and R. Zhang, “Intelligent reflecting surface-enhanced OFDMA: Channel estimation and reflection optimization,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 4, pp. 518–522, Apr. 2020.

[12] M. H. Khoshafa, T. Ngatched, and M. H. Ahmed, “On the physical layer security of underlay relay-aided device-to-device communications,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7609–7621, Jul. 2020.

[13] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, “Secure transmission in wiretap channels using full-duplex relay-aided D2D communications with outdated CSI,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 8, pp. 1216–1220, Aug. 2020.

[14] A.-A. A. Boulogeorgos and A. Alexiou, “Performance analysis of reconfigurable intelligent surface-assisted wireless systems and comparison with relaying,” *IEEE Access*, vol. 8, pp. 94 463â94 483, Jun 2020.

[15] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah and C. Yuen, “Reconfigurable intelligent surfaces for energy efficiency in wireless communication,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.

[16] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, “Robust and secure wireless communications via intelligent reflecting surfaces,” *IEEE Journal Sel. Areas in Commun.*, vol. 38, no. 11, pp. 2637–2652, Nov. 2020.

[17] L. Dong and H.-M. Wang, “Secure MIMO transmission via intelligent reflecting surface,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 787–790, Jan. 2020.

[18] M. Cui, G. Zhang, and R. Zhang, “Secure wireless communication via intelligent reflecting surface,” *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, May 2019.

[19] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*, McGraw-Hill Education, 2002.

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

[21] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[22] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[23] *The Wolfram Functions Site*, "Wolfram Research. (Oct. 2001). [Online]. Available: http://functions.wolfram.com/07.34.03.0606.01

[24] *The Wolfram Functions Site*, "Wolfram Research. (Oct. 2001). [Online]. Available: http://functions.wolfram.com/07.34.03.0228.01

[25] Ö. Özdogan, E. Björnson and E. G. Larsson, "Intelligent reflecting surfaces: Physics, propagation, and pathloss modeling," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 581–585, May 2020

[26] H. Guo, Y. Liang, J. Chen and E. G. Larsson, "Weighted sum-rate maximization for reconfigurable intelligent surface aided wireless networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3064–3076, Feb. 2020.

[27] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Jun. 2019

[28] R. Long, Y. -C. Liang, Y. Pei and E. G. Larsson, "Active reconfigurable intelligent surface aided wireless communications," *IEEE Trans Wireless Commun.*, Mar. 2021.

[29] Z. Zhang, L. Dai, X. Chen, C. Liu, F. Yang, R. Schober, and H. V. Poor, "Active RIS vs. passive RIS: Which will prevail in 6G?," *arXiv preprint arXiv:2103.15154*, Mar. 2021.

[30] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*, McGraw-Hill Education, 2002.

[31] D. Sadhwani, R. N. Yadav, and S. Aggarwal, "Tighter bounds on the gaussian q function and its application in Nakagami-m fading channel," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 574–577, Oct. 2017.

[32] P. Xu, G. Chen, G. Pan and M. D. Renzo, “Ergodic secrecy capacity of RIS-assisted communication systems in the presence of discrete phase shifts and multiple eavesdroppers,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 629–633, Mar. 2021.

[33] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, “Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications,” *IEEE Access*, vol. 8, pp. 53 575–53 586, Mar. 2020.

[34] D. M. Pozar, S. D. Targonski and H. D. Syrigos, “Design of millimeter wave microstrip reflectarrays,” *IEEE Trans. Antennas Propag.*, vol. 45, no. 2, pp. 287–296, Feb. 1997.

[35] E. Carrasco and J. A. Encinar, “Reflectarray antennas: A review,” in *Proc. Forum Electromagn. Res. Methods Appl. Technol. (FERMAT)*, vol. 16, Aug. 2016.

[36] R. Deng, F. Yang, S. Xu and M. Li, “A Low-cost metal-only reflectarray using modified slot-type phoenix element with 360Â◦ phase coverage,” *IEEE Trans. Antennas Propag.*, vol. 64, no. 4, pp. 1556–1560, Apr. 2016.

[37] H. Yang et al., “A 1600-element dual-frequency electronically reconfigurable reflectarray at X/Ku-band,” *IEEE Trans. Antennas Propag.*, vol. 65, no. 6, pp. 3024–3032, Jun. 2017.

[38] A. Zappone, M. Di Renzo, F. Shams, X. Qian and M. Debbah, “Overhead-aware design of reconfigurable intelligent surfaces in smart Radio environments,” *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 126–141, Jan. 2021.

[39] M. E. Bialkowski, A. W. Robinson, and H. J. Song, “Design, development, and testing of X-band amplifying reflectarrays,” *IEEE Trans. Antennas Propag.*, vol. 50, no. 8, pp. 1065–1076, Aug. 2002.

Chapter 7

Reconfigurable Intelligent Surfaces-Aided Secure Underlay CR Networks

7.1 Abstract

In this chapter, we investigate a RIS-aided wireless communication system in an underlay cognitive radio network. An RIS is utilized to adjust its reflecting elements to enhance the secondary network data transmission while improving the primary network's secrecy performance concurrently. Specifically, analytical results for the outage probability for the secondary network, the secrecy outage probability, and the probability of non-zero secrecy capacity for the primary network are derived in closed-form. Simulation and analytical results are presented to verify the derived expressions' correctness and the effectiveness of the proposed scenario. Furthermore, asymptotic analysis is carried out.

7.2 Introduction

Mobile wireless communication has experienced rapid development in data traffic due to the dramatic growth of smart devices. According to Cisco, the average number of mobiles per capita will be 3.6 by 2023 [1], leading to an enormous demand for radio spectrum resources, including bandwidth and energy. Consequently, spectral efficiency and energy efficiency are becoming two crucial principles for designing future wireless networks [2]. Cognitive radio (CR) has been proposed in [3] as an efficient technique to improve spectral efficiency. In CR networks, the spectrum can be shared by two different networks, the primary network (PN) and the secondary network (SN), provided that the produced interference from the SN to the PN is controlled by interference constraint. In [4], the RIS technology has been employed to aid data transmission in CR networks. The authors in [5] proposed an RIS-assisted CR system to enhance the secondary's achievable rate by taking the interference effect on the primary users into account.

In this chapter, we propose a secure RIS-aided underlay cognitive network. To the best of our knowledge, no work has been reported in the literature investigating the use of RIS to enhance the PLS of the PN and improve the SN transmission link simultaneously. Furthermore, by taking into account the interference produced by the SN and the RIS on the PN, the impact of the RIS on the PN security is evaluated. The main contributions of this chapter are listed as follows:

- The RIS is introduced to enhance the robustness and reliability of the SN communication, while simultaneously improving the PLS of the PN.
- To compensate for the spectrum sharing, the RIS technology is utilized as a friendly jammer to ensure a high-secrecy performance for the PN, consequently enabling a win-win situation between the two networks, i.e., security provisioning of the PN and high reliability and robustness for the SN.

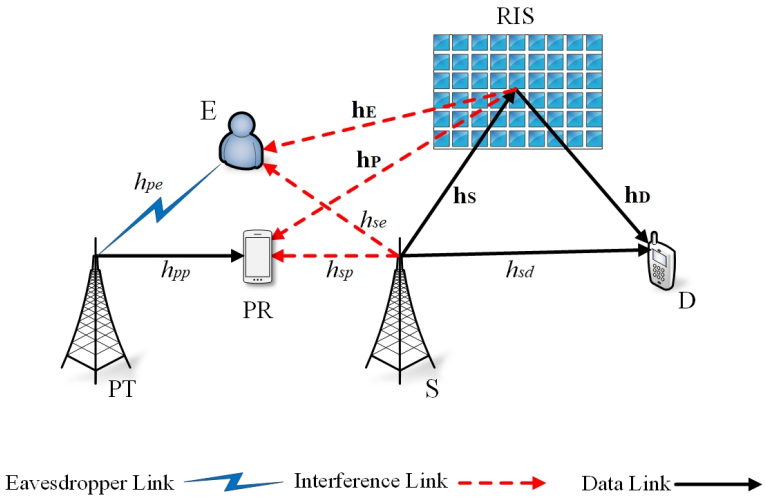


Fig. 7.1: System Model.

- The SN outage probability is investigated, and a novel analytical expression is derived. Moreover, the PN secrecy performance is examined, and closed-form expressions for the SOP and PNSC are also derived.
- Asymptotic analysis is carried out for the SOP to get more insights into the effects of the proposed system's parameters.
- The accuracy of our analyses is verified through extensive Monte-Carlo simulations.

7.3 System Model

As shown in Fig. 7.1, we consider an underlay cognitive network where the SN shares the licensed spectrum of the PN. The SN consists of a single-antenna secondary transmitter, S, and a single-antenna secondary receiver, D. The PN consists of a primary transmitter, PT, and a primary receiver, PR, each equipped with a single antenna. PT and PR are communicating in the presence of a single-antenna eavesdropper, E. It is worth mentioning that the direct links from S to D, PR, and E are considered. An RIS is deployed on a surrounding building's facade to assist S in improving the propagation conditions by providing

high-quality virtual link from S to D, while serving as a jammer towards E, resulting in an enhanced secrecy rate for the PN. The RIS is made of N reflecting elements. It is assumed that the CSI of S is perfectly known at the RIS to maximize the received SNR at D. However, E is considered as passive, and thus its CSI is not available at both the RIS and the PT.

All the channels are assumed to undergo Rayleigh fading. The channel coefficients for the S $\rightarrow$ RIS, RIS $\rightarrow$ D, S $\rightarrow$ D, PT $\rightarrow$ PR, PT $\rightarrow$ E, RIS $\rightarrow$ E, RIS $\rightarrow$ PR, S $\rightarrow$ E, and S $\rightarrow$ PR links are denoted as $\mathbf{h_S}$[1], $\mathbf{h_D}$, h_{sd}, h_{pp}, h_{pe}, $\mathbf{h_E}$, $\mathbf{h_P}$, h_{se}, and h_{sp}, respectively. The signals reflected by the RIS two or more times are neglected due to severe path loss. Thus, the received signal at D can be expressed as

$$y_D = \sqrt{P_s}\, x_s \left[\sum_{i=1}^{N} h_{s_i}\, h_{d_i}\, e^{j\phi_i} + h_{sd} \right] + n_d, \tag{7.1}$$

where P_s is the SN transmission power, x_s is the SN transmitted signal, and n_d is the AWGN at D. In addition, h_{s_i} and h_{d_i} are complex Gaussian RVs with a zero mean and unit variance, and ϕ_i is the adjustable phase applied by the i^{th} reflecting element of the RIS. Moreover, we assume that the PT is far away from the RIS and D and, therefore, it does not impose any real interference. Consequently, the interference at the RIS and D from PT is negligible; this is a well-known assumption that is widely used in the literature (e.g. [6], [7]). Furthermore, the phases of the channels h_{s_i} and h_{d_i} are assumed to be perfectly known at the RIS. Hence, the optimal phase shift at the RIS is selected to maximize the SNR at D [8], [9]. Besides, we assume that the reflected gain of the i^{th} metasurface is equal to 1 [8], [10]. The received signal at the PR can be expressed as

$$y_P = \sqrt{P_p}\, h_{pp}\, x_p + \sqrt{P_s}\; x_s \left[\sum_{i=1}^{N} h_{s_i}\, h_{p_i}\, e^{j\phi_i} + h_{sp} \right] + n_p, \tag{7.2}$$

[1] The bold font is used to indicate vectors.

where P_p is the PN transmission power, x_p is the PN transmitted signal, and n_p is the AWGN at the PR. The received signal at the E is given by

$$y_E = \sqrt{P_p}\, h_{pe}\, x_p + \sqrt{P_s}\, x_s \left[\sum_{i=1}^{N} h_{s_i}\, h_{e_i}\, e^{j\phi_i} + h_{se} \right] + n_e, \tag{7.3}$$

where h_{e_i} is the channel coefficient between the i^{th} element of the RIS and the E, and n_e is the AWGN at the E.

7.4 Performance Analysis

In this section, the SN outage probability, P_{out}, the PN SOP, the asymptotic SOP, and the PN's PNSC are investigated.

7.4.1 CR Outage Probability

For the SN, the outage probability, P_{out}, is defined by

$$P_{out} = \Pr\left(\gamma_D \leq \vartheta_b\right) = F_{\gamma_D}(\vartheta_b), \tag{7.4}$$

where $\vartheta_b = 2^{\mathcal{R}_d} - 1$, $\mathcal{R}_d$ is the data rate of the SN transmission, and γ_D is the instantaneous SNR for the CR link which is given by

$$\gamma_D = \frac{P_s}{\sigma_d^2} \left| \sum_{i=1}^{N} h_{s_i}\, h_{d_i}\, e^{j\phi_i} + h_{sd} \right|^2. \tag{7.5}$$

In the underlay CR system, the transmitted power from S, P_s, must be under a certain level to limit the interference. With this in mind, P_s can be constrained as $P_s\, Y_P \leq \mathcal{Q}$, where Y_P is the channel fading coefficient from the RIS and S, respectively, and $\mathcal{Q}$ is the interference temperature limit. To elaborate, Y_P consists of both the direct link from S and

the reflected link from the RIS, while $\mathcal{Q}$ represents the maximum tolerated interference power at the PR. From the primary user perspective, setting $P_s = \frac{\mathcal{Q}}{Y_P}$ is the worst case scenario which still guarantees its reliable operation [11]. From (7.2), Y_P can be expressed as

$$Y_P = \left| \sum_{i=1}^{N} h_{s_i} \, h_{p_i} \, e^{j\phi_i} + h_{sp} \right|^2, \tag{7.6}$$

where $\sum_{i=1}^{N} h_{s_i} \, h_{p_i} \, e^{j\phi_i} + h_{sp}$ can be approximated as a complex Gaussian RV. Hence, Y_{P} can be approximated by an exponential RV with a parameter $\lambda_{\mathrm{P}} = N + 1$. Therefore, its probability density function (PDF) can be expressed as

$$f_{Y_P}(\gamma) = \frac{1}{\lambda_P} \exp\left(-\frac{\gamma}{\lambda_P}\right). \tag{7.7}$$

Now, by replacing P_s with $\frac{\mathcal{Q}}{Y_P}$ in (7.5), γ_D can be obtained as

$$\gamma_D = \frac{\mathcal{Q}}{Y_P \, \sigma_d^2} \left| \sum_{i=1}^{N} h_{s_i} \, h_{d_i} \, e^{j\phi_i} + h_{sd} \right|^2 = \frac{Y_D}{Y_P}, \tag{7.8}$$

where $Y_D = \Omega \left(\sum_{i=1}^{N} |h_{s_i}| \, |h_{d_i}| + |h_{sd}| \right)^2$, $\Omega = \frac{\mathcal{Q}}{\sigma_d^2}$. According to the central limit theorem, $\chi_1 = \sum_{i=1}^{N} |h_{s_i}| \, |h_{d_i}|$ can be approximated as a Gaussian RV with a mean value $\mu = \frac{N\pi}{4}$ and variance $\sigma^2 = N\left(1 - \frac{\pi}{16}\right)$ [8]. Moreover, $\chi_2 = |h_{sd}|$ is a Rayleigh-distributed RV with a parameter λ_D. Thus, the PDFs of χ_1 and χ_2 are given by

$$f_{\chi_1}(\gamma) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(\frac{-(\gamma - \mu)^2}{2\sigma^2} \right), \tag{7.9}$$

and

$$f_{\chi_2}(\gamma) = \frac{\gamma}{\lambda_D} \exp\left(-\frac{\gamma^2}{2\lambda_D} \right), \tag{7.10}$$

respectively. Hence, Y_D can be expressed as $Y_D = \Omega \left(\chi_1 + \chi_2\right)^2$, leading to its cumulative distribution function (CDF) given by [12]

$$F_{Y_D}(\gamma) = \frac{1}{2}\left[\text{erf}\left(\frac{\vartheta_1\sqrt{\gamma}-\mu}{\sqrt{2\sigma^2}}\right) + \text{erf}\left(\frac{\mu}{\sqrt{2\sigma^2}}\right)\right] - \frac{\sqrt{\lambda_D}}{2\zeta_1}\exp\left(\frac{-\left(\vartheta_1\sqrt{\gamma}-\mu\right)^2}{2\zeta_1^2}\right) \times \text{erf}\left(\frac{\zeta_4\sqrt{\gamma}-\zeta_5}{\zeta_1\zeta_2}\right) - \frac{\sqrt{\lambda_D}}{2\zeta_1}\exp\left(\frac{-\left(\vartheta_1\sqrt{\gamma}-\mu\right)^2}{2\zeta_1^2}\right)\text{erf}\left(\frac{\zeta_3\sqrt{\gamma}+\zeta_5}{\zeta_1\zeta_2}\right), \tag{7.11}$$

where $\vartheta_1 = \Omega^{-1}$, $\zeta_1 = \sqrt{\sigma^2+\lambda_D}$, $\zeta_2 = \sqrt{2\sigma^2\lambda_D}$, $\zeta_3 = \sigma^2\vartheta_1$, $\zeta_4 = \lambda_D\vartheta_1$, $\zeta_5 = \lambda_D\,\mu$, and $\text{erf}(.)$ is the error function [13, eq. (8.250.1)]. P_{out}, which is defined in (7.4), can be further mathematically written as [14]

$$P_{out} = \int_0^\infty F_{Y_D}(\gamma\, x)\, f_{Y_P}(x)\, dx. \tag{7.12}$$

However, utilizing the expression in (7.11) to evaluate $F_{\gamma_D}(\gamma)$ is not mathematically tractable. Thus, the following alternative expression for the erf function [15]

$$\text{erf}\left(x\right) \approx \begin{cases} 1 - \sum_{i=1}^{4} \Psi_i \exp\left(-\Delta_i\, x^2\right) & x \geq 0 \\ -1 + \sum_{i=1}^{4} \Psi_i \exp\left(-\Delta_i\, x^2\right) & x < 0, \end{cases} \tag{7.13}$$

where $\Psi = [1/8, 1/4, 1/4, 1/4]$ and $\Delta = [1, 2, 20/3, 20/17]$, can be utilized. By plugging (7.11) into (7.12) with the help of (7.13) and [13, eq. (2.33.1)], P_{out} can be derived as

$$P_{out} = \mathcal{I}_1 - \mathcal{I}_2 - \mathcal{I}_3, \tag{7.14}$$

where $\mathcal{I}_1$, $\mathcal{I}_2$, and $\mathcal{I}_3$ are shown as

$$\begin{aligned}\mathcal{I}_1 =& \sum_{i=1}^{4} \frac{\Psi_i \exp\left(-\frac{a_2}{2}\right)}{4b_1^2\sqrt{(a_2/2)^3}\lambda_P}\left[2\sqrt{a_1}\left(\exp\left(b_2\left(a_2-a_1b_2\right)\right)-2\right)+\exp\left(\frac{a_2^2}{4a_1}\right)\sqrt{\pi}\left(a_2-2a_1b_2\right)\right.\\ &\left.\times\left(\text{erfc}\left(\frac{a_2}{2\sqrt{a_1}}\right)-\text{erf}\left(\frac{a_2}{2\sqrt{a_1}}\right)+\text{erf}\left(\frac{a_2-2a_1b_2}{2\sqrt{a_1}}\right)\right)\right]+\exp\left(\frac{-b_2^2}{b_1^2\lambda_P}\right)\\ &+\frac{1}{2}\left(\text{erf}\left(\frac{\mu}{\sqrt{2\sigma^2}}\right)-1\right),\end{aligned} \tag{7.15}$$

$$\begin{aligned}\mathcal{I}_2 =& \frac{\exp\left(-c_3\right)\Xi_1}{4}\left[\frac{1}{\sqrt{c_1^3}}\left(2\sqrt{c_1}\left(2-\exp\left(\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)\left(c_2-c_1\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)\right)\right)\right)\right.\right.\\ &\left.-\Xi_2\sqrt{\pi}\exp\left(\frac{c_2^2}{4c_1}\right)\left(\text{erf}\left(\frac{\Xi_2}{2\sqrt{c_1}}\right)-\text{erf}\left(\frac{c_2}{2\sqrt{c_1}}\right)+\text{erfc}\left(\frac{c_2}{2\sqrt{c_1}}\right)\right)\right)+\sum_{i=1}^{4}\frac{\Psi_i}{\sqrt{c_4^3}}\\ &\left(2\sqrt{c_4}\left(\exp\left(\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)\left(c_2-c_4\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)\right)\right)-2\right)+\Xi_3\sqrt{\pi}\exp\left(\frac{c_2^2}{4c_4}\right)\left(\text{erf}\left(\frac{\Xi_3}{2\sqrt{c_4}}\right)\right.\\ &\left.\left.-\text{erf}\left(\frac{c_2}{2\sqrt{c_4}}\right)+\text{erfc}\left(\frac{c_2}{2\sqrt{c_4}}\right)\right)\right)\right],\end{aligned} \tag{7.16}$$

$$\begin{aligned}\mathcal{I}_3 =& \frac{\Xi_4}{4}\exp\left(-\left(\upsilon_3-\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)\upsilon_2\right)\right)\left[\upsilon_1^{-\frac{3}{2}}\exp\left(-\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)^2\upsilon_1\right)\left(-\Xi_5\sqrt{\pi}\ \exp\left(\frac{\Xi_5^2}{4\upsilon_1}\right)\right.\right.\\ &\left.\text{erf}\left(\frac{\Xi_5}{2\sqrt{\upsilon_1}}\right)+2\sqrt{\upsilon_1}\right)+\sum_{i=1}^{4}\frac{\Psi_i}{\sqrt{\upsilon_4^3}}\exp\left(-\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right)^2\upsilon_4\right)\left(-2\sqrt{\upsilon_4}+\Xi_6\sqrt{\pi}\ \exp\left(\frac{\Xi_6^2}{4\upsilon_4}\right)\right.\\ &\left.\left.\text{erf}\left(\frac{\Xi_6}{2\sqrt{\upsilon_4}}\right)\right)\right],\end{aligned} \tag{7.17}$$

where

$b_1 = \frac{\vartheta_1\sqrt{\gamma}}{\sqrt{2\sigma^2}},\ b_2 = \frac{\mu}{\sqrt{2\sigma^2}},\ a_1 = \frac{1}{\lambda_p\, b_1^2} + \Delta_i,\ a_2 = \frac{2b_2}{\lambda_p\, b_1^2},\ \Xi_1 = \frac{\zeta_1\zeta_2^2\sqrt{\lambda_D}}{\lambda_P\zeta_4^2},\ \Xi_2 = c_2 - 2c_1\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right),$

$\Xi_3 = c_2 - 2c_4\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right), \quad c_1 = \frac{\vartheta_1^2\zeta_2^2}{2\zeta_4^2} + \frac{\zeta_1^2\zeta_2^2}{\lambda_P\zeta_4^2\gamma}, \quad c_2 = \frac{\zeta_2}{\zeta_1\zeta_4^2\gamma}\left(\vartheta_1\left(\vartheta_1\zeta_5\gamma - \mu\zeta_4\gamma\right) + \frac{2\zeta_1^2\zeta_5}{\lambda_P}\right),$

$c_3 = \frac{\zeta_5^2}{\lambda_P\zeta_4^2} + \frac{1}{2\zeta_1^2}\left(\frac{\vartheta_1\zeta_5}{\zeta_4} - \mu\right)^2, \quad c_4 = c_1 + \Delta_i, \upsilon_1 = \frac{\vartheta_1^2\zeta_2^2\gamma}{2\zeta_3^2} + \frac{\zeta_1^2\zeta_2^2}{\lambda_P\zeta_3^2},$
$\upsilon_2 = \frac{\zeta_2}{\zeta_1\zeta_3^2}\left(\vartheta_1\left(\vartheta_1\zeta_5\gamma + \mu\zeta_3\sqrt{\gamma}\right) + \frac{2\zeta_1^2\zeta_5}{\lambda_P}\right), \quad \upsilon_3 = \frac{\zeta_5^2}{\lambda_P\zeta_3^2} + \frac{1}{2\zeta_1^2}\left(\frac{\vartheta_1\zeta_5\sqrt{\gamma}}{\zeta_3} + \mu\right)^2, \quad \upsilon_4 =$

$\upsilon_1 + \Delta_i, \quad \Xi_4 = \frac{\zeta_1\zeta_2^2\sqrt{\lambda_D}}{\lambda_P\zeta_3^2}, \quad \Xi_5 = 2\upsilon_1\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right) - \upsilon_2, \quad \text{and } \Xi_6 = 2\upsilon_4\left(\frac{\zeta_5}{\zeta_1\zeta_2}\right) - \upsilon_2.$

Now, P_{out} can be obtained by plugging (7.14) into (7.4).

7.4.2 Secrecy Outage Probability

The SOP can be defined as the probability that the achievable secrecy rate is less than a predefined target secrecy rate, $\mathcal{R}_s$, for the cellular transmission. Based on this, the SOP is given by

$$\text{SOP} = \Pr\left(C_S < \mathcal{R}_s\right), \tag{7.18}$$

where C_S is the secrecy capacity, which is given by

$$C_S = \begin{cases} C_P - C_E, & \gamma_P > \gamma_E, \\ 0, & \gamma_P \leq \gamma_E, \end{cases} \tag{7.19}$$

where C_P and C_E denote the PN and the E capacities, respectively, and γ_P and γ_E are the instantaneous SINR at the PR and the E, respectively. In this regard, C_P is given by

$$C_P = \log_2\Big(1 + \gamma_P\Big), \tag{7.20}$$

where γ_P is given by

$$\gamma_P = \frac{P_p\left|h_{pp}\right|^2}{P_s\, Y_P + \sigma_p^2}. \tag{7.21}$$

Now, by replacing P_s in (7.21) with $\frac{\mathcal{Q}}{Y_P}$ yields

$$\gamma_P = \frac{P_p \left|h_{pp}\right|^2}{\mathcal{Q} + \sigma_p^2} = \omega \ \left|h_{pp}\right|^2, \tag{7.22}$$

where $\omega = \frac{\bar{\gamma}_p}{\frac{\mathcal{Q}}{\sigma_p^2}+1}$, and $\bar{\gamma}_p = \frac{P_p}{\sigma_p^2}$. In addition, C_E can be obtained by

$$C_E = \log_2\Big(1 + \gamma_E\Big), \tag{7.23}$$

where γ_E is given by

$$\begin{aligned} \gamma_E &= \frac{P_p \left|h_{pe}\right|^2}{P_s \left|\sum_{i=1}^{N} h_{s_i}\, h_{e_i}\, e^{j\phi_i} + h_{se}\right|^2 + \sigma_e^2} \\ &= \frac{\gamma_{pe}}{Y_E + 1}, \end{aligned} \tag{7.24}$$

where $Y_E = \bar{\gamma}_{se} \left|\sum_{i=1}^{N} h_{s_i}\, h_{e_i}\, e^{j\phi_i} + h_{se}\right|^2$, $\bar{\gamma}_{se} = \frac{P_s}{\sigma_e^2}$, $\gamma_{pe} = \bar{\gamma}_e \ \left|h_{pe}\right|^2$, and $\bar{\gamma}_e = \frac{P_p}{\sigma_e^2}$. The term Y_E can be approximated by an exponential RV with a parameter $\lambda_{\mathrm{E}} = N\,\bar{\gamma}_{se} + \bar{\gamma}_{se}$. Hence, the PDF of Y_E can be expressed as

$$f_{Y_E}\left(\gamma\right) = \frac{1}{\lambda_E}\ \exp\left(-\frac{\gamma}{\lambda_E}\right). \tag{7.25}$$

The PDF of γ_E can be derived using

$$f_{\gamma_E}(\gamma) = \int_0^{\infty} (x+1)\, f_{\gamma_{pe}}(\gamma\,(x+1))\, f_{Y_E}\left(x\right) dx, \tag{7.26}$$

where $f_{\gamma_{pe}}(.)$ is given by

$$f_{\gamma_{pe}}\left(\gamma\right) = \frac{1}{\bar{\gamma}_e}\ \exp\left(-\frac{\gamma}{\bar{\gamma}_e}\right). \tag{7.27}$$

By substituting (7.27) and (7.25) in (7.26), $f_{\gamma_E}(\gamma)$ can be obtained as

$$f_{\gamma_E}(\gamma) = \exp\left(-\frac{\gamma}{\bar{\gamma}_e}\right) \frac{(\bar{\gamma}_e(1+\lambda_E)+\lambda_E\,\gamma)}{(\bar{\gamma}_e+\lambda_E\,\gamma)^2}. \tag{7.28}$$

Now, the SOP can be formulated as

$$\text{SOP} = \int_0^\infty F_{\gamma_P}(\beta\,\gamma+\alpha)\, f_{\gamma_E}(\gamma)\, d\gamma, \tag{7.29}$$

where $\beta = 2^{\mathcal{R}_s}$, $\alpha = \beta - 1$, and $F_{\gamma_P}(.)$ is given by

$$F_{\gamma_P}(\gamma) = \left(1 - \exp\left(-\frac{\gamma}{\omega}\right)\right). \tag{7.30}$$

By plugging (7.30) and (7.28) in (7.29), and using partial fraction expansion, then [13, eq. (3.382.4)], the SOP can be derived as

$$\begin{aligned}\text{SOP} =& \frac{\exp\left(-\frac{\alpha}{\omega}\right)}{\lambda_E\,\omega}\left[\lambda_E\,\omega\left(\exp\left(\frac{\alpha}{\omega}\right)-1\right)+\exp\left(\frac{\bar{\gamma}_e\,(\beta\,\bar{\gamma}_e+\omega)}{\lambda_E\,\omega}\right)\right.\\ &\left.\left(\beta\,\lambda_E^2+\omega\,(\bar{\gamma}_e-1)\right)\Gamma\left(0,\frac{\bar{\gamma}_e\,(\beta\,\bar{\gamma}_e+\omega)}{\lambda_E\,\omega}\right)\right].\end{aligned} \tag{7.31}$$

7.4.3 Asymptotic Secrecy Outage Analysis

To acquire more insights on the system design, the asymptotic SOP, SOP$^\infty$, is examined when $\gamma_p \to \infty$. In this scenario, we consider that $\overline{\gamma}_p >> \overline{\gamma}_e$. SOP$^\infty$ can be written as

$$\text{SOP}^\infty = (\mathcal{G}_a\overline{\gamma}_d)^{-\mathcal{G}_d} + \mathcal{O}(\overline{\gamma}_d^{-\mathcal{G}_d}), \tag{7.32}$$

where $\mathcal{G}_d$ is the secrecy diversity order, $\mathcal{G}_a$ is the secrecy array gain, and $\mathcal{O}(.)$ is the higher order terms. Mathematically speaking, to derive the SOP$^\infty$, the asymptotic CDF, $F^\infty_{\gamma_p}(\gamma)$, is first obtained by following the same steps in the derivation of [16, eq. (42)]. By plugging

$F_{\gamma_p}^{\infty}(\gamma)$ into (7.29), and using partial fraction expansion, then [13, eq. (3.382.4)], after performing some algebraic manipulations, it turns out that $\mathcal{G}_d$ = 1 and $\mathcal{G}_a$ is given by

$$\mathcal{G}_a = \left[\left(\frac{\beta\,\bar{\gamma}_e}{\sqrt{\lambda_E}}\left(\frac{1}{\sqrt{\lambda_E}}W_{-1,-0.5}\left(\frac{1}{\lambda_E}\right) + W_{-1.5,-1}\left(\frac{1}{\lambda_E}\right)\right) + \alpha\left(\frac{1}{\sqrt{\lambda_E}}W_{-0.5,0}\left(\frac{1}{\lambda_E}\right)\right.\right.\right.$$
$$\left.\left.\left. + W_{-1,0.5}\left(\frac{1}{\lambda_E}\right)\right)\right)\exp\left(\frac{1}{\lambda_E}\right)\right]^{-1}, \tag{7.33}$$

where $W_{a,b}(.)$ is the Whittaker function [13, eq. (9.220.4)].

7.4.4 Probability of Non-zero Secrecy Capacity

The non-zero secrecy capacity is obtained when $\gamma_P > \gamma_E$. The PNSC can be obtained by

$$\text{PNSC} = \Pr\left(\gamma_P > \gamma_E\right) = 1 - \int_0^{\infty} F_{\gamma_P}(\gamma)\, f_{\gamma_E}(\gamma)\, d\gamma. \tag{7.34}$$

By plugging (7.30) and (7.28) in (7.34), and using partial fraction expansion, then [13, eq. (3.382.4)], the PNSC can be derived as

$$\text{PNSC} = 1 - \frac{1}{\lambda_E\,\omega}\left[\exp\left(\frac{\bar{\gamma}_e\left(\bar{\gamma}_e+\omega\right)}{\lambda_E\,\omega}\right)\left(\lambda_E^2 + \omega\left(\bar{\gamma}_e - 1\right)\right)\Gamma\left(0, \frac{\bar{\gamma}_e\left(\bar{\gamma}_e+\omega\right)}{\lambda_E\,\omega}\right)\right]. \tag{7.35}$$

7.5 Results and Discussions

In this section, numerical results of the CR outage probability, the primary SOP, and the primary PNSC are presented and compared with those obtained through Monte-Carlo simulations. In this respect, the effect of different related parameters on the CR outage probability, the primary SOP, and primary PNSC of the proposed system model are investigated. Unless otherwise stated, numerical and simulation results are obtained considering the following

parameters: $\mathcal{Q}$ = 10 dBW, $\bar{\gamma}_{se}$ = 5 dB, $\mathcal{R}_b$ = 1 b/s/Hz, λ_D = 2, and β = 1.003.

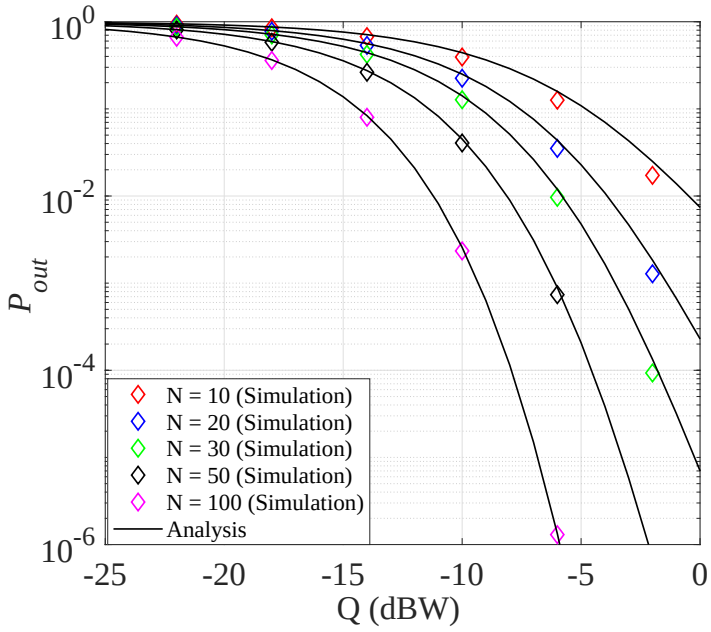


Fig. 7.2: The secondary outage probability, P_{out}, vs. $\mathcal{Q}$, for different values of the number of reflecting elements, N, where $\mathcal{R}_d = 1$ b/s/Hz.

Figure 7.2 plots the analytical and simulation results of the outage probability of the RIS-assisted CR, P_{out}, versus $\mathcal{Q}$, for different values of N at the RIS. As shown in this figure, P_{out} of the SN transmission decreases dramatically when $\mathcal{Q}$ increases. That is, the reliability of SN communication increases as N increases. As an illustration, $\mathcal{Q}$ decreases by approximately 4 dB, using an RIS with N = 20 compared with N = 50 to achieve a SN outage probability of 10^{-2}. Furthermore, simulation and numerical results agree perfectly, confirming the accuracy of our analysis.

P_{out} is shown in Fig. 7.3 for different schemes and compared with the proposed system model. Towards this end, the relay-aided transmission [17], phase shift error [18], and unavailability of the direct link between S and D [16] [19] scenarios are introduced and the results obtained through Monte-Carlo simulations. To elaborate on the performance loss caused by discrete phase shifts, simulation results with the phase error of each reflector

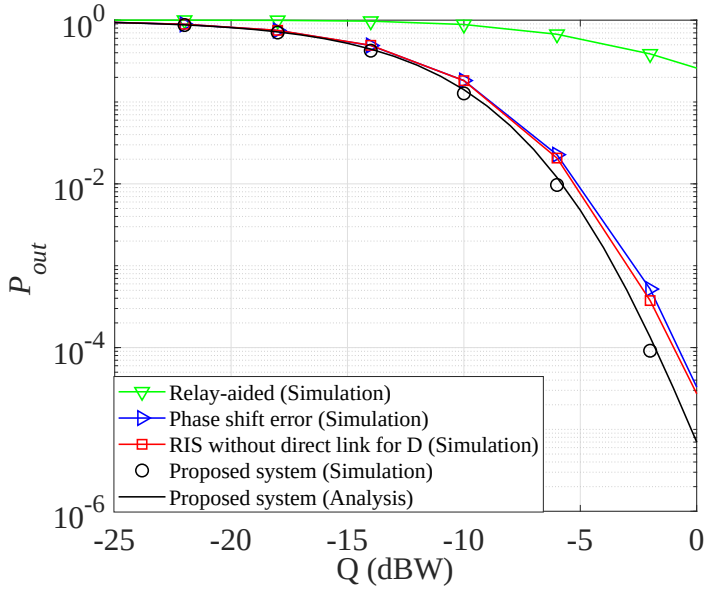


Fig. 7.3: The secondary outage probability, P_{out}, vs. $\mathcal{Q}$, for different scenarios, where $N = 30$, $\mathcal{R}_d = 1$ b/s/Hz.

uniformly distributed in $\left\{-\frac{\pi}{4}, \frac{\pi}{4}\right\}$ are provided. It can be observed that the SN's reliability is improved by utilizing the RIS in the presence of the S-D link compared to other scenarios. This is due to the fact that the RIS can maximize the received SNR at D and thus improve the channel quality of the SN. It is worth mentioning that the proposed system model has the best performance. Furthermore, simulation and numerical results agree perfectly, verifying the correctness of our analysis.

The SOP is shown in Fig. 7.4 versus $\bar{\gamma}_p$, for different values of N. The SNR at the E, $\bar{\gamma}_e$, takes two possible values: 0 dB and 10 dB. The SOP decreases as N increases, showing the influence of the jamming signals from the RIS on the E. Consequently, the PN secrecy performance is improved. Moreover, the SOP is enhanced as $\bar{\gamma}_p$ increases and $\bar{\gamma}_e$ decreases. As revealed in our analysis and simulation, improved secrecy performance can be achieved using RIS as a friendly jammer. This is because the wiretapped signal is degraded at the E due to the jamming signals generated by the RIS, resulting in more secure PN transmission. The asymptotic results are also included, and an excellent match with the

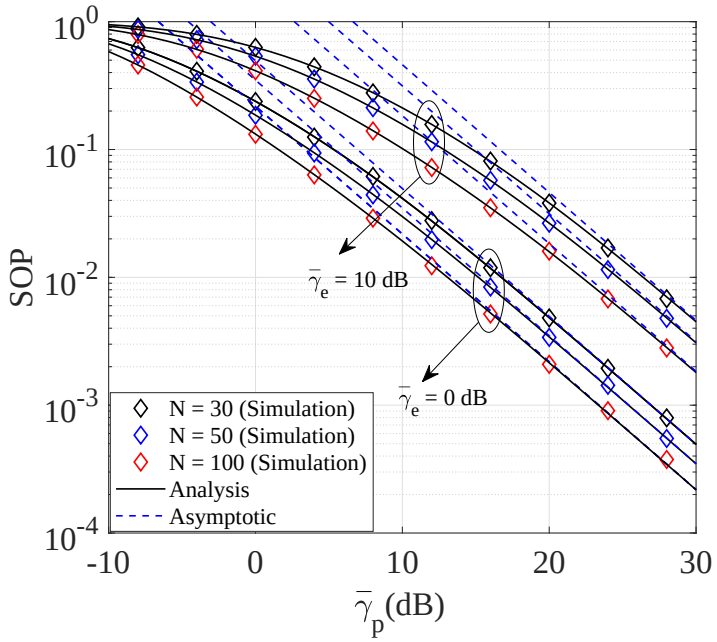


Fig. 7.4: The primary secrecy outage probability, SOP, vs. $\bar{\gamma}_p$, for different values of the number of reflecting elements, N.

exact ones can be seen as $\bar{\gamma}_p \to \infty$, confirming the precision of the expressions of $\mathcal{G}_a$ and $\mathcal{G}_d$. Furthermore, theoretical results and simulation results agree perfectly, verifying the exactness of our analysis.

Figure 7.5 plots the PNSC versus $\bar{\gamma}_p$. It can be noted that the PNSC improves as $\bar{\gamma}_p$ increases for a fixed $\bar{\gamma}_e$. Moreover, the PNSC improves with decreasing $\bar{\gamma}_e$. Further, it is also remarkable that the PNSC increases as N increases. Interestingly, secure transmission is guaranteed as N increases. Analytical results are also found to match simulation results, validating the accuracy of our analysis.

7.6 Conclusion

In this chapter, the RIS technology is exploited to improve the reliability and robustness of the SN communication and enhance the PN's secrecy performance simultaneously in

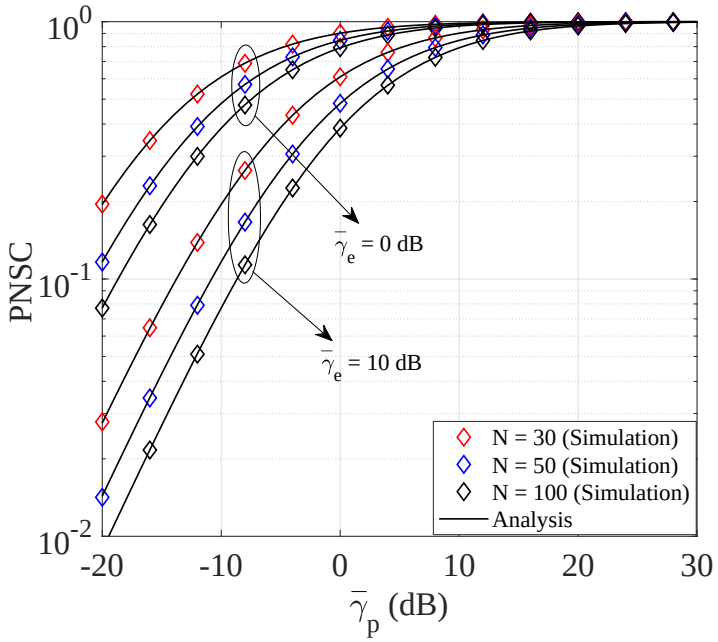


Fig. 7.5: The primary probability of non-zero secrecy capacity, PNSC, vs. $\bar{\gamma}_p$, for different values of the number of reflecting elements, N.

a cognitive radio network. New analytical expressions are derived for the SN's outage probability and the PN's SOP. The accuracy of these expressions is verified through Monte-Carlo simulations. As revealed by the analytical and simulation results, the PN's SOP, the PNSC, and the SN's outage probability are concurrently improved, confirming the benefits of utilizing the RIS technology.

References

[1] *Cisco Annual Internet Report (2018–2023) White Paper.*, "Available [Online]: http://goo.gl/ylTuVx, Mar. 2020.

[2] W. Zhang, C.-X. Wang, X. Ge, and Y. Chen, "Enhanced 5G cognitive radio networks based on spectrum sharing and spectrum aggregation," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6304–6316, Dec. 2018.

[3] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE personal commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[4] L. Zhang, Y. Wang, W. Tao, Z. Jia, T. Song, and C. Pan, "Intelligent reflecting surface aided MIMO cognitive radio systems," *IEEE Trans. Veh. Technol*, vol. 69, no. 10, pp. 11 445–11 457, Oct. 2020.

[5] J. Yuan, Y. -C. Liang, J. Joung, G. Feng and E. G. Larsson, "Intelligent reflecting surface-assisted cognitive radio system," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 675-687, Jan. 2021.

[6] J. Lee, H. Wang, J. G. Andrews, and D. Hong, "Outage probability of cognitive relay networks with interference constraints," *IEEE Trans Wireless Commun.*, vol. 10, no. 2, pp. 390–395, Feb. 2011.

[7] H. Lei et al., “On secrecy outage of relay selection in underlay cognitive radio networks over Nakagami-m fading channels,” *IEEE Trans Cognitive Commun. Netw.*, vol. 3, no. 4, pp. 614–627, Dec. 2017.

[8] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, “Wireless communications through reconfigurable intelligent surfaces,” *IEEE Access*, vol. 7, pp. 116 753–116 773, Jul. 2019.

[9] E. Björnson, Ö. Özdogan and Larsson, G. Erik, “Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying?,” *IEEE Wireless Commun. Lett*, vol. 9, no. 2, pp. 244–248, Feb. 2020.

[10] X. Guan, Q. Wu, and R. Zhang, “Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[11] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, “Dual antenna selection in secure cognitive radio networks,” *IEEE Trans. Veh. Tech.*, vol. 65, no. 10, pp. 7993–8002, Dec. 2016.

[12] L. Yang, et al., “Secrecy performance analysis of RIS-aided wireless communication systems,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12296–12300, Oct. 2020.

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

[14] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*, McGraw-Hill Education, 2002.

[15] D. Sadhwani, R. N. Yadav, and S. Aggarwal, “Tighter bounds on the gaussian Q function and its application in Nakagami-m fading channel,” *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 574–577, Oct. 2017.

[16] M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, “On the physical layer security of underlay relay-aided device-to-device communications,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7609–7621, Jul. 2020.

[17] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, “Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications,” *IEEE Access*, vol. 8, pp. 53575–53586, Mar. 2020.

[18] P. Xu, G. Chen, G. Pan and M. D. Renzo, “Ergodic secrecy capacity of RIS-assisted communication systems in the presence of discrete phase shifts and multiple eavesdroppers,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 629–633, Mar. 2021.

[19] M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, “Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications,” *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1443–1447, May 2021.

Chapter 8

Conclusions and Future Work

In this final chapter, we summarize the contributions presented in previous chapters and discuss several potential future directions for investigation.

8.1 Conclusions and Future Work

In this chapter, we first highlight the contributions of this thesis. Then, we propose some research topics as future works.

8.1.1 Conclusions

In this thesis, we focus on the PLS in 5G and beyond wireless networks enabling technologies. In the following, we summarise the major contributions of each chapter as follows:

In Chapter 2, we have proposed a cooperative scheme, whereby the D2D pair, in return for being allowed to share the spectrum band of the cellular network, serves as a friendly jammer through its MIMO relay to degrade the wiretapped signal at an eavesdropper. The proposed system model aims to show that spectrum sharing is advantageous for both D2D communications and cellular networks concerning reliability and robustness for the former

and PLS enhancement for the latter, in which the perfect and outdated CSI are considered. More importantly, the benefits due to the cooperation scheme are verified through extensive numerical and simulation results. The results show enhancement of the robustness and reliability of D2D communication and simultaneous improvement of the cellular network's PLS by generating jamming signals towards the eavesdropper. Thus, enabling a win-win situation is achieved between the two networks, i.e., security provisioning for the cellular user and high reliability and robustness for the D2D users.

In Chapter 3, a secure system model is designed to improve the secrecy performance of the cellular network and the reliability of the D2D communications simultaneously. To this end, an FD MIMO relay is employed to confuse the eavesdropper by generating jamming signals while ensuring improved transmission performance for the D2D system. Two practical combining techniques, SC or MRC, are utilized to combine the wiretapped signals at the eavesdropper. Considering a practical scenario in which the CSI of the eavesdropper's channel is unknown, a dual antenna selection scheme at the relay is proposed. This is an appealing and practical scheme where spectrum sharing is beneficial for the D2D and cellular networks in terms of reliability enhancement and security provisioning, respectively. The perfect and outdated CSI are considered. A comprehensive analysis is undertaken to evaluate the performance of the proposed system model, and new closed-form expressions for the D2D outage probability, the cellular SOP, and the cellular PNSC are derived. An asymptotic analysis is carried out to gain more insights into the effect of the various system parameters on the SOP.

In Chapter 4, the ORS and SRS schemes are utilized to enhance the inband underlay D2D secrecy performance. Two practical combining approaches, MRC and SC, are used to increase the eavesdropped signals. For combining techniques and relay selection schemes, new closed-form expressions for the D2D SOP and PNSC are derived. Most noteworthy in the obtained results is the fact that the ORS scheme consistently outperforms the SRS

scheme, assuming that the CSI of the wiretapped link is available. That is, the ORS guarantees the optimal secrecy performance for D2D communications. Additionally, the impact of D2D relays is investigated. It is observed, under these combining techniques, that increasing D2D relays enhances the D2D secrecy performance. The asymptotic results, which give a better understanding of the influence of the main system parameters on the SOP, are provided. As revealed in our analysis and confirmed through simulations, the diversity order is equal for combining approaches and relay selection schemes. These results also show that the number of antennas at the eavesdropper does not influence the diversity order. Moreover, we verified that, under both ORS and SRS schemes, increasing the number of antennas at the eavesdropper degrades the secrecy performance of D2D communications. Furthermore, the secrecy performance of underlay multihop D2D relaying is studied where closed-form expressions for the outage probability, the SOP, and the probability of non-zero secrecy capacity are derived. Simulation results validating the derived analytical expressions are provided. The results revealed the effect of the different number of D2D multihop relays on the security level of the D2D communications.

In Chapter 5, EH technology and dual-antenna selection are employed in the underlying system to enhance the reliability and robustness of the CR network and improve the security level of the primary network concurrently. To this end, multiple antennas for receiving and transmitting data are employed at the secondary receiver to enhance the CR network's reliability and robustness and confuse the eavesdropper by generating jamming signals, respectively. New analytical expressions are derived for the CR outage probability, primary SOP, and primary PNSC. In addition, asymptotic analysis is provided to get insight into the parameters of the proposed system model. The accuracy of these expressions is verified through Monte-Carlo simulations.

In Chapter 6, the RIS technology is investigated to enhance the reliability and robustness of D2D communication and improve the security level of the cellular network concurrently.

As compensation for spectrum sharing, the RIS serves as a friendly jammer to ensure a high-security level for the cellular network, thus enabling a win-win situation between the two networks, i.e., security provisioning for the cellular user and high reliability and robustness for the D2D users. New analytical expressions are derived for the cellular SOP, the PNSC and the D2D outage probability. Moreover, we have investigated the design of active elements in RIS to overcome the double-fading problem introduced in the RIS-aided link in a wireless communications system. Towards this end, each active RIS element amplifies the reflected incident signal rather than only reflecting it as done in passive RIS modules. As revealed in our analysis and simulation, the use of active elements leads to a drastic reduction in the size of RIS to achieve a given performance level. Furthermore, a practical design for active RIS is proposed.

In Chapter 7, the RIS technology is exploited to improve the reliability and robustness of the SN communication and enhance the PN's secrecy performance simultaneously in a cognitive radio network. New analytical expressions are derived for the SN's outage probability and the PN's SOP. The accuracy of these expressions is verified through Monte-Carlo simulations. As revealed by the analytical and simulation results, the PN's SOP and the PNSC and the SN's outage probability are concurrently improved, confirming the benefits of utilizing the RIS technology.

8.1.2 Future Work

The work presented in this thesis opens the door for future investigations, including the following:

- Employing machine-learning tools, specifically deep reinforcement learning (DRL), has gained momentum as promising tools than traditional ones to address challenging PLS of wireless systems. DRL is considered a revolution in artificial intelligence (AI), representing a promising move toward developing autonomous systems. DRL

has many advantages, such as obtaining the solution of sophisticated network optimizations, allowing network entities to learn and build knowledge about the communication and networking environment, and providing autonomous decision-making. These ground-breaking advantages are leading to improve the PLS of 6G wireless networks. Designing secure wireless systems using DRL tools is an important research point.

- Notwithstanding the RIS advantages, various practical problems in terms of PLS improvements should be addressed. For confounding the eavesdroppers' signals, IRS passive beamforming, which requires perfect CSI, can be utilized. However, achieving perfect CSI is practically challenging. Thus, investigating RIS-aided PLS enhancement for the next generation wireless communication networks considering the outdated/imperfect CSI of the eavesdroppers can be considered another direction for future work.

- With the accelerated advancement of the next-generation wireless networks, unmanned aerial vehicles (UAVs) have received considerable attention. The advantages of UAV communications are multi-fold and include high mobility, line-of-sight (LoS) transmission, and low cost UAVs have been widely utilized in several scenarios to improve communication quality. The PLS of the RIS-aided UAV communication system is another worthy topic to be investigated. More research is required to design effective and efficient secure RIS-aided UAV communication schemes for practical scenarios.

In conclusion, more investigations can be done regarding improving the PLS in 5G and beyond wireless networks enabling technologies. The DRL and RIS-aided approach should be considered for future investigations.