VŠB - Technical University of Ostrava

Faculty of Electrical Engineering and Computer Science

Impact of Hardware Impairments on Secrecy Performances of Wireless Relay Systems

PHD THESIS

2019 MSc. Phu Tran Tin

VŠB - Technical University of Ostrava
Faculty of Electrical Engineering and Computer Science
Department of Telecommunications

Impact of Hardware Impairments on Secrecy Performances of Wireless Relay Systems

Ph.D. Thesis

Doctoral Study Branch: 2601V018 Communication Technology

Doctoral Study Programme: P1807 Computer Science, Communication Technology and Applied Mathematics

2019 MSc. Phu Tran Tin

FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
DEPARTMENT OF TELECOMMUNICATIONS

Impact of Hardware Impairments on Secrecy Performances of Wireless Relay Systems

Ph.D. Thesis; Delivered in February, 2019

Doctoral Study Programme:

P1807 Computer Science, Communication Technology and Applied Mathematics

Doctoral Study Branch:

2601V018 Communication Technology

PhD. Student: MSc. Phu Tran Tin
VŠB - Technical University of Ostrava
Faculty of Electrical Engineering and Computer Science
Department of Telecommunications
17. listopadu 2172/15, 708 00 Ostrava, Czech Republic
tin.tran.phu.st@vsb.cz

Supervisor: Prof. Ing. Miroslav Vozňák, Ph.D.
VŠB - Technical University of Ostrava
Faculty of Electrical Engineering and Computer Science
Department of Telecommunications
17. listopadu 2172/15, 708 00 Ostrava, Czech Republic
miroslav.voznak@vsb.cz

OSTRAVA, 2019

DECLARATION

I declare that this thesis was written on the basis of original research conducted by me under the guidance of my supervisor at the Faculty of Electrical Engineering and Computer Science at VŠB - Technical University of Ostrava as a candidate for the Doctor of Communication Technology.

My work included below was conducted under the supervision of prof. Dr. Miroslav Vozňák. This thesis has never been submitted for any other degree or award at any other universities or educational institution.

This is a true copy of the thesis, including required final revisions, as accepted by my examiners. I understand that my thesis may be made electronically available to the public.

……...

(Author's Signature)

ACKNOWLEDGEMENT

This thesis marks the end of my journey in obtaining my Ph.D. It has been a period of intense learning, not only in the scientific arena but also on a personal level. Writing this dissertation has had a great personal impact and I would like to reflect on the people who have supported and helped me so much throughout this period.

First and foremost, I would like to express my deepest appreciation to my supervisor **prof. Dr. Miroslav Vozňák** for his careful guidance and providing me with the best possible work environment. He helped me tremendously in acquiring knowledge on many topics, both related and unrelated to this thesis. He continually and convincingly conveyed a spirit of adventure in regard to research and scholarship. Without his guidance and persistent help, this dissertation would not have been possible.

Special thanks to **Dr. Tran Trung Duy**, my co-supervisor in Vietnam, for providing insight into some of the problems encountered along the way. He helped me understand new topics quickly and guided me through effective research methods. Under his guidance, I successfully overcame many difficulties and learned much. I remember with delight the moments when he offered me valuable suggestions and corrections and reviewed my progress in the thesis. I hope to continue working with him in my future endeavours. I would also like to thank the National Foundation for Science and Technology Development (Nafosted 102.04-2017.317) for supporting me while I completed the thesis.

I am also extremely indebted to Dr. Lukaš Sevcik and Mr. Jakub Jalowiczor for providing the necessary infrastructure and resources to accomplish my research work. I am very grateful to them for their valuable advice, constructive criticism and extensive discussions concerning my work.

I also wish to express thanks to my student colleagues Messrs. Tan and Tam for providing friendship, encouragement and a fun-filled environment.

Finally, I wish to thank members of my family for their support and encouragement throughout my studies.

ABSTRACT

Security is one of the most important issues in wireless communication. Because using wireless channels entails broadcasting data transmissions, malicious nodes can eavesdrop on wireless transmission, which leads to insecure data transmission. Traditional security methods are based on cryptography. Recently, physical-layer security (PLS) has gained much attention as an efficient method of obtaining secure information without using cryptography. PLS protocols employ the physical characteristics of wireless channels such as channel state information (CSI) and the distances between connection links in order to enhance secrecy performances in wireless systems. To enhance secrecy performances, the dual-hop/multi-hop relay protocols can be used efficiently.

However, according to my best knowledge, there are few published works considering the impact of hardware impairments on secrecy performances for the wireless relaying networks. Hence, this dissertation examines the diversity-based relay protocols for wireless communication networks in order to improve secrecy performances in presence of hardware imperfections. First, new dual-hop and multi-hop cooperative relaying schemes with various relay selection methods are proposed in order to obtain improved secrecy performance compared with the existing schemes. Second, new joint relay and jammer selection protocols are also considered in order to improve the channel capacity for data links while reducing the channel capacity of eavesdropping links. Finally, this dissertation proposes harvest-to-transmit and harvest-to-jam protocols, where the relay and jammer nodes harvest energy from the radio frequency signal for use in the data transmission and the jamming process, respectively.

To evaluate the performance of the proposed protocols over fading channels, this dissertation focuses on deriving the closed-form expressions for secrecy performances. Then, the derived expressions are verified by Monte Carlo simulations, which also present the advantages of the proposed protocols.

Keywords: physical layer security, secrecy performance, relay network, energy harvesting, secrecy outage probability

ABSTRAKT

Bezpečnost je jedním z hlavních témat v oblasti bezdrátové komunikace. Jelikož použití bezdrátových kanálů vyžaduje vysílání datových přenosů, útočníci mohou tento přenos odposlouchávat, což vede k bezpečnostním hrozbám. Tradiční metoda zabezpečení je založena na kryptografii. Zabezpečení fyzické vrstvy (physical-layer security; PLS) v poslední době získalo velkou pozornost jako efektivní způsob pro zajištění bezpečnosti informace bez použití kryptografie. PLS protokoly využívají fyzikálních vlastností bezdrátového kanálu, jako je například informace o stavu kanálu (CSI) a vzdálenosti komunikačních linek pro zvýšení bezpečnosti bezdrátových systémů. Pro zvýšení efektivity utajení lze účinně využít dual-hop/multi-hop přenosových protokolů.

Nicméně, jak je autorovi této práce známo, publikovaných je pouze malé množství prací, které se zabývají vlivem hardwarových nedokonalostí (hardware impairments) na výslednou efektivitu utajení pro bezdrátové přenosové sítě (relaying networks). Tato disertační práce tudíž zkoumá přenosové „diversity-based" protokoly pro bezdrátové komunikační sítě za účelem zlepšení efektivity utajení v případě výskytu hardwarové nedokonalosti. V první řadě došlo k navržení nových dual-hop a multi-hop spolupracujících přenosových schémat s rozmanitými metodami výběru přenosového uzlu za účelem dosažení zlepšení efektivity utajení v porovnání s již existujícími schématy. Následně jsou pro zlepšení kapacity datového kanálu uvažovány taktéž nové protokoly pro spojovací přenosové uzly (joint relay) a pro výběr zdroje rušení (jammer), zatímco dochází ke snižování kapacity kanálu pro odposlech. V neposlední řadě tato disertační práce navrhuje protokoly využití energie pro vysílání (harvest-to-transmit) a využití energie pro rušení (harvest-to-jam), kde přenosové a rušící uzly získávají energii z rádiového signálu pro použití k datovému přenosu a procesu rušení.

Pro vyhodnocení efektivity navržených protokolů nad únikovými kanály se tato disertační práce zaměřuje na odvození výrazů v uzavřené formě pro efektivitu utajení. Následně jsou odvozené výrazy ověřeny pomocí Monte Carlo simulací, které také ukazují výhody navržených protokolů.

Klíčová slova: Zabezpečení fyzické vrstvy, efektivita utajení, přenosová síť, získávání energie, pravděpodobnost výpadku utajení

CONTENTS

TABLE OF FIGURES

ABBREVIATIONS

AF	Amplify and Forward
AWGN	Additive White Gaussian Noise
ASC	Average Secrecy Capacity
CSI	Channel State Information
CCI	Co-Channel Interference
CR	Cognitive Radio
DF	Decode and Forward
EGC	Equal Gain Combining
EH	Energy Harvesting
FRS	Full Relay Selection
HI	Hardware Impairments
IQI	In-phase and Quadrature Imbalance
OFDMA	Orthogonal Frequency-Division Multiple Access
OP	Outage Probability
IC	Interference Cancelation
IP	Intercept Probability
MIMO	Multiple Input Multiple Output
MRC	Maximal Ratio Combining
MRT	Maximal Ratio Transmission
PRS	Partial Relay Selection
PLS	Physical-layer Security
PNSC	Probability of Non-zero Secrecy Capacity
QoS	Quality of Service
RF	Radio Frequency
RF	Randomize and Forward
RV	Random Variable
SC	Selection Combining
SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
SS	Successful and Secure Communication
TAS	Transmit Antenna Selection

1. INTRODUCTION

1.1. Motivation and goals

Nowadays, wireless communication [1] is the fastest growing segment in the communications industry. As such, it has captured the attention of the media and the imagination of the public. Cellular systems have experienced exponential growth over the last decade and there are currently around two billion users worldwide. Indeed, cellular phones have become a critical business tool and a part of everyday life in most countries and are rapidly supplanting antiquated wire systems in many countries.

Wireless relaying networks [2]-[3] are widely used to mitigate the impact of fading environments as well as to enhance network coverage. In this model, the relay nodes help the data transition from a source node to a desired destination. Cooperative relaying protocols can provide the outstanding performance for wireless networks, such as extending the zone of coverage and increasing gain diversity and the quality of service (QoS). In a dual-hop relaying network [3]-[4], the information can be transferred to the destination node through one selected relay. In the multi-hop scenarios [5]-[6], when the distance between the source and the destination is far, the wireless systems need more than one hop to transmit the source signal. Because of their numerous advantages (e.g. improved coverage, throughput, system capacity, power/battery life, etc.), dual-hop/multi-hop relaying protocols have recently attracted significant attention in both academia and industry [7]. The most common relaying strategies are decode-and-forward (DF) and amplify-and-forward (AF). While the DF relay decodes, re-modulates and retransmits a received signal to the destination, the AF one simply amplifies and retransmits the signal without decoding. Compared to the AF technique, the complexity of the DF one is significantly higher due to its full processing capability. In addition, the DF protocol also requires a sophisticated media access control layer, which is unnecessary in the AF protocol. In cooperative relaying networks, relay selection is one of critical issue to improve the system performance over fading channels. So far, various relay selection protocols have been proposed and analysed in dual-hop networks [8]-[9] and multi-hop networks [PTT06].

Recently, physical-layer security (PLS) [10]-[11] has gained much attention as a simple method of obtaining secure information without using cryptography. Because of the broadcast properties of radio channels, the data transmission can be overheard by eavesdroppers. Normally, in order to protect the transmitted data, encryption methods can be applied efficiently. However, installing and implementing these methods can be complicated and costly. In PLS, the physical properties such as channel state information (CSI) and the distances between connection links are used to obtain security. The performance of secured communication networks is measured by secrecy capacity, which is different between the channel capacity of the data and the eavesdropping links [12]-[13]. Relying on the obtained secrecy capacity, important performance metrics such as average secrecy capacity (ASC), secrecy outage probability (SOP) and probability of non-zero secrecy capacity (PNSC) are commonly used. Recently, the authors in [14]-[15] evaluated the secrecy performance of secured communication protocols using the "intercept probability (IP)" concept. Intercept probability is defined as the probability that the signal-to-noise ratio (SNR) received at the eavesdropper is higher than a predetermined threshold [14]-[15], which is also considered the probability that the eavesdropper can overhear the transmitted information successfully. Indeed, once the eavesdropper can receive the data correctly, the security of the transmitted data is no

longer guaranteed. Hence, IP is also an important performance metric in evaluating the security level of wireless systems.

To enhance the secrecy performances in wireless networks, again, cooperative relaying protocols (with relay selection methods) can be applied efficiently. In [16]-[17], the authors investigated the secured communication at the cooperative phase with various relay selection methods. In published works [18], two fundamental relaying protocols in PLS, i.e. decode-and-forward (DF) and randomize-and-forward (RF), were introduced. In the DF method, the source and the relay use the same codebook to forward the source data to the destination. If the eavesdropper can overhear the data transmitted by the source and the relay, this node can employ combining techniques such as maximal ratio combining (MRC), equal gain combining (EGC), selection combining (SC), etc. to enhance the decoding efficiency of the data overheard. Unlike the DF protocol, in the RF protocol, the relay node generates a randomized codebook to preclude the eavesdropper from the data combination. Next, in [19], the secured communication in a multicast underlay cognitive radio network with partial relay selection methods was proposed and analysed. The authors in [14] studied the security-reliability trade-off for cooperative cognitive networks by evaluating intercept probability (IP) at the eavesdropper and outage probability (OP) at authorized nodes. The published work [15] proposed relay selection methods to improve the outage performance of the data link and to reduce the intercept probability (IP) of the eavesdropping link.

Furthermore, researchers have recently considered cooperative jamming techniques to enhance the secrecy performance. By employing jammer nodes to generate noise to the eavesdropper, the channel capacity of the eavesdropping links significantly decreases. As a result, the secrecy capacity increases, which leads to the improvement of the secrecy performance. In [20]-[21], cooperative jamming methods were investigated. The results in [20]-[21] showed that the secured protocols using the jamming methods obtained better performance than conventional ones. However, it was noted that the jamming signals from the jamming nodes could create interference in other devices in the network. The jamming nodes also used their transmit power to generate "informationless" data, which in turn could reduce the energy usage efficiency. Recently, radio frequency (RF) energy harvesting (EH) methods have been considered to solve the energy efficiency in cooperative jamming based on physical-layer security. In [22], the authors proposed a secured relaying protocol in which one of the full energy relays is selected to transmit data from the source to the destination, while another energy-constrained relay harvests energy from the source's radio frequency signals to generate artificial noise to the eavesdropper. Published works [23] studied the trade-off between the intercept probability (IP) and the outage probability for underlay cognitive radio networks. In this model, a secondary transmitter transmits secondary data to a secondary receiver in the presence of a secondary eavesdropper that attempts to overhear the transmitted data. Moreover, a secondary jammer which harvests energy from the RF signals received from the secondary transmitter is also used to transmit jamming signals to the secondary eavesdropper.

Until now, almost all of the published works related to physical layer security (PLS) have assumed that the transceiver hardware in wireless devices is flawless. However, in practice, their transceivers are imperfect because of the non-linearity of the amplifiers, phase noises and I/Q imbalance [24]-[26]. **To the best of my knowledge, some research has been published on the impact of hardware impairments on secrecy performances.** In particular, the authors in [27] studied the

effects of I/Q imbalance on the secrecy capacity of one-hop orthogonal frequency-division multiple access (OFDMA) communication systems. In [15], the authors investigated the impact of hardware impairments on the performance of secondary networks in an underlay cognitive radio network in relation to outage probability (OP) and intercept probability (IP). In [28], the impact of hardware impairments on secrecy performance in multi-hop randomize-and-forward (RF) relaying networks was studied in relation to the probability of non-zero secrecy capacity (PNSC).

Motivated by the above, this thesis mainly investigates the impact of hardware impairments on the secrecy performance of cooperative relaying protocols in wireless networks. In order to compensate for secrecy performance loss because of hardware imperfections, cooperative relaying schemes are also proposed and analysed.

Therefore, the main goals of the thesis are as follows:

- First, the secrecy performances of the relay protocols in the presence of the hardware noises are evaluated. Particularly, cooperative relay schemes in which the impact of hardware noises on the received signal-to-noise ratio (SNR) at both the authorized nodes and the non-authorized nodes (eavesdroppers), will be investigated. As mentioned above, in practice, the transceiver hardware of cheap wireless devices is affected by impairments. Therefore, taking hardware impairments into evaluating the secrecy performances will give more practical results.
- Second, to enhance the secrecy performances for wireless networks under the impact of fading environments and hardware noises, this thesis proposes new relaying protocols with new relay selection methods. Particularly, new multi-hop/dual-hop decode-and-forward (DF) and randomize-and-forward (RF) scenarios are proposed and analyzed.
- Third, to further improve the secrecy performances, new joint jammer and relay selection protocols are proposed and investigated. Also, the performances of the proposed schemes are evaluated in presence of hardware imperfections.
- Next, harvest-to-transmit and harvest-to-jam relay methods to enhance the secrecy performances are also studied. As discussed above, the relay and jammer nodes that are limited devices will harvest the RF energy to forward the source data to the destination and generate the jamming noises to the eavesdropper, respectively. This technique not only obtains high secrecy performances but also provides high power savings for the jamming nodes.
- Fifthly, under the impact of the hardware impairments, the instantaneous secrecy capacity of the proposed protocols is re-formulated. Then, this dissertation attempts to evaluate the secrecy performances of the proposed protocols by deriving mathematical expressions for the average secrecy capacity (ASC), secrecy outage probability (SOP), probability of non-zero secrecy capacity (PNSC) as well as outage and intercept probabilities (OP and IP) over fading channels with the impact of hardware noises.
- Moreover, the thesis attempts to derive the closed-form expressions for the secrecy performances. The closed-form formulas are easy-to-compute expressions which can be used by researchers to design and optimize the wireless systems.

- Finally, Monte Carlo simulations are performed to verify the correction of the derived expressions, to show the advantages of the proposed methods and to compare the performances between the proposed protocols and the existing ones.

1.2. Thesis structure

The thesis is organized as follows. Chapter 2 describes the state of the art. Chapter 3 describes the aims of the thesis and presents preliminary works and schedules. Chapter 4 presents the knowledge background employed in the thesis. Discussions are given in Chapters 5, 6, 7 and 8, where the results of the proposed methods are demonstrated and evaluated. Chapter 9 concludes the thesis and describes potential future work.

2. STATE OF THE ART

In a wireless environment, because of the nature of the broadcast, the network is vulnerable to attack and eavesdropping through wireless communication. Several studies have been conducted to improve security systems in wireless networks. As a consequence, many solutions offered in different layers exist. The current security approach is to apply encryption and authentication techniques (such as WPA, WPA2-AES, WPA2-TKIP, WPA3, etc.) and are often deployed at the application layer. But these security solutions are increasingly difficult to deploy and ineffective because of continually changing integrated requirements, computing techniques and wireless attack methods. In this thesis, a background on physical layer security (PLS) is provided along with related work.

Most attacks in the physical layer can be categorised as eavesdropping-based attacks. Eavesdropping attacks are unauthorized compromise of the data traffic between legitimate nodes. Traffic analysis attacks are an example of an eavesdropping-based attack type, where the content of the data is not compromised but the transmitter and receiver nodes are detected. These types of attacks are typically approached via cryptographic algorithms implemented at higher network layers. However, a new approach is to prevent attack in the physical layer by using the physical characteristics of the wireless channel for secure communication.

To address this issue, a new direction of study is being explored to find ways of enhancing the security of wireless networks in the physical layer. A physical layer security approach builds on information security theory: a secure wireless communication system if legacy channel capacity is greater than illegal channel capacity [10], [29].

This approach is simple yet effective, as it focuses on solving the problem of security at the information level in order to limit the possibility of obtaining information illegally.

There are two major research directions in physical layer information security: physical layer security information based on a security key (Key-Based Secrecy) [30]-[32] and physical layer security information without a security key (Keyless Secrecy) [33]-[35]. For this thesis, keyless secrecy was researched, and signal-based methods are therefore its main focus.

In 1975, the pioneering work of Wyner [10] demonstrated perfect secrecy when an eavesdropper's channel was a degraded version of the main communication channel. These early studies demonstrated that positive secrecy capacity can be achieved in a wireless communication network with noisier channels in the presence of eavesdroppers. The impact of these works remained limited until the arrival of enabling technologies such as smart antennas, increased computational capabilities of electronic devices and multi-input multi-output (MIMO) systems.

Later, in the 2000s, multi-antenna systems enabled a very useful technique referred to as beam forming. The publications [36]-[37] examined secrecy performance in MIMO networks, while the authors of [38]-[39] presented the Artificial Noise (AN) technique to reduce the capacity channel of the eavesdropping link. The papers [40]-[41] proposed Transmit Antenna Selection methods (TAS) to enhance secrecy performance in MIMO networks.

Furthermore, in [40], the authors showed that using selection combining techniques (SC) with a multi-antenna eavesdropper had the same effect as many eavesdroppers equipped with single

antennas and that Secrecy Outage Probability (SOP) increased when the number of antennas at the eavesdropper increased. The publication [PTT06] described the Cooperative Jamming (CJ) method, its results showing that secrecy performance was enhanced significantly compared to no CJ. In [42], the authors assessed the effect of Co-Channel Interference (CCI) [42]-[44] on secrecy performance in the systems.

In the relevant research section of this thesis, a wireless communication network model using artificial noise over Rayleigh fading channels is considered. To evaluate the secrecy performance of the model, the following factors were analysed and evaluated: secrecy capacity, secrecy probability and secrecy outage probability in wireless network systems such as relay networks, multi relay networks, cluster networks and cognitive radio systems. The effect of undesired conditions such as channel estimation error and hardware impairment on secrecy performance in relay networks were also investigated. In order to test and verify the mathematical analysis, a Monte Carlo simulation was set up and run for each analysis result.

3. AIMS

To the best of my knowledge, until now, there have been several published works ([15], [27], [28]) related to performance evaluation for the secured relay networks under the impact of hardware impairments. Motivated by this, the thesis mainly focuses on evaluating this effect on the secrecy performances of cooperative relaying protocols with various relay and/or jammer selection methods.

3.1. Aim 1

Research on wireless relaying networks with relay selection methods to enhance the secrecy performances over fading channels under the impact of hardware impairments:

- First, I will evaluate new dual-hop and multi-hop relaying protocols with various relay selection methods in conventional wireless networks and cognitive radio wireless networks to compare their efficiency.
- Second, relay selection methods will be applied into cooperative routing protocols and cluster-based relay systems to raise the secrecy performances.
- Next, I will compare the instantaneous secrecy capacity of the proposed methods with and without hardware noises presence. Then, secrecy performances will be evaluated via both theoretical analysis and computer simulations.
- Finally, the outage probability (OP) of the data links and the intercept probability of the eavesdropping links will be used to evaluate the security-reliability tradeoff for the proposed protocols.

3.2. Aim 2

A new proposal and evaluation of joint relay and jammer selection protocols to further improve secrecy performances for cooperation-based relaying networks:

- First, proposing new joint relay and jammer selection protocols to enhance secrecy performances for wireless relaying systems under the impact of hardware imperfection.
- Second, new joint selection methods will be applied to both conventional wireless networks and cognitive radio (CR) networks.
- Finally, the secrecy performances and the tradeoff between OP and IP of the proposed methods will be evaluated via simulation and analysis.

3.3. Aim 3

A new proposal and evaluation of cooperative relaying and jamming protocols using energy harvesting techniques:

- First, proposing new relaying protocols where the limited energy relays have to harvest the energy from the radio frequency signal for forwarding the source data to the destination.
- Second, new jammer selection protocols are proposed. In the proposed methods, the jammer nodes also harvest the energy to generate the jamming noises to the eavesdropper.

- Finally, the secrecy performances and the tradeoff between OP and IP of the proposed protocols in the impact of fading environments and hardware imperfection will be evaluated via both simulation and theoretical results.

4. BACKGROUND

4.1. Secrecy performances

Because of the broadcast nature of the wireless medium, secured communication in wireless networks has become a critical issue. Recently, physical-layer security [10]-[11] has gained much attention as an efficient method to obtain the secure transmission without using cipher codes.

Figure 4.1 shows a simple system model of secured communication, where Alice (A) communicates with Bob (B), while Eva (E) attempts to eavesdrop on the information that Alice discusses with Bob.

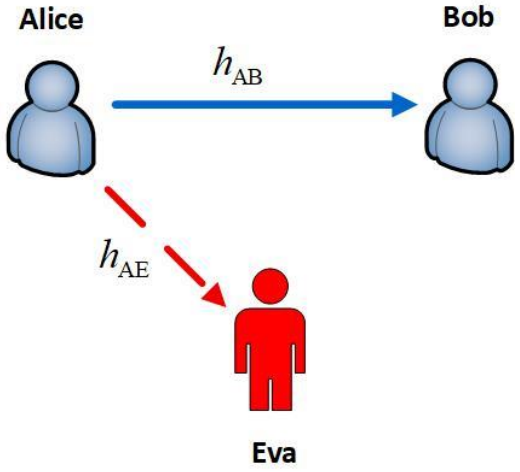

Figure 4.1. *A fundamental system model of physical-layer security (PLS).*

The data received at B and E due to A's data transmission can be respectively expressed as

$$\begin{aligned} y_{\mathrm{B}} &= \sqrt{P} h_{\mathrm{AB}} s + n_{\mathrm{B}}, \\ y_{\mathrm{E}} &= \sqrt{P} h_{\mathrm{AE}} s + n_{\mathrm{E}}, \end{aligned} \tag{4.1}$$

where P is the transmit power of A, h_{AB} and h_{AE} are the channel coefficients of the $\mathrm{A} \to \mathrm{B}$ and $\mathrm{A} \to \mathrm{E}$ links, respectively, s is the data transmitted by A, n_{B} and n_{E} are additive white Gaussian noise (AWGN) at B and E, respectively. n_{B} and n_{E} are zero-mean Gaussian random variables (RVs).

From (4.1), the instantaneous signal-to-noise ratios (SNRs) received at B and E are expressed by

$$\begin{aligned} \gamma_{\mathrm{B}} &= \frac{P |h_{\mathrm{AB}}|^2}{N_0}, \\ \gamma_{\mathrm{E}} &= \frac{P |h_{\mathrm{AE}}|^2}{N_0}, \end{aligned} \tag{4.2}$$

respectively, where we assume that $E\{s\} = 1$ with $E\{.\}$ is an expected operator, and N_0 is the variance of n_{B} and n_{E}, i.e. $N_0 = \mathrm{var}\{n_{\mathrm{B}}\} = \mathrm{var}\{n_{\mathrm{E}}\}$.

From (4.2), the instantaneous channel capacity obtained at B and E can be given, respectively, as follows:

$$\begin{aligned} C_{\mathrm{B}} &= \log_2\left(1+\gamma_{\mathrm{B}}\right), \\ C_{\mathrm{E}} &= \log_2\left(1+\gamma_{\mathrm{E}}\right). \end{aligned} \tag{4.3}$$

From the definition of secrecy capacity in [16]-[19], the secrecy capacity of the system presented in Figure 4.1 can be expressed as

$$\begin{aligned} C_{\mathrm{sec}} &= \max\left(0, C_{\mathrm{B}} - C_{\mathrm{E}}\right) \\ &= \max\left(0, \log_2\left(\frac{1+\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{E}}}\right)\right). \end{aligned} \tag{4.4}$$

We can observe from (4.4) that the secrecy capacity C_{sec} has a non-negative value.

From (4.4), the secrecy outage probability (SOP) can be given as in [16]-[19]:

$$\mathrm{SOP} = \Pr\left(C_{\mathrm{sec}} < C_{th}\right), \tag{4.5}$$

where $C_{th}\left(C_{th} > 0\right)$ is a predetermined threshold.

Furthermore, the probability of non-zero secrecy capacity (PNSC) can be expressed as the following equation:

$$\begin{aligned} \mathrm{PNSC} &= \Pr\left(C_{\mathrm{sec}} > 0\right) \\ &= \Pr\left(\max\left(0, \log_2\left(\frac{1+\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{E}}}\right)\right) > 0\right) \\ &= \Pr\left(\gamma_{\mathrm{B}} > \gamma_{\mathrm{E}}\right). \end{aligned} \tag{4.6}$$

Next, the average secrecy capacity (ASC) can be obtained by

$$\begin{aligned} \mathrm{ASC} &= E\left\{C_{\mathrm{sec}}\right\} \\ &= E\left\{\max\left(0, \log_2\left(\frac{1+\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{E}}}\right)\right)\right\}, \end{aligned} \tag{4.7}$$

where $E\{.\}$ is the expected operator.

In [14]-[15], the authors evaluated the performance of PLS-based relay protocols by considering the outage probability (OP) of the data links and the intercept probability (IP) of the eavesdropping links. Indeed, the OP and IP probabilities can be defined, respectively, as

$$\begin{aligned} \mathrm{OP} &= \Pr\left(\gamma_{\mathrm{B}} < \gamma_{th}\right), \\ \mathrm{IP} &= \Pr\left(\gamma_{\mathrm{E}} \geq \gamma_{th}\right), \end{aligned} \tag{4.8}$$

where γ_{th} is a predetermined threshold, and the data link is considered in outage if the SNR γ_{B} is lower. However, it can be assumed that Eva decodes Alice's information correctly if the received SNR γ_{E} is higher than γ_{th}, which refers to the intercept probability.

From (4.8), we can observe that to decrease the outage probability (OP), Alice can transmit the data with higher transmit power. However, when the transmit power increases, the intercept probability (IP) at Eva also increases. Therefore, a trade-off exists between the security and reliability (between IP and OP), which will be studied in this thesis.

4.2. Hardware impairments (HI)

In practice, the hardware transceivers of wireless devices are imperfect because of the non-linearity of the amplifiers, phase noises and I/Q imbalance (IQI) [24]-[26], which significantly degrades performances of wireless systems.

Let us consider the data transmission between the nodes, i.e. $\mathrm{A} \to \mathrm{B}$ and $\mathrm{A} \to \mathrm{E}$; with the presence of hardware impairments (HI), the received data at B and E can be rewritten as in [24]-[26]:

$$\begin{aligned} y_{\mathrm{B}} &= \sqrt{P} h_{\mathrm{AB}} \left(s + \nu_{t,\mathrm{A}} \right) + \nu_{t,\mathrm{B}} + n_{\mathrm{B}}, \\ y_{\mathrm{E}} &= \sqrt{P} h_{\mathrm{AE}} \left(s + \nu_{t,\mathrm{A}} \right) + \nu_{t,\mathrm{E}} + n_{\mathrm{E}}, \end{aligned} \tag{4.9}$$

where $\nu_{t,\mathrm{A}}$ is hardware noise caused by the impairments in the transmitter A, $\nu_{t,\mathrm{B}}$ and $\nu_{t,\mathrm{E}}$ are hardware noises caused by the impairments in the receiver B and E, respectively.

As given in [24]-[26], the noises $\nu_{t,\mathrm{A}}$, $\nu_{t,\mathrm{B}}$ and $\nu_{t,\mathrm{E}}$ can be modelled as Gaussian random variables (RVs) with zero-mean, and their variances can be given, respectively, as

$$\begin{aligned} &\mathrm{var}\left\{ \nu_{t,\mathrm{A}} \right\} = \kappa_{t,\mathrm{A}}^2, \\ &\mathrm{var}\left\{ \nu_{t,\mathrm{B}} \right\} = \kappa_{r,\mathrm{B}}^2 P |h_{\mathrm{AB}}|^2, \\ &\mathrm{var}\left\{ \nu_{t,\mathrm{E}} \right\} = \kappa_{r,\mathrm{E}}^2 P |h_{\mathrm{AE}}|^2, \end{aligned} \tag{4.10}$$

where $\kappa_{t,\mathrm{A}}^2, \kappa_{r,\mathrm{B}}^2$ and $\kappa_{r,\mathrm{E}}^2$ are constants characterizing the level of hardware impairments at A, B and E, respectively.

From (4.9) and (4.10), we can express the SNR received at B and E as

$$\begin{aligned} \gamma_{\mathrm{B}} &= \frac{P |h_{\mathrm{AB}}|^2}{\left(\kappa_{t,\mathrm{A}}^2 + \kappa_{r,\mathrm{B}}^2 \right) P |h_{\mathrm{AB}}|^2 + N_0}, \\ \gamma_{\mathrm{E}} &= \frac{P |h_{\mathrm{AE}}|^2}{\left(\kappa_{t,\mathrm{A}}^2 + \kappa_{r,\mathrm{E}}^2 \right) P |h_{\mathrm{AE}}|^2 + N_0}. \end{aligned} \tag{4.11}$$

Therefore, the secrecy capacity with hardware noises at both B and E can be expressed by the following equation:

$$
\begin{aligned}
C_{\text{sec}} &= \max\left(0, C_{\text{B}} - C_{\text{E}}\right) \\
&= \max\left(0, \log_2\left(1+\gamma_{\text{B}}\right) - \log_2\left(1+\gamma_{\text{E}}\right)\right) \\
&= \max\left(0, \log_2\left(1+\frac{P|h_{\text{AB}}|^2}{\left(\kappa_{t,\text{A}}^2+\kappa_{r,\text{B}}^2\right)P|h_{\text{AB}}|^2+N_0}\right) - \log_2\left(1+\frac{P|h_{\text{AE}}|^2}{\left(\kappa_{t,\text{A}}^2+\kappa_{r,\text{E}}^2\right)P|h_{\text{AE}}|^2+N_0}\right)\right) \\
&= \max\left(0, \log_2\left(1+\frac{P|h_{\text{AB}}|^2}{\kappa_{\text{AB}}P|h_{\text{AB}}|^2+N_0}\right) - \log_2\left(1+\frac{P|h_{\text{AE}}|^2}{\kappa_{\text{AE}}P|h_{\text{AE}}|^2+N_0}\right)\right),
\end{aligned}
\tag{4.12}
$$

where $\kappa_{\text{AB}} = \kappa_{t,\text{A}}^2 + \kappa_{r,\text{B}}^2, \kappa_{\text{AE}} = \kappa_{t,\text{A}}^2 + \kappa_{r,\text{E}}^2$ are the total hardware impairment level of the $\text{A} \to \text{B}$ and $\text{A} \to \text{E}$ links, respectively.

When all of the hardware transceivers are perfect, i.e. $\kappa_{t,\text{A}}^2 = \kappa_{r,\text{B}}^2 = \kappa_{r,\text{E}}^2 = 0,$ equation (4.12) reduces to equation (4.4).

Comments: From (4.12), we can observe that hardware noises reduce the channel capacity of both the data and eavesdropping links. **A question arises here is that how the hardware impairments impact on the secrecy performance**? Answering this question is the main content of the thesis.

4.3. Cooperative jamming

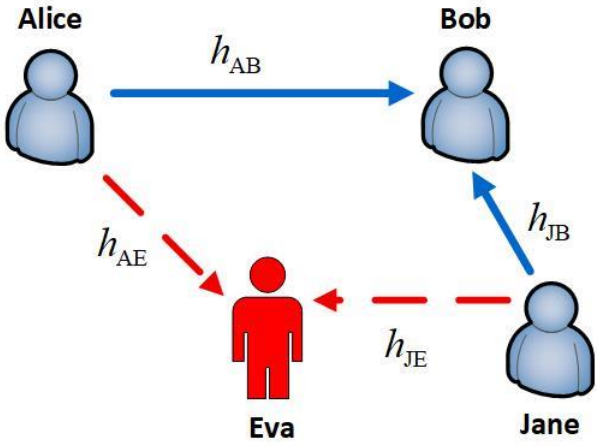

Figure 4.2 *System model of cooperative jamming method.*

Figure 4.2 presents a cooperative jamming model, where Jane (J) (Alice and Bob's friend) help the secured communication between Alice and Bob by generating noise to Eva so that Eva cannot eavesdrop on Alice's data. With the interference caused by J, the received SNR at B and E can be rewritten from (4.11) as

$$
\begin{aligned}
\gamma_{\text{B}} &= \frac{P|h_{\text{AB}}|^2}{\kappa_{\text{AB}}P|h_{\text{AB}}|^2 + P_J|h_{\text{JB}}|^2 + N_0}, \\
\gamma_{\text{E}} &= \frac{P|h_{\text{AE}}|^2}{\kappa_{\text{AE}}P|h_{\text{AE}}|^2 + P_J|h_{\text{JE}}|^2 + N_0},
\end{aligned}
\tag{4.13}
$$

where P_J is the transmit power of J, h_{JB} and h_{JE} are fading channel coefficients of the $J \to B$ and $J \to E$ links, respectively, $P_J |h_{JB}|^2$ and $P_J |h_{JE}|^2$ are co-channel interference (CI) components.

However, if Jane is near Bob and they can exchange the secured information about the jamming noise (Eva cannot overhear this information); Bob can remove the CI component from the received signal. In this case, the SNR at B is same as that in (4.11), while the SNR received at E is same as (4.13), i.e.

$$\begin{aligned} \gamma_B &= \frac{P|h_{AB}|^2}{\kappa_{AB} P|h_{AB}|^2 + N_0}, \\ \gamma_E &= \frac{P|h_{AE}|^2}{\kappa_{AE} P|h_{AE}|^2 + P_J|h_{JE}|^2 + N_0}. \end{aligned} \tag{4.14}$$

From (4.14), the secrecy capacity can be calculated as follows:

$$\begin{aligned} C_{sec} &= \max\left(0, C_B - C_E\right) \\ &= \max\left(0, \log_2\left(1 + \frac{P|h_{AB}|^2}{\kappa_{AB} P|h_{AB}|^2 + N_0}\right) - \log_2\left(1 + \frac{P|h_{AE}|^2}{\kappa_{AE} P|h_{AE}|^2 + P_J|h_{JE}|^2 + N_0}\right)\right). \end{aligned} \tag{4.15}$$

From (4.12) and (4.15), we can observe that the secrecy capacity in (4.15) is higher than in (4.12). The cooperative jamming methods with interference cancelation (IC) at the authorized receiver are widely used in PLS to enhance the secrecy performances (see [20], [22], [23] and references therein). It is obvious that once B can remove the interference, the secrecy capacity significantly increases. Indeed, the results in [20]-[23] showed that the secured protocols using jamming methods obtains better performance than with conventional methods.

Comments: Cooperative jamming protocols are some of the main contents of the thesis. Moreover, cooperative harvest-to-jam models will be proposed and analysed.

4.4. Multi-hop Cooperative Transmission Protocol

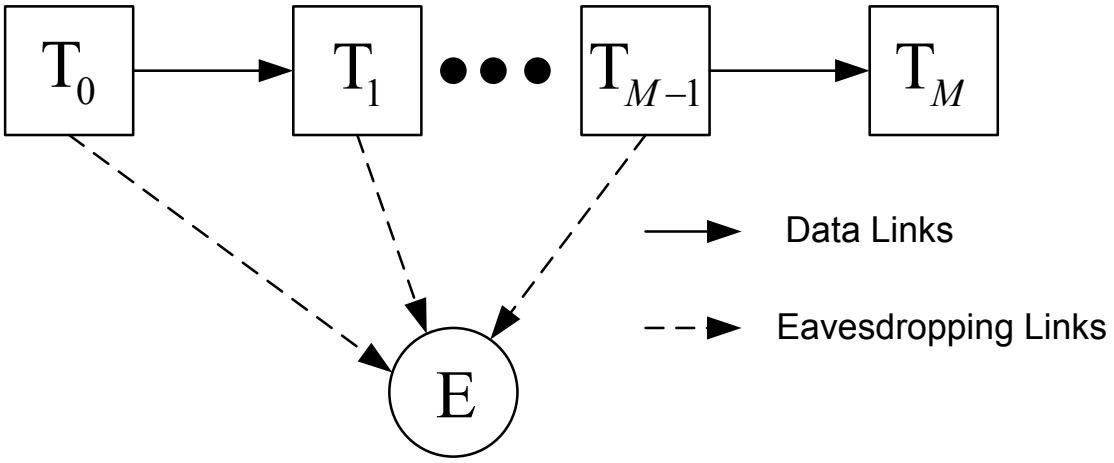

Figure 4.3. *System model of Multi-hop Cooperative Transmission Protocol.*

Figure 4.3 shows a system model of an M-hop relay protocol, where source T_0 communicates with destination T_M using the multi-hop method with the assistance of $M-1$ relay nodes denoted by T_1, $\mathrm{T}_2, \ldots, \mathrm{T}_{M-1}$. In this network, eavesdropper E attempts to listen in on the data transmitted by the source and relays.

All of the nodes are equipped with only a single antenna. As a result, the data transmission between the source and the destination is performed via M orthogonal time slots. The randomize-and-forward (RF) technique [PTT03], [18], [19] is used to avoid the eavesdropper in the combined data transmitted from the source and the relays using the maximal ratio combining (MRC) technique. We assume that all of the channels between two arbitrary nodes are Rayleigh fading. We also assume that the eavesdropper is an active node, and hence authorized transmitters such as the source and relay nodes can obtain perfect channel state information (CSI) between themselves and node E.

Considering the data transmission between transmitter X and receiver Y, where $\mathrm{X} \in \{\mathrm{T}_m\}$ and $\mathrm{Y} \in \{\mathrm{T}_m, \mathrm{E}\}$, $m = 0,1,2,...,M$, the received data at Y because of transmission at X can be given as in [PTT03], [25], [46]:

$$z = \sqrt{P_{\mathrm{X}}} h_{\mathrm{XY}} \left(x + \eta_{t,\mathrm{X}} \right) + \eta_{r,\mathrm{Y}} + n_{\mathrm{Y}}, \tag{4.16}$$

where P_{X} is the transmit power of the transmitter X, h_{XY} is Rayleigh fading channel of the X-Y link, $\eta_{t,\mathrm{X}}$ is hardware noise caused by impairments in the transmitter X, $\eta_{r,\mathrm{Y}}$ is hardware noise caused by the impairments in the receiver Y and n_{Y} is Gaussian noise at receiver Y.

As with [PTT03], [25], [46], the noises $\eta_{t,\mathrm{X}}$, $\eta_{r,\mathrm{Y}}$ and n_{Y} can be modelled as zero-mean Gaussian random variables (RVs) with zero-mean. Furthermore, their variances can be given, respectively, as

$$\begin{aligned} \sigma^2_{\eta_{t,\mathrm{X}}} &= \kappa^2_{t,\mathrm{X}}, \\ \sigma^2_{\eta_{r,\mathrm{Y}}} &= \kappa^2_{r,\mathrm{Y}} P_{\mathrm{X}} |h_{\mathrm{XY}}|^2, \\ \sigma^2_{n_{\mathrm{Y}}} &= N_0, \end{aligned} \tag{4.17}$$

where $\kappa^2_{t,\mathrm{X}}$ and $\kappa^2_{r,\mathrm{Y}}$ are constants characterizing the level of hardware impairments.

From (4.16) and (4.17), we can determine the instantaneous signal-to-noise ratio (SNR) of the X-Y link by

$$\begin{aligned} \Psi_{\mathrm{XY}} &= \frac{P_{\mathrm{X}} |h_{\mathrm{XY}}|^2}{\left(\kappa^2_{t,\mathrm{X}} + \kappa^2_{r,\mathrm{Y}} \right) P_{\mathrm{X}} |h_{\mathrm{XY}}|^2 + N_0} \\ &= \frac{P_{\mathrm{X}} \gamma_{\mathrm{XY}}}{\kappa_{\mathrm{XY}} P_{\mathrm{X}} \gamma_{\mathrm{XY}} + N_0}, \end{aligned} \tag{4.18}$$

where $\kappa_{\mathrm{XY}} = \kappa_{t,\mathrm{X}}^2 + \kappa_{r,\mathrm{Y}}^2$ is the total level of hardware impairments on the X-Y link and $\gamma_{\mathrm{XY}} = |h_{\mathrm{XY}}|^2$ is channel gain. For ease of presentation and analysis, let us denote κ_{D} and κ_{E} as the total level of hardware impairments on the data links and eavesdropper links, respectively, i.e. $\kappa_{\mathrm{D}} = \tau_{\mathrm{T}_i\mathrm{T}_j}$ and $\kappa_{\mathrm{E}} = \kappa_{\mathrm{T}_i\mathrm{E}}, \ \forall i, j \in \{0,1,2,...,M\}$.

Because h_{XY} is a Rayleigh fading coefficient, channel gain γ_{XY} is an exponential RV whose CDF and PDF are given, respectively, as

$$\begin{aligned} F_{\gamma_{\mathrm{XY}}}(x) &= 1 - \exp(-\lambda_{\mathrm{XY}} x), \\ f_{\gamma_{\mathrm{XY}}}(x) &= \lambda_{\mathrm{XY}} \exp(-\lambda_{\mathrm{XY}} x), \end{aligned} \tag{4.19}$$

where λ_{XY} is a parameter of RV γ_{XY}, i.e. $\lambda_{\mathrm{XY}} = 1/E\{\gamma_{\mathrm{XY}}\}$ and $E\{.\}$ is an expected operation. In addition, λ_{XY} can be modelled as in [3], [46], [48]: $\lambda_{\mathrm{XY}} = d_{\mathrm{XY}}^{\beta}$, where d_{XY} is the distance between X and Y, and β is a path-loss exponent.

Using (4.18), we can write the SNR received at eavesdropper E from the transmission of transmitter T_{m-1} $(m = 1,2,...,M)$ as

$$\Psi_{\mathrm{T}_{m-1}\mathrm{E}} = \frac{P_{\mathrm{T}_{m-1}} \gamma_{\mathrm{T}_{m-1}\mathrm{E}}}{\kappa_{\mathrm{E}} P_{\mathrm{T}_{m-1}} \gamma_{\mathrm{T}_{m-1}\mathrm{E}} + N_0}. \tag{4.20}$$

So that eavesdropper E cannot decode the source data successfully, i.e. $\Psi_{\mathrm{T}_{m-1}\mathrm{E}} \le \gamma_{th}$ (γ_{th} is a predetermined outage threshold), the maximum transmit power of T_{m-1} can be given by

$$P_{\mathrm{T}_{m-1}} = \frac{N_0 \gamma_{th}}{(1 - \kappa_{\mathrm{E}} \gamma_{th}) \gamma_{\mathrm{T}_{m-1}\mathrm{E}}}. \tag{4.21}$$

In (4.21), we assume that the hardware impairment level κ_{E} is small enough so that the value of $\kappa_{\mathrm{E}} \gamma_{th}$ is less than 1 [48].

Next, the operation of the proposed protocol is described. At first, if the number of hops is even, the *M*-hop route is sub-divided into two hops and the incremental cooperative transmission is realized on each $\mathrm{T}_k \to \mathrm{T}_{k+1} \to \mathrm{T}_{k+2}$ link (Figure. 4.4), where $k = 2n$ and $n = 0,1,...,M/2$. If M is odd, cooperative communication is also performed in groups of two-hops, and direct transmission is used for the last hop (Figure. 4.5).

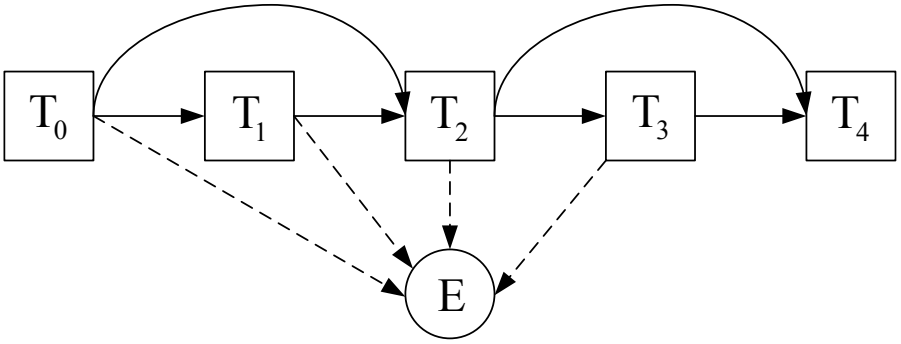

Figure 4.4. *Cooperative transmission in the MCT protocol when M=4.*

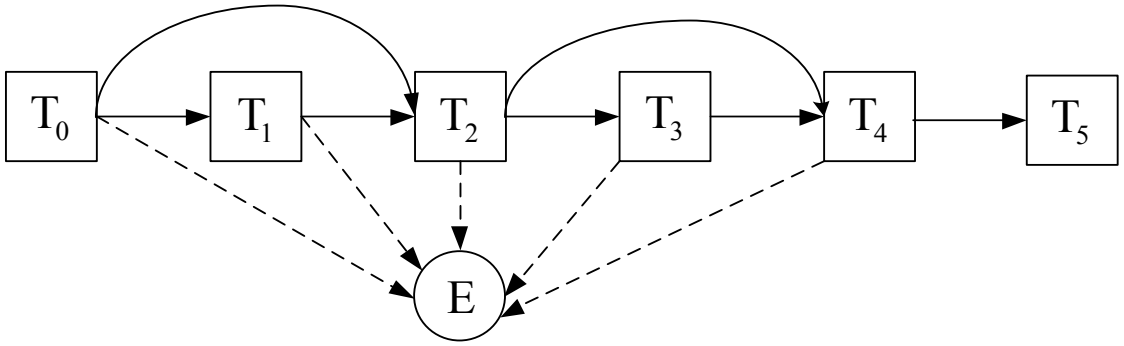

Figure 4.5. *Cooperative transmission in the MCT protocol when M=5.*

Let us consider the cooperative transmission on the $\mathrm{T}_k \to \mathrm{T}_{k+1} \to \mathrm{T}_{k+2}$ cooperative link. First, T_k broadcasts data to T_{k+1} and T_{k+2} using the transmit power given in (4.20). Then, T_{k+1} and T_{k+2} attempt to decode the received data. If T_{k+2} can receive the data correctly, it feeds back an ACK message to T_k and T_{k+1}, and then cooperates with T_{k+3} to send the decoded data to T_{k+4}. However, if T_{k+2} fails to decode the received data, it has to generate a NACK message to inform the decoding status. In this case, T_{k+1} would retransmit the data to T_{k+2} if this node can decode it successfully. If the decoding status at T_{k+2} is incorrect again, the data is dropped. Otherwise, the incremental cooperation procedure would be repeated on the $\mathrm{T}_{k+2} \to \mathrm{T}_{k+3} \to \mathrm{T}_{k+4}$ link until the destination can receive the source data successfully. In the case when the number of hops M is odd, T_{M-1} directly sends the data to T_M at the last hop.

For performance comparison, let us consider the multi-hop direct transmission protocol (MDT), where direct transmission is employed at each hop [PTT03].

From (4.20) and (4.21), the instantaneous SNR of the $\mathrm{T}_{m-1} \to \mathrm{T}_m$ link can be expressed as

$$\begin{aligned} \Psi_{\mathrm{T}_{m-1}\mathrm{T}_m} &= \frac{P_{\mathrm{T}_{m-1}} \gamma_{\mathrm{T}_{m-1}\mathrm{T}_m}}{\kappa_{\mathrm{D}} P_{\mathrm{T}_{m-1}} \gamma_{\mathrm{T}_{m-1}\mathrm{T}_m} + N_0} \\ &= \frac{\rho_{th} \gamma_{\mathrm{T}_{m-1}\mathrm{T}_m} / \gamma_{\mathrm{T}_{m-1}\mathrm{E}}}{\kappa_{\mathrm{D}} \rho_{th} \gamma_{\mathrm{T}_{m-1}\mathrm{T}_m} / \gamma_{\mathrm{T}_{m-1}\mathrm{E}} + 1}, \end{aligned} \tag{4.22}$$

where $\rho_{th} = \gamma_{th} / \left(1 - \kappa_{\mathrm{E}} \gamma_{th}\right)$.

Hence, the secrecy capacity obtained at node T_{m-1} because of transmission at node T_m in the presence of eavesdropper E is calculated as in [13] by

$$\begin{aligned} C_{\mathrm{sec}} &= \max\left(0, \log_2\left(1 + \Psi_{\mathrm{T}_{m-1}\mathrm{T}_m}\right) - \log_2\left(1 + \Psi_{\mathrm{T}_{m-1}\mathrm{E}}\right)\right) \\ &= \max\left(0, \log_2\left(\frac{1 + \Psi_{\mathrm{T}_{m-1}\mathrm{T}_m}}{1 + \Psi_{\mathrm{T}_{m-1}\mathrm{E}}}\right)\right). \end{aligned} \tag{4.23}$$

4.5. Power beacon-aided multi-hop relaying networks

As illustrated in Figure 4.6, source T_0 wants to send its data to destination T_K with the help of $K-1$ relay nodes, denoted as $\mathrm{T}_1, \mathrm{T}_2, ..., \mathrm{T}_{K-1}$. Transmitter T_k has to harvest energy from the power beacon (B) to use for data transmission, where $k = 0, 1, ..., K-1$. Assume that all nodes are equipped with a single-antenna and operate in half-duplex mode. As a result, data transmission is split into K orthogonal time slots.

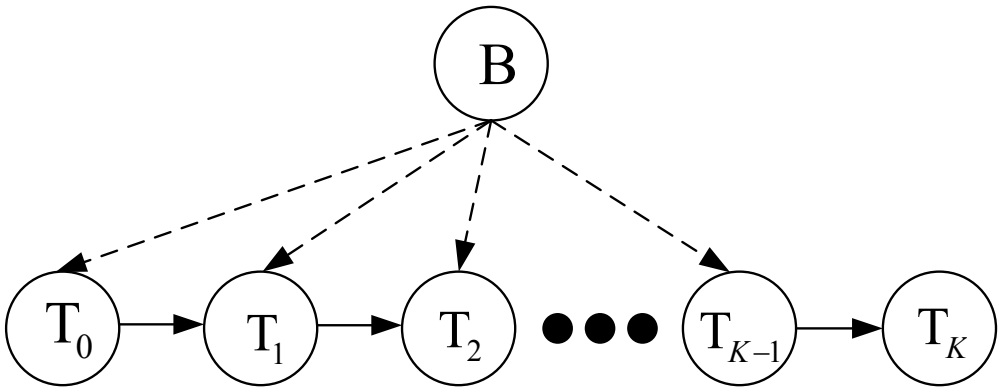

Figure 4.6. *System model of the proposed protocol.*

Let us denote Q as the total transmission time between the source and destination. Hence, the transmission time allocated for each time slot is given as $\tau = Q / K$. Moreover, at each time slot, transmitter T_k spends time $\alpha\tau$ to harvest the energy from radio frequency (RF) signals generated by B, and the remaining time $(1-\alpha)\tau$ is used to forward the source data to the next hop, where $0 < \alpha < 1$. The energy that T_k can harvest is expressed as

$$\mathrm{E}_k = \eta \alpha \tau P \gamma_{\mathrm{B},k}, \tag{4.24}$$

where η $(0 \le \eta \le 1)$ is the energy conversion efficiency, P is the transmit power of B and $\gamma_{\mathrm{B},k}$ is the channel gain between B and T_k.

From (4.24), the transmit power of T_k is calculated as

$$P_k = \frac{\mathrm{E}_k}{(1-\alpha)\tau} = \mu P \gamma_{\mathrm{B},k}, \tag{4.25}$$

where

$$\mu = \frac{\eta\alpha}{1-\alpha}. \tag{4.26}$$

Comment 1. We assume that the frequencies used for the EH phase are different from those used for data transmission so that no interference occurs in the signals received at the receivers.

Let us consider data transmission at the k-th time slot, where transmitter T_{k-1} sends the source data to receiver T_k, where $k = 1,...,K$. To enhance system throughput, node T_{k-1} combines N signals to create a superimposed data as

$$x_c = \sum_{n=1}^{N} \sqrt{a_n P_{k-1} x_n}, \tag{4.27}$$

where a_n are power allocation coefficients, x_n is the transmitted signal, $n = 1,2,...,N$, $\sum_{n=1}^{N} a_n = 1$ and $a_1 > a_2 > ... > a_N$.

Comment 2. Conventionally, a K-hop relaying protocol using the orthogonal multiple access (OMA) technique only obtains a data rate of $1/K$. Hence, by simultaneously transmitting N signals, code and frequency, our proposed scheme can obtain a data rate of N/K.

Assuming that the SIC process is perfect [49]-[54], the instantaneous SNR obtained at T_k used to decode signal x_n under the impact of hardware impairments can be expressed as

$$\psi_k^n = \begin{cases} \dfrac{a_n P_{k-1}\gamma_{\mathrm{D},k}}{\kappa^2 P_{k-1}\gamma_{\mathrm{D},k} + \sum_{i=n+1}^{N} a_i P_{k-1}\gamma_{\mathrm{D},k} + \sigma^2}, & \text{if } n<N \\ \dfrac{a_N P_{k-1}\gamma_{\mathrm{D},k}}{\kappa^2 P_k \gamma_{\mathrm{D},k} + \sigma^2}, & \text{if } n=N \end{cases}, \tag{4.28}$$

where $\gamma_{\mathrm{D},k}$ is the channel gain between T_{k-1} and T_k, κ^2 is the total hardware impairment level on all of the data links [25], [26], [46] and σ^2 is the variance of Gaussian noise at all of the receivers.

Substituting (4.25) into (4.28), which yields

$$\psi_k^n = \begin{cases} \dfrac{\mu a_n \Delta\gamma_{\mathrm{B},k-1}\gamma_{\mathrm{D},k}}{\left(\kappa^2 + \sum_{i=n+1}^{N} a_i\right)\mu\Delta\gamma_{\mathrm{B},k-1}\gamma_{\mathrm{D},k} + 1}, & \text{if } n<N \\ \dfrac{\mu a_N \Delta\gamma_{\mathrm{B},k-1}\gamma_{\mathrm{D},k}}{\kappa^2\mu\Delta\gamma_{\mathrm{B},k-1}\gamma_{\mathrm{D},k} + 1}, & \text{if } n=N \end{cases}, \tag{4.29}$$

where $\Delta = P/\sigma^2$ is transmit SNR.

Moreover, the instantaneous channel capacity of signal x_n is then calculated as

$$C_k^n = (1-\alpha)\tau \log_2\left(1+\psi_k^n\right). \tag{4.30}$$

Using a decode-and-forward (DF) relaying technique, the end-to-end channel capacity of signal x_n can be expressed as

$$C_{\text{e2e}}^{n} = \min_{k=1,2,\ldots,K} \left(C_{k}^{n} \right). \tag{4.31}$$

Finally, the throughput of the proposed scheme can be defined, similarly to [PTT06]:

$$\text{TP}_{\text{NOMA}} = \left(1-\alpha\right)\tau C_{\text{th}} \sum_{n=1}^{N} \Pr\left(C_{\text{e2e}}^{n} \geq C_{\text{th}} \right), \tag{4.32}$$

where C_{th} is the target rate.

For baseline comparison, this thesis also considers the PB-EH multi-hop relaying scheme without using NOMA (named OMA). In this method, T_{k-1} only sends one signal to T_{k} using transmit power P_{k-1}. The throughput of this scheme is defined as

$$\text{TP}_{\text{OMA}} = \left(1-\alpha\right)\tau C_{\text{th}} \Pr\left(C_{\text{e2e}}^{\text{wo}} \geq C_{\text{th}} \right), \tag{4.33}$$

where

$$C_{\text{e2e}}^{\text{wo}} = \min_{k=1,2,\ldots,K} \left(\left(1-\alpha\right)\tau \log_2 \left(1 + \frac{\mu\Delta\gamma_{\text{B},k-1}\gamma_{\text{D},k}}{\kappa^2 \mu\Delta\gamma_{\text{B},k-1}\gamma_{\text{D},k} + 1} \right) \right). \tag{4.34}$$

5. RELAY SELECTION METHODS IN COGNITIVE NETWORKS

In this chapter, the first aim mentioned in Chapter 3 will be clarified. The main idea is to study physical-layer security issue in dual-hop underlay cognitive radio networks in the presence of hardware impairments. The transmit power of secondary relays under the interference constraint at the primary user and the intercept probability constraint at the eavesdropper is first derived. Then, various relay selection methods are employed to improve the outage performance of the secondary networks. For performance evaluation and comparison, the exact closed-form expressions of outage probability over the Rayleigh fading channel are derived. Finally, the derived expressions are verified using Monte Carlo simulations.

5.1. Motivations

Recently, diversity-based relaying communication [2], [4] has gained much attention as a promising technique to mitigate the effect of a fading environment. This technique has also been widely used in underlay cognitive radio to improve performance in secondary networks [55], [56]. In underlay cognitive radio networks, secondary users (SUs) can use the same licensed band as primary users (PUs), provided that the interferences caused by their operations are lower than the permissible threshold required by the primary users (PUs) [57].

Physical-layer security is a simple method to guarantee the security of wireless communications without using complex cryptographic methods [10]. Again, cooperative relaying protocols are used in order to improve secrecy performance in a secured communication network. The authors in [17] proposed relay selection methods for cooperative networks with secrecy constraints. Published work [16] considered joint relay and jammer selection methods, where the best relay was used to forward source data to the destination, while the optimal jammer relay generated limited interference to eavesdroppers. In [20], the authors evaluated the secrecy outage probability of secondary networks with various relay jammer selection schemes at the cooperative phase. In [19], dual-hop secured multicast networks in underlay cognitive radio with partial relay selection were proposed and analysed. The authors in [58], [59] considered security versus reliability for cooperative relay networks via performance metrics such as intercept probability at the eavesdropper and outage probability at authorized nodes.

However, performance analysis in [10], [16], [17], [19], [20], [58] and [59] is based on the assumption that the transceiver hardware of the terminals is perfect. In practice, because of phase noises and nonlinear amplifier and I/Q imbalance, transceivers suffer from hardware impairments [24], [26] that degrade performance in wireless networks. The authors in [27] first studied secrecy performance in the presence of the hardware imperfections. The authors in [27] particularly considered the effects of I/Q imbalance on the performance of OFDMA secured systems.

In this chapter relay selection methods are employed to improve the outage performance of secondary networks under the interference constraint at the primary user, the constraint of intercept probability (IP) at the eavesdropper and the presence of hardware imperfection. Unlike [58]-[59], by constraining the IP at the eavesdropper, a closed-form expression of the secondary relays

transmit power is given. In the first proposed scheme, the active relay providing the highest channel gain to the destination is selected to forward the source data to the destination. In the second, the best relay is chosen to maximize the signal-to-noise ratio (SNR) obtained at the secondary destination. In contrast to [16], [17], [19], [20], exact closed-form expressions of outage probability for secondary networks over a Rayleigh fading channel are derived. Finally, Monte-Carlo simulations are presented to validate these derivations. The results show that the proposed methods outperform the conventional relay selection method in which the relay is randomly selected.

5.2. System model

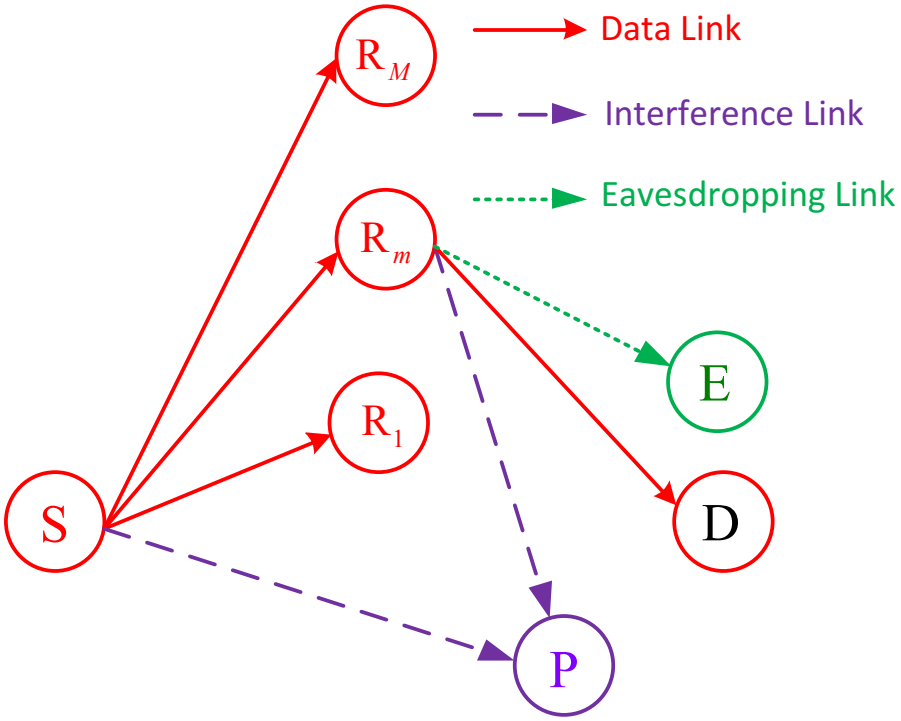

Figure 5.1. *Secure communication in dual-hop underlay cognitive radio networks.*

Figure 5.1 presents a system model of the proposed protocol, where a secondary source (S) communicates with a secondary destination (D) with help from M secondary relays, i.e. $\mathrm{R}_m\left(m=1,2,...,M\right)$. We assume that no direct link exists between S and D because of the great distance and deep fading. Secondary transmitters such as the source and relays must adapt their transmit power to satisfy a maximum interference threshold I_{th} at the primary user (P). In the secondary network, an eavesdropper E attempts to eavesdrop on the data transmitted to the destination. We assume that the eavesdropper is near the destination and cannot listen in on the data transmitted by the source. We also assume that the secondary relays are close together and form a cluster [15]. All of the terminals are equipped with a single antenna and operate in half-duplex mode. Hence, data transmission is achieved through a time division technique over orthogonal channels.

Let d_1, d_2, d_3, d_4 and d_5 denote the distances of $\mathrm{S}\to\mathrm{R}_m$, $\mathrm{R}_m\to\mathrm{D}$, $\mathrm{S}\to\mathrm{P}$, $\mathrm{R}_m\to\mathrm{P}$, and

$\mathrm{R}_m \to \mathrm{E}$ links, respectively. We also denote $h_{1i}, h_{2i}, h_3, h_{4i}$ and h_{5i} as the channel coefficients of $\mathrm{S} \to \mathrm{R}_m, \mathrm{R}_m \to \mathrm{D}$, $\mathrm{S} \to \mathrm{P}$, $\mathrm{R}_m \to \mathrm{P}$, and $\mathrm{R}_m \to \mathrm{E}$ links, respectively. We assume that all of the channels follow a Rayleigh fading distribution. Hence, the channel gains $\gamma_{1i} = |h_{1i}|^2, \gamma_{2i} = |h_{2i}|^2, \gamma_3 = |h_3|^2$, $\gamma_{4i} = |h_{4i}|^2$ and $\gamma_{5i} = |h_{5i}|^2$ follow exponential distributions. To consider path-loss, the parameters $\gamma_{1i}, \gamma_{2i}, \gamma_3, \gamma_{4i}$, and γ_{5i} can be modelled as [3] $\lambda_1 = d_1^\beta$, $\lambda_2 = d_2^\beta$, $\lambda_3 = d_3^\beta$, $\lambda_4 = d_4^\beta$, and $\lambda_5 = d_5^\beta$, respectively, where β is the path-loss exponent.

As with [61], the maximum transmit power of source S under the interference constraint and hardware impairments can be given as

$$P_0 = \frac{I_{th}}{\gamma_3 (1+\kappa)}, \tag{5.1}$$

where κ is the constant characterizing the total level of hardware impairments at the transmitters and receivers.

The instantaneous signal-to-noise ratio (SNR) of the $\mathrm{S} \to \mathrm{R}_m$ link can then be obtained as

$$\begin{aligned} \Psi_{1m} &= \frac{P_0 \gamma_{1m}}{\kappa P_0 \gamma_{1m} + N_0} \\ &= \frac{Q \gamma_{1m} / \gamma_3}{\kappa Q \gamma_{1m} / \gamma_3 + 1}, \end{aligned} \tag{5.2}$$

where N_0 is the variance of Gaussian noise, which is assumed to be the same at all receivers, i.e. the relay, destination and eavesdropper, and $Q = I_{th} / N_0 / (1+\kappa)$.

Next, the operation of the proposed protocol is described: at the first time slot, source S broadcasts its data to all of the relays. The relays then attempt to decode the source's data from the received data. Let us denote W_1 and W_2 as the set of relays that decode the signal successfully and unsuccessfully, respectively. Without loss of generality, we can assume that $W_1 = \{R_1, R_2, ..., R_N\}$ and $W_2 = \{R_{N+1}, R_{N+2}, ..., R_M\}$, where N is the cardinality of the set W_1, $N \in \{0,1,2,...,M\}$. Particularly, if N=0, no relay can forward the source data to the destination. If $N \geq 1$, the system can choose a relay to forward the source data.

We assume that a relay is in outage if the received SNR at that node is below the outage threshold γ_{th}. Otherwise, we assume that the relay successfully receives the data. Therefore, the probability that the number of active relay equal to N is calculated as follows:

$$\begin{aligned} \mathrm{P}(|W_1| = N) &= C_M^N \Pr\begin{pmatrix} \Psi_{11} \geq \gamma_{th}, ..., \Psi_{1N} \geq \gamma_{th}, \\ \Psi_{1N+1} < \gamma_{th}, ..., \Psi_{1M} < \gamma_{th} \end{pmatrix} \\ &= C_M^N \Pr\left(\frac{\gamma_{11}}{\gamma_3} \geq \rho, ..., \frac{\gamma_{1N}}{\gamma_3} \geq \rho, \frac{\gamma_{1N+1}}{\gamma_3} < \rho, ..., \frac{\gamma_{1M}}{\gamma_3} < \rho \right), \end{aligned} \tag{5.3}$$

where $C_M^N = \frac{M!}{N!(M-N)!}$ and $\rho = \frac{\gamma_{th}}{(1-\kappa\gamma_{th})Q}$.

In (5.3), only the case where $\kappa\gamma_{th} < 1$ is considered. Indeed, in practice, the hardware impairment level is small, and hence the condition of $\kappa\gamma_{th} < 1$ is assumed satisfied [25].

Next, (5.3) can be re-written as:

$$\mathrm{P}(|W_1| = N) = C_M^N \int_0^{+\infty} \begin{pmatrix} f_{\gamma_3}(x)\left[F_{\gamma_1}(\rho x)\right]^{M-N} \\ \times\left[1-F_{\gamma_1}(\rho x)\right]^{N} \end{pmatrix} dx. \tag{5.4}$$

Using the PDF and CDF of the exponential random variables, i.e. $f_{\gamma_3}(x) = \lambda_3 \exp(-\lambda_3 x)$ and $F_{\gamma_1}(y) = 1-\exp(-\lambda_1 y)$, we obtain

$$\mathrm{P}(|W_1| = N) = C_M^N \int_0^{+\infty} \begin{bmatrix} \lambda_3 \exp(-\lambda_3 x)\left(1-\exp(-\lambda_1\rho x)\right)^{M-N} \\ \times\exp(-N\lambda_1\rho x) \end{bmatrix} dx. \tag{5.5}$$

Using the binomial expansion for $\left(1-\exp(-\lambda_1\rho x)\right)^{M-N}$ and after calculating the integrals, an exact closed-form expression for $\mathrm{P}(|W_1| = N)$ can be given by

$$\mathrm{P}(|W_1| = N) = \sum_{j=0}^{M-N} (-1)^j \frac{C_{M-N}^j C_M^N \lambda_3}{\lambda_3 + (j+N)\lambda_1\rho}. \tag{5.6}$$

More specially, when $N = 0$, we can obtain

$$\mathrm{P}(|W_1| = 0) = \sum_{j=0}^{M} (-1)^j C_M^j \frac{\lambda_3}{\lambda_3 + j\lambda_1\rho}. \tag{5.7}$$

5.3. Performance analysis

5.3.1. Intercept probability (IP) at the eavesdropper

Let us denote P_j as the transmit power of relay R_j. First, the received SNR at the eavesdropper because of transmission at relay R_j can be expressed as

$$\Upsilon_{ej} = \frac{\mathrm{P}_j\gamma_{5j}}{\kappa\mathrm{P}_j\gamma_{5j} + N_0}. \tag{5.8}$$

As with [58]-[59], the intercept probability can be computed by

$$\begin{aligned}\text{IP}&=\Pr\left(\Upsilon_{ej}\geq\gamma_{th}\right)\\&=\Pr\left(\frac{\text{P}_j\gamma_{5j}}{\kappa\text{P}_j\gamma_{5j}+N_0}\geq\gamma_{th}\right)\\&=\Pr\left(\gamma_{5j}\geq\frac{N_0\gamma_{th}}{\left(1-\kappa\gamma_{th}\right)\text{P}_j}\right)\\&=\exp\left(-\frac{\lambda_5 N_0\theta}{\text{P}_j}\right),\end{aligned}\tag{5.9}$$

where $\theta=\gamma_{th}/\left(1-\kappa\gamma_{th}\right)$.

The IP at the eavesdropper must be lower than a predetermined value, i.e. ε. Hence, the constraint of transmit power P_j can be found by

$$\text{IP}\leq\varepsilon\Leftrightarrow\text{P}_j\leq\frac{\lambda_5 N_0\theta}{\ln\left(1/\varepsilon\right)}.\tag{5.10}$$

Furthermore, to satisfy the interference constraint at the primary user, transmit power P_j must be adjusted such that $\text{P}_j\leq I_{th}/\gamma_{4j}/\left(1+\kappa\right)$. Hence, the maximum transmit power at relay P_j is given as

$$\begin{aligned}\text{P}_j&=\min\left(\frac{\lambda_5 N_0\theta}{\ln\left(1/\varepsilon\right)},\frac{I_{th}}{\gamma_{4j}\left(1+\kappa\right)}\right)\\&=N_0\min\left(W,\frac{Q}{\gamma_{4j}}\right),\end{aligned}\tag{5.11}$$

where $W=\lambda_5\theta/\ln\left(1/\varepsilon\right)$.

From the transmit power in (5.10), the received SNR at the destination is given by

$$\begin{aligned}\Psi_{2j}&=\frac{\text{P}_j\gamma_{2j}}{\kappa\text{P}_j\gamma_{2j}+N_0}\\&=\frac{\min\left(W,Q/\gamma_{4j}\right)\gamma_{2j}}{\kappa\min\left(W,Q/\gamma_{4j}\right)\gamma_{2j}+1}.\end{aligned}\tag{5.12}$$

5.3.2. Relay selection methods

This section considers the conventional relay selection protocol, named PR0, in which an active relay, e.g. R_a is selected randomly to forward source data to the destination.

In the second proposed protocol, named PR1, the active relay which has the highest channel gain to the destination is selected for cooperation. Let us denote R_b as the selected relay. The relay selection strategy can be given as

$$\mathrm{R}_b : \gamma_{2b} = \max_{j=1,2,\ldots,N} \left(\gamma_{2j} \right). \tag{5.13}$$

Finally, an optimal relay selection method is proposed, where the best relay R_c is selected to maximize the SNR received at the destination, i.e.

$$\mathrm{R}_c : \Psi_{2c} = \max_{j=1,2,\ldots,N} \left(\Psi_{2j} \right). \tag{5.14}$$

In this section, the outage probability (OP) of the considered protocols is also derived. Generally, the OP of the PRX protocol (X = 0, 1, 2) can be expressed as

$$\mathrm{OP}_{\mathrm{X}} = \mathrm{P}\left(|W_1| = 0 \right) + \sum_{N=1}^{M} \mathrm{P}\left(|W_1| = N \right) \Pr\left(\Psi_{2y} < \gamma_{th} \right), \tag{5.15}$$

where $y = a, b, c$, corresponding to X = 0, 1, 2, respectively.

By applying [62, (eq. (A.1))], the probability $\Pr\left(\Psi_{2a} < \gamma_{th} \right)$ in (15) can be expressed as

$$\Pr\left(\Psi_{2a} < \gamma_{th} \right) = 1 - \exp\left(-\frac{\lambda_2 \theta}{W} \right) + \frac{\lambda_2 \theta}{\lambda_2 \theta + \lambda_4 Q} \exp\left(-\frac{\lambda_2 \theta + \lambda_4 Q}{W} \right). \tag{5.16}$$

Combining (5.6), (5.7), (5.15) and (5.16), an exact closed-form expression of the OP for the PR0 protocol is given by

$$\begin{aligned} \mathrm{OP}_0 = & \sum_{j=0}^{M} (-1)^j C_M^j \frac{\lambda_3}{\lambda_3 + j\lambda_1 \rho} + \sum_{N=1}^{M} \sum_{j=0}^{M-N} (-1)^j \frac{C_{M-N}^j C_M^N \lambda_3}{\lambda_3 + (j+N)\lambda_1 \rho} \\ & \times \left[1 - \exp\left(-\frac{\lambda_2 \theta}{W} \right) + \frac{\lambda_2 \theta}{\lambda_2 \theta + \lambda_4 Q} \exp\left(-\frac{\lambda_2 \theta + \lambda_4 Q}{W} \right) \right]. \end{aligned} \tag{5.17}$$

For the PR1 protocol, let us first consider the probability $\Pr\left(\Psi_{2b} < \gamma_{th} \right)$, which can be expressed as

$$\begin{aligned} \Pr\left(\Psi_{2b} < \gamma_{th} \right) &= \Pr\left(\frac{\min\left(W, Q/\gamma_{4b} \right) \gamma_{2b}}{\kappa \min\left(W, Q/\gamma_{4b} \right) \gamma_{2b} + 1} < \gamma_{th} \right) \\ &= \Pr\left(\min\left(W, \frac{Q}{\gamma_{4b}} \right) \gamma_{2b} < \theta \right) \\ &= \underbrace{\Pr\left(\gamma_{4b} < \frac{Q}{W}, \gamma_{2b} < \frac{\theta}{W} \right)}_{I_1} + \underbrace{\Pr\left(\gamma_{4b} \geq \frac{Q}{W}, \frac{\gamma_{2b}}{\gamma_{4b}} < \frac{\theta}{Q} \right)}_{I_2}. \end{aligned} \tag{5.18}$$

Furthermore, the CDF of γ_{2b} can be given as in [19] as

$$\begin{aligned} F_{\gamma_{2b}}(y) &= \Pr\left(\gamma_{2b} < y \right) \\ &= \left(1 - \exp\left(-\lambda_2 y \right) \right)^N \\ &= \sum_{t=0}^{N} (-1)^t C_N^t \exp\left(-t\lambda_2 y \right). \end{aligned} \tag{5.19}$$

From (5.18) and (5.19), we obtain the probability I_1 as

$$
\begin{aligned}
I_1 &= \Pr\left(\gamma_{4b} < \frac{Q}{W}\right)\Pr\left(\gamma_{2b} < \frac{\theta}{W}\right) \\
&= \left(1-\exp\left(-\lambda_4 \frac{Q}{W}\right)\right)\left(1-\exp\left(-\lambda_2 \frac{\theta}{W}\right)\right)^N .
\end{aligned} \tag{5.20}
$$

Next, the probability I_2 in (5.18) can be expressed by

$$
I_2 = \int_{Q/W}^{+\infty} f_{\gamma_{4b}}(x) F_{\gamma_{2b}}\left(\frac{\theta}{Q}x\right) dx. \tag{5.21}
$$

Putting (5.19) and (5.21) together, and after some careful manipulation, we obtain

$$
I_2 = \sum_{t=0}^{N} (-1)^t C_N^t \frac{\lambda_4 Q}{t\lambda_2\theta + \lambda_4 Q} \exp\left(-\frac{t\lambda_2\theta + \lambda_4 Q}{W}\right). \tag{5.22}
$$

From the results obtained above, an exact closed-form expression of the OP for the PR1 protocol is given as

$$
\begin{aligned}
\mathrm{OP}_1 = {} & \sum_{j=0}^{M} (-1)^j C_M^j \frac{\lambda_3}{\lambda_3 + j\lambda_1\rho} + \sum_{N=1}^{M}\sum_{j=0}^{M-N} (-1)^j \frac{C_{M-N}^j C_M^N \lambda_3}{\lambda_3 + (j+N)\lambda_1\rho} \\
& \times \left[\begin{array}{l} \left(1-\exp\left(-\lambda_4 \frac{Q}{W}\right)\right)\left(1-\exp\left(-\lambda_2 \frac{\theta}{W}\right)\right)^N \\ + \sum_{t=0}^{N} (-1)^t C_N^t \frac{\lambda_4 Q}{t\lambda_2\theta + \lambda_4 Q} \exp\left(-\frac{t\lambda_2\theta + \lambda_4 Q}{W}\right) \end{array} \right].
\end{aligned} \tag{5.23}
$$

Next, from the relay selection method proposed in (5.14), it is obvious that

$$
\begin{aligned}
\Pr(\Psi_{2c} < \gamma_{th}) &= \Pr\left(\max_{j=1,2,\ldots,N}(\Psi_{2j}) < \gamma_{th}\right) \\
&= \left(\Pr(\Psi_{2a} < \gamma_{th})\right)^N \\
&= \left(1-\exp\left(-\frac{\lambda_2\rho}{W}\right) + \frac{\lambda_2\rho}{\lambda_2\rho + \lambda_4 Q}\exp\left(-\frac{\lambda_2\rho + \lambda_4 Q}{W}\right)\right)^N .
\end{aligned} \tag{5.24}
$$

Hence, an exact closed-form expression of the OP for the PR2 protocol can be expressed as (5.25) below:

$$
\begin{aligned}
\mathrm{OP}_2 = {} & \sum_{j=0}^{M} (-1)^j C_M^j \frac{\lambda_3}{\lambda_3 + j\lambda_1\rho} + \sum_{N=1}^{M}\sum_{j=0}^{M-N} (-1)^j \frac{C_{M-N}^j C_M^N \lambda_3}{\lambda_3 + (j+N)\lambda_1\rho} \\
& \times \left(1-\exp\left(-\frac{\lambda_2\rho}{W}\right) + \frac{\lambda_2\rho}{\lambda_2\rho + \lambda_4 Q}\exp\left(-\frac{\lambda_2\rho + \lambda_4 Q}{W}\right)\right)^N .
\end{aligned} \tag{5.25}
$$

5.4. Numerical results

In this section, various Monte Carlo simulations are presented to verify the theoretical results derived above. In each Monte-Carlo simulation, 10^6 trials were performed in which the channel coefficients between two terminals were randomly generated. The simulation results were then

obtained by the number of trials that the secondary system was in outage divided by 10^6. The derived equations (5.17), (5.23) and (5.25) were used to present the theoretical results. In a two-dimensional network, the co-ordinates of the source, destination, relay, primary user and eavesdropper were assumed as $(0,0),(1,0),(0.5,0),(0.5,0.5)$ and $(1,y_{\mathrm{E}})$, respectively, where $0<y_{\mathrm{E}}<0.5$. The simulation assumed that the path-loss exponent (β) equals 3 and the outage threshold (γ_{th}) equals 1.

The outage probability of the secondary network as a function of Q in dB is shown in Figure 5.2. In this simulation, the number of relays is 4 $(M=4)$, the hardware impairment level is 0.1 $(\kappa=0.1)$ and the IP threshold is set at 0.3 $(\varepsilon=0.3)$. It can be observed from Figure 5.2 that the OP of the PR2 protocol is lowest, while that of the PR0 protocol is highest. This is because the PR1 and PR2 protocols use transmit diversity, which enhances the reliability of data transmission. It can also be seen that the OP decreases with an increasing Q value.

Figure 5.3 shows the outage probability as a function of the IP threshold when $M=5$, $\kappa=0$ and $Q=0$ dB. As we can observe, the outage performance of three protocols decreases as ε increases. The transmit power of the selected relay also increases with higher value of ε. Again, the PR2 protocol obtains the best performance while the performance of the PR1 protocol is between those of the PR0 and PR2 protocols.

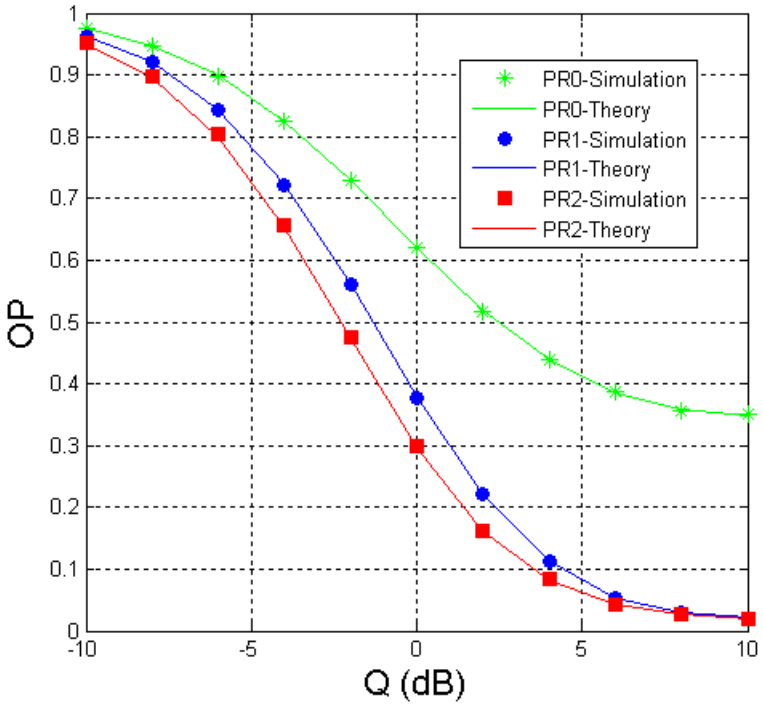

Figure 5.2. *Outage probability (OP) as a function of Q in dB when* $M=4$, $\kappa=0.1$, $y_{\mathrm{E}}=0.5$ *and* $\varepsilon=0.3$.

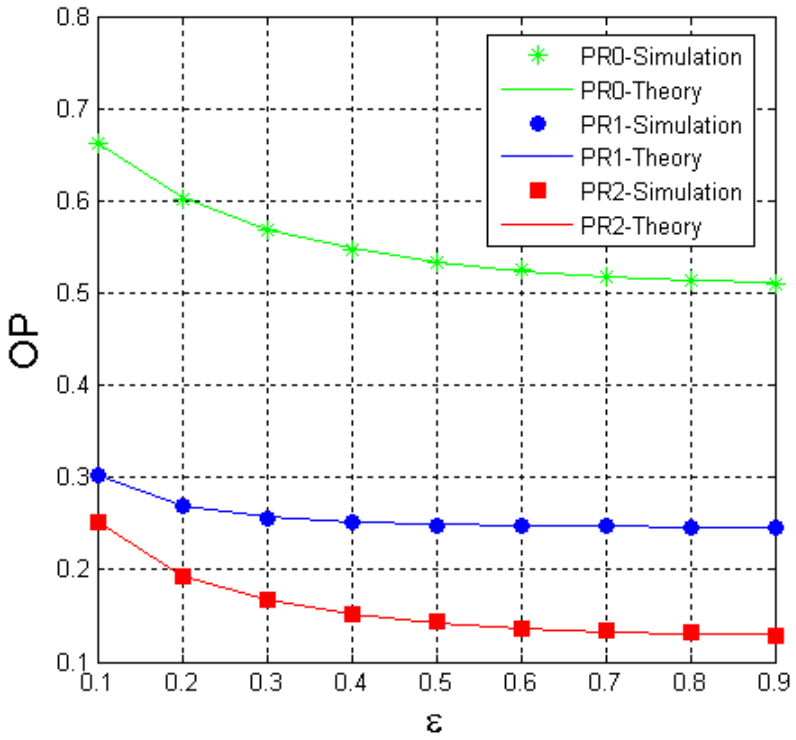

Figure 5.3. *Outage probability (OP) as a function of* ε *when* $M = 5$, $\kappa = 0$, $y_E = 0.5$ *and* $Q = 0$ *dB.*

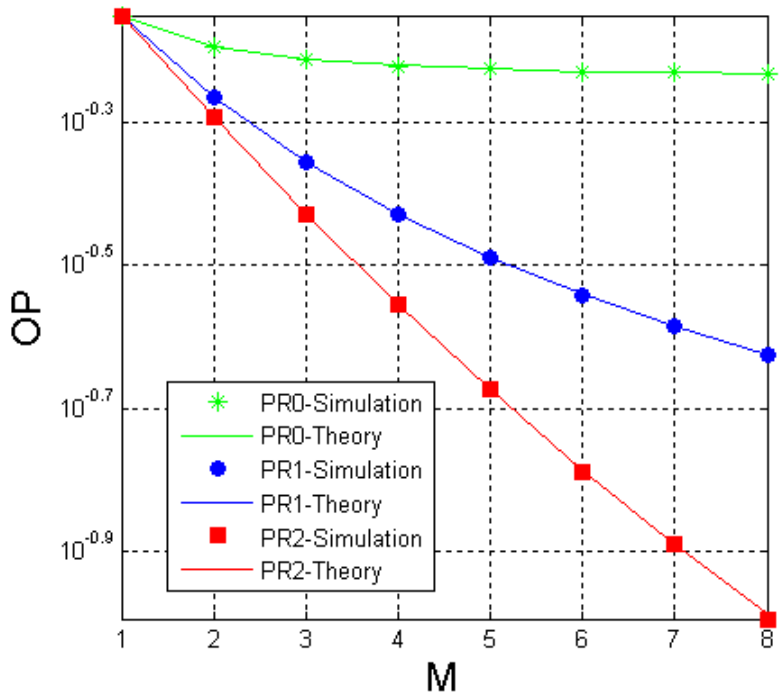

Figure 5.4. *Outage probability (OP) as a function of* M *when* $\varepsilon = 0.4$, $\kappa = 0.1$, $y_E = 0.5$ *and* $Q = 0$ *dB.*

Figure 5.4 illustrates the outage probability as a function of the number of relays when $\varepsilon = 0.4$, $\kappa = 0.1$ and $Q = 0$ dB. As we can observe, the OP of the PR1 and PR2 protocols significantly

decreases as the number of relays increases, while the outage performance of the PR0 protocol slightly decreases.

In Figure 5.5, the impact of the hardware impairment level on the outage performance when $\varepsilon = 0.1$, $M = 3$ and $Q = 0$ dB is illustrated. As shown in this figure, the OP of three protocols rapidly increases when the level κ increases.

Figure 5.6 shows the impact of the eavesdropper's positions on outage performance of the PR0, PR1 and PR2 protocols by changing the value y_E from 0.1 to 1. The remaining simulation parameters can be listed as follows: $\varepsilon = 0.1$, $\kappa = 0$, $M = 3$ and $Q = 0$ dB. We can see from this figure that the OP values of the considered protocols decrease as y_E increases. It is because of the fact that with a higher value y_E, the eavesdropper is far from the source and relays, and hence the transmit power of the secondary relays also increases. It can also be seen that when the eavesdropper is near the secondary destination, the PR1 and PR2 methods have the same performance.

From Figures 5.2–5.6, we can see that the simulation results (simulation) matched the theoretical results (theory) very well, which validates our derivations.

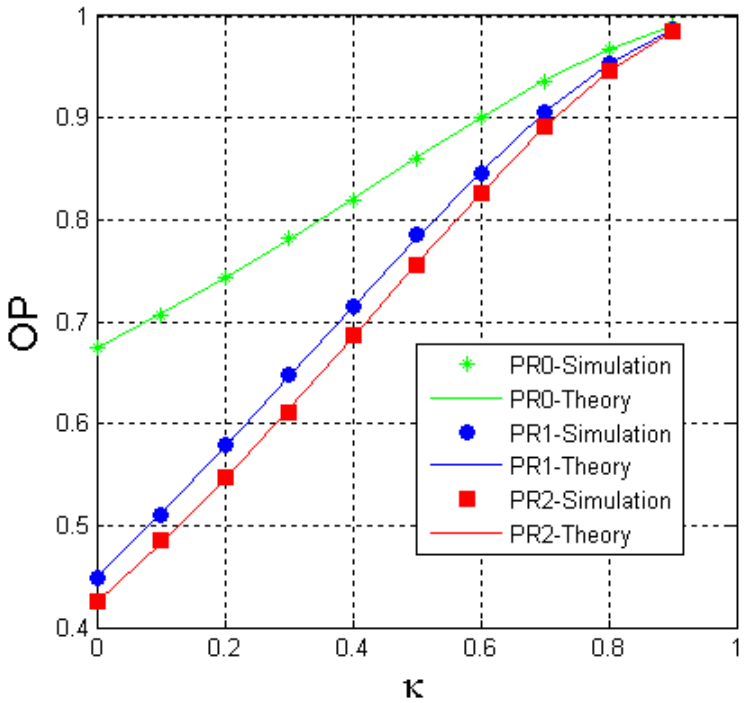

Figure 5.5. *Outage probability (OP) as a function of* κ *when* $\varepsilon = 0.1$, $M = 3$, $y_E = 0.5$ *and* $Q = 0$ *dB.*

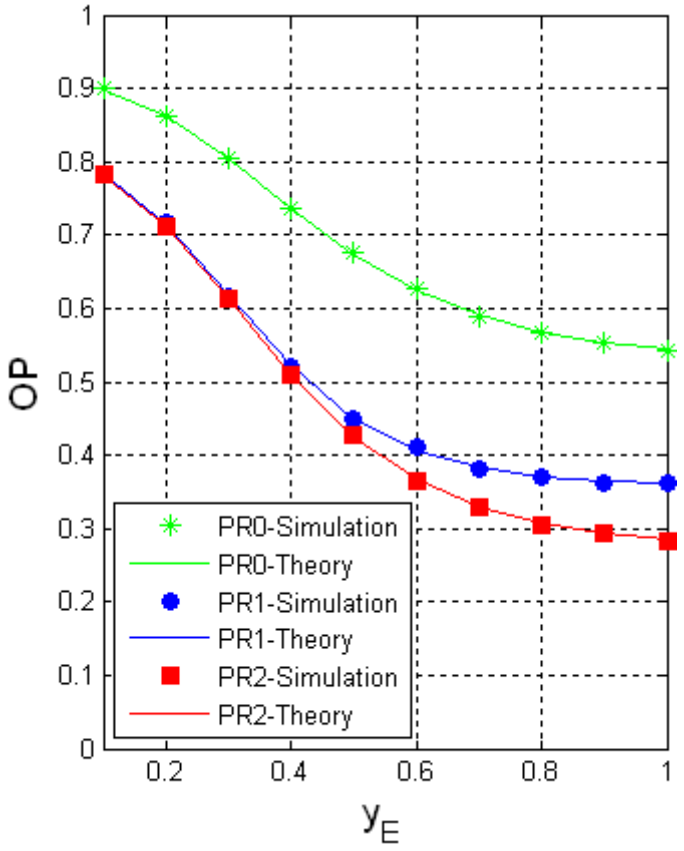

Figure 5.6. *Outage probability (OP) as a function of* y_E *when* $\varepsilon = 0.1$, $\kappa = 0$, $M = 3$ *and* $Q = 0\,dB$.

5.5. Summary

In this Chapter, physical layer security in underlay cognitive radio networks was studied. Two relay selection methods were proposed to improve the outage performance of the secondary network under the interference constraint at the primary user and intercept probability constraint at the eavesdropper. The exact closed-form expressions of the outage probability were presented and verified with Monte Carlo simulations. The results show that the proposed protocols outperformed the random relay selection protocol. Both methods also obtained higher performance when the number of relays increased. Moreover, hardware impairments have a significant impact on system performance.

6. COGNITIVE RADIO NETWORKS EMPLOYING COOPERATIVE MULTI-HOP TRANSMISSION

In this chapter, a cooperative multi-hop secured transmission protocol in cognitive radio (CR) networks is proposed and addresses the first aim. In the proposed protocol, a secondary source attempts to transmit data to a secondary destination with the assistance of multiple secondary relays and in the presence of a secondary eavesdropper which attempts to decode the transmitted data. The secondary transmitters, such as the secondary source and relays, operate in an underlay mode, where they must adjust the transmit power to satisfy the interference constraint required by the primary network. The impact of hardware imperfection at authorized nodes and the eavesdropper on system secrecy performance is also investigated. The effective signal-to-interference-plus-noise ratio (SINR), secrecy capacity under the constraints of maximum transmit power, interference threshold and hardware impairment levels are determined. For relaxed impairment levels, the exact and asymptotic expressions of end-to-end secrecy outage probability (SOP) over Rayleigh fading channels are derived by using the recursive method. The derived expressions are then verified with Monte Carlo simulations, which also show that the proposed scheme outperformed the multi-hop direct transmission protocol.

6.1. Motivations

Security is one of the most important issues in wireless communication [65-67]. Because using wireless channels entails broadcasting data transmissions, malicious nodes can eavesdrop on wireless transmission, which leads to insecurity in the data transmission. Traditional security methods are based on cryptography [63]-[65]. In this technique, the public-key and private key protocols are used to guarantee security. Recently, the security framework of the physical layer, called the wiretap channel [10], [66], has been gaining much attention. The basic idea of physical-layer security is to use the physical characteristics of wireless channels to guarantee secure communications. To improve the security of physical-layer communication, diversity-based transmission protocols with relay selection methods have been proposed. In [17], [67], opportunistic relay selection methods were applied to maximize the instantaneous secrecy rate. The literature [68] evaluated the secrecy performance of a heterogeneous channel system in which the authorized transmitter and receiver were equipped with maximal ratio combining (MRC) and selection combining (SC) techniques, respectively. In [16], [69], the authors considered the joint relay and jammer selection methods to enhance the channel capacity of the data links and to reduce the data rate received at the eavesdroppers.

Recently, cooperative cognitive secured transmission protocols have gained much attention by researchers. Published work [20] proposed various relay and jammer selection scenarios to enhance secrecy performance of the secondary network operating in underlay mode. The literature [12] considered secrecy performance enhancement for MIMO cognitive radio (CR) networks. In [26], the authors studied partial and full relay selection methods for dual-hop underlay relaying schemes. In [19], various partial selection schemes were proposed to enhance secrecy performance of underlay multi-cast CR methods. In [71], the end-to-end secrecy capacity of the multi-hop decode-and-forward relaying system was investigated. However, published works [12], [19], [20], [26] and

[71] assumed that the transceiver hardware of wireless terminal is perfect. In practice, it suffers from impairments because of phase noises, amplifier-amplitude non-linearity and in-phase and quadrature imbalance (IQI) [25], [72]. In [27], the authors studied the impact of hardware imperfection on secrecy capacity. In particular, published work [27] considered the effects of IQI in one-hop OFDMA communication systems.

To the best of my knowledge, no work related to cooperative multi-hop physical-layer security in underlay CR networks has been published. This has provided motivation to propose such a scheme and evaluate its performance. In the proposed protocol, a secondary source attempts to transmit data to a secondary destination with the assistance of multiple secondary relays. In the secondary network, a secondary eavesdropper listens in on the data transmitted by the secondary transmitters, which must adjust their transmit power to satisfy the interference constraint required by the primary network. At each time slot of the data transmission, the secondary source or the secondary relays transmit the source data to the secondary destination. If the destination can securely receive the source data, it returns an ACK message in response. Otherwise, a NACK message is generated by the destination to request retransmission from another relay. To evaluate the performance of the proposed protocol, the secrecy capacity in the presence of the interference threshold and hardware impairments was determined. For relaxed impairment levels, the exact and asymptotic expressions of the end-to-end secrecy outage probability (SOP) over Rayleigh fading channels were derived using the recursive method. Monte Carlo simulations were performed to verify the theoretical derivations and to demonstrate the advantages of the proposed method. The results also show that the proposed scheme outperformed the multi-hop direct transmission protocol.

6.2. System model

Figure 6.1 describes an *M*-hop secondary network in which the secondary source (N_0) communicates with the secondary destination (N_M) via *M*-1 secondary relay nodes denoted as N_1, N_2, …, N_{M-1}. The relay nodes are numbered according to the distance to the destination, i.e. relay N_{M-1} is the nearest and relay N_1 is the furthest. In the underlay CR network, the secondary transmitters, such as the source and relays, must adapt their transmit power to satisfy a maximum interference threshold I_{th}, at the primary user (PU). The maximum transmit power constraint P_{th} also exists for the secondary transmitters. In the secondary network, eavesdropper (E) attempts to receive and decode the source data transmitted by secondary transmitters, such as the source and relays. Before describing the operation of the proposed protocol, assumptions used in this chapter are given.

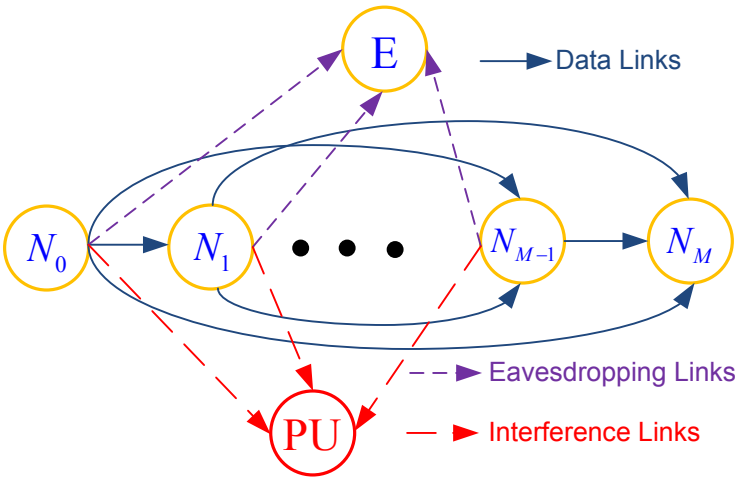

Figure 6.1. *System model of the cooperative multi-hop transmission protocol in an underlay CR network.*

Assumptions

- All of the relays are within radio range of the source and destination nodes.
- The relay nodes know their positions and the positions of other nodes.
- Channels between any two terminals are subject to block and flat Rayleigh fading.
- Each node has a single half-duplex radio and a single antenna. Because of the half-duplex constraint, a time-division channel allocation scheme is employed in order to achieve orthogonal channels.
- For ease of presentation and analysis, all of the nodes are assumed to have the same structure so that impairment levels are the same.
- The data transmission between two secondary nodes is considered secure if the obtained secrecy capacity is higher than a positive threshold R_S. Otherwise, the data cannot be transmitted securely, which is referred to as a secrecy outage event.
- When the data transmission between the secondary transmitter and secondary receiver is secure, it can be assumed that secondary receiver can decode the data successfully.

Operation of the proposed scheme

Operation of the proposed protocol, named Multi-hop Cooperative Transmission (MCT), is performed using the cooperative multi-hop technique proposed in [73] as follows:

At the first time slot, the source broadcasts its data to the destination. If the destination receives the source data securely, it sends an acknowledge message (ACK) to inform the source (and all relays) to start a new transmission. Otherwise, the destination generates a negative acknowledge message (NACK) to request retransmission. In the proposed protocol, after receiving a NACK message, the relay N_{M-1} sends a control signal to indicate the decoding status. In particular, if this node securely receives the data, it sends the ACK message and forwards the decoded data to the destination in next time slot. Otherwise, it also transmits the NACK message to inform. In this case, the relay N_{M-2} in turn sends control signals, and if it receives the data securely, it becomes the new source.

This procedure repeats until the system can find a secured relay that is nearest to the destination for retransmission. Generally, at the *k*th time slot $(k \geq 1)$, let us denote the current transmitter as N_{i_k}, where $i_k \in \{0,1,2,...,M-1\}$ and $i_1 = 0$. I also denote DS_k as the set of relays from the node N_{i_k+1} to the destination, i.e. $DS_k = \{N_{i_k+1}, N_{i_k+2}, ..., N_M\}$. In this time slot, node N_{i_k} transmits the source data to all of the nodes belonging to set DS_k. Also, if the destination decodes the source data securely, the data transmission ends. Otherwise, a secure relay belonging to set DS_k and nearest to the destination (having the highest index value) will become the new source and repeat the process that node N_{i_k} performs. After the *k*th time slot, let us denote DA_k as the set of secure relays, i.e. $DA_k = \{N_{k_1}, N_{k_2}, ..., N_{k_r}\}$, where $DA_k \subset DS_k$, $k_1 < k_2 < ... < k_r$ and $0 \leq r \leq M - i_k$. Also denoted are the relays that cannot receive data securely and are assumed included in set DF_k, where $DF_k = \{N_{k_{r+1}}, N_{k_2}, ..., N_{k_{M-i_k}}\}$, with $k_{r+1} < k_{r+2} < ... < k_{M-i_k-1} < k_{M-i_k}$ and $N_{k_{M-i_k}} = N_M$. With the process mentioned above, it is obvious that relay N_{k_r} will become the new source and broadcast the data to the destination and the relays between itself and the destination at time slot $k+1$. This process is repeated until the destination can securely receive the data or there is no relay between the transmitting source and the destination that can securely receive. In order to avoid the eavesdropper combining the received data at each time slot, the source and secured relays use the randomize-and-forward (RF) protocol [19]. In particular, these nodes randomly generate the code-books to confuse the eavesdropper.

To demonstrate the advantages of the proposed protocol, the secrecy performance of the MCT protocol was compared to that of the multi-hop direct transmission protocol (MDT). In the MDT scheme, data is transmitted hop-by-hop from the source to the destination. Data transmission is split into M orthogonal time slots. At the *m*th time slot, where $m = 1,2,...,M$, node N_m transmits the source data to node N_{m+1}. If communication between N_m and N_{m+1} is secure, node N_{m+1} will forward the data to the next hop in the next time slot. Otherwise, the data transmission is insecure, and the secrecy outage event occurs (in this case, communication at the remaining hops is no longer necessary). As with the MCT protocol, the source and relays in the MDT protocol use the RF technique.

Derivation of signal-to-interference-plus-noise ratio (SINR) and secrecy capacity

Let d_{N_i,N_j}, $d_{N_i,\mathrm{PU}}$ and $d_{N_i,\mathrm{E}}$ denote the distances of the $N_i \to N_j$, $N_i \to \mathrm{PU}$ and $N_i \to \mathrm{E}$ links, respectively, where $i, j \in \{0,1,...,M-1,M\}$. Also, h_{N_i,N_j}, $h_{N_i,\mathrm{PU}}$ and $h_{N_i,\mathrm{E}}$ are denoted as the channel coefficients of the $N_i \to N_j$, $N_i \to \mathrm{PU}$ and $N_i \to \mathrm{E}$ links, respectively. Because the channels experience a Rayleigh fading distribution, channel gains such as $\gamma_{i,j} = |h_{N_i,N_j}|^2$, $\gamma_{i,P} = |h_{N_i,\mathrm{PU}}|^2$ and $\gamma_{i,E} = |h_{N_i,\mathrm{E}}|^2$ follow exponential distributions [19]. To take path-loss into

account, the parameters of the random variables (RVs) $\gamma_{i,j}$, $\gamma_{i,P}$ and $\gamma_{i,E}$ can be modelled as follows [73]: $\lambda_{i,j} = d^{\beta}_{N_i,N_j}$, $\lambda_{i,P} = d^{\beta}_{N_i,PU}$ and $\lambda_{i,E} = d^{\beta}_{N_i,E}$, where β is the path-loss exponent.

Let us consider the communication between transmitter X and receiver Y $\left(\mathrm{X} \in \{N_0, N_1, ..., N_M\}, \mathrm{Y} \in \{N_1, N_2, ..., N_M, \mathrm{E}, \mathrm{PU}\}\right)$, the received data at node Y because of transmission at node X can be given as (see [25], [72])

$$y = \sqrt{P_{\mathrm{X}}} h_{\mathrm{X,Y}} \left(x_0 + \eta_{t,\mathrm{X}}\right) + \eta_{r,\mathrm{Y}} + \nu_{\mathrm{Y}}, \tag{6.1}$$

where x_0 is the transmitted data, P_{X} is the transmit power of transmitter X, $h_{\mathrm{X,Y}}$ is the channel coefficient of the X-Y link, $\eta_{t,\mathrm{X}}$ is hardware noise caused by the impairments in transmitter X, $\eta_{r,\mathrm{Y}}$ is hardware noise caused by the impairments in receiver Y and ν_{Y} is Gaussian noise at receiver Y.

As in [25], [72], the noise components $\eta_{t,\mathrm{X}}$, $\eta_{r,\mathrm{Y}}$ and ν_{Y} can be modelled as Gaussian random variables (RVs) with zero-mean, and their variances can be given, respectively, as

$$\begin{aligned} &\mathrm{var}\{\eta_{t,\mathrm{X}}\} = \kappa_t^2, \\ &\mathrm{var}\{\eta_{r,\mathrm{Y}}\} = \kappa_r^2 P_{\mathrm{X}} |h_{\mathrm{X,Y}}|^2, \\ &\mathrm{var}\{\nu_{\mathrm{Y}}\} = \sigma_0^2, \end{aligned} \tag{6.2}$$

where κ_t^2 and κ_r^2 are constants characterizing the level of hardware impairments at the transmitter and receiver nodes, respectively.

From (6.1) and (6.2), the instantaneous signal-to-interference-plus-noise ratio (SINR) of the X-Y link is expressed as

$$\begin{aligned} \Psi_{\mathrm{X,Y}} &= \frac{P_{\mathrm{X}} |h_{\mathrm{X,Y}}|^2}{\left(\kappa_t^2 + \kappa_r^2\right) P_{\mathrm{X}} |h_{\mathrm{X,Y}}|^2 + \sigma_0^2} \\ &= \frac{P_{\mathrm{X}} |h_{\mathrm{X,Y}}|^2}{\kappa P_{\mathrm{X}} |h_{\mathrm{X,Y}}|^2 + \sigma_0^2}, \end{aligned} \tag{6.3}$$

where $\kappa = \kappa_t^2 + \kappa_r^2$.

Let us consider the transmit power P_{X} of node X in the underlay CR network. First, the value P_{X} is below the maximum transmit power, i.e. $P_{\mathrm{X}} \le P_{th}$. Second, the interference caused at PU because of transmission at node X must be below the interference threshold I_{th}, i.e.

$$\left(1 + \kappa\right) P_{\mathrm{X}} |h_{\mathrm{X,PU}}|^2 \le I_{th} \Leftrightarrow P_{\mathrm{X}} \le \frac{I_{th}}{\left(1 + \kappa\right) |h_{\mathrm{X,PU}}|^2}. \tag{6.4}$$

Therefore, the maximum transmit power of node X can be given by

$$P_{\mathrm{X}} = \min\left(P_{th}, \frac{I_{th}}{(1+\kappa)\,|\,h_{\mathrm{X,PU}}\,|^2} \right) = P_{th} \min\left(1, \frac{\mu}{(1+\kappa)\,|\,h_{\mathrm{X,PU}}\,|^2} \right), \tag{6.5}$$

where $\mu = I_{th} / P_{th}$ is assumed to be a constant [67].

Combining (6.3) and (6.5) yields

$$\Psi_{\mathrm{X,Y}} = \frac{P \min\left(1, \frac{\mu}{(1+\kappa)\,|\,h_{\mathrm{X,PU}}\,|^2} \right) |\,h_{\mathrm{X,Y}}\,|^2}{\kappa P \min\left(1, \frac{\mu}{(1+\kappa)\,|\,h_{\mathrm{X,PU}}\,|^2} \right) |\,h_{\mathrm{X,Y}}\,|^2 + 1}, \tag{6.6}$$

where $P = P_{th} / \sigma_0^2$.

From (6.6), the SINR for the $N_i \to N_j$ and $N_i \to \mathrm{E}$ links, where $i, j \in \{0,1,...,M\}$, can be expressed, respectively, as

$$\Psi_{i,j} = \frac{P \min\left(1, \mu / \gamma_{i,\mathrm{P}}\right) \gamma_{i,j}}{\kappa P \min\left(1, \mu / \gamma_{i,\mathrm{P}}\right) \gamma_{i,j} + 1}, \tag{6.7}$$

$$\Psi_{i,\mathrm{E}} = \frac{P \min\left(1, \mu / \gamma_{i,\mathrm{P}}\right) \gamma_{i,\mathrm{E}}}{\kappa P \min\left(1, \mu / \gamma_{i,\mathrm{P}}\right) \gamma_{i,\mathrm{E}} + 1}. \tag{6.8}$$

When the transceiver hardware of all nodes is perfect, i.e. $\kappa = \kappa_t^2 = \kappa_r^2 = 0$, equations (6.7) and (6.8) can be rewritten as

$$\Psi_{i,j} = P \min\left(1, \frac{\mu}{\gamma_{i,\mathrm{P}}} \right) \gamma_{i,j}, \tag{6.9}$$

$$\Psi_{i,\mathrm{E}} = P \min\left(1, \frac{\mu}{\gamma_{i,\mathrm{P}}} \right) \gamma_{i,\mathrm{E}}. \tag{6.10}$$

Hence, the secrecy capacity obtained at node N_j because of transmission at node N_i in the presence of eavesdropper E is calculated as in [19] by

$$R_{i,j} = \max\left(0, \log_2\left(1+\Psi_{i,j}\right) - \log_2\left(1+\Psi_{i,\mathrm{E}}\right)\right) = \left[\log_2\left(\frac{1+\Psi_{i,j}}{1+\Psi_{i,\mathrm{E}}} \right) \right]^+, \tag{6.11}$$

where $[x]^+ = \max(0, x)$.

From (6.7), (6.8) and (6.11), because $\Psi_{i,j} \overset{P\to+\infty}{\approx} 1/\kappa$ and $\Psi_{i,\mathrm{E}} \overset{P\to+\infty}{\approx} 1/\kappa$, the secrecy capacity at high P regime can be given as

$$R_{i,j} \overset{P\to+\infty}{\approx} 0. \tag{6.12}$$

Moreover, as $\kappa = 0$, we approximate (6.11) by

$$R_{i,j} \overset{P\to+\infty}{\approx} \left[\log_2\left(\frac{\gamma_{i,j}}{\gamma_{i,\mathrm{E}}}\right)\right]^+. \tag{6.13}$$

6.3. Performance analysis

First, let us consider the secrecy outage probability (SOP) of the transmission between nodes N_i and N_j, which can be formulated as

$$\begin{aligned}\mathrm{SOP}_{i,j}^{\mathrm{DT}} &= \Pr\left(R_{i,j} < R_S\right) \\ &= \Pr\left(\frac{1+\Psi_{i,j}}{1+\Psi_{i,E}} < \rho\right),\end{aligned} \tag{6.14}$$

where $\rho = 2^{R_S}\ (\rho > 1)$.

From (6.12) and (6.14), it is obvious that when $\kappa > 0$, secured communication between nodes N_i and N_j at high P region is almost in outage, i.e. $\mathrm{SOP}_{i,j}^{\mathrm{DT}} \overset{P\to+\infty}{\approx} 1$.

Now, when the transceiver hardware is perfect $(\kappa = 0)$, the exact closed-form expression for $\mathrm{SOP}_{i,j}^{\mathrm{DT}}$ can be derived. Setting $x = \gamma_{i,\mathrm{P}}$, $\mathrm{SOP}_{i,j}^{\mathrm{DT}}$ conditioned on x can be expressed as

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}}(x) = \Pr\left(\gamma_{i,j} < \frac{\rho-1}{P\min(1,\mu/x)} + \rho\gamma_{i,\mathrm{E}}\right). \tag{6.15}$$

Because of the independence of $\gamma_{i,j}$ and $\gamma_{i,\mathrm{E}}$, (6.15) can be expressed as follows:

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}}(x) = \int_0^{+\infty} f_{\gamma_{i,\mathrm{E}}}(y) F_{\gamma_{i_j}}\left(\frac{\rho-1}{P\min(1,\mu/x)} + \rho y\right) dy. \tag{6.16}$$

Substituting the probability density function (PDF) of the exponential RV $\gamma_{i,\mathrm{E}}$, i.e. $f_{\gamma_{i,\mathrm{E}}}(y) = \lambda_{i,\mathrm{E}}\exp\left(-\lambda_{i,\mathrm{E}}y\right)$, and the cumulative distribution function (CDF) of the exponential RV $\gamma_{i,j}$, i.e. $F_{\gamma_{i,j}}(y) = 1-\exp\left(-\lambda_{i,j}y\right)$ into (6.16) and after some manipulation, we obtain

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}}(x) = 1 - \frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}} + \lambda_{i,j}\rho}\exp\left(-\frac{\rho-1}{P\min(1,\mu/x)}\right). \tag{6.17}$$

Next, the probability $\mathrm{SOP}_{i,j}^{\mathrm{DT}}$ can be expressed from $\mathrm{SOP}_{i,j}^{\mathrm{DT}}(x)$ as follows:

$$\begin{aligned}\mathrm{SOP}_{i,j}^{\mathrm{DT}} &= \int_0^{+\infty} \mathrm{SOP}_{i,j}^{\mathrm{DT}}(x) f_{\gamma_{i,\mathrm{P}}}(x) dx \\ &= \int_0^{\mu} \left(1 - \frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}} + \lambda_{i,j}\rho} \exp\left(-\frac{\rho - 1}{P}\right)\right) \lambda_{i,\mathrm{P}} \exp\left(-\lambda_{i,\mathrm{P}} x\right) dx \\ &+ \int_{\mu}^{+\infty} \left(1 - \frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}} + \lambda_{i,j}\rho} \exp\left(-\frac{\rho - 1}{P\mu} x\right)\right) \lambda_{i,\mathrm{P}} \exp\left(-\lambda_{i,\mathrm{P}} x\right) dx.\end{aligned} \tag{6.18}$$

After some careful manipulation, we obtain an exact closed-form expression for $\mathrm{SOP}_{i,j}^{\mathrm{DT}}$ as follows:

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}} = 1 - \frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}} + \lambda_{i,j}\rho} \left[\begin{array}{l} \left(1 - \exp\left(-\lambda_{i,\mathrm{P}}\mu\right)\right) \exp\left(-\lambda_{i,j} \dfrac{\rho - 1}{P}\right) \\ + \dfrac{\lambda_{i,\mathrm{P}} P\mu}{\lambda_{i,\mathrm{P}} P\mu + \lambda_{i,j}(\rho - 1)} \exp\left(-\lambda_{i,\mathrm{P}}\mu - \lambda_{i,j} \dfrac{\rho - 1}{P}\right) \end{array} \right]. \tag{6.19}$$

Furthermore, by using the approximation in (6.13), an asymptotic closed-form expression for $\mathrm{SOP}_{i,j}^{\mathrm{DT}}$ at high P values can be provided by

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}} \overset{P \to +\infty}{\approx} \Pr\left(\frac{\gamma_{i,j}}{\gamma_{i,\mathrm{E}}} < \rho\right) = 1 - \frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}} + \lambda_{i,j}\rho}. \tag{6.20}$$

6.3.1. Multi-hop direct transmission protocol (MDT)

In the MDT protocol, since the data transmission on each hop is independent, the end-to-end SOP of the MDT protocol is given by

$$\mathrm{SOP}_{0,M}^{\mathrm{MDT}} = 1 - \prod_{m=1}^{M} \left(1 - \mathrm{SOP}_{m-1,m}^{\mathrm{DT}}\right). \tag{6.21}$$

In (6.21), the term $\prod_{m=1}^{M} \left(1 - \mathrm{SOP}_{m-1,m}^{\mathrm{DT}}\right)$ represents the case where data transmission is secure at all of the hops.

In addition, when the hardware impairments are relaxed, i.e. $\kappa = 0$, substituting (6.19) into (6.21), an exact closed-form expression for the end-to-end SOP of the MDT protocol can be given as

$$\mathrm{SOP}_{0,M}^{\mathrm{MDT}} = 1 - \prod_{i=1}^{M} \left\{ \frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}} + \lambda_{i,j}\rho} \left[\begin{array}{l} \left(1 - \exp\left(-\lambda_{i,\mathrm{P}}\mu\right)\right) \exp\left(-\lambda_{i,j} \dfrac{\rho - 1}{P}\right) \\ + \dfrac{\lambda_{i,P} P\mu}{\lambda_{i,\mathrm{P}} P\mu + \lambda_{i,j}(\rho - 1)} \exp\left(-\lambda_{i,\mathrm{P}}\mu - \lambda_{i,j} \dfrac{\rho - 1}{P}\right) \end{array} \right] \right\}. \tag{6.22}$$

At high P region, an approximate closed-form expression for (6.22) can be obtained by

$$\mathrm{SOP}_{0,M}^{\mathrm{MDT}} \overset{P\to+\infty}{\approx} 1-\prod_{i=1}^{M}\frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}}+\lambda_{i,j}\rho}. \tag{6.23}$$

It can be observed from (6.23) that the end-to-end SOP at high transmit SNR does not depend on the value of P.

6.3.2. Cooperative multi-hop transmission protocol (CMT)

In this sub-section, the exact expression for the end-to-end SOP is derived by using a recursive expression. Let us consider SOP at the time slot k, which can be expressed by

$$\begin{aligned}\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}} &= \sum_{DA_k}\Pr\left(\begin{array}{l}\dfrac{1+\Psi_{i_k,k_1}}{1+\Psi_{i_k,E}}\ge\rho,\dfrac{1+\Psi_{i_k,k_2}}{1+\Psi_{i_k,E}}\ge\rho,...,\dfrac{1+\Psi_{i_k,k_r}}{1+\Psi_{i_k,E}}\ge\rho,\\ \dfrac{1+\Psi_{i_k,k_{r+1}}}{1+\Psi_{i_k,E}}<\rho,\dfrac{1+\Psi_{i_k,k_{r+2}}}{1+\Psi_{i_k,E}}<\rho,...,\dfrac{1+\Psi_{i_k,k_{M-i_k}}}{1+\Psi_{i_k,E}}<\rho,\end{array}\right)\\ &= \sum_{DA_k}\Pr\left(\begin{array}{l}\dfrac{1+P\min\left(1,\mu/\gamma_{i_k,P}\right)\gamma_{i_k,k_1}}{1+P\min\left(1,\mu/\gamma_{i_k,P}\right)\gamma_{i_k,E}}\ge\rho,...,\dfrac{1+P\min\left(1,\mu/\gamma_{i_k,P}\right)\gamma_{i_k,k_r}}{1+P\min\left(1,\mu/\gamma_{i_k,P}\right)\gamma_{i_k,E}}\ge\rho,\\ \dfrac{1+P\min\left(1,\mu/\gamma_{i_k,P}\right)\gamma_{i_k,k_{r+1}}}{1+P\min\left(1,\mu/\gamma_{i_k,P}\right)\gamma_{i_k,E}}<\rho,...,\dfrac{1+P\min\left(1,\mu/\gamma_{i_k,P}\right)\gamma_{i_k,k_{M-i_k}}}{1+P\min\left(1,\mu/\gamma_{i_k,P}\right)\gamma_{i_k,E}}<\rho\end{array}\right).\end{aligned} \tag{6.24}$$

We are reminded that at the kth time slot, the current transmitting node is N_{i_k} and DA_k is the set of active relays that can securely receive source data from node N_{i_k}.

Lemma 1*:* When $\kappa=0$, $\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}}$ can be expressed by the following equation:

$$\begin{aligned}\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}} &= \sum_{DA_k}\frac{\lambda_{i_k,E}}{\lambda_{i_k,E}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\rho}\left[\begin{array}{l}\exp\left(-\sum_{t=1}^{r}\dfrac{\lambda_{i_k,k_t}(\rho-1)}{P}\right)\left(1-\exp\left(-\lambda_{i_k,P}\mu\right)\right)\\ +\dfrac{\lambda_{i_k,P}P\mu}{\lambda_{i_k,P}P\mu+\sum_{t=1}^{r}\lambda_{i_k,k_t}(\rho-1)}\exp\left(-\lambda_{i_k,P}\mu-\sum_{t=1}^{r}\lambda_{i_k,k_t}\dfrac{(\rho-1)}{P}\right)\end{array}\right]\\ &+\sum_{DA_k}\sum_{v=1}^{M-i_k-r}(-1)^{v}\sum_{\substack{N_{j1},...,N_{jv}\in DF_k\\ j_1<j_2<...<j_v}}^{M-i_k-r}\frac{\lambda_{i_k,E}}{\lambda_{i_k,E}+\left(\sum_{t=1}^{v}\lambda_{i_k,j_v}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\right)\rho}\\ &\times\left[\begin{array}{l}\exp\left(-\left(\sum_{t=1}^{v}\lambda_{i_k,j_v}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\right)\dfrac{\rho-1}{P}\right)\left(1-\exp\left(-\lambda_{i_k,P}\mu\right)\right)\\ +\dfrac{\lambda_{i_k,P}P\mu}{\lambda_{i_k,P}P\mu+\left(\lambda_{i_k,E}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\right)(\rho-1)}\exp\left(-\lambda_{i_k,P}\mu-\left(\sum_{t=1}^{v}\lambda_{i_k,j_v}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\right)\dfrac{\rho-1}{P}\right)\end{array}\right].\end{aligned} \tag{6.25}$$

Proof: First let $x=\gamma_{i_k,E}$ and $y=\gamma_{i_k,P}$, and $\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}}$ conditioned on x and y can be given as

$$\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}}(x,y)=\sum_{DA_k}\left[\prod_{t=1}^{r}\exp\left(-\lambda_{i_k,k_t}\left(\frac{\rho-1}{P\min(1,\mu/y)}+\rho x\right)\right)\prod_{v=1}^{M-i_k-r}\left(1-\exp\left(-\lambda_{i_k,k_v}\left(\frac{\rho-1}{P\min(1,\mu/y)}+\rho x\right)\right)\right)\right]$$

$$=\sum_{DA_k}\exp\left(-\sum_{t=1}^{r}\lambda_{i_k,k_t}\left(\frac{\rho-1}{P\min(1,\mu/y)}+\rho x\right)\right) \tag{6.26}$$

$$+\sum_{DA_k}\sum_{v=1}^{M-i_k-r}(-1)^{v}\sum_{\substack{N_{j1},\ldots,N_{j_v}\in DF_k\\ j_1<j_2<\ldots<j_v}}^{M-i_k-r}\exp\left(-\left(\sum_{t=1}^{v}\lambda_{i_k,j_v}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\right)\left(\frac{\rho-1}{P\min(1,\mu/y)}+\rho x\right)\right).$$

Then, $\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}}$ can be expressed as

$$\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}}=\int_0^{+\infty}f_{\gamma_{i_k,P}}(y)\underbrace{\left[\int_0^{+\infty}f_{\gamma_{i_k,E}}(x)\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}}(x,y)dx\right]}_{I_1}dy. \tag{6.27}$$

Considering the integral I_1 marked in (6.27), it can be expressed by the following equation:

$$I_1=\int_0^{+\infty}\lambda_{i_k,E}\exp\left(-\lambda_{i_k,E}x\right)\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}}(x,y)dx$$

$$=\sum_{DA_k}\frac{\lambda_{i_k,E}}{\lambda_{i_k,E}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\rho}\exp\left(-\sum_{t=1}^{r}\frac{\lambda_{i_k,k_t}(\rho-1)}{P\min(1,\mu/y)}\right) \tag{6.28}$$

$$+\sum_{DA_k}\sum_{v=1}^{M-i_k-r}(-1)^{v}\sum_{\substack{N_{j_1},\ldots,N_{j_v}\in DF_k\\ j_1<j_2<\ldots<j_v}}^{M-i_k-r}\frac{\lambda_{i_k,E}\exp\left(-\left(\sum_{t=1}^{v}\lambda_{i_k,j_v}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\right)\frac{\rho-1}{P\min(1,\mu/y)}\right)}{\lambda_{i_k,E}+\left(\sum_{t=1}^{v}\lambda_{i_k,j_v}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\right)\rho}.$$

Substituting (6.28) into (6.27) and after some manipulation, we obtain (6.25) and finish the proof.

Next, at high transmit power, i.e. $P\to+\infty$, by using (6.13) and in the same manner as (6.26)–(6.28), the asymptotic expression of $\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}}$ can be obtained:

$$\mathrm{SOP}_{N_{i_k},DA_k}^{\mathrm{CMT}}\overset{P\to+\infty}{\approx}\sum_{DA_k}\frac{\lambda_{i_k,E}}{\lambda_{i_k,E}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\rho}$$

$$+\sum_{DA_k}\sum_{v=1}^{M-i_k-r}(-1)^{v}\sum_{\substack{N_{j1},\ldots,N_{j_v}\in DF_k\\ j_1<j_2<\ldots<j_v}}^{M-i_k-r}\frac{\lambda_{i_k,E}}{\lambda_{i_k,E}+\left(\sum_{t=1}^{v}\lambda_{i_k,j_v}+\sum_{t=1}^{r}\lambda_{i_k,k_t}\right)\rho}. \tag{6.29}$$

Finally, the end-to-end SOP of the CMT protocol can be calculated with a recursive expression as follows:

$$\mathrm{SOP}_{0,M}^{\mathrm{CMT}}=\mathrm{SOP}_{N_0,DA_1}^{\mathrm{CMT}}, \tag{6.30}$$

where $\mathrm{SOP}_{N_0,DA_1}^{\mathrm{CMT}}$ is given as in (6.25).

Finally, by using (6.29), we can obtain the asymptotic expression of the end-to-end SOP for the CMT protocol, which also does not depend on the value of *P*.

6.4. Numerical results

In this section, various Monte Carlo simulations are presented to verify the theoretical results derived in Section 6.3. For each Monte-Carlo simulation, 10^6 trials were conducted in which the channel coefficients between two nodes were randomly generated. The simulation results were then calculated by the number of trials in the considered systems that were in outage divided by 10^6. The derived equations (6.22), (6.23), (6.29) and (6.30) were used to present the theoretical results. For the simulation environment, a two-dimensional network was considered in which the co-ordinates of the node $N_i\left(i\in\{0,1,...,M\}\right)$, the primary user, and eavesdropper were $(0,i/M)$, (x_{PU},y_{PU}) and (x_E,y_E), respectively. Hence, the link distances were calculated by $d_{N_i,N_j}=|i-j|/M$, $d_{N_i,PU}=\sqrt{(i/M-x_{PU})^2+y_{\mathrm{PU}}^2}$ and $d_{N_i,E}=\sqrt{(i/M-x_E)^2+y_E^2}$. In all of the simulations, the path-loss exponent β was assumed to equal 3.

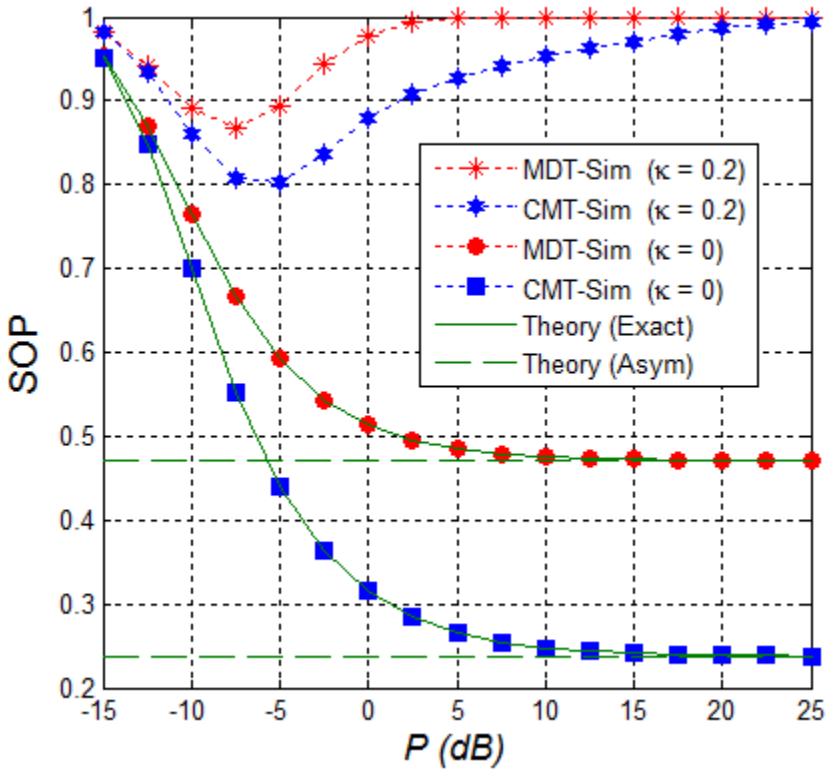

Figure 6.2. *End-to-end secrecy outage probability (SOP) as a function of P in dB when* $P\in[-15\,\mathrm{dB},25\,\mathrm{dB}]$, $\mu=0.5$, $M=4$, $R_S=1$, $\kappa\in\{0,0.2\}$, $(x_{PU},y_{PU})=(-0.5,-1)$ *and* $(x_E,y_E)=(0.5,0.5)$.

Figure 6.2 presents the end-to-end SOP of the MDT and CMT protocols as a function of the transmit SNR $\left(P=P_{th}/\sigma_0^2\right)$ in dB. In this simulation, the target rate $R_S=1$, the ratio $\mu=0.5$ and

the number of hops M = 4. The primary users and eavesdroppers were also placed at positions $(-0.5,-1)$ and $(0.5,0.5)$, respectively. As we can observe, the proposed protocol (CMT) outperformed the MDT protocol for all P values. This is because the MCT protocol uses the diversity relaying scheme, which enhances security in the data transmission. We can also observe that when the transceiver hardware is perfect $(\kappa = 0)$, the secrecy performance of both protocols converges to asymptotic results, which are independent of the P values. However, as $\kappa = 0.2$, the values of SOP reach 1 at high P region, which validates the statement in Section 6.3. Moreover, a value of P exists at which the secrecy performance of the considered protocols is best. As shown in this figure, the optimal transmit SNRs in the CMT and MDT protocols are -5 dB and -7.5 dB, respectively. Finally, it is worth noting that the simulation results (Sim) matched the theoretical results (Theory (Exact)) very well and that at high P regimes, the simulation results converge nicely to asymptotes (Theory (Asym)). These validate the correction of our derivations expressed in Section 6.3.

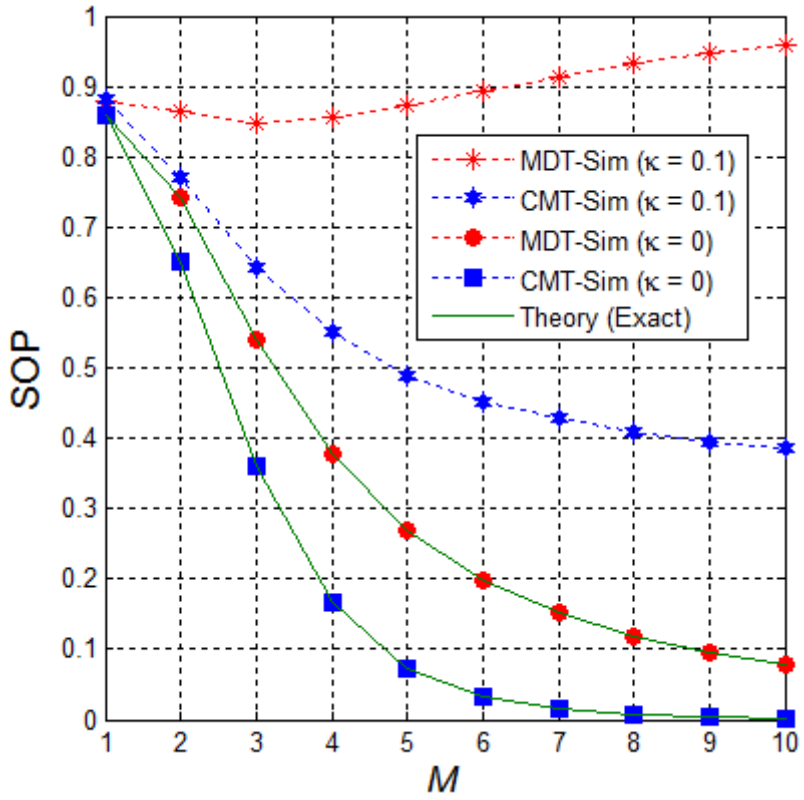

Figure 6.3. *End-to-end secrecy outage probability (SOP) as a function of* M *when* $P = 5$ dB, $\mu = 1$, $M \in [1,10]$, $R_S = 0.5$, $\kappa \in \{0, 0.1\}$, $(x_{PU}, y_{PU}) = (-0.5, -0.5)$ *and* $(x_E, y_E) = (0.5, 0.5)$.

In Figure 6.3, the number of hops (M) is changed and the variant of the end-to-end SOP can be observed. In this figure, the value of P, μ, R_S, x_{PU}, y_{PU}, x_E, and y_E are assigned 5 dB, 1, 0.5, -0.5, -0.5, 0.5 and 0.5, respectively. As observed, with the perfect transceiver, i.e. $\kappa = 0$, the secrecy performance of the MDT and CMT protocols was better as the number of hops increased. For the CMT protocol, this result was still true with the presence of hardware imperfection ($\kappa = 0.1$), though the performance of the MDT protocol severely degraded with a higher number

of hops. Again, the results in this figure validate the theoretical results provided in the previous section.

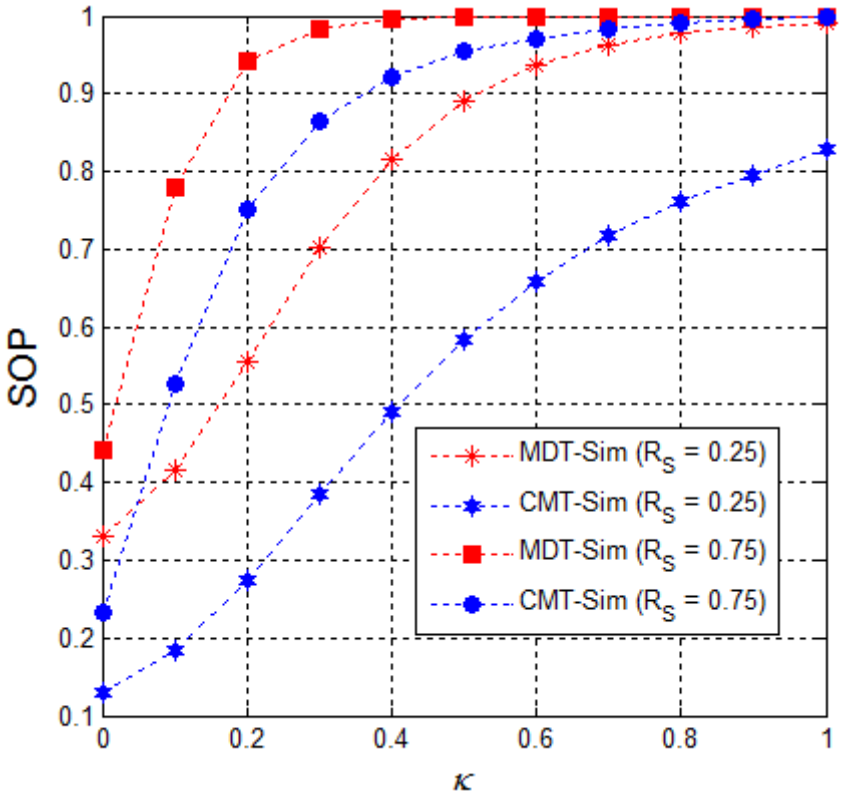

Figure 6.4. *End-to-end secrecy outage probability (SOP) as a function of* κ *when* $P = 0\,\text{dB}$, $\mu = 1$, $M = 4$, $R_S \in \{0.25, 0.75\}$, $\kappa \in [0,1]$, $(x_{PU}, y_{PU}) = (-0.5, -1)$ *and* $(x_E, y_E) = (0.5, 0.5)$.

Figure 6.4 illustrates the impact of the hardware impairment level (κ) on secrecy performance in the CMT and MDT protocols when $P = 0$ dB, $\mu = 1$, $M = 4$, $x_{PU} = -0.5$, $y_{PU} = -1$, $x_E = 0.5$ and $y_E = 0.5$. Similarly, the proposed scheme obtained better performance than the MDT scheme. Figure 6.4 also shows that the SOP values rapidly increased as the κ value increased. The performance of the considered methods was also significantly enhanced with a lower value of the target rate R_S.

Figure 6.5 shows the effect of the positions of the eavesdropper on the end-to-end SOP. In particular, the value of y_E is fixed while changing x_E from 0 to 1. The remaining parameters were set at $P = 10\,\text{dB}$, $\mu = 1$, $M = 4$, $R_S = 1$, $\kappa = 0$, $x_{PU} = -0.5$ and $y_{PU} = -0.1$. It can be seen that the end-to-end SOP of the CMT protocol mostly decreased as x_E increased, while that of the MDT increased at a small x_E value and decreased at high x_E regions. We can observe from this figure that the performance of the MDT protocol is worst as x_E is around 0.4.

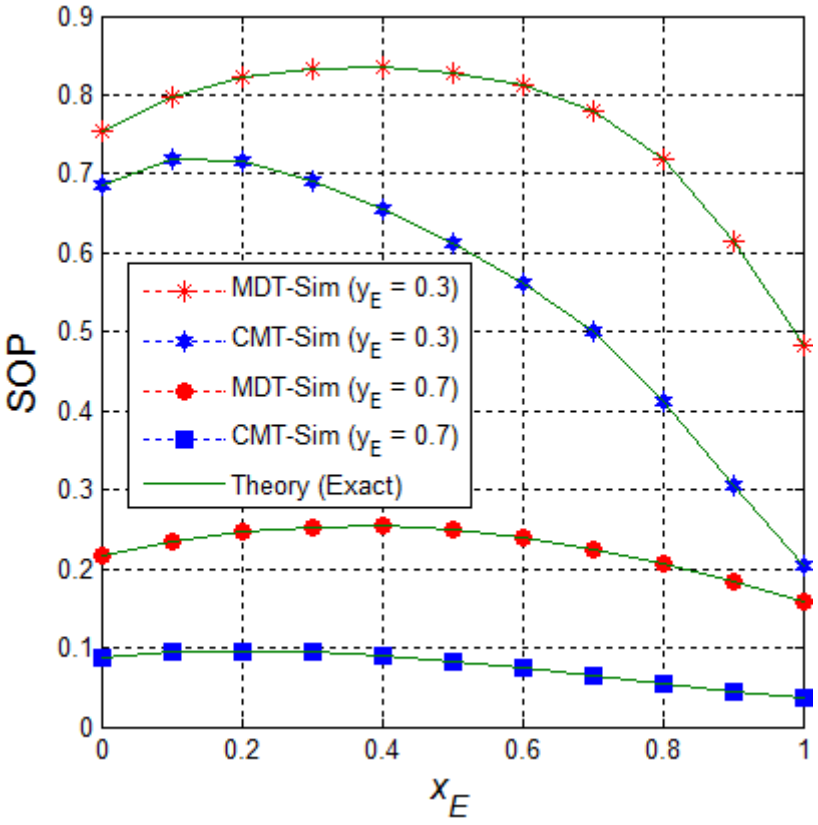

Figure 6.5. *End-to-end secrecy outage probability (SOP) as a function of* x_E *when* $P = 10\,\text{dB}$, $\mu = 1$, $M = 4$, $R_S = 1$, $\kappa = 0$, $(x_{PU}, y_{PU}) = (-0.5, -1)$, $x_E \in [0,1]$ *and* $y_E \in \{0.3, 0.7\}$.

6.5. Summary

In this chapter, the cooperative multi-hop transmission protocol (CMT) in underlay cognitive radio networks with the presence of the eavesdropper was proposed. Because the proposed scheme uses transmit diversity, it significantly outperforms the conventional multi-hop direct transmission protocol (MDT) in terms of end-to-end secrecy outage probability (SOP). The interesting results obtained for this chapter can be listed as follows:

- When the transceiver hardware of the nodes was imperfect, the secrecy performance severely degraded. In particular, the value of the end-to-end SOP rapidly increased with a higher transmit signal-to-noise ratio (SNR) and a higher impairment level.
- In the presence of hardware noises, an optimal value of the transmit SNR existed at which the secrecy performance of the CMT and DMT schemes were best.
- The performance of the proposed protocol was better as the number of hops increased.

For relaxed hardware impairments, the exact and asymptotic expressions of the end-to-end SOP for the CMT and MDT protocols were derived. Computer simulations were then performed to verify the derived expressions.

7. JOINT RELAY AND JAMMER SELECTION METHODS IN CLUSTER NETWORKS

In this chapter, joint relay and jammer selection protocols are proposed to enhance secrecy performance in cluster-based multi-hop networks and demonstrate the second aim. In particular, without channel state information (CSI) of the eavesdropping links, one of the available nodes at each cluster is selected to forward the source data, relying on the CSI of the data links, while a jammer node is randomly chosen to generate artificial noises to an eavesdropper. The impact of hardware noises on the secrecy performance of the proposed protocols is also investigated. For perfect transceiver hardware, the exact closed-form expressions of secrecy outage probability (SOP) for the proposed protocols over a Rayleigh fading channel are derived. Monte Carlo computer simulations are then performed to verify the theoretical results.

7.1. Motivations

Recently, physical-layer security (PLS) [10]-[11] has gained much attention as an efficient method of obtaining secure information without using cryptography. PLS protocols employ the physical characteristics of wireless channels such as channel state information (CSI) and the distances between the connection links to enhance secrecy performance in wireless systems. In [17]-[18], the authors proposed relay and jammer selection schemes to maximize secrecy capacity for decode-and-forward (DF) relaying networks. The authors in [18] considered the randomize-and-forward (RF) scenario in which the code books of the source data are randomly generated by the source and relay. In [19], [20] and [70], secrecy performance of cooperative cognitive radio networks was evaluated in terms of secrecy outage probability (SOP) and probability of non-zero secrecy capacity (PNSC). The published work [42] investigated the impact of co-channel interference and Nth best relay selection on secrecy performance. In [60], cluster-based multi-hop protocols were proposed to reduce the SOP and enhance average secrecy capacity (ASC). In particular, with relay selection methods applied for each dual-hop, secrecy performance can be significantly improved compared to random selection and the conventional best relay selection methods. However, the implementation of these protocols that require perfect CSIs across two hops is difficult work. Moreover, the authors in [60] did not consider jammer selection methods.

In this chapter, joint relay and jammer selection protocols are proposed to enhance the SOP performance for a cluster-based multi-hop network. The contributions of this thesis can be listed as follows:

- Two selection methods are proposed: in the first, named BEST, one of available nodes at each hop is selected by using the channel state information (CSI) between nodes at two adjacent clusters. Then, from the remaining relays at each cluster, a node is randomly selected to transmit jamming signals to the eavesdropper. In the second, denoted by RAND, both relay and jammer nodes are randomly chosen at each cluster.
- Unlike [60], two proposed protocols use the randomize-and-forward (RF) technique to avoid the eavesdropper in the combination of received signals.
- The impact of hardware impairments [72] on secrecy performance is investigated.

- Exact closed-form expressions of secrecy outage probability (SOP) are derived for the proposed protocols over a Rayleigh fading channel when the hardware impairments are relaxed.
- The optimal transmit power allocated to the data and the jamming signals is studied, including the optimal number of hops between the source and destination.
- Computer simulations are presented to verify the derivations.

7.2. System model

Figure 7.1 describes the system model of the proposed protocols where source T_0 attempts to transmit data to the destination T_M using the multi-hop relaying approach. We assume that there are M-1 clusters between source T_0 and destination T_M and that the destination is in the Mth cluster. We also assume that the nth cluster has K_n nodes, where $n = 1,2,...,M$ and $K_n \geq 2$. In this network, eavesdropper E listens in on the data transmitted by the source and relay nodes at the clusters. All of the terminals are equipped with a single antenna, and the RF technique [18] is employed to confuse the eavesdropper. Furthermore, because of the half-duplex constraint, data transmission would be realized by time division multiple access (TDMA) via M orthogonal time slots.

The notations and definitions that will be used in this chapter are now introduced. Let K_n relays in the cluster nth be denoted as $R_{n,1}, R_{n,2}, ..., R_{n,K_n}$. Next, T_n and J_n are denoted as the selected relay and jammer at the nth cluster, respectively, where $\{\mathrm{T}_n, \mathrm{J}_n\} \in \{R_{n,1}, R_{n,2}, ..., R_{n,K_n}\}$. Let γ_{XY} denote the channel gain of the link between nodes X and Y, where $\{\mathrm{X}, \mathrm{Y}\} \in \{R_{n,1}, R_{n,2}, ..., R_{n,K_n}\}$. We assume that all of the channels are Rayleigh fading, hence, channel gain γ_{XY} is an exponential random variable (RV) whose parameter is $\lambda_{\mathrm{XY}} = d_{\mathrm{XY}}^{\beta}$, where d_{XY} is the distance between X and Y, and β is the path-loss exponent [60].

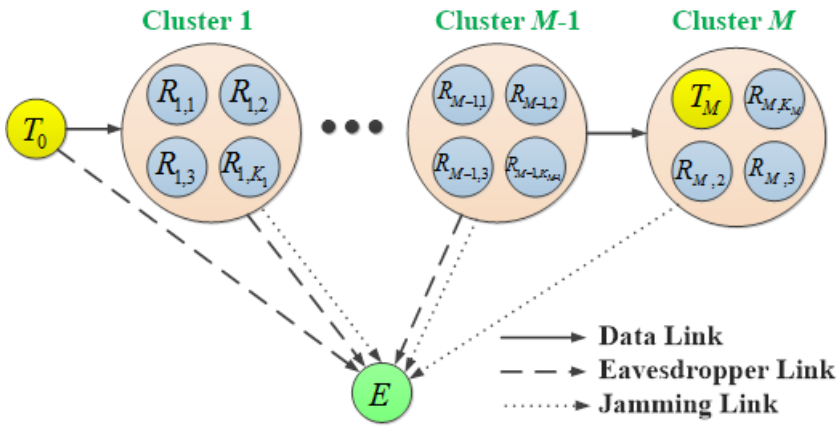

Figure 7.1. *System model of the proposed methods.*

7.3. Performance analysis

The relay and jammer selection methods are described in this section. In the BEST protocol, the relay T_n is selected using the following method:

$$\mathrm{T}_n : \gamma_{\mathrm{T}_{n-1}\mathrm{T}_n} = \max_{i=1,2,..,K_n} \left(\gamma_{\mathrm{T}_{n-1}R_{n,i}} \right). \tag{7.1}$$

Equation (7.1) implies that the node in the nth cluster providing the highest channel gain to the previous relay T_{n-1} is considered the best relay. Then, one of $K_n - 1$ remaining nodes is randomly selected to generate jamming noises to the eavesdropper.

Remark: No relay selection is performed at the Mth cluster because the destination T_M is determined before the source T_0 transmits its data.

By contrast to the BEST protocol, in the RAND protocol, both relay T_n and jammer J_n are randomly selected from K_n available nodes of the nth cluster.

For a fair comparison with conventional methods, we can assume that the total transmit power of the nodes T_n and J_n is fixed by P. More specifically, the transmit power is allocated to the nodes T_n and J_n, respectively, as $P_{\mathrm{T}_n} = \alpha P$ and $P_{\mathrm{J}_n} = (1-\alpha)P$, where $0 < \alpha \leq 1$. The data transmission of the proposed protocols is hop-by-hop. Let us consider the communication at the nth hop: relay T_{n-1} sends the source data to the selected relay T_n. At the same time, jammer J_n generates the jamming signals to eavesdropper E. Because of the short distance between T_n and J_n, we can assume that these nodes exchange secure control messages so that node T_n can cancel the interference received from node J_n. Under the impact of hardware noise, the channel capacity of the $\mathrm{T}_{n-1} \to \mathrm{T}_n$ link can be given as

$$\begin{aligned} C_{\mathrm{D},n} &= \frac{1}{M}\log_2\left(1 + \frac{\alpha P \gamma_{\mathrm{T}_{n-1}\mathrm{T}_n} / N_0}{\alpha\kappa^2 P \gamma_{\mathrm{T}_{n-1}\mathrm{T}_n} / N_0 + 1}\right) \\ &= \frac{1}{M}\log_2\left(1 + \frac{\alpha\Delta\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}}{1 + \alpha\kappa^2\Delta\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}}\right), \end{aligned} \tag{7.2}$$

where the factor M^{-1} indicates the data transmission is split into M time slots [60], N_0 is the variance of Gaussian noise, κ^2 is the total hardware impairments at transmitter T_{n-1} and receiver T_n [60], and $\Delta = P / N_0$ is the transmit signal-to-noise ratio (SNR).

When the transceiver hardware is perfect, i.e. $\kappa^2 = 0$, equation (7.2) can be rewritten as

$$C_{\mathrm{D},n} = \frac{1}{M}\log_2\left(1 + \alpha\Delta\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}\right). \tag{7.3}$$

Considering the $\mathrm{T}_{n-1} \to \mathrm{E}$ link, channel capacity in the presence of co-channel interference from J_n and the hardware impairments can be given as (see [72])

$$C_{\mathrm{E},n} = \frac{1}{M}\log_2\left(1+\frac{\alpha P\gamma_{\mathrm{T}_{n-1}\mathrm{E}}}{\alpha\kappa^2 P\gamma_{\mathrm{T}_{n-1}\mathrm{E}}+\left(1+\kappa^2\right)\left(1-\alpha\right)P\gamma_{\mathrm{J}_n\mathrm{E}}+N_0}\right) = \frac{1}{M}\log_2\left(1+\frac{\Delta\alpha\gamma_{\mathrm{T}_{n-1}\mathrm{E}}}{1+\kappa^2\Delta\alpha\gamma_{\mathrm{T}_{n-1}\mathrm{E}}+\left(1+\kappa^2\right)\left(1-\alpha\right)\Delta\gamma_{\mathrm{J}_n\mathrm{E}}}\right). \tag{7.4}$$

In the case of $\kappa^2 = 0$, from (7.4), we have

$$C_{\mathrm{E},n} = \frac{1}{M}\log_2\left(1+\frac{\Delta\alpha\gamma_{\mathrm{T}_{n-1}\mathrm{E}}}{1+\left(1-\alpha\right)\Delta\gamma_{\mathrm{J}_n\mathrm{E}}}\right). \tag{7.5}$$

Next, secrecy capacity at the nth hop can be obtained by

$$C_{\mathrm{Sec},n} = \max\left(0, C_{\mathrm{D},n} - C_{\mathrm{E},n}\right). \tag{7.6}$$

Because the RF technique is used, the end-to-end secrecy capacity of the proposed protocol can be expressed as [18]

$$C_{\mathrm{Sec}}^{\mathrm{e2e}} = \min_{n=1,2,\ldots,M}\left(C_{\mathrm{Sec},n}\right). \tag{7.7}$$

7.3.1. Secrecy outage probability (SOP)

In this section, the exact closed-form expressions of secrecy outage probability (SOP) are derived for the BEST and RAND protocols. SOP is defined as the probability that end-to-end secrecy capacity is below a positive predetermined value, i.e. C_{th}. Hence, we can express SOP by the following equation:

$$\begin{aligned}\mathrm{OP}_{\mathrm{Sec}} &= \Pr\left(C_{\mathrm{Sec}}^{\mathrm{e2e}} < C_{th}\right)\\ &= \Pr\left(\min_{n=1,2,\ldots,M}\left(C_{\mathrm{Sec},n}\right) < C_{th}\right)\\ &= 1-\prod_{n=1}^{M}\left(1-\Pr\left(C_{\mathrm{Sec},n} < C_{th}\right)\right).\end{aligned} \tag{7.8}$$

If the hardware transceiver is perfect, combining (7.3), (7.5), (7.6) and (7.8) we obtain

$$\mathrm{OP}_{\mathrm{Sec}} = 1-\prod_{n=1}^{M}\left[1-\Pr\left(\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n} < \frac{\phi-1}{\alpha\Delta}+\frac{\phi\gamma_{\mathrm{T}_{n-1}\mathrm{E}}}{1+\left(1-\alpha\right)\Delta\gamma_{\mathrm{J}_n\mathrm{E}}}\right)\right], \tag{7.9}$$

where OP_n

where $\phi = 2^{MC_{\mathrm{th}}}$.

It is noted from (7.9) that in order to calculate $\mathrm{OP}_{\mathrm{Sec}}$, we need to calculate OP_n. In the following section, expressions of OP_n for the RAND and BEST protocols are provided.

7.3.2. The RAND protocol

First, the probability OP_n can be rewritten as

$$\mathrm{OP}_n = \int_0^{+\infty} F_{\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}}\left(\frac{\phi-1}{\alpha\Delta}+z\right) f_Z(z)\,dz, \tag{7.10}$$

where $Z = \dfrac{\phi\gamma_{\mathrm{T}_{n-1}\mathrm{E}}}{1+(1-\alpha)\Delta\gamma_{\mathrm{J}_n\mathrm{E}}}$, $F_{\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}}\left(\dfrac{\phi-1}{\alpha\Delta}+z\right)$ is the cumulative distribution function (CDF) of RV $\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}$ and $f_Z(z)$ is the probability density function (PDF) of Z.

Because $\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}$ is an exponential random variable (RV) with the parameter $\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}$, the CDF $F_{\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}}\left(\dfrac{\phi-1}{\alpha\Delta}+z\right)$ can be obtained by

$$F_{\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}}\left(\frac{\phi-1}{\alpha\Delta}+z\right) = 1-\exp\left(-\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\frac{\phi-1}{\alpha\Delta}\right)\exp\left(-\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}z\right). \tag{7.11}$$

For the CDF $F_Z(z)$, we have

$$\begin{aligned} F_Z(z) &= \Pr(Z<z) \\ &= \Pr\left(\frac{\phi\gamma_{\mathrm{T}_{n-1}\mathrm{E}}}{1+(1-\alpha)\Delta\gamma_{\mathrm{J}_n\mathrm{E}}}<z\right) \\ &= \int_0^{+\infty} F_{\gamma_{\mathrm{T}_{n-1}\mathrm{E}}}\left(\frac{z}{\phi}+\frac{(1-\alpha)\Delta}{\phi}zy\right) f_{\gamma_{\mathrm{J}_n\mathrm{E}}}(y)\,dy. \end{aligned} \tag{7.12}$$

By substituting the CDF and PDF of the exponential RVs $\gamma_{\mathrm{T}_{n-1}\mathrm{E}}$ and $\gamma_{\mathrm{J}_n\mathrm{E}}$ into (7.12) and after some manipulation, the CDF $F_Z(z)$ can be given as

$$\begin{aligned} F_Z(z) &= 1-\frac{\lambda_{\mathrm{T}_n\mathrm{E}}\phi}{\lambda_{\mathrm{T}_n\mathrm{E}}\phi+\lambda_{\mathrm{T}_{n-1}\mathrm{E}}(1-\alpha)\Delta z}\exp\left(-\frac{\lambda_{\mathrm{T}_{n-1}\mathrm{E}}}{\phi}z\right) \\ &= 1-\frac{\omega_{1n}}{z+\omega_{1n}}\exp(-\omega_{2n}z), \end{aligned} \tag{7.13}$$

where $\omega_{1n} = \lambda_{\mathrm{T}_n\mathrm{E}}\phi/\left(\lambda_{\mathrm{T}_{n-1}\mathrm{E}}(1-\alpha)\Delta\right)$ and $\omega_{2n} = \lambda_{\mathrm{T}_{n-1}\mathrm{E}}/\phi$.

From (7.13), the corresponding PDF $f_Z(z)$ is expressed by (14) as

$$f_Z(z) = \frac{\omega_{1n}}{(z+\omega_{1n})^2}\exp(-\omega_{2n}z)+\frac{\omega_{1n}\omega_{2n}}{z+\omega_{1n}}\exp(-\omega_{2n}z). \tag{7.14}$$

Substituting (7.11) and (7.14) into (7.10), after calculating the integrals, the exact closed-form expression for the probability OP_n can be computed by

$$\mathrm{OP}_n = 1-\left[\begin{array}{l} 1-\omega_{1n}\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\exp\left(\omega_{1n}\left(\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}+\omega_{2n}\right)\right) \\ \quad\times E_1\left(\omega_{1n}\left(\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}+\omega_{2n}\right)\right) \end{array}\right]\exp\left(-\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\frac{\phi-1}{\Delta}\right), \tag{7.15}$$

where $E_1(x)=\int_x^{+\infty}\exp(-t)/t\,dt$ is an exponential integral function. Then, substituting (7.15) into (7.9), the closed-form expression of the SOP for the RAND protocol is obtained.

Moreover, when $\alpha=1$, which means there is no transmit power allocated to the jammer node, (7.15) can be rewritten as the following closed-form expression:

$$\mathrm{OP}_n=1-\frac{\lambda_{\mathrm{T}_{n-1}\mathrm{E}}}{\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\phi+\lambda_{\mathrm{T}_{n-1}\mathrm{E}}}\exp\left(-\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\frac{\phi-1}{\Delta}\right). \tag{7.16}$$

7.3.3. The BEST protocol

Since there is no relay selection method at the last hop, the probability OP_M in this protocol can be provided using (7.15):

$$\mathrm{OP}_M=1-\left[\begin{array}{l}1-\omega_{1M}\lambda_{\mathrm{T}_{M-1}\mathrm{T}_M}\exp\left(\omega_{1M}\left(\lambda_{\mathrm{T}_{M-1}\mathrm{T}_M}+\omega_{2M}\right)\right)\\ \quad\times E_1\left(\omega_1\left(\lambda_{\mathrm{T}_{M-1}\mathrm{T}_M}+\omega_{2M}\right)\right)\end{array}\right]\exp\left(-\lambda_{\mathrm{T}_{M-1}\mathrm{T}_M}\frac{\phi-1}{\Delta}\right). \tag{7.17}$$

Next, the probability OP_n with $1\le n<M$ is calculated. By contrast to (7.11), the CDF $F_{\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}}\left(\frac{\phi-1}{\alpha\Delta}+z\right)$ in this case is given by

$$\begin{aligned}F_{\gamma_{\mathrm{T}_{n-1}\mathrm{T}_n}}\left(\frac{\phi-1}{\alpha\Delta}+z\right)&=\left[1-\exp\left(-\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\frac{\phi-1}{\alpha\Delta}\right)\exp\left(-\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}z\right)\right]^{K_n}\\&=1-\sum_{t=1}^{K_n}(-1)^{t+1}C_{K_n}^t\exp\left(-t\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\frac{\phi-1}{\alpha\Delta}\right)\exp\left(-t\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}z\right).\end{aligned} \tag{7.18}$$

Putting (7.10), (7.14) and (7.18) together and after some careful manipulation, we obtain

$$\mathrm{OP}_n=1-\sum_{t=1}^{K_n}(-1)^{t+1}C_{K_n}^t\left[\begin{array}{l}1-t\omega_{1n}\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\exp\left(\omega_{1n}\left(\omega_{2n}+t\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\right)\right)\\ \quad\times E_1\left(\omega_{1n}\left(\omega_{2n}+t\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\right)\right)\end{array}\right]\exp\left(-t\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\frac{\phi-1}{\alpha\Delta}\right). \tag{7.19}$$

Finally, with $\alpha=1$, the exact closed-form formula of OP_n is given as

$$\mathrm{OP}_n=\begin{cases}1-\sum_{t=1}^{K_n}(-1)^{t+1}C_{K_n}^t\frac{\lambda_{\mathrm{T}_{n-1}\mathrm{E}}}{\lambda_{\mathrm{T}_{n-1}\mathrm{E}}+t\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\phi}\exp\left(-t\lambda_{\mathrm{T}_{n-1}\mathrm{T}_n}\frac{\phi-1}{\Delta}\right); & \text{if } 1\le n<M\\ 1-\frac{\lambda_{\mathrm{T}_{M-1}\mathrm{E}}}{\lambda_{\mathrm{T}_{M-1}\mathrm{T}_M}\phi+\lambda_{\mathrm{T}_{M-1}\mathrm{E}}}\exp\left(-\lambda_{\mathrm{T}_{M-1}\mathrm{T}_M}\frac{\phi-1}{\Delta}\right); & \text{if } n=M\end{cases}. \tag{7.20}$$

7.4. Numerical results

In this section, Monte-Carlo simulations verify the theoretical derivations provided in Section 7.3. In the simulation environment, a two-dimensional plane is considered in which the coordinates of source T_0, relays T_n (jammers J_{n+1}) and the eavesdropper are (0,0), $(1/M,0)$, (1,0) and

$(0.5, 0.5)$, respectively. In all the simulations, the path-loss exponent β equals 3, and the target rate C_{th} is set at 1.

Figure 7.2 considers the impact of hardware impairments on the secrecy outage probability (SOP) when the number of the cluster is 2 ($M = 2$), the number of nodes in each cluster is 3 ($K_1 = K_2 = 3$) and the fraction α equals 0.3. As illustrated, the SOP values of the RAND and BEST protocols rapidly increased as κ^2 increased. For all of the cases presented, the secrecy performance of the BEST protocol is better than that of the RAND protocol. The simulation results (Sim) also show that the performance of both protocols increased when the transmit SNR $\Delta(P / N_0)$ increased.

Figure 7.3 shows the secrecy performance of the proposed protocols as a function of the transmit SNR in dB when the transceiver hardware is perfect $(\kappa^2 = 0)$. In this figure, the number of clusters is equal to 3 ($M = 3$) and the number of nodes in each cluster is 3, 2, 3 ($K_1 = 2, K_2 = 3, K_3 = 2$). As shown in Figure 7.2, the BEST protocol outperforms the RAND protocol and the performance gain is about 2.5 dB at $\text{SOP} = 10^{-2}$. Also, the SOP value of both protocols decreased as Δ increased. It can also be observed that in almost all values of Δ, the BEST and RAND schemes obtained better performance when the fraction α equalled 0.2. It is worth noting that the simulation results (Sim) matched the theoretical results (Theory) very well, which validates the correction of the theoretical derivations.

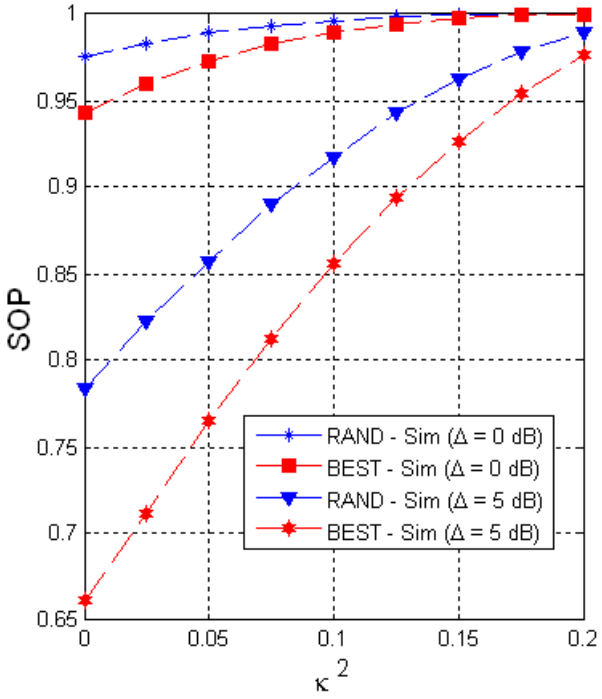

Figure 7.2. *Secrecy outage probability (SOP) as a function of the hardware impairment level* κ^2 *in dB when* $M = 2$, $K_1 = K_2 = 3$ *and* $\alpha = 0.3$.

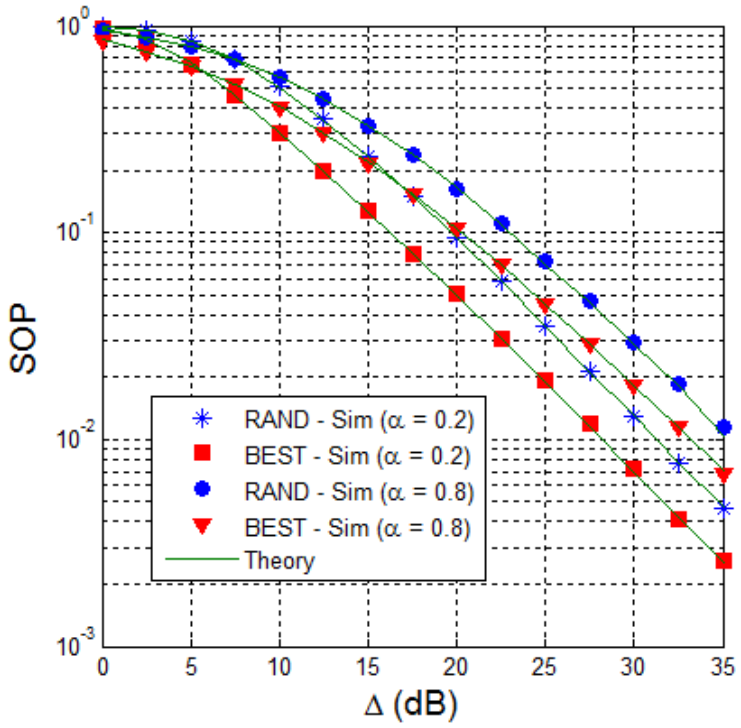

Figure 7.3. *Secrecy outage probability (SOP) as a function of the transmit SNR* $\Delta\left(P/N_0\right)$ *in dB when* $M=3$, $K_1=2, K_2=3, K_3=2$ *and* $\kappa^2=0$.

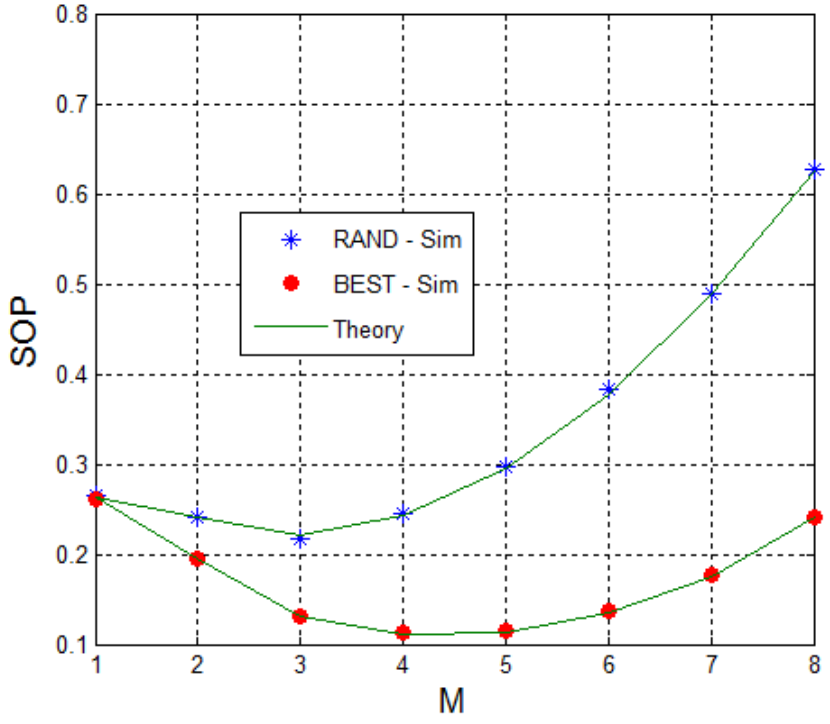

Figure 7.4. *Secrecy outage probability (SOP) as a function of the number of hops* M *when* $\Delta=15$ *dB,* $\alpha=0.5$, $K_n=3\ \forall n$ *and* $\kappa^2=0$.

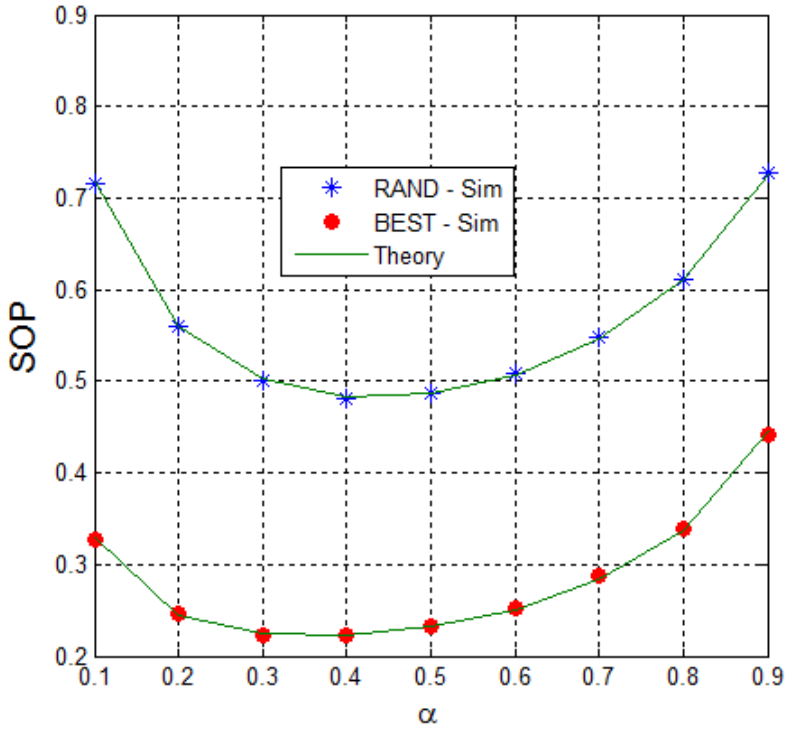

Figure 7.5. *Secrecy outage probability (SOP) as a function of the fraction* α *when* $\Delta = 10$ *dB,* $M = 4$, $K_n = 4\ \forall n$ *and* $\kappa^2 = 0$.

Figure 7.4 shows the SOP performance as a function of the number of hops. In this simulation, I fix the number of nodes at each cluster by 3. The remaining parameters can be listed as follows: $\Delta = 15$ dB, $\alpha = 0.5$ and $\kappa^2 = 0$. Again, the value SOP of the BEST protocol is lower than that of the RAND one. Moreover, in both protocols, there exists an optimal value of M so that the secrecy performance is best. For example, in Figure 7.4, the SOP of the BEST (RAND) method is lowest when $M = 4\ (M = 3)$.

Figure 7.5 illustrates the impact of the fraction of the transmit power (α) on secrecy performance when $\Delta = 10$dB, $M = 4$, $K_n = 4\ \forall n$ and $\kappa^2 = 0$. As shown in Figure 7.5, the value α significantly effects the SOP value. An optimal value α also exists when secrecy performance is best. Finally, we can see from Figures 7.4 and 7.5 that the simulation and theoretical results agree, which again verifies the derivations.

7.5. Summary

In this chapter, the secrecy outage probability (SOP) of two joint relay and jammer selection protocols in cluster-based multi-hop networks was proposed and evaluated. Exact closed-form expressions of SOP over Rayleigh fading channels were derived, which were verified with Monte Carlo simulations. The results demonstrated that the BEST protocol always outperformed the RAND protocol. Hardware noise also had a significant impact on the SOP values. Finally, the secrecy performance of both protocols was optimized by appropriately assigning the value of the number of hops and the value of the fraction of the transmit power.

8. TRANSMIT ANTENNA SELECTION AND HARVEST-TO-JAM TECHNIQUES

In this chapter, the third aim of this dissertation is investigated. A secure communication protocol is proposed, and its performance evaluated while exploiting cooperative jammer nodes harvesting energy from radio frequency (RF) signals from the source and interference sources to generate jamming noises to the eavesdropper. The data transmission terminates as soon as the destination can receive a sufficient number of encoded packets for decoding the original data of the source. To obtain secure communication, the destination must receive sufficient encoded packets before the eavesdropper. Exact closed-form expressions of outage probability (OP), probability of successful and secure communication (SS), intercept probability (IP) and average number of time slots used by the source over a Rayleigh fading channel are derived. Monte Carlo simulations are then performed to verify the theoretical results.

8.1. Motivations

Physical-layer security (PLS) [10]-[11], [66], [74] has attracted much attention from researchers as an efficient method of obtaining security in wireless communication systems. To enhance secrecy performance, transmit diversity techniques can be employed. In [75]-[78], MIMO-based transmit-receive methods such as Transmit Antenna Selection-Maximal Ratio Combining (TAS-MRC), Maximal Ratio Transmission-MRC (MRT-MRC), MRT-Selection Combining (MRT-SC), MRT-SC were proposed and analysed. The performance of secure communication protocols could also be enhanced with cooperative relaying methods [18], [20], [79]-[80]. In [81]-[83], the authors proposed cooperative jamming techniques to reduce the quality in eavesdropping channels. The results demonstrated that the schemes combining the transmit diversity and jamming techniques outperformed the conventional cooperative methods without using jamming [21], [84]-[85]. However, energy efficiency may become a critical issue when the jammer nodes continuously transmit artificial noise by using their energy.

Radio frequency (RF) energy harvesting (EH) is an efficient method for prolonging the lifetime of energy-constrained wireless devices without recharging batteries [86]-[93]. Wireless devices can harvest energy from full-energy nodes [86]-[87], power stations deployed in networks [89]-[90] or from co-channel interferences caused by external sources [92]-[93]. In [94]-[95], the authors proposed harvest-to-jam methods in which the jammers could harvest energy from the RF signals and then use it to generate artificial noise.

Fountain codes (FCs), or rateless erasure codes, [96]-[98] have drawn much attention because of their simple implementation. In FCs, a transmitter uses a Fountain encoder to generate a limitless number of encoded packets and then transmit them to the intended receivers. If the receivers can receive a sufficient number of encoded packets, they can recover the original message of the transmitter. In a wireless channel broadcast, encoded packets can be listened in on by eavesdroppers. Security therefore becomes a critical issue for FC-based communication systems. Recently, some works considering secure communication protocols with FCs have been published [99]-[101]. In [99], the authors proposed a secure delivery scheme in which security can be achieved if the legitimate user receives enough Fountain packets before the eavesdropper. In [100],

a dynamic Fountain-encoded at a transmitter was proposed to enhance data security. The authors of [101] proposed an FC-based cooperative relay protocol. In [101], the source and jammer cooperate to remove interference components in the received signals at the destination.

In this chapter, a secure communication scheme exploiting FCs is proposed. A multi-antenna source in the proposed protocol selects its best antenna to transmit encoded packets to a single-antenna destination while in presence of a single-antenna eavesdropper that attempts to listen in on the source information. Both the destination and eavesdropper are affected by noise caused by hardware impairments [25]-[26], [102] and interference sources. To reduce the quality of the eavesdropping links, a cooperative jammer node harvests energy from the RF signals of the source and interference sources to generate noise to the eavesdropper. When the destination can receive sufficient encoded packets to decode the original data, it sends feedback to the source to terminate the transmission. As a result, to obtain secure transmission, the destination must receive a sufficient number of encoded packets before the eavesdropper, otherwise, the original information is intercepted. For performance evaluation, exact closed-form expressions of outage probability (OP), probability of successful and secure communication (SS), intercept probability (IP) and average number of the time slots used by the source over a Rayleigh fading channel were derived. Finally, Monte Carlo simulations were performed to verify the theoretical results.

8.2. System model

Figure 8.1 illustrates the system model of the proposed protocol, where the source node (S) equipped with M antennas communicates with the single-antenna destination (D) in the presence of a single-antenna eavesdropper (E) that attempts to listen in on the source data. All of the receivers, such as D and E, suffer from co-channel interference caused by K ambient sources (denoted by $\mathrm{I}_1, \mathrm{I}_2, ..., \mathrm{I}_K$). To reduce the quality of the eavesdropping link, a cooperative jamming technique can be used, where a single antenna jammer (J) is employed to continuously generate artificial noise to E. We assume that nodes D and J can cooperate with each other so that D can remove the co-channel interference generated by J [79], [83]-[84]. Jammer (J) also uses the energy harvested from the RF signals of the source and interference sources for transmitting jamming signals.

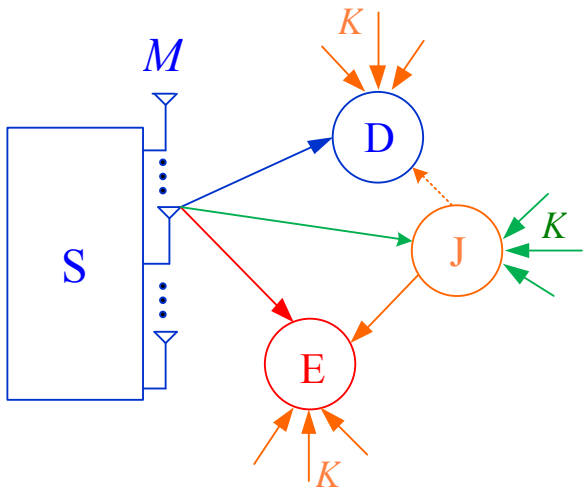

Figure 8.1. *System model of the proposed protocol.*

The source divides its original data into L packets, which are encoded appropriately to create the encoded packets. Then, at each time slot, the source uses the TAS technique to send each encoded packet to the destination. At the same time, the eavesdropper tries to receive the encoded packet. We assume that the destination and eavesdropper can successfully obtain the original data if they can correctly receive at least H encoded packets, where $H=(1+\varepsilon)L$, and ε is the decoding overhead that depends on the concrete code design [94]-[95]. After the destination receives a sufficient number of encoded packets, it will send an ACK message to inform the source to stop data transmission. In this case, if the eavesdropper cannot obtain enough encoded packets, it cannot obtain the source data, otherwise, the original data of the source will be intercepted.

Let us consider data transmission at an arbitrary time slot. Let $\gamma_{\mathrm{S}_m\mathrm{D}}$, $\gamma_{\mathrm{S}_m\mathrm{E}}$ and $\gamma_{\mathrm{S}_m\mathrm{J}}$ denote channel gains between the mth antenna of the source and nodes D, E and J, respectively, where $m=1,2,...,M$. Let $\gamma_{\mathrm{I}_k\mathrm{D}}$, $\gamma_{\mathrm{I}_k\mathrm{E}}$, $\gamma_{\mathrm{I}_k\mathrm{J}}$ and γ_{JE} also be the channel gains of the $\mathrm{I}_k\to\mathrm{D}$, $\mathrm{I}_k\to\mathrm{E}$, $\mathrm{I}_k\to\mathrm{J}$ and $\mathrm{J}\to\mathrm{E}$ links, respectively, where $k=1,2,...,K$. We assume all of the link channels are block and flat Rayleigh fading that remains constant in a single time slot but independently changes over other time slots. The channel gain γ_{XY}, $\left(\mathrm{X},\mathrm{Y}\in\{\mathrm{S}_m,\mathrm{D},\mathrm{E},\mathrm{J},\mathrm{I}_k\}\right)$ is an exponential random variable (RV) whose cumulative distribution function (CDF) and probability density function (PDF) are given, respectively as

$$F_{\gamma_{\mathrm{XY}}}(z)=1-\exp(-\lambda_{\mathrm{XY}}x),\ f_{\gamma_{\mathrm{XY}}}(z)=\lambda_{\mathrm{XY}}\exp(-\lambda_{\mathrm{XY}}x), \tag{8.1}$$

where λ_{XY} is a parameter of γ_{XY}, i.e. $\lambda_{\mathrm{XY}}=1/E\{\gamma_{\mathrm{XY}}\}$, and $E\{.\}$ is an expected operator.

We assume that the RVs $\gamma_{\mathrm{S}_m\mathrm{D}}\left(\gamma_{\mathrm{S}_m\mathrm{E}},\gamma_{\mathrm{S}_m\mathrm{J}}\right)$ are independent and identical, i.e. $\lambda_{\mathrm{S}_m\mathrm{D}}=\lambda_{\mathrm{SD}}$ $\left(\lambda_{\mathrm{S}_m\mathrm{E}}=\lambda_{\mathrm{SE}},\lambda_{\mathrm{S}_m\mathrm{J}}=\lambda_{\mathrm{SJ}}\right)$ for all m. Conversely, the RVs $\gamma_{\mathrm{I}_k\mathrm{D}}\left(\gamma_{\mathrm{I}_k\mathrm{E}},\gamma_{\mathrm{I}_k\mathrm{J}}\right)$ are assumed to be independent and non-identical, i.e. $\lambda_{\mathrm{I}_k\mathrm{D}}\neq\lambda_{\mathrm{I}_l\mathrm{D}}$ $\left(\lambda_{\mathrm{I}_k\mathrm{E}}\neq\lambda_{\mathrm{I}_l\mathrm{E}},\lambda_{\mathrm{I}_k\mathrm{J}}\neq\lambda_{\mathrm{I}_l\mathrm{J}}\right)$ as $k\neq l$, where $l\in\{1,2,...,K\}$

Using the TAS technique, the source selects the best transmit antenna to send the encoded packet to the destination using the following method:

$$b=\arg\max_{m=1,2,...,M}\left(\gamma_{\mathrm{S}_m\mathrm{D}}\right), \tag{8.2}$$

where $b\in\{1,2,...,M\}$.

Furthermore, the CDF of $\gamma_{\mathrm{S}_b\mathrm{D}}$ can be obtained by

$$\begin{aligned}F_{\gamma_{\mathrm{S}_b\mathrm{D}}}(x)&=\Pr\left(\max_{m=1,2,...,M}\left(\gamma_{\mathrm{S}_m\mathrm{D}}\right)<x\right)=\left[\Pr\left(\gamma_{\mathrm{S}_m\mathrm{D}}<x\right)\right]^M\\&=\left[1-\exp(-\lambda_{\mathrm{SD}}x)\right]^M\\&=1+\sum_{m=1}^{M}(-1)^m C_M^m\exp(-m\lambda_{\mathrm{SD}}x),\end{aligned} \tag{8.3}$$

where $C_M^m=M!/m!/(M-m)!$ is a binomial coefficient.

Let us denote T as the block time of each time slot: a duration of $\alpha \mathrm{T}(0 \le \alpha \le 1)$ is used for the jammer node to harvest the energy from the source and interference sources, and the remaining time $((1-\alpha)\mathrm{T})$ is spent for data transmission. The energy harvested by the jammer is therefore expressed as

$$\mathrm{EH} = \eta \alpha \mathrm{T}\left(P_{\mathrm{S}} \gamma_{\mathrm{S}_b \mathrm{J}} + \sum_{k=1}^{K} P_{\mathrm{I}_k} \gamma_{\mathrm{I}_k \mathrm{J}} \right), \tag{8.4}$$

where $\eta(0 \le \eta \le 1)$ is an energy conversion efficiency, P_{S} and P_{I_k} are the transmit power of the source (S) and interference sources I_k, respectively.

Next, the average transmit power of the jammer used for the data transmission phase can be expressed as

$$P_{\mathrm{J}} = \frac{\mathrm{EH}}{(1-\alpha)\mathrm{T}} = \chi \left(P_{\mathrm{S}} \gamma_{\mathrm{S}_b \mathrm{J}} + \sum_{k=1}^{K} P_{\mathrm{I}_k} \gamma_{\mathrm{I}_k \mathrm{J}} \right), \tag{8.5}$$

where $\chi = \eta\alpha / (1-\alpha)$.

It is worth noting that implementing the TAS method is simpler than the MRT method, as it only requires the index of the best antenna that can be fed back by the destination (not feedback to all of the channel state information (CSI) as in MRT). The best transmit antenna selection can also be performed before the EH phase, and the time used for this process can be ignored as compared to the EH and packet transmission phases. Finally, the source uses the selected antenna during each time slot for both EH and data transmission purposes.

Assuming that the destination can perfectly remove interference caused by node J, the instantaneous signal-to-interference-plus-noise ratio (SINR) received by the destination under joint impact of co-channel interference and hardware impairments can be expressed similarly to [101, eq. (3)-(4)] as

$$\begin{aligned} \Psi_{\mathrm{D}} &= \frac{P_{\mathrm{S}} \gamma_{\mathrm{S}_b \mathrm{D}}}{\kappa_{\mathrm{D}}^2 P_{\mathrm{S}} \gamma_{\mathrm{S}_b \mathrm{D}} + \sum_{k=1}^{K} P_{\mathrm{I}_k} \gamma_{\mathrm{I}_k \mathrm{D}} + N_0} \\ &= \frac{Q_{\mathrm{S}} \gamma_{\mathrm{S}_b \mathrm{D}}}{\kappa_{\mathrm{D}}^2 Q_{\mathrm{S}} \gamma_{\mathrm{S}_b \mathrm{D}} + \sum_{k=1}^{K} Q_{\mathrm{I}_k} \gamma_{\mathrm{I}_k \mathrm{D}} + 1}, \end{aligned} \tag{8.6}$$

where N_0 is the variance of additive noise, which is assumed to be same at all receivers, and κ_{D}^2 is the total hardware impairment level of the $\mathrm{S}_b \to \mathrm{D}$ links, $Q_{\mathrm{S}} = P_{\mathrm{S}} / N_0$ and $Q_{\mathrm{I}_k} = P_{\mathrm{I}_k} / N_0$.

Because the eavesdropper cannot remove the jamming signals, the instantaneous SINR obtained at this node is given as

$$\Psi_{\mathrm{E}} = \frac{P_{\mathrm{S}} \gamma_{\mathrm{S}_b \mathrm{E}}}{\kappa_{\mathrm{E}}^2 P_{\mathrm{S}} \gamma_{\mathrm{S}_b \mathrm{E}} + P_{\mathrm{J}} \gamma_{\mathrm{JE}} + \sum_{k=1}^{K} P_{\mathrm{I}_k} \gamma_{\mathrm{I}_k \mathrm{D}} + N_0}, \tag{8.7}$$

where κ_{E}^2 is the total hardware impairment level of the $\mathrm{S}_b \to \mathrm{E}$ links.

Substituting (8.5) into (8.7), we obtain

$$\Psi_{\mathrm{E}}=\frac{Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{E}}}{\kappa_{\mathrm{E}}^2 Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{E}}+\chi\left(Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{J}}+\sum_{k=1}^{K}Q_{\mathrm{I}_k}\gamma_{\mathrm{I}_k\mathrm{J}}\right)\gamma_{\mathrm{JE}}+\sum_{k=1}^{K}Q_{\mathrm{I}_k}\gamma_{\mathrm{I}_k\mathrm{E}}+1}. \tag{8.8}$$

Next, the expressions of the data rate for the data and eavesdropping links are given, respectively, by

$$\begin{aligned} C_{\mathrm{D}}&=(1-\alpha)\mathrm{T}\log_2(1+\Psi_{\mathrm{D}}),\\ C_{\mathrm{E}}&=(1-\alpha)\mathrm{T}\log_2(1+\Psi_{\mathrm{E}}). \end{aligned} \tag{8.9}$$

We assume that each encoded packet can be decoded successfully if the achievable data rate is higher than a predetermined target rate (denoted by C_{th}), otherwise, the encoded packet cannot be received correctly. Hence, the probability that the destination cannot receive one encoded packet correctly is expressed as

$$\Pr(C_{\mathrm{D}}<C_{\mathrm{th}})=\Pr(\Psi_{\mathrm{D}}<\theta_{\mathrm{th}})=\rho_{\mathrm{D}}, \tag{8.10}$$

where

$$\theta_{\mathrm{th}}=2^{\wedge}\left(\frac{C_{\mathrm{th}}}{(1-\alpha)\mathrm{T}}\right)-1. \tag{8.11}$$

Note that the probability of successful decoding for one encoded packet at D is calculated by $\Pr(C_{\mathrm{D}}\geq C_{\mathrm{th}})=1-\rho_{\mathrm{D}}$. Similarly, the probability that one encoded packet can be received correctly or incorrectly by the eavesdropper are given, respectively, by

$$\begin{aligned} \Pr(C_{\mathrm{E}}<C_{\mathrm{th}})&=\Pr(\Psi_{\mathrm{E}}<\theta_{\mathrm{th}})=\rho_{\mathrm{E}},\\ \Pr(C_{\mathrm{E}}\geq C_{\mathrm{th}})&=\Pr(\Psi_{\mathrm{E}}\geq\theta_{\mathrm{th}})=1-\rho_{\mathrm{E}}. \end{aligned} \tag{8.12}$$

Consider a delay-constrained system in which the maximum number of time slots that can be used for transmitting encoded packets are limited by $N_{\mathrm{th}}\,(N_{\mathrm{th}}\geq H)$. This means that the destination cannot recover the original data if it cannot successfully receive H encoded packets within N_{th} time slots. Let us denote $N_{\mathrm{S}}\,(H\leq N_{\mathrm{S}}\leq N_{\mathrm{th}})$ as the number of time slots used by the source (or the number of the encoded packets sent by the source), N_{D} and N_{E} $(0\leq N_{\mathrm{D}},N_{\mathrm{E}}\leq H)$ as the number of the encoded packets received by nodes D and E, respectively, after the source stops its transmission.

Then, the outage probability (OP) of the proposed protocol is expressed as follows:

$$\mathrm{OP}=\Pr(N_{\mathrm{D}}<H\mid N_{\mathrm{S}}=N_{\mathrm{th}}). \tag{8.13}$$

Next, the probability that the source-destination transmission is successful and secure (SS) is given by

$$\mathrm{SS}=\Pr(N_{\mathrm{D}}=H,N_{\mathrm{E}}<H\mid N_{\mathrm{S}}\leq N_{\mathrm{th}}). \tag{8.14}$$

Equation (8.14) implies that the destination can receive a sufficient number of encoded packets $\left(N_{\mathrm{D}}=H\right)$ before the eavesdropper $\left(N_{\mathrm{E}}<H\right)$ when the number of time slots used is less than or equal to N_{th} $\left(N_{\mathrm{S}}\le N_{\mathrm{th}}\right)$.

Let us consider the intercept probability (IP) defined as the probability that the eavesdropper can obtain H encoded packets before or at the same time as the destination:

$$\mathrm{IP}=\Pr\left(N_{\mathrm{E}}=H,N_{\mathrm{D}}\le H\mid N_{\mathrm{S}}\le N_{\mathrm{th}}\right). \tag{8.15}$$

Note from (8.15), that when the eavesdropper obtains H encoded packets, it does not need to receive more encoded packets, regardless of whether the source will transmit encoded packets in the next time slots. Instead, it will start to decode the original data of the source.

Finally, the average number of time slots used to transmit encoded packets to the destination was studied and can be expressed as

$$\mathrm{TS}=\sum_{v=0}^{H-1}N_{\mathrm{th}}\Pr\left(N_{\mathrm{D}}=v\mid N_{\mathrm{S}}=N_{\mathrm{th}}\right)+\sum_{t=H}^{N_{\mathrm{th}}}t\Pr\left(N_{\mathrm{D}}=H\mid N_{\mathrm{S}}=t\right). \tag{8.16}$$

In (8.16), $\Pr\left(N_{\mathrm{D}}=v\mid N_{\mathrm{S}}=N_{\mathrm{th}}\right)$ is the probability that the number of encoded packets received at D is $v\left(0\le v<H\right)$ when S uses N_{th} time slots (D is in outage) and $\Pr\left(N_{\mathrm{D}}=H\mid N_{\mathrm{S}}=t\right)$ is the probability that D can obtain a sufficient number of encoded packets within t time slots, where $H\le t\le N_{\mathrm{th}}$ (data transmission is successful).

8.3. Performance analysis

Derivations of ρ_{D} and ρ_{E}

Proposition 1: If $1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}}\le 0$, then $\rho_{\mathrm{D}}=1$, and if $1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}}>0,$ we obtain an exact closed-form expression of ρ_{D} as

$$\rho_{\mathrm{D}}=1+\sum_{m=1}^{M}\left(-1\right)^m C_M^m\exp\left(-m\lambda_{\mathrm{SD}}\omega_0\right)\times\left[\prod_{k=1}^{K}\frac{\lambda_{\mathrm{I}_k\mathrm{D}}}{\lambda_{\mathrm{I}_k\mathrm{D}}+m\lambda_{\mathrm{SD}}\omega_k}\right]. \tag{8.17}$$

Proof:

From (8.6) and (8.10), we obtain

$$\begin{aligned}\rho_{\mathrm{D}}&=\Pr\left(\frac{Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{D}}}{\kappa_{\mathrm{D}}^2Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{D}}+\sum_{k=1}^{K}Q_{\mathrm{I}_k}\gamma_{\mathrm{I}_k\mathrm{D}}+1}<\theta_{\mathrm{th}}\right)\\&=\Pr\left(\left(1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}}\right)Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{D}}<\sum_{k=1}^{K}Q_{\mathrm{I}_k}\theta_{\mathrm{th}}\gamma_{\mathrm{I}_k\mathrm{D}}+\theta_{\mathrm{th}}\right).\end{aligned} \tag{8.18}$$

From (8.18), we can observe that if $1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}}\le 0$, then $\rho_{\mathrm{D}}=1$, and if $1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}}>0$, we can rewrite (8.18) as

$$\rho_{\mathrm{D}} = \Pr\left(\gamma_{\mathrm{S}_b\mathrm{D}} < \sum_{k=1}^{K} \omega_k \gamma_{\mathrm{I}_k\mathrm{D}} + \omega_0 \right), \tag{8.19}$$

where,

$$\omega_0 = \frac{\theta_{\mathrm{th}}}{\left(1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}}\right)Q_{\mathrm{S}}}, \omega_k = \frac{\theta_{\mathrm{th}}Q_{\mathrm{I}_k}}{\left(1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}}\right)Q_{\mathrm{S}}}. \tag{8.20}$$

Equation (8.19) can therefore be rewritten as

$$\rho_{\mathrm{D}} = \int_0^{+\infty}\int_0^{+\infty}....\int_0^{+\infty} F_{\gamma_{\mathrm{S}_b\mathrm{D}}}\left(\sum_{k=1}^{K} \omega_k x_k + \omega_0 \right) f_{\gamma_{\mathrm{I}_1\mathrm{D}}}(x_1) f_{\gamma_{\mathrm{I}_2\mathrm{D}}}(x_2)...f_{\gamma_{\mathrm{I}_K\mathrm{D}}}(x_K)\, dx_1 dx_2 ... dx_K. \tag{8.21}$$

Using the CDF obtained by (8.3), we have

$$\begin{aligned} F_{\gamma_{\mathrm{S}_b\mathrm{D}}}\left(\sum_{k=1}^{K} \omega_k x_k + \omega_0 \right) &= \left(1 - \exp\left(-\lambda_{\mathrm{SD}} \left(\sum_{k=1}^{K} \omega_k x_k + \omega_0 \right) \right) \right)^M \\ &= 1 + \sum_{m=1}^{M} (-1)^m C_M^m \exp\left(-m\lambda_{\mathrm{SD}}\omega_0\right) \exp\left(-m\lambda_{\mathrm{SD}} \sum_{k=1}^{K} \omega_k x_k \right). \end{aligned} \tag{8.22}$$

Substituting (8.22) and the PDF of $\gamma_{\mathrm{I}_k\mathrm{D}}$ given by (8.1) and after some manipulations, we obtain (8.17), and the proof is complete.

Proposition 2: If $1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}} \le 0$, then $\rho_{\mathrm{E}} = 1$, and if $1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}} > 0$, we obtain an exact closed-form expression of ρ_{E} as

$$\rho_{\mathrm{E}} = 1 - \left(\prod_{k=1}^{K} \frac{\lambda_{\mathrm{I}_k\mathrm{E}}}{\lambda_{\mathrm{I}_k\mathrm{E}} + \lambda_{\mathrm{SE}}\vartheta_k} \right) \times \exp\left(-\lambda_{\mathrm{SE}}\vartheta_0\right) \times \left[\begin{array}{l} \dfrac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}} \beta_0 \exp\left(\dfrac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}} \right) E_1\left(\dfrac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}} \right) \\ + \displaystyle\sum_{k=1}^{K} \dfrac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}} \beta_k \exp\left(\dfrac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}} \right) E_1\left(\dfrac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}} \right) \end{array} \right]. \tag{8.23}$$

***Proof*:**

Combining (8) and (12), we have

$$\begin{aligned} \rho_{\mathrm{E}} &= \Pr\left(\frac{Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{E}}}{\kappa_{\mathrm{E}}^2 Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{E}} + \chi\left(Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{J}} + \sum_{k=1}^{K} Q_{\mathrm{I}_k}\gamma_{\mathrm{I}_k\mathrm{J}} \right)\gamma_{\mathrm{JE}} + \sum_{k=1}^{K} Q_{\mathrm{I}_k}\gamma_{\mathrm{I}_k\mathrm{E}} + 1} < \theta_{\mathrm{th}} \right) \\ &= \Pr\left(\left(1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}}\right) Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{E}} < \chi\theta_{\mathrm{th}} \left(Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{J}} + \sum_{k=1}^{K} Q_{\mathrm{I}_k}\gamma_{\mathrm{I}_k\mathrm{J}} \right)\gamma_{\mathrm{JE}} + \theta_{\mathrm{th}} \sum_{k=1}^{K} Q_{\mathrm{I}_k}\gamma_{\mathrm{I}_k\mathrm{E}} + \theta_{\mathrm{th}} \right). \end{aligned} \tag{8.24}$$

We observe from (8.24) that if $1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}} \le 0$, then $\rho_{\mathrm{E}} = 1$, and if $1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}} > 0$, we can rewrite (8.24) as

$$\rho_{\mathrm{E}} = \Pr\left(\gamma_{\mathrm{S}_b\mathrm{E}} < \vartheta_0 + \sum_{k=1}^{K} \vartheta_k \gamma_{\mathrm{I}_k\mathrm{E}} + \left(\mu_0\gamma_{\mathrm{S}_b\mathrm{J}} + \sum_{k=1}^{K} \mu_k\gamma_{\mathrm{I}_k\mathrm{J}} \right)\gamma_{\mathrm{JE}} \right), \tag{8.25}$$

where

$$\vartheta_0 = \frac{\theta_{\text{th}}}{\left(1-\kappa_{\text{E}}^2\theta_{\text{th}}\right)Q_{\text{S}}},\ \vartheta_k = \frac{\theta_{\text{th}}Q_{\text{I}_k}}{\left(1-\kappa_{\text{E}}^2\theta_{\text{th}}\right)Q_{\text{S}}},\ \mu_0 = \frac{\chi\theta_{\text{th}}}{1-\kappa_{\text{E}}^2\theta_{\text{th}}},\ \mu_k = \frac{\chi\theta_{\text{th}}Q_{\text{I}_k}}{\left(1-\kappa_{\text{E}}^2\theta_{\text{th}}\right)Q_{\text{S}}}. \tag{8.26}$$

Setting $Z = \left(\mu_0\gamma_{\text{S}_b\text{J}} + \sum_{k=1}^{K}\mu_k\gamma_{\text{I}_k\text{J}}\right)\gamma_{\text{JE}}$, from (8.25), we have

$$\rho_{\text{E}} = \int_0^{+\infty}\int_0^{+\infty}\cdots\int_0^{+\infty} F_{\gamma_{\text{S}_b\text{E}}}\left(\vartheta_0 + \sum_{k=1}^{K}\vartheta_k x_k + z\right) f_{\gamma_{\text{I}_1\text{E}}}(x_1)\ldots f_{\gamma_{\text{I}_K\text{E}}}(x_K) f_Z(z)\,dx_1\ldots dx_K dz. \tag{8.27}$$

Substituting the CDF of $\gamma_{\text{S}_b\text{E}}$ and the PDF of $\gamma_{\text{I}_k\text{D}}$ provided by (8.1) into (8.27) and some manipulation yields

$$\rho_{\text{E}} = 1 - \left(\prod_{k=1}^{K}\frac{\lambda_{\text{I}_k\text{E}}}{\lambda_{\text{I}_k\text{E}}+\lambda_{\text{SE}}\vartheta_k}\right)\exp\left(-\lambda_{\text{SE}}\vartheta_0\right)\underbrace{\int_0^{+\infty}\exp\left(-\lambda_{\text{SE}}z\right) f_Z(z)\,dz}_{I}. \tag{8.28}$$

Now, our objective is to calculate the integral I in (8.28). However, we should rewrite I in the following form:

$$\begin{aligned} I &= \int_0^{+\infty}\exp\left(-\lambda_{\text{SE}}z\right) f_Z(z)\,dz \\ &= \int_0^{+\infty}\lambda_{\text{SE}}\exp\left(-\lambda_{\text{SE}}z\right)F_Z(z)\,dz. \end{aligned} \tag{8.29}$$

Next, we attempt to find the CDF of Z. Setting $Y = \mu_0\gamma_{\text{S}_b\text{J}} + \sum_{k=1}^{K}\mu_k\gamma_{\text{I}_k\text{J}}$, the CDF of Z can be expressed as

$$\begin{aligned} F_Z(z) &= \Pr\left(Z < z\right) \\ &= \Pr\left(Y\gamma_{\text{JE}} < z\right) \\ &= \int_0^{+\infty} F_Y\left(\frac{z}{x}\right)\lambda_{\text{JE}}\exp\left(-\lambda_{\text{JE}}x\right)dx. \end{aligned} \tag{8.30}$$

Before calculating the CDF of Y, note that Y is the sum of the exponential RVs, i.e. $\mu_0\gamma_{\text{S}_b\text{J}}$ and $\mu_k\gamma_{\text{I}_k\text{J}}$. Indeed, because $\gamma_{\text{S}_b\text{J}}$ and $\gamma_{\text{I}_k\text{J}}$ are exponential RVs whose parameters are λ_{SJ} and $\lambda_{\text{I}_k\text{J}}$, respectively, hence $\mu_0\gamma_{\text{S}_b\text{J}}$ and $\mu_k\gamma_{\text{I}_k\text{J}}$ are also exponential RVs, and their parameters are $\lambda_{\text{SJ}}/\mu_0$ and $\lambda_{\text{I}_k\text{J}}/\mu_k$, respectively. Hence, the CDF of Y can be given as

$$F_Y(y) = 1 - \beta_0\exp\left(-\Omega_{\text{SJ}}y\right) - \sum_{k=1}^{K}\beta_k\exp\left(-\Omega_{\text{I}_k\text{J}}y\right), \tag{8.31}$$

where

$$
\begin{aligned}
\Omega_{\mathrm{SJ}} &= \frac{\lambda_{\mathrm{SJ}}}{\mu_0}, \\
\Omega_{\mathrm{I}_k\mathrm{J}} &= \frac{\lambda_{\mathrm{I}_k\mathrm{J}}}{\mu_k}, \\
\beta_0 &= \prod_{k=1}^{K} \frac{\Omega_{\mathrm{I}_k\mathrm{J}}}{\Omega_{\mathrm{I}_k\mathrm{J}} - \Omega_{\mathrm{SJ}}}, \\
\beta_k &= \frac{\Omega_{\mathrm{SJ}}}{\Omega_{\mathrm{SJ}} - \Omega_{\mathrm{I}_k\mathrm{J}}} \prod_{t=1, t\neq k}^{K} \frac{\Omega_{\mathrm{I}_t\mathrm{J}}}{\Omega_{\mathrm{I}_t\mathrm{J}} - \Omega_{\mathrm{I}_k\mathrm{J}}}.
\end{aligned}
\tag{8.32}
$$

Substituting (8.30) into (8.31), we obtain

$$
\begin{aligned}
F_Z(z) = 1 &- \beta_0 \int_0^{+\infty} \lambda_{\mathrm{JE}} \exp\left(-\lambda_{\mathrm{JE}} x\right) \exp\left(-\Omega_{\mathrm{SJ}} \frac{z}{x}\right) dy \\
&- \sum_{k=1}^{K} \beta_k \int_0^{+\infty} \lambda_{\mathrm{JE}} \exp\left(-\lambda_{\mathrm{JE}} x\right) \exp\left(-\Omega_{\mathrm{I}_k\mathrm{J}} \frac{z}{x}\right) dy.
\end{aligned}
\tag{8.33}
$$

Using [25, eq. (3.324.1)] on the corresponding integrals in (8.33), we arrive at

$$
F_Z(z) = 1 - 2\beta_0 \sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}} z} K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}} z}\right) - \sum_{k=1}^{K} 2\beta_k \sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}} z} K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}} z}\right), \tag{8.34}
$$

where $K_1(.)$ is a modified Bessel function of the second kind [25].

Substituting (8.34) into (8.29) then yields

$$
\begin{aligned}
I = 1 &- 2\beta_0 \int_0^{+\infty} \lambda_{\mathrm{SE}} \exp\left(-\lambda_{\mathrm{SE}} z\right) \sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}} z} K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}} z}\right) dz \\
&- \sum_{k=1}^{K} 2\beta_k \int_0^{+\infty} \lambda_{\mathrm{SE}} \exp\left(-\lambda_{\mathrm{SE}} z\right) \sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}} z} K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}} z}\right) dz.
\end{aligned}
\tag{8.35}
$$

By changing the variable $t = \sqrt{z}$, we can rewrite (8.35) as

$$
\begin{aligned}
I = 1 &- 4\lambda_{\mathrm{SE}} \sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}} \beta_0 \int_0^{+\infty} t^2 \exp\left(-\lambda_{\mathrm{SE}} t^2\right) K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}} t\right) dt \\
&- \sum_{k=1}^{K} 4\lambda_{\mathrm{SE}} \sqrt{\Omega_{\mathrm{I}_k\mathrm{J}}\lambda_{\mathrm{JE}}} \beta_k \int_0^{+\infty} t^2 \exp\left(-\lambda_{\mathrm{SE}} t^2\right) K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}} t\right) dt.
\end{aligned}
\tag{8.36}
$$

Applying [25, eq. (6.631.3)] to the corresponding integrals in (8.36), we obtain

$$
I = 1 - \beta_0 \exp\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{2\lambda_{\mathrm{SE}}}\right) W_{-1,1/2}\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}}\right) - \sum_{k=1}^{K} \beta_k \exp\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{2\lambda_{\mathrm{SE}}}\right) W_{-1,1/2}\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}}\right), \tag{8.37}
$$

where $W_{-1,1/2}(.)$ is the Whittaker function [25].

From [26, eq. (46)], we also have

$$
\exp\left(\frac{x}{2}\right) W_{-1,1/2}(x) = 1 - x\exp(x) E_1(x), \tag{8.38}
$$

where $E_1(.)$ is an exponential integral function [25].

Combining (8.37) and (8.38) and after some manipulations, we obtain

$$I = \frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}}\beta_0 \exp\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}}\right)E_1\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}}\right)+\sum_{k=1}^{K}\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}}\beta_k \exp\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}}\right)E_1\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}}\right). \tag{8.39}$$

It is worth noting that to obtain (8.39), the following equation was used:

$$\beta_0 + \sum_{k=1}^{K}\beta_k = 1. \tag{8.40}$$

Finally, substituting (8.39) into (8.28), we obtain (8.23), and the proof is complete.

8.3.1. Analysis of outage probability (OP)

As defined in (8.13), an exact closed-form expression of OP can be provided as follows:

$$\mathrm{OP} = \sum_{N_{\mathrm{D}}=0}^{H-1} C_{N_{\mathrm{th}}}^{N_{\mathrm{D}}}\left(1-\rho_{\mathrm{D}}\right)^{N_{\mathrm{D}}}\left(\rho_{\mathrm{D}}\right)^{N_{\mathrm{th}}-N_{\mathrm{D}}}. \tag{8.41}$$

Note that from (8.41) the possible values of N_{D} are from 0 to $H-1$, and there are $C_{N_{\mathrm{th}}}^{N_{\mathrm{D}}}$ possible cases for each value of N_{D}.

8.3.2. Analysis of successful and secure communication (SS)

From (8.14), we can rewrite SS as

$$\mathrm{SS} = \sum_{u=H}^{N_{\mathrm{th}}}\Pr\left(N_{\mathrm{D}} = H \mid N_{\mathrm{S}} = u\right)\times\sum_{t=0}^{H-1}\Pr\left(N_{\mathrm{E}} = t \mid N_{\mathrm{S}} = u\right). \tag{8.42}$$

In (8.42), $\Pr\left(N_{\mathrm{D}} = H \mid N_{\mathrm{S}} = u\right)$ is the probability that the destination can correctly receive H encoded packets when the number of time slots used is u. Since the data transmission between the source and the destination ends in the u-th time slot, $\Pr\left(N_{\mathrm{D}} = H \mid N_{\mathrm{S}} = u\right)$ is calculated as in [95, eq. (8)]:

$$\Pr\left(N_{\mathrm{D}} = H \mid N_{\mathrm{S}} = u\right) = C_{u-1}^{u-H}\left(1-\rho_{\mathrm{D}}\right)^{H}\left(\rho_{\mathrm{D}}\right)^{u-H}. \tag{8.43}$$

$\Pr\left(N_{\mathrm{E}} = t \mid N_{\mathrm{S}} = u\right)$ in (8.42) also presents the probability that the number of encoded packets obtained by the eavesdropper is t. Similar to (8.19), we have

$$\Pr\left(N_{\mathrm{E}} = t \mid N_{\mathrm{S}} = u\right) = C_{u}^{t}\left(1-\rho_{\mathrm{E}}\right)^{t}\left(\rho_{\mathrm{E}}\right)^{u-t}. \tag{8.44}$$

Substituting (8.43) and (8.44) into (8.42), an exact closed-form expression of SS can be given as

$$\mathrm{SS} = \sum_{u=H}^{N_{\mathrm{th}}}\left[C_{u-1}^{u-H}\left(1-\rho_{\mathrm{D}}\right)^{H}\left(\rho_{\mathrm{D}}\right)^{u-H}\times\sum_{t=0}^{H-1}C_{u}^{t}\left(1-\rho_{\mathrm{E}}\right)^{t}\left(\rho_{\mathrm{E}}\right)^{u-t}\right]. \tag{8.45}$$

8.3.3. Analysis of intercept probability (IP)

The intercept probability (IP) in (8.15) can be rewritten as

$$\mathrm{IP}=\sum_{u=H}^{N_{\mathrm{th}}}\Pr\left(N_{\mathrm{E}}=H\mid N_{\mathrm{S}}=u\right)\times\left[\Pr\left(N_{\mathrm{D}}=H\mid N_{\mathrm{S}}=u\right)+\sum_{v=0}^{H-1}\Pr\left(N_{\mathrm{D}}=v\mid N_{\mathrm{S}}=u\right)\right]. \tag{8.46}$$

In (8.46), $\Pr\left(N_{\mathrm{E}}=H\mid N_{\mathrm{S}}=u\right)$ is the probability that the eavesdropper can receive a sufficient number of encoded packets in u time slots, which can be calculated similarly to (8.43) as

$$\Pr\left(N_{\mathrm{E}}=H\mid N_{\mathrm{S}}=u\right)=C_{u-1}^{u-H}\left(1-\rho_{\mathrm{E}}\right)^{H}\left(\rho_{\mathrm{E}}\right)^{u-H}. \tag{8.47}$$

Next, $\Pr\left(N_{\mathrm{D}}=H\mid N_{\mathrm{S}}=u\right)$ in (8.46) is calculated with (8.43), and $\Pr\left(N_{\mathrm{D}}=v\mid N_{\mathrm{S}}=u\right)$ in (8.46) can be obtained by

$$\Pr\left(N_{\mathrm{D}}=v\mid N_{\mathrm{S}}=u\right)=C_{u}^{v}\left(1-\rho_{\mathrm{D}}\right)^{v}\left(\rho_{\mathrm{D}}\right)^{u-v}. \tag{8.48}$$

Putting (8.43), (8.46), (8.47) and (8.48) together, we obtain

$$\mathrm{IP}=\sum_{u=H}^{N_{\mathrm{th}}}\left[C_{u-1}^{u-H}\left(1-\rho_{\mathrm{E}}\right)^{H}\left(\rho_{\mathrm{E}}\right)^{u-H}\right]\times\left[C_{u-1}^{u-H}\left(1-\rho_{\mathrm{D}}\right)^{H}\left(\rho_{\mathrm{D}}\right)^{u-H}+\sum_{v=0}^{H-1}C_{u}^{v}\left(1-\rho_{\mathrm{D}}\right)^{v}\left(\rho_{\mathrm{D}}\right)^{u-v}\right]. \tag{8.49}$$

8.3.4. Analysis of average number of time slots (TS)

Similarly, the probability $\Pr\left(N_{\mathrm{D}}=v\mid N_{\mathrm{S}}=N_{\mathrm{th}}\right)$ and $\Pr\left(N_{\mathrm{D}}=H\mid N_{\mathrm{S}}=t\right)$ in (8.16) can be calculated, respectively, as

$$\begin{aligned}\Pr\left(N_{\mathrm{D}}=v\mid N_{\mathrm{S}}=N_{\mathrm{th}}\right)&=C_{N_{\mathrm{th}}}^{v}\left(1-\rho_{\mathrm{D}}\right)^{v}\left(\rho_{\mathrm{D}}\right)^{N_{\mathrm{th}}-H},\\ \Pr\left(N_{\mathrm{D}}=H\mid N_{\mathrm{S}}=t\right)&=C_{t-1}^{t-H}\left(1-\rho_{\mathrm{D}}\right)^{H}\left(\rho_{\mathrm{D}}\right)^{t-H}.\end{aligned} \tag{8.50}$$

Substituting (8.50) into (8.16), we obtain an exact closed-form formula for the average number of time slots used by the source:

$$\mathrm{TS}=N_{\mathrm{th}}\sum_{v=0}^{H-1}C_{N_{\mathrm{th}}}^{v}\left(1-\rho_{\mathrm{D}}\right)^{v}\left(\rho_{\mathrm{D}}\right)^{N_{\mathrm{th}}-v}+\sum_{t=H}^{N_{\mathrm{th}}}tC_{t-1}^{t-H}\left(1-\rho_{\mathrm{D}}\right)^{H}\left(\rho_{\mathrm{D}}\right)^{t-H}. \tag{8.51}$$

8.4. Numerical results

In this section, Monte Carlo simulations are presented to verify the theoretical results. For illustrative purposes, the required number of encoded packets in all of the simulations was fixed at 10 $\left(H=10\right)$, the energy conversion efficiency was 1 $\left(\eta=1\right)$, the total block time was 1 $\left(\mathrm{T}=1\right)$, the number of the interference sources was 3 $\left(K=3\right)$, the parameters of the interference links were $\lambda_{\mathrm{I_1D}}=\lambda_{\mathrm{I_1E}}=\lambda_{\mathrm{I_1J}}=3$, $\lambda_{\mathrm{I_2D}}=\lambda_{\mathrm{I_2E}}=\lambda_{\mathrm{I_2J}}=4$ and $\lambda_{\mathrm{I_3D}}=\lambda_{\mathrm{I_3E}}=\lambda_{\mathrm{I_3J}}=5$, the parameters of the remaining links were 1 $\left(\lambda_{\mathrm{SD}}=\lambda_{\mathrm{SE}}=\lambda_{\mathrm{SJ}}=\lambda_{\mathrm{JE}}=1\right)$. The simulation and theoretical results are marked in the figures as Sim and Theo, respectively.

Figure 8.2 shows the probability ρ_{D} and ρ_{E} as a function of Q_{S} in dB. The number of antenna equipped by the source was set to 3 $\left(M=3\right)$, the fraction of time allocated for the EH phase was fixed at 0.3 $\left(\alpha=0.3\right)$, the hardware impairment levels were assigned $\kappa_{\mathrm{D}}^{2}=\kappa_{\mathrm{E}}^{2}=0.1$, and the target

rate was set to 0.75 $(C_{\text{th}} = 0.75)$. It can be seen from Figure 8.2 that ρ_{D} and ρ_{E} decreased as Q_{S} increased and Q_{I} decreased. However, ρ_{D} was much smaller than ρ_{E} in medium and high Q_{S} regimes. We can also obverse that the simulation and theoretical results agree, which validates our derivations.

Figure 8.3 shows the outage performance of the proposed protocol as a function of Q_{S} in dB with $Q_{\text{I}} = 7.5$ dB, $M = 2$, $\alpha = 0.1$, $\kappa_{\text{D}}^2 = \kappa_{\text{E}}^2 = 0$ and $C_{\text{th}} = 1$. Figure 8.3 also indicates that the impact of the co-channel interference on the performance was negative, i.e. the value of OP was very high at low Q_{S} regimes. In particular, when the value of Q_{S} was lower than that of Q_{I}, OP was almost equal to 1. We can also observe that outage performance was better with a high value of N_{th}, as the source had more time slots to transmit encoded packets to the destination.

Figure 8.4 shows the value of SS as a function of Q_{S} in dB when $Q_{\text{I}} = 10$ dB, $\alpha = 0.1$, $\kappa_{\text{D}}^2 = 0.1$, $\kappa_{\text{E}}^2 = 0$, $N_{\text{th}} = 20$ and $C_{\text{th}} = 1.5$. We can see that the proposed protocol obtained a higher value of SS when more antennas were equipped at the source. SS also increased as Q_{S} increased. This is because at high Q_{S} values, the destination almost obtained a sufficient number of encoded packets before the eavesdropper. However, it can be seen from Figure 8.4 that when the value of Q_{S} was very high, the value of SS slightly decreased because the eavesdropper had a high possibility of being able to listen in. Furthermore, SS performance in all values of *M* was almost same at high Q_{S} regimes.

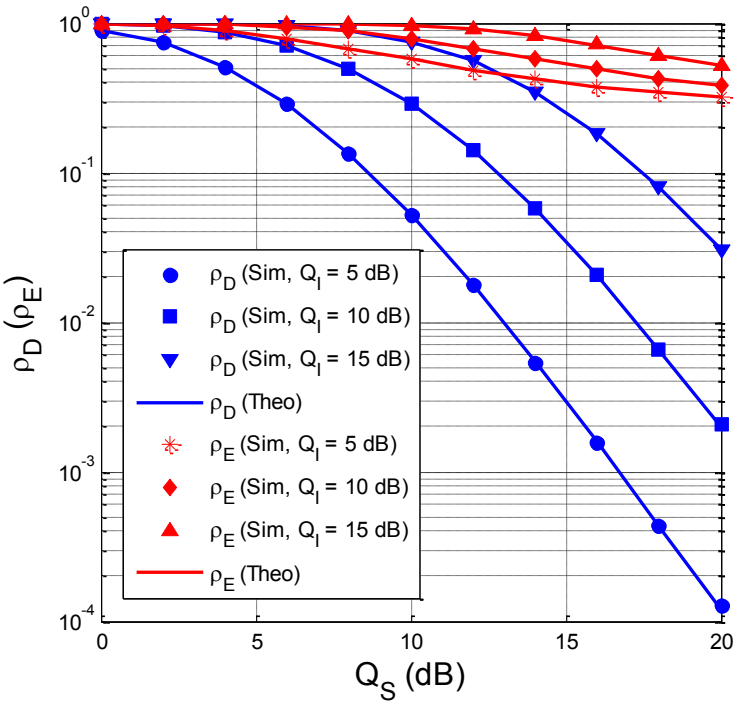

Figure 8.2. *ρ_{D} and ρ_{E} as a function of Q_{S} in dB when $M = 3$, $\alpha = 0.3$, $\kappa_{\text{D}}^2 = \kappa_{\text{E}}^2 = 0.1$ and $C_{\text{th}} = 0.75$.*

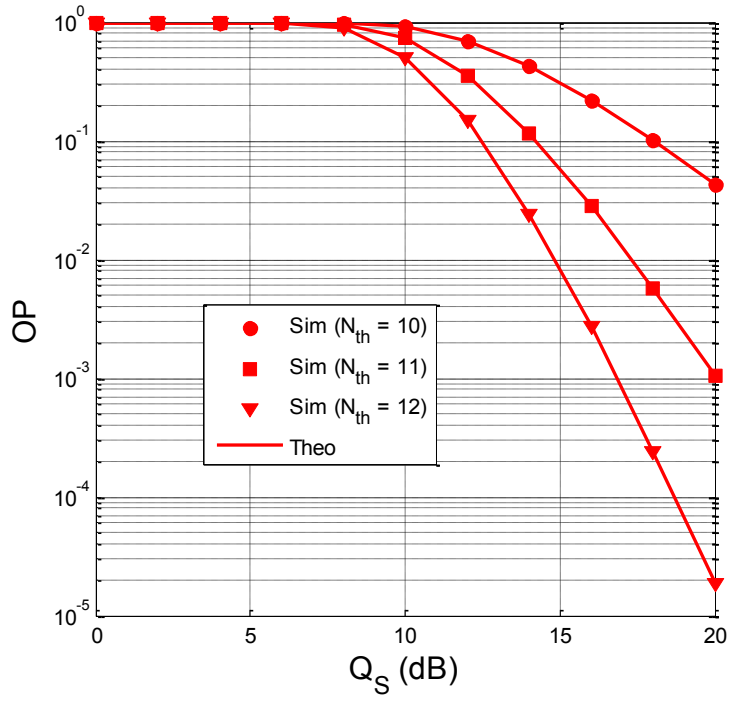

Figure 8.3. *OP as a function of* Q_S *in dB when* $Q_I = 7.5\ dB,\ M = 2,\ \alpha = 0.1,\ \kappa_D^2 = \kappa_E^2 = 0$ *and* $C_{th} = 1$.

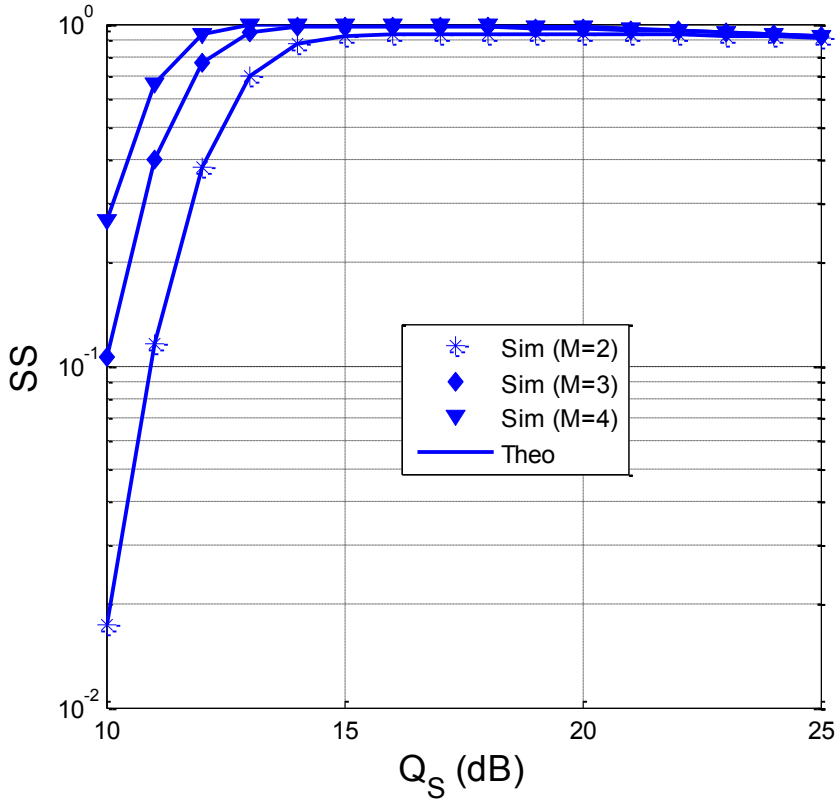

Figure 8.4. *SS as a function of* Q_S *in dB when* $Q_I = 10\,dB,\ \alpha = 0.1,\ \kappa_D^2 = 0.1, \kappa_D^2 = 0,\ N_{th} = 20$ *and* $C_{th} = 1.5$.

Figure 8.5 shows the value of SS as a function of α when $Q_S = Q_I = 15$ dB, $M = 3$, $\kappa_E^2 = 0.1$, $N_{th} = 15$ and $C_{th} = 0.7$. We can see that performance significantly degraded with high hardware impairment levels at the data links, i.e. κ_D^2 was high. We can also observe that the fraction of time allocated to the EH phase influenced the value of SS and that an optimal value of α when the value of SS was highest exists.

In Figure 8.6, the intercept probability of the proposed protocol is presented as a function of M when $Q_S = Q_I = 20$ dB, $\kappa_D^2 = 0.2$, $\alpha = 0.3$, $N_{th} = 20$ and $C_{th} = 0.5$. As shown, the value of IP decreased when more antennas were equipped at the source. Also, IP is lower when the hardware impairment level of the eavesdropping links was high.

Figure 8.7 illustrates the impact of N_{th} on the intercept probability as $Q_S = Q_I = 20$ dB, $M = 2$, $\kappa_D^2 = \kappa_E^2 = 0$, and $C_{th} = 0.5$. We can observe that the value of IP was higher when the number of N_{th} increased. However, when the number of N_{th} was high enough, the IP converged to a constant. As expected, IP was lower when more time was used for the EH phase (because the transmit power of the jammer was higher).

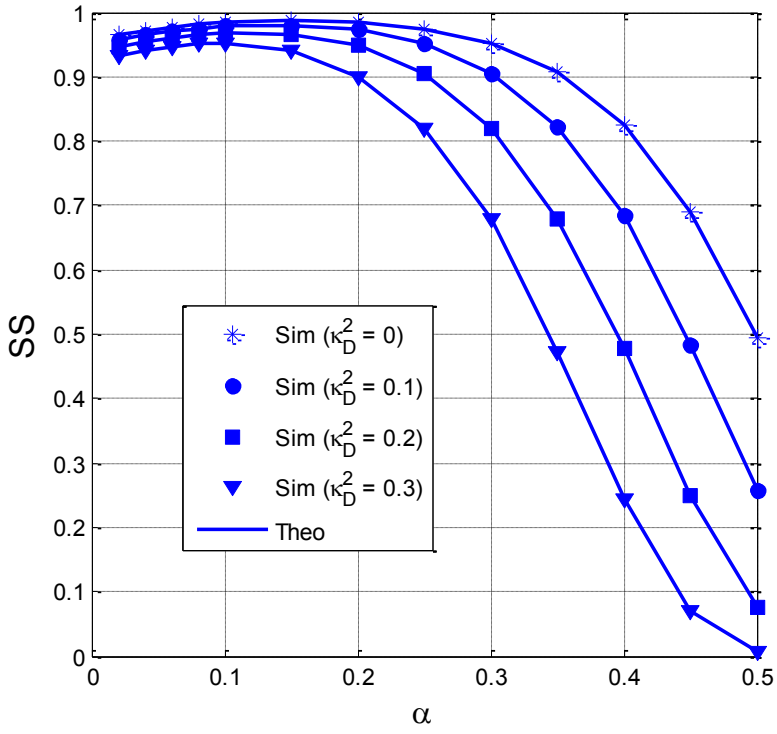

Figure 8.5. *SS as a function of* α *when* $Q_S = Q_I = 15$ *dB,* $M = 3$, $\kappa_E^2 = 0.1$, $N_{th} = 15$ *and* $C_{th} = 0.7$.

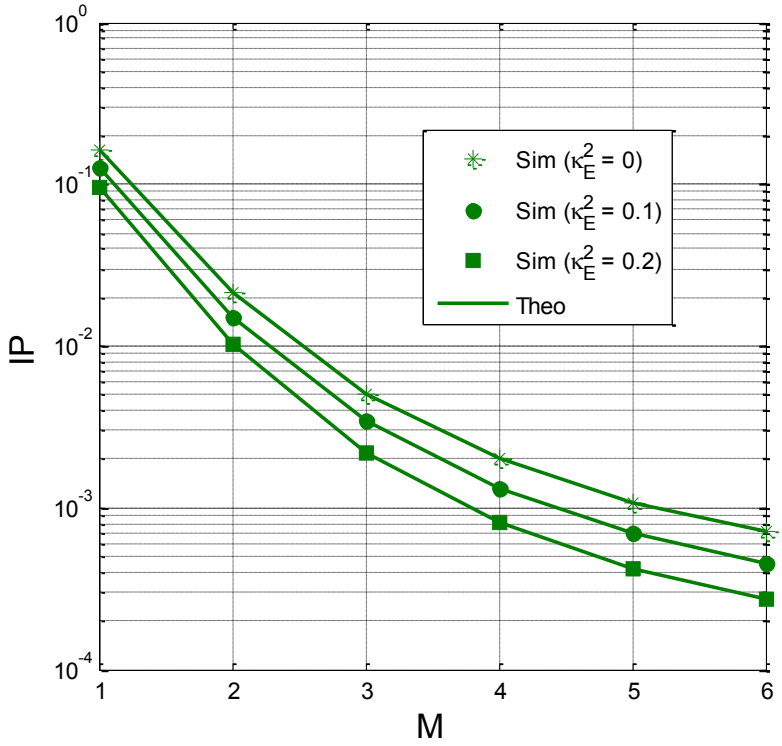

Figure 8.6. *IP as a function of* M *when* $Q_S = Q_I = 20\,dB$, $\kappa_D^2 = 0.2$, $\alpha = 0.3$, $N_{th} = 20$ *and* $C_{th} = 0.5$.

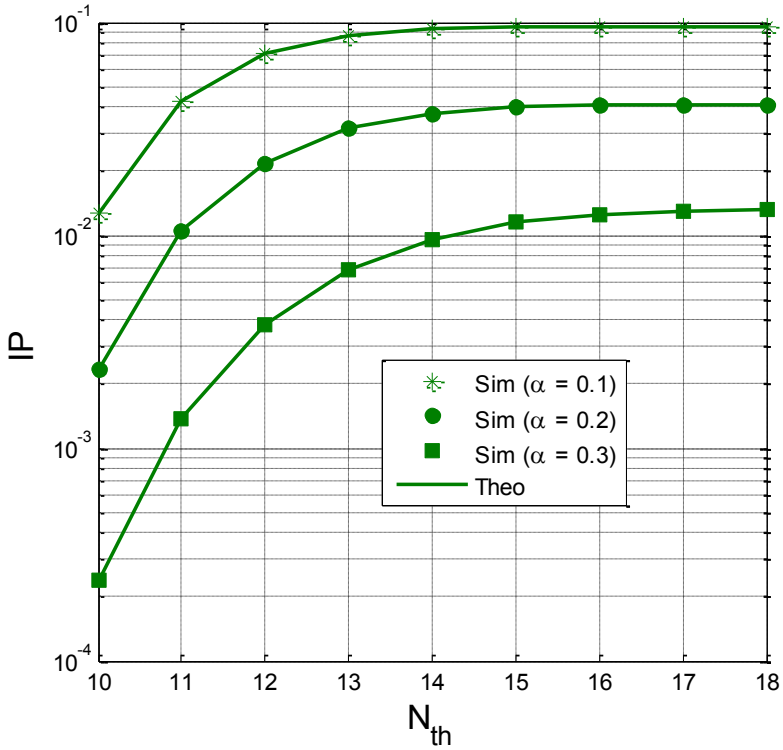

Figure 8.7. *IP as a function of* N_{th} *when* $Q_S = Q_I = 20\,dB$, $M = 2$, $\kappa_D^2 = \kappa_E^2 = 0$, *and* $C_{th} = 0.5$.

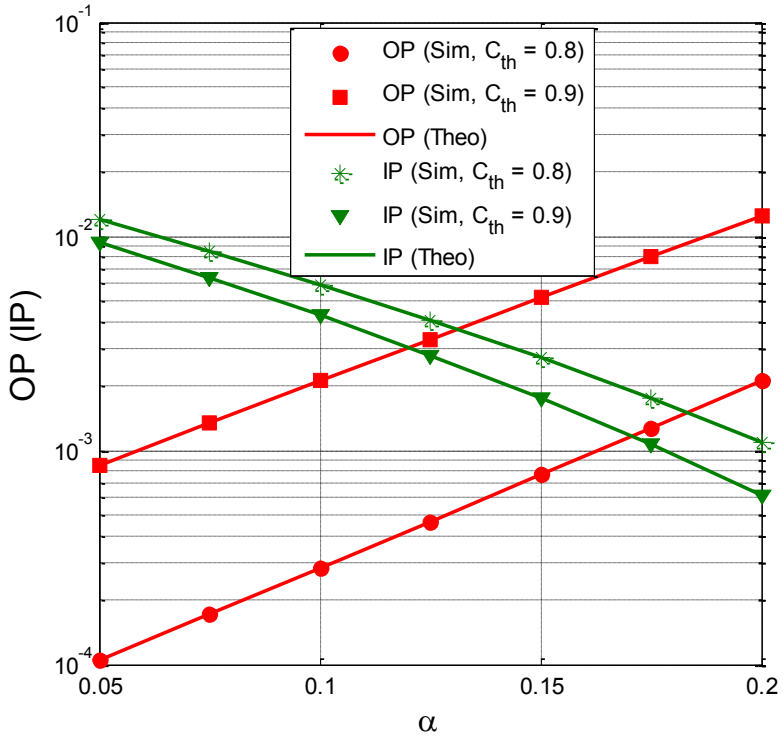

Figure 8.8. *OP and IP as a function of* α *when* $Q_S = Q_I = 15$ *dB,* $M = 4$, $\kappa_D^2 = \kappa_E^2 = 0$ *and* $N_{th} = 16$.

Figure 8.8 presents OP and IP as a function of α when $Q_S = Q_I = 15$ dB, $M = 4$, $\kappa_D^2 = \kappa_E^2 = 0$ and $N_{th} = 16$, and shows that a trade-off exists between OP and IP. Indeed, OP increased when the value of α increased, while IP decreased as α increased. We can also see that when $C_{th} = 0.8$, OP was below 10^{-3} when the value of α was higher than (about) 0.15, but the intercept probability was higher than 2.5×10^{-3}. OP also significantly decreased as the value of C_{th} decreased.

Figure 8.9 presents the average number of time slots as a function of Q_S in dB when $Q_I = 10$ dB, $\alpha = 0.2$, $\kappa_D^2 = \kappa_E^2 = 0.05$, $N_{th} = 17$ and $C_{th} = 1$. The number of time slots used decreased when the number of antennas and the transmit power of the source increased. Reducing the number of time slots also meant reducing the delay time, which is an important metric in wireless communication systems.

From Figures. 8.3-8.9, it is worth noting that the theoretical results and simulation results are in good agreement, which validates the theoretical derivations.

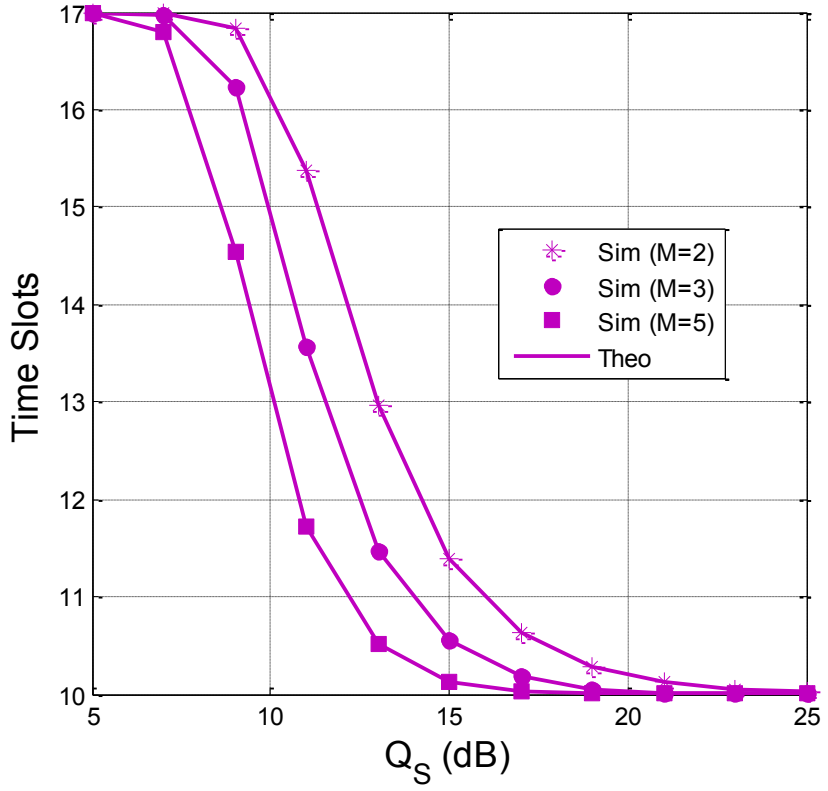

Figure 8.9. *Average number of time slots as a function of* Q_S *in dB when* $Q_I = 10\,dB$, $\alpha = 0.2$, $\kappa_D^2 = \kappa_E^2 = 0.05$ $N_{th} = 17$ *and* $C_{th} = 1$.

8.5. Summary

In this chapter, an FC-based MISO scheme was proposed using the TAS and EH-based cooperative jamming techniques for secure communication under the joint impact of hardware impairments and co-channel interference. The performance of the proposed scheme in outage probability (OP), the probability of successful and secure communication (SS), intercept probability (IP) and average number of the time slots was evaluated through both simulation and theory. The results showed that the hardware impairment levels, co-channel interference, fraction of time allocated to the EH phase and the number of transmit antennas at the source had a significant impact on system performance. A trade-off between security and reliability, i.e. between OP and IP, also exists. In conclusion, the fraction of time allocated to the EH phase should be designed appropriately to optimize system performance.

9. CONCLUSIONS AND FUTURE WORK

This thesis presented methods for creating and developing a framework under which eavesdropping and intelligent jamming problems are intertwined. As a general scenario, I envision a wireless network with nodes of similar capabilities, where nodes may create alliances aimed at either sharing confidential messages in the most efficient way or eavesdropping and disrupting an enemy alliance. As a consequence, they attempt to find and implement optimal strategies against both eavesdropping and jamming. By contrast, enemies may collaborate in order to obtain as much information about their opponents as possible and use it in an optimal manner to disrupt communication.

The thesis considered secrecy performance enhancement in wireless relaying networks under the impact of hardware impairments. The thesis also introduced the importance of researching physical-layer security and provided methods for improving secrecy performances. The secrecy performance of the proposed methods was also evaluated using both simulations and analyses. The results obtained can be used to design and optimize wireless systems in next generation wireless systems.

The three aims of thesis were discussed in the chapters as follows. *Aim 1* was presented in Chapters 5 and 6, where cooperative relaying protocols with relay selection methods in conventional wireless and cognitive radio networks were proposed and analysed. *Aim 2* was presented in Chapter 7, where joint relay and jammer selection protocols for enhancing secrecy performances were studied. *Aim 3* was presented in Chapter 8, where harvest-to-transmit and harvest-to-jam methods were proposed and investigated.

All three aims of the dissertation specified in Chapter 3 were fulfilled. *Aim 1* was published in [PTT01], [PTT03] and [PTT04], in which dual-hop and multi-hop relaying protocols in cognitive radio (CR) and conventional wireless networks were proposed for enhancing system performance. *Aim 2* was published in papers [PTT05], [PTT06] and proposed joint relay and jammer selection protocols in cluster-based relaying networks with and without the presence of the hardware impairments. *Aim 3* was published in papers [PTT02], [PTT07] and proposed harvest-to-transmit and harvest-to-jam methods for generating jamming noises to the eavesdropper.

In summary, wireless communication is susceptible to eavesdropping and jamming attacks. However, the wireless medium also offers ways to neutralize the loss of confidentiality such as: multi-user diversity, partial diversity multiple antennas and cooperation via overheard signals… So, my research for the purpose of proposing methods that can be used to achieve provable and quantifiable security capacity in wireless channel transmissions. The resulting schemes can be also implemented with signal processing, communications and coding technology.

I would like to continue researching WSN secrecy in my future work, especially to extend the issues covered in the second and third aims proposed in my dissertation. My new research intentions consist in studying new joint relay and jammer selection protocols with radio frequency energy harvesting.

REFERENCES

[1] A. Goldsmith, “Wireless Communications”, Cambridge University Press, 2005.

[2] J. N. Laneman, G. W. Wornell, “Distributed spacetime- coded protocols for exploiting cooperative diversity in wireless networks,” IEEE Trans. Inform. Theory, vol. 49, no. 10, pp. 2415-2425, Nov. 2003.

[3] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, “Cooperative diversity in wireless networks: efficient protocols and outage behaviour,” IEEE Trans. Inform. Theory, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[4] T. Q. Duong, T. T. Duy, M. Matthaiou, T. Tsiftsis, G. K. Karagiannidis, “Cognitive Cooperative Networks in Dual-Hop Asymmetric Fading Channels”, IEEE Global Communications Conference (Globecom), Atlanta, GA, pp. 977-983, Dec. 2013.

[5] J. Boyer, David D. Falconer, H. Yanikomeroglu, “Multihop diversity in wireless relaying channels,” IEEE Trans. on Commun., vol. 52, no. 10, pp. 1820-1830, 2004.

[6] G. K. Karagiannidis, “Performance bounds of multihop wireless communications with blind relays over generalized fading channels”, IEEE Trans. Wire. Commu., vol. 5, no. 3, pp. 498-503, 2006.

[7] M. Kakitani, G. Branteb and R. Souzas, “Energy Efficiency Analysis of a Two Dimensional Cooperative Wireless Sensor Network with Relay Selection”, Radioengineering, vol. 22, no. 2, pp. 549–557, 2013.

[8] V. Bao and H. Y. Kong, “Joint Adaptive Modulation and Distributed Switch and Stay for Partial Relay Selection Networks”, IEICE Trans Commun., vol.E95-B, no.02, pp. 668-671, 2012.

[9] T. T. Duy and H.Y. Kong, “Outage Analysis of Cognitive Spectrum Sharing for Two-way Relaying Schemes with Opportunistic Relay Selection over i.n.i.d. Rayleigh Fading Channels”, IEICE Transactions on Communications, vol. E96-B, no. 1, pp. 348-351, 2013.

[10] A. D. Wyner, “The wire-tap channel”, AT&T Bell Labs. Tech. J., vol. 54, no. 8, pp.1355–1387, 1975.

[11] P. K. Gopala, L. Lai and H. E. Gamal, “On the Secrecy Capacity of Fading Channels”, IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687-4698, 2008.

[12] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis and A. Nallanathan, “On the Security of Cognitive Radio Networks”, IEEE Transactions on Vehicular Technology, vol. 64, no. 8, pp. 3790 - 3795, 2015.

[13] S. Wang, X. Xu and W. Yang, “Physical Layer Security in Underlay CCRNs with Fixed Transmit Power”, KSII Transactions on Internet and Information Systems, vol. 9, no. 1, pp. 260-279, 2015.

[14] Y. Zou, B. Champagne, W. P. Zhu and L. Hanzo, “Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems,” IEEE Transactions on Communications, vol. 63, no. 1 pp. 215–228, 2015.

[15] P. T. D. Ngoc, T. T. Duy, V. N. Q. Bao and N. L. Nhat, "Security-Reliability Analysis for Underlay Cognitive Radio Networks with Relay Selection Methods under Impact of Hardware Noises," in Proc. of ATC 2016, pp. 174-179, 2016.

[16] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," IEEE Transactions on Wireless Communications, vol. 8, no. 10, pp. 5003–5011, 2009.

[17] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints", IET Communications, vol. 4, no. 15, pp. 1787–1791, 2010.

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

[19] T. T. Duy, P. N. Son, "Secrecy Performances of Multicast Underlay Cognitive Protocols with Partial Relay Selection and without Eavesdropper's Information", KSII Transactions on Internet and Information Systems, vol. 9, no. 11, pp. 4623-4643, 2015.

[20] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, Trung Q. Duong, "Relay Selection for Security Enhancement in Cognitive Relay Networks", IEEE Wireless Communications Letters, vol. 4, no. 1, pp. 46-49, 2015.

[21] T. T. Do, H. Q. Ngo, T. Q. Duong, T. J. Oechtering, and M. Skoglund "Massive MIMO Pilot Retransmission Strategies for Robustification against Jamming" IEEE Wireless Communications Letters, vol. 6, no. 1, pp. 58 – 61, 2017.

[22] C. T. Dung, N. T. Van, T. T. Duy, V. N. Q. Bao and N. L. Nhat , "Security Enhancement for dual-hop RF Protocols with Nth-best Partial Relay and EH-based Jammer", In Proc. of ComManTel2015, pp. 111-115, 2015.

[23] P. M. Quang, T. T. Duy and V. N. Q. Bao, "Performance Evaluation of Underlay Cognitive Radio Networks over Nakagami-m Fading Channels with Energy Harvesting", In Proc. of ATC2016, pp. 108 - 113, 2016.

[24] E. Bjornson, J. Hoydis, M. Kountouris, and M. Debbah, "Hardware impairments in large-scale miso systems: Energy efficiency, estimation, and capacity limits," in Proc. of DSP2013, pp. 1–6, 2013.

[25] E. Bjornson, M. Matthaiou, and M. Debbah, "A new look at dual-hop relaying: Performance limits with hardware impairments," IEEE Trans. Commun., vol. 61, no. 11, pp. 4512–4525, 2013.

[26] M. Matthaiou and A. Papadogiannis, "Two-way relaying under the presence of relay transceiver hardware impairments," IEEE Commun. Lett., vol. 17, no. 6, pp. 1136–1139, 2013.

[27] A. A. Boulogeorgos, D. S. Karas and G. K. Karagiannidis, "How much does I/Q Imbalance affect Secrecy Capacity?", IEEE Communications Letters, vol. 20, no. 7, p. 1305–1308, 2016.

[28] D. T. Hung, T. T. Duy, D. Q. Trinh, V. N. Q. Bao and T. Hanh, "Impact of Hardware Impairments on Secrecy Performance of Multi-hop Relay Networks in Presence of Multiple Eavesdroppers", In Proc. of NICS2016, pp. 113- 118, 2016.

[29] C. E. Shannon, "Communication theory of secrecy systems", Bell system technical journal, vol. 28, pp. 656-715, (1949).

[30] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, “Performance of transmit antenna selection physical layer security schemes”, IEEE Signal Process. Lett., vol. 19, no. 6, pp. 372–375, 2012.

[31] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, “Joint relay and jammer selection for secure two-way relay networks,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 310–320, 2012.

[32] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, “Physical layer security of TAS/MRC with antenna correlation”, IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 254 – 259, 2013.

[33] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and K. Karagiannidis, “Secure multiuser multiple amplify-and-forward relay networks in presence of multiple eavesdroppers”, in IEEE GLOBECOM, Austin, USA, 8-12 December, 2014.

[34] A. P. Shrestha and K. S. Kwak, “Performance of opportunistic scheduling for physical layer security with transmit antenna selection”, EURASIP Journal on Wireless Communications and Networking, vol. 2014:33, pp. 1–9, 2014.

[35] S. Liu, Y. Hong, and E. Viterbo, “Practical secrecy using artificial noise”, IEEE Communications Letter, vol. 17, no. 7, pp. 1483–1486, 2013.

[36] A. Khisti and G. W. Wornell, “Secure Transmission with Multiple Antennas - Part II: The MIMOME Wiretap Channel”, IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[37] 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.

[38] S. Goel and R. Negi, “Guaranteeing Secrecy Using Artificial Noise”, IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[39] A. Mukherjee and A. L. Swindlehurst, “Robust Beamforming for Secrecy in MIMO Wiretap Channels with Imperfect CSI”, IEEE Trans. Signal Process, vol. 59, no. 1, pp. 351-361. (Jan. 2011)

[40] V. U. Prabhu and M. R. D. Rodrigues, “On Wireless Channels with M-Antenna Eavesdroppers: Characterization of the Outage Probability and Outage Secrecy Capacity”, IEEE GLOBECOM, Miami, USA, pp. 1-6, Dec. 2010.

[41] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, “Secure Transmission via Transmit Antenna Selection in MIMO Wiretap Channels”, IEEE GLOBECOM, Anaheim, CA, pp. 807-812, Dec. 2012.

[42] T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao, “Secrecy Performance Analysis with Relay Selection Method under Impact of Co-Channel Interference”, IET Commun., vol. 9, no. 11, pp. 1427-1435, Jul. 2015.

[43] H. A. Suraweera, H. K. Garg, and A. Nallanathan, “Performance Analysis of Two Hop Amplify-and-Forward Systems with Interference at the Relay”, IEEE Commun. Lett., vol. 14, no. 8, pp. 692-694, Aug. 2010.

[44] E. Soleimani-Nasab, M. Matthaiou, M. Ardebilipour, and G. K. Karagiannidis, “Two-Way AF Relaying in the Presence of Co-Channel Interference”, IEEE Trans. Commun., vol. 61, no.8, pp. 3156-3169, Aug. 2013.

[45] T. N. Nguyen, T. D. Tran, G. T. Luu, P. T. Tran and M. Voznak, "Energy Harvesting-based Spectrum Access with Incremental Cooperation, Relay Selection and Hardware Noises", Radioengineering, vol. 26, no. 1, pp. 240-250, Apr. 2017.

[46] T. T. Duy and P. N. Son, "A Novel Adaptive Spectrum Access Protocol in Cognitive Radio with Primary Multicast Network, Secondary User Selection and Hardware Impairments," Telecommunications Systems, 2017 (Online First).

[47] T. T. Duy and H.Y. Kong, "Performance Analysis of Mixed Amplify-and-Forward and Decode-and-Forward Protocol in Underlay Cognitive Networks", China Communications, vol. 13, no. 3, pp. 115-126, Mar. 2016

[48] N. I. Miridakis, D. D. Vergados, A. Michalas, "Cooperative Relaying in Underlay Cognitive Systems with TAS/MRC, Spatial Correlation and Hardware Impairments", 2015 IEEE 82nd Vehicular Technology Conference (VTC Fall), Boston, pp. 1-5, 2015.

[49] Ding, Z., Z. Yang, P. Fan and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users", IEEE Signal Processing Letters. vol. 21, no. 12, pp. 1501–1505, 2014.

[50] Ding, Z., M. Peng and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems", IEEE Communications Letters, vol. 19, no. 8, pp. 1462–1465, 2015.

[51] Ding, Z., H. Dai and H. V. Poor, "Relay Selection for Cooperative NOMA", IEEE Wireless Communications Letters, vol. 5, no. 4, pp. 426–419, 2016.

[52] Liang, X., Y. Wu, D. W. Kwan, Y. Zuo, S. Jin and H. Zhu, "Outage Performance for Cooperative NOMA Transmission with an AF Relay", IEEE Communications Letters, vol. 21, no. 11, pp. 2428 – 2431, Nov. 2017.

[53] P. T. Tin, D. T. Hung, T. T. Duy and M. Voznak, "Security-Reliability Analysis of NOMA – Based Multi-Hop Relay Networks in Presence of an Active Eavesdropper with Imperfect Eavesdropping CSI", Advances in Electrical and Electronic Engineering, vol. 15, no. 4, pp. 591-597, Nov. 2017.

[54] F. Ding, H. Wang, S. Zhang and M. Dai, "Impact of Residual Hardware Impairments on Non-Orthogonal Multiple Access Based Amplify-and-Forward Relaying Networks", IEEE Access vol. 6, pp. 15117 – 1513, 2018.

[55] T. T. Duy, G. C. Alexandropoulos, T. T. Vu, N. S. Vo, T. Q. Duong, "Outage Performance of Cognitive Cooperative Networks with Relay Selection over Double-Rayleigh Fading Channels", IET Communications, vol. 10, no. 1, pp. 57-64, Jan. 2016.

[56] P. N. Son and H. Y. Kong, "Exact outage analysis of Energy Harvesting Underlay Cooperative Cognitive Networks," IEICE Transactions on Communications, vol. E98-B, no. 4, pp. 661-672, Apr. 2015.

[57] Y. Guo, G. Kang, N. Zhang, W. Zhou, P. Zhang, "Outage Performance of Relay assisted Cognitive radio System under Spectrum-sharing Constraints" Electronics Letters, vol. 46, pp.182-184, 2010.

[58] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in Proc. IEEE Intl Conf. on Commun. (ICC 2013), Budapest, Hungary, pp. 2183–2187, June 2013.

[59] 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, July 2014.

[60] T. T. Duy and H.Y. Kong, "Secrecy Performance Analysis of Multihop Transmission Protocols in Cluster Networks", Wireless Personal Communications (WPC), vol. 82, no. 4, pp. 2505-2518, June 2015.

[61] P. K. Sharma, P. K. Upadhyay, "Cognitive Relaying with Transceiver Hardware Impairments under Interference Constraints", IEEE Communications Letters, vol. 20, no. 4, pp. 820 – 823, 2016.

[62] T. T. Duy and H.Y. Kong, "On Performance Evaluation of Hybrid Decode-Amplify-Forward Relaying Protocol with Partial Relay Selection in Underlay Cognitive Networks", Journal of Communications and Networks (JCN), vol. 16, no. 5, pp. 502-511, Oct. 2014

[63] U. Ghosh, R. Datta, "P-TCP: A Prediction-based Secure Transmission Control Protocol for Wireless Ad Hoc Networks", IETE Journal of Research, vol. 59, no. 4, pp. 364-375, Jul. 2013.

[64] W. S. Alnumay, P. Chatterjee, U. Ghosh, "Energy Aware Secure Routing for Wireless Ad Hoc Networks", IETE Journal of Research, vol. 60, no. 1, pp. 50-59, Jan. 2014.

[65] H. Imai, S. Shin, K. Kobara, "How to Establish Secure Channels for Wireless Communications", IETE Journal of Research, vol. 52, no. 2-3, pp. 229-238, 2006.

[66] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[67] D.-B. Ha, Tung T. Vu, D. T. Tran, V.N,Q. Bao, "Secure Cognitive Reactive Decode-and-Forward Relay Networks: With and Without Eavesdropper", Wireless Personal Communications, vol. 85, no. 4, pp. 2619-2641, Dec. 2015.

[68] D.-D. Tran, D.-B. Ha, T.-H. Vu and E.-K. Hong, "Secrecy Analysis with MRC/SC-Based Eavesdropper over Heterogeneous Channels," IETE Journal of Research, vol. 61, no. 4, pp. 229-238, 2015.

[69] P. N. Son and H. Y. Kong, "An Integration of Source and Jammer for a Decode-and-Forward Two-way Scheme under Physical Layer Security," Wireless Personal Communications (WPC), vol. 79, no. 3, pp. 1741-1764, Dec. 2014.

[70] T. Q. Duong, D. T. Tran, M. Elkashlan, Nghi .H. Tran, Octavia A. Dobre, "Secured Cooperative Cognitive Radio Networks with Relay Selection", presented at IEEE Global Communications Conference, Austin, TX USA, pp. 3074 - 3079, Dec. 2014.

[71] E. R. Alotaibi, K. A. Hamdi, "Secure Relaying in Multihop Communication Systems", IEEE Communications Letters, vol. 20, no. 6, pp. 1120 – 1123, Jun. 2016.

[72] T. T. Duy, T. Q. Duong, D. B. da Costa, V. N. Q. Bao, M. Elkaslan, "Proactive relay selection with joint impact of hardware impairment and co-channel interference", IEEE Transactions on Communications, vol. 63, no. 5, pp. 1594–1606, May 2015.

[73] T. T. Duy and V.N.Q. Bao, "Outage performance of cooperative multihop transmission in cognitive underlay networks", presented at ComManTel 2013, HCM City, Viet Nam, Jan. 2013

[74] R. Liu, I. Maric, P. Spasojevic and R. D. Yates, “Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions,” IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2493 - 2507, June 2008.

[75] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong and W. Yang, “Secure Transmission in Cognitive MIMO Relaying Networks With Outdated Channel State Information,” IEEE Access, vol. 4, pp. 8212-8224, September 2016.

[76] Y. Huang, J. Wang, C. Zhong, T. Q. Duong and G. K. Karagiannidis, “Secure Transmission in Cooperative Relaying Networks With Multiple Antennas,” IEEE Transactions on Wireless Communications, vol. 15, no. 10, pp. 6843-6856, October 2016.

[77] M. Yang, D. Guo, Y. Huang, T. Q. Duong and B. Zhang, “Secure Multiuser Scheduling in Downlink Dual-Hop Regenerative Relay Networks Over Nakagami- m Fading Channels,” IEEE Transactions on Wireless Communications, vol. 15, no. 12, pp. 8009 - 8024, December 2016.

[78] 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 Transactions on Communications, vol. 66, no. 2, pp. 546-559, February 2018.

[79] K. G. Nagananda, “Secure Communications Over Opportunistic-Relay Channels,” Physical Communication, vol. 7, pp. 105-121, 2013.

[80] M. Obeed and W. Mesbah, “Efficient Algorithms for Physical Layer Security in Two-Way Relay Systems,” Physical Communication, vol. 28, pp. 78-88, 2018.

[81] K. Cao, Y. Cai, Y. Wu and W. Yang, “Cooperative Jamming for Secure Communication With Finite Alphabet Inputs,” IEEE Communications Letters, vol. 21, no. 9, pp. 2025 - 2028, September 2017.

[82] J.-M. Kang, J. Yang, J. Ha and Il-Min Kim, “Joint Design of Optimal Precoding and Cooperative Jamming for Multiuser Secure Broadcast Systems,” IEEE Transactions on Vehicular Technology, vol. 66, no. 11, pp. 10551 - 10556, November 2017.

[83] M. R. Abedi, N. Mokari and H. Saeedi, “How to manage resources to provide physical layer security: Active versus passive adversary?,” Physical Communication, vol. 27, pp. 143-149, 2018.

[84] N.-E. Wu and H.-J. Li, “Effect of Feedback Delay on Secure Cooperative Networks with Joint Relay and Jammer Selection,” IEEE Wireless Communications Letters, vol. 2, no. 4, pp. 415 - 418, August 2013.

[85] H. Guo, Z. Yang, L. Zhang, J. Zhu and Y. Zou, “Power-Constrained Secrecy Rate Maximization for Joint Relay and Jammer Selection Assisted Wireless Networks,” IEEE Transactions on Communications, vol. 65, no. 5, pp. 2180 - 2193, May 2017.

[86] X. Zhou, R. Zhang and C. K. Ho, “Wireless Information and Power Transfer: Architecture Design and Rate-Energy Tradeoff,” IEEE Transactions on Communications, vol. 61, no. 11, pp. 4754 - 4767, November 2013.

[87] A. A. Nasir, X. Zhou, S. Durrani and R. A. Kennedy, “Relaying Protocols for Wireless Energy Harvesting and Information Processing,” IEEE Transactions on Wireless Communications, vol. 12, no. 7, pp. 3622 - 3636, July 2013.

[88] L. Wang, K.-K. Wong, S. Jin, G. Zheng, R. W. Heath, "A New Look at Physical Layer Security, Caching, and Wireless Energy Harvesting for Heterogeneous Ultra-Dense Networks," IEEE Communications Magazine, vol. 56, no. 6, pp. 49-55, June 2018.

[89] C. Xu, M. Zheng, W. Liang, H. Yu and Y. C. Liang, "Outage Performance of Underlay Multihop Cognitive Relay Networks With Energy Harvesting," IEEE Communication Letters, vol. 20, no. 6, pp. 1148-1151, June 2016.

[90] C. Xu, M. Zheng, W. Liang, H. Yu and Y. C. Liang, "End-to-end Throughput Maximization for Underlay Multi-hop Cognitive Radio Networks with RF Energy Harvesting," IEEE Transactions on Wireless Communications, vol. 16, no. 6, pp. 3561-3572, June 2017.

[91] T. D. Hieu, T. D. Tran, B.-S. Kim, "Performance Enhancement for Multi-hop Harvest-to-Transmit WSNs with Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises," IEEE Sensors Journal, vol. 18, no. 12, pp. 5173 - 5186, Jun. 2018.

[92] G. Zhu, C. Zhong, H. A. Suraweera, G. K. Karagiannidis, Z. Zhang and T. A. Tsiftsis, "Wireless Information and Power Transfer in Relay Systems With Multiple Antennas and Interference," IEEE Transactions on Communications, vol. 63, no. 4, pp. 1400 - 1418, April 2015.

[93] E. Chen, M. Xia, DB da Costa and S. Aissa, "Multi-Hop Cooperative Relaying with Energy Harvesting from Co-Channel Interferences," IEEE Communications Letters, vol. 21, no. 5, pp. 1199-1202, May 2017.

[94] M. Liu and Y. Liu, "Power Allocation for Secure SWIPT Systems With Wireless-Powered Cooperative Jamming," IEEE Communications Letters, vol. 21, no. 6, pp. 1353 - 1356, June 2017.

[95] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li and F. Lin, "Wireless Powered Cooperative Jamming for Secure OFDM System," IEEE Transactions on Vehicular Technology, vol. 67, no. 2, pp. 1331 - 1346, February 2018.

[96] D. J. C. Mackay, "Fountain Codes," IEE Proceedings - Communications, vol. 152, pp. 1062-1068, December 2005.

[97] J. Castura and Y. Mao, "Rateless Coding Over Fading Channels," IEEE Communications Letters, vol. 10, no. 1, pp. 46 - 48, Jan. 2006.

[98] J. Castura and Y. Mao, "Rateless Coding for Wireless Relay Channels," IEEE Transactions on Wireless Communications, vol. 6, no. 5, pp. 1638-1642, May 2007.

[99] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting Fountain Codes for Secure Wireless Delivery," IEEE Communications Letters, vol. 18, no. 5, pp. 777-780, May 2014.

[100] W. Li, Q. Du, L. Sun, P. Ren, and Y. Wang, "Security Enhanced via Dynamic Fountain Code Design for Wireless Delivery," in Proc. of IEEE Wireless Communications and Networking Conference (WCNC2016), Doha, Quatar, April 2016, pp. 1-6.

[101] L. Sun, P. Ren, Q. Du, and Y. Wang, "Fountain-Coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks," IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 291-300, February 2016.

[102] R. Gomes, A. Hammoudeh, R. F.S. Caldeirinha, Z. Al-Daher, T. Fernandes, J. Reis, "Towards 5G: Performance Evaluation of 60 GHz UWB OFDM Communications under Both Channel and RF Impairments," Physical Communication, vol. 25, pp. 527-538, 2017.

[103] I. Gradshteyn, I. Ryzhik, “Table of Integrals, Series, and Products,” New York, USA, 2007.

RESEARCH RESULTS CITED IN THIS WORK

Web of science (WoS) journals

[PTT01] P. T. Tin, H. T. Dang, T. N. Nguyen, T. T. Duy and M. Voznak, “Secrecy performance enhancement for underlay cognitive radio networks employing cooperative multi-hop transmission with and without presence of hardware impairments,” Entropy, 21 (2), art. No. 217, 2019. DOI: 10.3390/e21020217.

[PTT02] P. T. Tin, N. M. Pham, P. T. Tran, T. T. Duy and M. Voznak, "Secrecy performance of TAS/SC-based multi-hop harvest-to-transmit cognitive WSNs under joint constraint of interference and hardware imperfection,” Sensors (Basel, Switzerland), 19 (5), 2019. DOI: 10.3390/s19051160.

[PTT03] P. T. Tin, D. T. Hung, T. T. Duy and M. Voznak, "Analysis of probability of non-zero secrecy capacity for multi-hop networks in presence of hardware impairments over nakagami-m fading channels,” Radioengineering, 25 (4), pp. 774-782, 2016. DOI: 10.13164/re.2016.0774.

Other journals or proceedings of international conferences

[PTT04] P. T. Tin, T. T. Duy and M. Voznak, "Relay selection methods in cognitive networks under interference and intercept probability constraint in presence of hardware noises," in Proc. of KTTO 2016, Malenovice, Czech Republic, Sep. 2016. ISBN 978-80-248-3959-2.

[PTT05] P. T. Tin, P. M. Nam, T. T. Duy and M. Voznak, “Security reliability analysis for cognitive multi-hop protocol in cluster networks with hardware imperfection,” IEIE Transactions on Smart Processing & Computing, Vol.6, No.3, pp. 200-209, March 2017. DOI: 10.5573/IEIESPC.2017.6.3.200.

[PTT06] P. T. Tin, T. T. Duy, T. T. Phuong and M. Voznak, "Secrecy performance of joint relay and jammer selection methods in cluster networks: With and without hardware noises,” Lecture Notes in Electrical Engineering, LNEE, Vol. 415, pp. 769-779, 2017. DOI: 10.1007/978-3-319-50904-4_78.

[PTT07] P. T. Tin, P. M. Nam, T. T. Duy, P. T. Tran and M. Voznak, “Throughput analysis of power beacon-aided multi-hop relaying networks employing non-orthogonal multiple access with hardware impairments,” in Proc. Of The 5th International Conference on Advanced Engineering - Theory and Applications 2018 (AETA 2018), LNEE, Vol. 554, Sep. 2018. ISBN 978-3-030-14907-9.

LIST OF RESEARCH RESULTS AND ACTIVITIES

Publication activities

I provide the following list indexed results in relevant scientific databases in order to document my research activities within the entire period of my doctoral study:

- **ORCID**: https://orcid.org/0000-0002-5793-4627
- **Research ID**: F-4786-2019
- **Articles** indexed in **Web of Science**: 7 articles in journals
- **Papers** in Conf. Proc. Indexed in **Web of Science**: 4 conference papers
- **Articles** indexed in **SCOPUS**: 6 articles in journals
- **Papers** in Conf. Proc. Indexed in **SCOPUS**: 2 conference papers
- h-index according to Web of Science: 2 (10 citations)
- h-index according to Scopus: 2 (16 citations)

Project memberships and participations

- In 2015–2018, a member of the WiCOM group at Ton Duc Thang University (TDTU), Wireless Communications Research Group, head of group: prof. Vozňák.
- In 2019, a researcher in the project "Networks and Communication Technologies for Smart Cities I", No. SP2019/41, conducted by Dr. Řezáč at VSB - Technical University of Ostrava.
- In 2018, a researcher in the project "Networks and Communication Technologies for Smart Cities I", No. SP2018/59, conducted by Dr. Řezáč at VSB - Technical University of Ostrava.
- In 2017, a researcher in the project "Networks and their Security, Modelling, Simulation, Knowledge Retrieval and Communication Technologies for Smart Cities", No. SP2017/74, conducted by prof. Vozňák at VSB-Technical University of Ostrava.

Results with a wider relation to the topic of the dissertation indexed in the Web of Science journals

1. T. N. Nguyen, T. H. Q. Minh, P. T. Tran, M. Voznak, T. T. Duy, T. L. Nguyen, P. T. Tin, "Performance enhancement for energy harvesting based two-way relay protocols in wireless ad-hoc networks with partial and full relay selection methods", Ad hoc Networks, vol. 84, pp. 178-187, 2018. (SCIE).
2. T. N. Nguyen, P. T. Tin, D. H. Ha, M. Voznak, T. P. Tran, M. Tran, T. L. Nguyen, "Hybrid TSR–PSR Alternate Energy Harvesting Relay Network over Rician Fading Channels: Outage Probability and SER Analysis", Sensors, vol. 18, no. 11, pp. 3839, 2018. (SCIE).
3. T. N. Nguyen, M. Tran, P. T. Tran, P. T. Tin, T. L. Nguyen, D. H. Hung and M. Voznak, "On the Performance of Power Splitting Energy Harvested Wireless Full-Duplex Relaying Network with Imperfect CSI over Dissimilar Channels", Security and Communication Networks, vol. 2018, Article ID 6036087, 11 pages, 2018. (SCIE).

4. P. M. Nam, D. T. Do, N. T. Tung and P. T. Tin, "Energy harvesting assisted cognitive radio: random location-based transceivers scheme and performance analysis", Telecommunication Systems, vol. 67, no. 1, pp. 123-132, 2017. (SCIE).

Other results indexed in Scopus, IEEE-Xplore, conference proceedings

1. P. T. Tin, T. T. Duy, "Power Allocation Strategies for Dual-hop Relay Protocols with Best Relay Selection under Constraint of Intercept Probability," ICT Express, First Online, 2018 (SCOPUS).
2. P. T. Tin, D. T. Hung, T. T. Duy and M. Voznak, "Security-Reliability Analysis of NOMA – Based Multi-Hop Relay Networks In Presence Of an Active Eavesdropper With Imperfect Eavesdropping CSI," Advances in Electrical and Electronic Engineering (AEEE), vol. 15, no. 4, pp. 591-597, Nov. 2017. (SCOPUS)
3. P. T. Tin, T. H. Q. Minh, T. N. Nguyen and M. Voznak, "System Performance Analysis of Half-Duplex Relay Network over Rician fading channel", Telkomnika, vol.16, no.1, pp.189-199, Feb. 2018. (SCOPUS)
4. P. T. Tin, T. H. Q. Minh, T. N. Nguyen and T. L. Nguyen, "A new look at energy harvesting half-duplex DF power splitting protocol relay network over Rician channel in case of maximizing capacity", Indonesian Journal of Electrical Engineering and Computer Science, vol.13, no.1, pp. 249-257, Jan. 2019. (SCOPUS)
5. P. T. Tin, L. A. Vu, T. N. Nguyen and T. L. Nguyen, "User selection protocol in DF cooperative networks with hybrid TSR-PSR protocol based full-duplex energy harvesting over Rayleigh fading channel: system performance analysis", Indonesian Journal of Electrical Engineering and Computer Science, vol.13, no.2, pp. 534-542, Feb.2019. (SCOPUS)
6. P. T. Tin, T. H. Q. Minh, T. N. Nguyen and T. L. Nguyen, "System performance analysis of hybrid time-power switching protocol of EH bidirectional relaying network in amplify-and-forward mode", Indonesian Journal of Electrical Engineering and Computer Science, vol.14, no.1, pp. 118-126, Apr.2019. (SCOPUS)
7. L. G. Thien, P. T. Tin, T. T. Duy and M. Voznak, "Performance Evaluation of Multi-hop Cooperative Transmission Protocol with Hardware Noises and Presence of Eavesdropper", The International Conference on Systems Science and Engineering 2017 (ICSSE 2017), Mar. 2017.
8. T. N. Nguyen, P. T. Tin, P. T. Tran, T. H. Q. Minh and M. Voznak, "Power-Splitting Protocol in Power Beacon-assisted Energy Harvesting Full-Duplex Relaying Networks: Performance Analysis", in Proc. Of 11th IFIP Wireless and Mobile Networking Conference (WMNC 2018), Praha, Czech Republic, Sep. 2018.
9. T. N. Nguyen, M. Voznak, P. T. Tran, T. H. Q. Minh, P. T. Tin, and T. L. Nguyen, "Outage Probability Analysis of Power Splitting Power-Beacon Assisted Energy Harvesting Relay Wireless Communication Networks", 2018 IEEE/ACM 22nd International Symposium on Distributed Simulation and Real Time Applications (DS-RT), Spain, 2018.