10-23-2015 12:00 AM

# Secrecy Enhancement in Cooperative Relaying Systems

Elham Nosrati, *The University of Western Ontario*

Supervisor: Dr. Xianbin Wang, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Master of Engineering Science degree in Electrical and Computer Engineering

# SECRECY ENHANCEMENT IN COOPERATIVE RELAYING SYSTEMS
(Thesis format: Monograph)

by

Elham Nosrati

Graduate Program in Electrical and Computer Engineering

A thesis submitted in partial fulfillment
of the requirements for the degree of
Masters of Science in Engineering

The School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

# Abstract

Cooperative communications is obviously an evolution in wireless networks due to its noticeable advantages such as increasing the coverage as well as combating fading and shadowing effects. However, the broadcast characteristic of a wireless medium which is exploited in cooperative communications leads to a variety of security vulnerabilities. As cooperative communication networks are globally expanded, they expose security attacks and threats more than ever. Primarily, researchers have focused on upper layers of network architectures to meet the requirements for secure cooperative transmission while the upper-layer security solutions are incapable of combating a number of security threats, e.g., jamming attacks. To address this issue, physical-layer security has been recommended as a complementary solution in the literature.

In this thesis, physical layer attacks of the cooperative communication systems are studied, and corresponding security techniques including cooperative jamming, beamforming and diversity approaches are investigated. In addition, a novel security solution for a two-hop decode-and-forward relaying system is presented where the transmitters insert a random phase shift to the modulated data of each hop. The random phase shift is created based on a shared secret among communicating entities. Thus, the injected phase shift confuses the eavesdropper and secrecy capacity improves.

Furthermore, a cooperative jamming strategy for multi-hop decode-and-forward relaying systems is presented where multiple non-colluding illegitimate nodes can overhear the communication. The jamming signal is created by the transmitter of each hop while being sent with the primary signal. The jamming signal is known at the intended receiver as it is according to a secret common knowledge between the communicating entities. Hence, artificial noise misleads the eavesdroppers, and decreases their signal-to-noise-ratio. As a result, secrecy capacity of the system is improved. Finally, power allocation among cooperative jamming and main signal is proposed to ensure that suggested scheme enhances secrecy.

**Keywords:** Cooperative communication, physical layer, secrecy

*"Do not worry about your difficulties in mathematics, I can assure you mine are still greater."*

*Albert Einstein*

# Statement of Co-authorship

The thesis presented here has been written by Elham Nosrati under supervision of Dr. Xianbin Wang. The material presented in chapter three has been published in the proceedings of international conference of communication 2015 (ICC 2015) as follows.

- Elham Nosrati, Xianbin Wang and Arash Khabbazibasmenj, "Secrecy Capacity Enhancement in Two-hop DF Relaying Systems in the Presence of Eavesdropper", Presented at IEEE ICC 2015 Communication and Information Systems Security Symposium ('ICC'15 (11) CISS'), London, UK.

The material presented in chapter four is currently under peer review for publication in IEEE 83rd Vehicular Technology Conference (VTC2016-Spring) as below.

- Elham Nosrati, Xianbin Wang, Arash Khabbazibasmenj and Auon Muhammad Akhtar, "Secrecy Enhancement via Cooperative Relays in Multi-hop Communication Systems", Submitted to IEEE 83rd Vehicular Technology Conference (VTC2016-Spring), Nanjing, China.

# Acknowledgment

First, I wish to express my sincere appreciation to my supervisor Dr. Xianbin Wang for his guidance, support, valuable advise and encouragement. I would like to thank Dr. Wang for giving me the opportunity to work under his supervision and be a member of his research team. Sincere thanks to the examining committee, Dr. Weiming Shen, Dr. Lyndon Brown and Dr. Girma Bitsuamlak.

Special thanks to Dr. Arash Khabbazibasmenj and Dr. Auon Muhammad Akhtar for their insightful hints and helpful discussions.

I would like to thank my husband, Ali, who is a source of unending support, for his understanding throughout the thesis process. Deep thanks to my brothers for their continuous support. I would like to specially thank Reza and Azar for giving me the home feeling since I came to Canada. Last but by no means least, I owe infinite thanks to my lovely parents. I am truly thankful beyond words to my parents for all love and encourage they gave me.

# Abbreviations

| | |
|---|---|
| **AF** | Amplify-and-forward |
| **AWGN** | Additive white Gaussian noise |
| **BBWC** | Bidirectional wiretap channel |
| **BCC** | Broadcast channel with confidential messages |
| **BS** | Base station |
| **CRN** | Cognitive radio network |
| **CSI** | Channel state information |
| **DDoS** | Distributed denial of service |
| **DF** | Decode-and-forward |
| **DoS** | Denial of service |
| **DSSS** | Direct sequence spread spectrum |
| **ESC** | Ergodic secrecy capacity |
| **FHP** | Frequency hopping pattern |
| **FHSS** | Frequency hopping spread spectrum |
| **LA** | Learning attack |
| **LTE** | Long-term evolution |
| **MAC** | Media access control |
| **MIMO** | Multiple-input and multiple-output |
| **MITM** | Man in the middle |
| **MRC** | Maximum ratio combining |
| **OSI** | Open systems interconnection |
| **PN** | Pseudo noise |
| **PUE** | Primary user emulation |
| **RIP** | Routing Information Protocol |
| **SS** | Spread Spectrum |
| **SSL** | Secure Sockets Layer |
| **SNR** | Signal-to-noise-ratio |
| **TDD** | Time Division Duplex |
| **TCP** | Transmission control protocol |
| **TLS** | Transport layer security |
| **UDP** | User datagram protocol |
| **UE** | User equipment |
| **WPA** | Wi-Fi protected access |
| **WSN** | Wireless sensor networks |

# Nomenclature

| | |
|---|---|
| $E\{.\}$ | Mathematical expectation |
| $P(.)$ | Cumulative distribution funtion |
| $p(.)$ | Probability density funtion |
| $Pr.(.)$ | Probability |
| $[x]^+$ | $\max\{0, x\}$ |

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction to Security of Wireless Communications

Wireless communication is one of the most important achievements of mankind since it provides transmission of information over faraway nodes without requiring the wires. Long-distance radio transmission was invented by Guglielmo Marconi in 1901 [1]. Since then, many advantages of wireless communications have facilitated humans life. For example, the mobility of wireless communications provides services for the users in almost anywhere and increases the coverage. It can be in a mall, in an airport or in a park. Interestingly, the *no-wired* nature of wireless communications, makes it very convenient for using, compared to the wired systems in which a cable is always required while the length of the cable could be a major concern. Moreover, the wireless systems are capable of providing service for a large number of users. For example, it is expected that by 2020, and the time that 5G will be deployed, there is a larger number of cellphone subscribers in the world such that each macro-cell must serve up to 1000 subscribers [2]. In addition, wireless communication systems have cheaper installation and maintenance costs compared to the terrestrial communications in which not only all paths must be wired, but also changes in the cabling plan involve additional fees.

On the other hand, the widespread users of wireless communications are now suffering from security issues more than ever. For instance, in early 2015, a cyber security consultant claimed that he was able to control the aircraft engine by connecting to the onboard wifi [3]. Moreover, lack of security in the applications installed on cellphones has been frequently exploited by hackers to track users and access their information. Therefore, it can be said that although the broadcast nature of wireless medium, which reverts back to radio propagation, eases human lives, it intensively introduces many security vulnerabilities and issues. Hereon, it must be pointed out that unfortunately the ever increasing rate of wireless communication deployments and applications on one side, and the rate of corresponding security solutions on the other side, are not matched. Thus, this noticeable gap needs to be addressed. However, the wired systems are not impacted by the security issues as much as the wireless systems because of their closed architecture. In this chapter, due to the importance of security in wireless communication systems, the objective is to study the background and the basis of the security in wireless communication systems.

## 1.1 Background of Security in Wireless Communications

Availability of wireless medium, which is utilized by wireless communication systems, has led to a variety of security risks and threats. It is vital to enhance the security of wireless communications since it is very easy for eavesdroppers to overhear wireless signals that are transmitted in the air.

The key concepts of wireless communications security is classified into four categories which each attack usually intends to threaten one or more categories. Thus, it is necessary to be aware of associated principals to provide security solutions and protect systems against attacks. Thereby, the principals of the security of wireless communication systems are presented as following.

### 1.1.1 Authentication and Non-reputation

The goal of authentication process is to confirm the identity of message transmitter. In general, prior to any data transmission, mutual authentication between communicating parties is required. Authentication via exclusive media access control (MAC) address is maybe the most common technique in today's networks. However, other layers may also be involved in the authentication. For example, user name and password can be exploited as authentication tools in the application layer [4]. Moreover, non-reputation is used to ensure that neither the source nor the receiver of the message can deny communication occurrence. In this regard, digital signatures are adopted where any node has its exclusive fingerprint which reveals its identity [5].

### 1.1.2 Confidentiality and Access-control

The confidentiality strategies are set to protect the information from disclosure by illegitimate entities. Primarily, cryptography and encryption techniques have been utilized in upper layers of protocol stack to provide confidentiality. Recently, other methods such as cooperative jamming have also been proposed to achieve this goal [4]. It must be pointed out that some attacks aim at analyzing network traffic to obtain certain information, e.g., transmission frequency, or spatial location of the nodes. Thus, *access control* mechanisms are employed to define a diverse level of access for different entities. Notably, because of broadcast characteristic of the wireless medium there are many obstacles to provide a comprehensive access-control strategy [5].

### 1.1.3 Data Integrity

Data integrity is to ensure that the received data has not been altered or modified during data transmission. It is significantly important to detect any alternation or manipulation in the data packets with the least amount of latency and false alarm rate. Man in the middle (MITM) attacks may target the data integrity as they overhear the communication and they may set up new communication routes and insert corrupted packets [4].

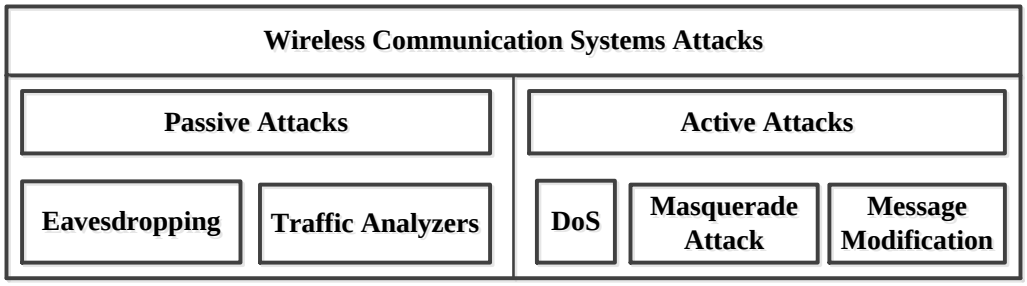


Figure 1.1: Common wireless communication systems passive and active attacks

### 1.1.4 Availability

Ensuring that legitimate entities can access the network and have a robust communication is termed *availability* [5]. For instance, denial of service (DoS) and distributed denial of service (DDoS) attacks (i) may target the availability of a network, (ii) occupy the network resources; and (iii) result in denial of service for authorized nodes.

Notably, the aforementioned security requirements (availability, authentication, non-reputation, data integrity, confidentiality and access control) are complementary to secure wireless communications. In other word, they must be provided simultaneously to ensure that the communication is secure.

## 1.2 Attacks Classification in Wireless communication Systems

In this section, attacks of wireless communication systems are classified based on their active and passive behaviors, as seen in Fig. 1.1.

### 1.2.1 Passive Attacks

Passive attacks only monitor and analyze traffic. The main passive attacks are as following.

#### Passive Eavesdroppers

Passive wiretappers, also known as passive eavesdroppers, are a type of passive attacks which overhear the communication while they are not capable of any alternation or modification of the transmitted message [6]. The illegitimate nodes can overhear the communication and target the confidentiality of the messages as seen in Fig. 1.2. This attacks is called passive eavesdropping attack or wiretapping attacks in the literature.

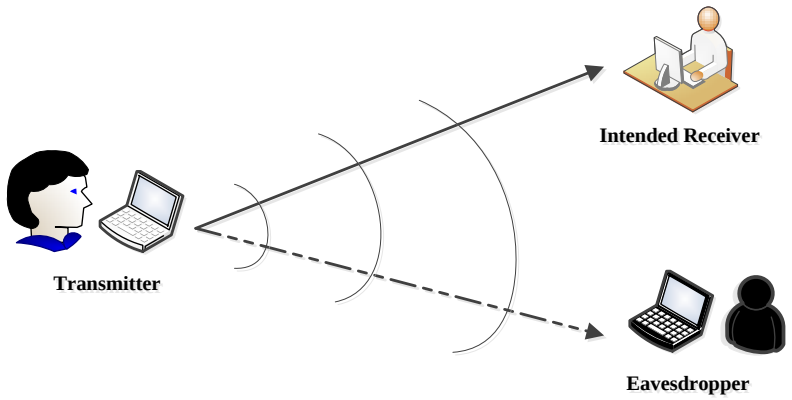


Figure 1.2: Wiretapping attack

#### Traffic Analyzers

Traffic analyzers are another group of passive attacks which do not make any modification in the message, but they are able to reveal sensitive information by analyzing the traffic, e.g., transmission frequency, or spatial location of the communicating parties, or session length and identities of source/receiver [5].

### 1.2.2 Active Attacks

Active attacks are a category of attacks which are capable of making modifications and changes in messages. For example, they are able to delete a certain message and add to the other. The most common active attacks are as follows.

#### Denial of Service Attacks

Some attacks try to use network resources so the network can no longer serve the authorized nodes. This type of attacks are called denial of service attacks in the literature and they can take place at different layers of the protocol stack. Distributed denial of service attacks are a more severe type of DoS attacks. In DoS attacks, one device and one connection is exploited by the attack to threat the victim. Whereas, in DDoS attacks, multiple devices, computers and connections are exploited by the attack for threatening the victim node.

#### Message Modification

Message modification includes any change, alternation, deletion or addition of the original message [5].

### Masquerade Attacks

There are cases in which illegitimate entity exploits a fake or forged identity so the network considers it as an authorized entity and therefore it can misuse network resources [5]. This type of attack is called masquerade attack in the literature.

## 1.3 Security Threats from OSI Layers Perspective

Examining current issues in wireless communication systems reveals that different security threats are targeting different layers of communication systems. At this point, major security threats of different layers of the open systems interconnection (OSI) are briefly reviewed.

- Physical layer is vulnerable to security issues due to the accessibility of wireless medium by unauthorized entities. For example, eavesdropping attacks are one of the physical layer attacks. In other cases, active attacks drop down the communication signal by overwhelming the bandwidth via jamming signals. This attack is termed jamming attack [5].

- In the context of the MAC layer attacks, there are attacks such as MAC spoofing and MAC address theft which target the authentication procedure. Denial of service attacks and man in the middle attacks may also target the MAC layer [7], [8]. In particular, MITM attacks may be the active eavesdroppers and send the threat packets via setting up connections to their victims, while the communicating parties are supposed to communicate directly. Another group of MAC layer attacks generate numerous number of MAC addresses per minute such that MAC address table of the victim device is overwhelmed [9].

- IP spoofing, routing attack and packet sniffing are targeting the network layer. IP spoofing can be via either forging or falsifying the packet's IP addresses such that the receiver cannot access the true IP address of the packet's source. Routing attacks damage routing protocol by: (i) eliminating certain routes, (ii) advertising routes to the nodes which does not exist, (iii) updating the routing tables with faulty tables, etc. Moreover, packet sniffing is a network layer attack which can access the confidential information via analyzing network traffic [10], [11].

- Transport layer uses either transmission control protocol (TCP) or user datagram protocol (UDP). TCP is termed after a *connection-oriented* protocol in which the transmitter can ensure the receipt of the message by the receiver via an acknowledge message. On the contrary, UDP protocol is *connectionless* where the packets are only sent, and therefore, the transmitter cannot ensure about the reliability of the communication. However, UDP protocol has less latency and network overheads, compared to TCP protocol. Flooding attacks can exploit the TCP protocol via sending numerous packets to a target and consuming the victim's resources as the target receives the flooding packets and needs to send the acknowledgement messages [12]. Similarly, flooding UDP packets can threat the transport layer by sending a large number of UDP packets while target's

resources are consumed by the attack and cannot serve the legitimate nodes. Notably, flooding attacks usually result in denial of service [13], [14].

- Regarding the application layer, viruses, worms and trojan horse are the most well-known attacks. Technically speaking, a virus is attached to a program or a file and travels from one device to the other once the user transfers files or installs programs. Viruses spread the infections and the threats. Similarly, worms also travel from a device to another, but the user is not involved. Trojan horse is a malicious software which initially is seen as a helpful and interesting program to convince the user for installation. Blended threats are a combination of viruses, worms and trojan horse attacks that cause severe threats. DDoS are also a common application layer attack [15], [16].

Table 1.1 summarizes the common attacks of different layers of the OSI model.

Table 1.1: Layered overview of wireless systems attacks

| OSI Layer | Sample Attacks |
|---|---|
| Physical layer | Wiretapping attack, jamming attack |
| MAC layer | MAC address spoofing, identity theft, DoS, MITM, MAC flood |
| Network layer | IP spoofing, routing attack, packet sniffing |
| Transport layer | UDP flooding attacks, TCP flooding attacks, DoS |
| Application Layer | Viruses, worms, Trojan horse, blended threats, DDoS attacks |

## 1.4 Overview of Security Improvement: From a Layered Networking Architecture Perspective

In this section, various security enhancement mechanisms from a layered networking architecture perspective are reviewed. Herein, physical layer security is confined to a brief introduction whereas detailed technical discussion is referred to chapter 2. It is obvious that different networking layers are threatened by security attacks and in today's security enhancement approaches, most layers are involved. Such an approach mainly includes the upper layers of the protocol stack, except the physical layer.

Only recently, there has been a growing interest in security enhancement techniques via physical layer [17]. However different methods can be simultaneously used to achieve the most promising results. For example, authentication of users can be realized via exploiting various authentication methods such as MAC address authentication or plain password authentication. On the other hand, a number of security methods have enhanced security through involvement of multiple OSI layers. For instance, a secret key for cryptography purposes can be generated based on the physical characteristics of the communication parties or the medium involved, e.g., the reciprocal channel.

*Cryptography* techniques adopt primarily mathematical tools and secret keys to secure the communication systems against illegitimate entities. The main objective of cryptography is providing data confidentiality, data integrity, authentication, and non-repudiation through different networking layers. To this end, *public and private key* cryptography are introduced

which are also, respectively, termed as *asymmetric and symmetric key* cryptography. In symmetric key cryptography, similar keys are adopted for encryption and decryption purposes. Whereas, in asymmetric key cryptography, public key is exploited to encrypt a message and the message can only be decrypted by the specific related private key [4]. Using initial upper-layer cryptography techniques, one error in the received plain text results in plenty of errors in the decrypted plain text. Thus, in more recent studies, advance encryption standard (AES) and turbo coding are combined because turbo coding is capable of error correction. Cryptography at physical layer can be through spread spectrum (SS) techniques which are further studied in chapter 2.

The physical layer attack scenarios are mainly based on the existence of the eavesdropper which tries to wiretap the transmission. In order to overcome this issue, friendly jamming, information-theoretic security, beamforming and diversity techniques or combined methods have been proposed in the literature. Jamming attacks are the other types of the threats to the physical layer security and it has been suggested to use spread spectrum techniques to impair them [18], [19]. More recent works have proposed authentication techniques which are based on the physical layer approaches.

In the context of MAC layer and to prevent MAC flooding attack, it is possible to make certain restrictions for each port in the sense of limiting the number of MAC addresses to be received from each port. Another alternative solution is using fixed MAC Addresses although this solution is not applicable in large scale networks [20], [21].

Wi-Fi protected access (WPA) and Wi-Fi protected access 2 (WPA2) are the two extensively utilized authentication protocols in the networking layer. Furthermore, the second version of Routing Information Protocol (RIP-V2) has been presented to prevent the a group of routing attacks. In order to prevent packet sniffing, cryptographs techniques are used [20], [21]. In addition, certain software and hardwares are already in the market as *anti-sniffers* (e.g., Kitty-Litter The Anti-Sniffer)[22].

To secure the transport layer, transport layer security (TLS) and secure sockets layer (SSL) have been utilized which in essence are cryptographic protocols to secure the transmission. Username and password can be used in the application layer to enhance the security as it is very common to have different user name and passwords for different applications and sometimes an application requires multiple passwords.

## 1.5 Motivation of the Thesis

Cooperative communications via relay nodes has been considered as an interesting solution in communication systems where reliable direct transmission between source and intended destination is not possible. The principle of cooperative communication reverts back to [23] where capacity analysis of a two-hop communication system was devised. However, deployment of relays in communication systems has been growing continuously and it has spread to Wimax and cellular communications [24]. To be more precise, the standardizations of 3GPP LTE-Advanced, IEEE 802.16j, and IEEE 802.16m already contain relay-based communications [24].

Relaying communication is specified by cooperation strategies which is termed as *relaying protocols* in the literature, e.g., amplify-and forward (AF), decode-and-forward (DF),

compress-and-forward [24]. Many existing studies have compared the relaying strategies based on reliability performance parameters [25]-[27]. Taking another point of view, some recent works have studied cooperative communications from secrecy perspective [28]-[30]. Accordingly, the notion of *collaborative secrecy* was introduced where the relays have the potential to secure the communication. Following this idea, relays have been used as cooperative nodes to improve the secrecy via performing different roles. Towards this goal, upper-layer security techniques have been widely studied in the literature while physical layer techniques are complementary schemes to obtain better results. For example, Multiple-input and multiple-output (MIMO) relays are used to reduce the received SNR at the unauthorized entities [28],[31]. Herein, the focus of this thesis is on physical layer cooperative roles of the relays in order to improve the security.

One of the main intuitions behind this work is that many communication entities such as amplify-and-forward relays, repeaters and wireless sensor networks are not capable of handling complex security methods due to their hardware limitations. Therefore, physical layer security can be adopted in these systems to secure the communication. Moreover, in some cases communication is only through lower layers of the protocol stack (e.g, communication via repeaters). Thus, physical layer security flourish as a prominent security improvement technique.

In the context of collaborative relaying, cooperative jamming has been widely studied where relays can be utilized as temporary jammers to create intentional noise at the adversary node to enhance security [32]-[34]. However, this technique has a number of disadvantages. First, cooperative jamming strategies require additional node to generate the jamming which is expensive in terms of hardware. Furthermore, conventional cooperative jamming strategies increase the complexity since network overheads increase for the purpose of providing coordination between the helper and the main network. Hence, there is a need to provide alternative solutions which overcome the aforementioned shortcomings.

## 1.6 Research Objectives

The objectives of the current work are summarized as below.

- The first goal includes the followings: (i) to comprehensively study the physical layer security of cooperative communication systems in terms of security attacks, (ii) to investigate existing security improvement techniques, and (iii) to address advantages or shortcoming of current solutions. This primary goal is a guide to further provide security improvement schemes.

- The second objective is to provide a novel solution for two-hop communication systems which rectifies the shortcomings of conventional cooperative jamming strategies.

- The third goal is to present a cost-effective and energy-efficient security enhancement solution for multi-hop communication systems where power consumption and complexity considerations are well noted.

## 1.7 Contributions

Major contributions of this thesis, based on the proposed security solutions for cooperative communication systems in chapter 3 and 4, are stated below.

- In chapter 3, a two-hop DF relaying systems is presented where communication takes place in the presence of an external eavesdropper which can intercept the communications of both hops. Considering this system model the following results are obtained: (i) A novel security solution is proposed which exploits the randomness of the channel between the communicating parties and introduces a phase shift to the modulated data such that the adversary node is not aware of it. It is proven that the proposed scheme can increase the secrecy capacity of the system by degrading the received SNR at illegitimate entities. (ii) Secrecy performance analysis of the system model is presented. (iii) It is shown that increasing the transmit power can have *harmful or helpful* impact on secrecy, depending on where the eavesdropper is located. For instance, it is demonstrated that if the eavesdropper is an adjacent neighbor to the transmitter, raising the transmit power results in more leakage of the signal to the illegitimate entity and therefore secrecy of the system is degraded.

- In chapter 4, a multi-hop DF relaying system is considered where there exist multiple non-colluding eavesdroppers. The contributions related to this system are stated at this point: (i) Inspired by [35], a new way of using cooperative jamming is extended to the aforementioned system to enhance the secrecy. In the proposed strategy, on the contrary with traditional cooperative jamming, extra helper is not needed and the transmitter creates the intentional jamming. (ii) Secrecy performance of the aforementioned system is analyzed. (iii) Power allocation strategies are presented to improve the security by optimally allocating the power to the friendly jamming and the primary signal. It is illustrated that using the optimal power assignment boosts the ergodic secrecy capacity. (iv) It is shown that diverse parameters impact the optimal power allocation factor among which channel state information (CSI) of the adversary nodes must be noted particularly. (v) Since accessing the CSI of the adversary nodes may not be feasible in many cases, the sub-optimal solution is given which does not require the CSI of the adversary nodes. The sub-optimal solution can be considered as close bound for the optimal solution if the illegitimate entity is close to the transmitter.

## 1.8 Thesis Outline

This thesis is organized as follows:

In chapter 2, the importance and advantages of physical layer security are studied. Secrecy performance criteria in the physical layer are introduced and defined in this chapter. Next, Physical layer attacks are examined. Then, a literature survey on the earlier physical-layer security strategies is provided where cooperative jamming, information-theoretic security, diversity, beamforming and spread spectrum are reviewed. Later on this chapter, the study is focused on a specific security case, where the relay node is not trusted but it is required to have the relaying role. This chapter is finished with using the physical layer in practical wireless communication

networks such as ad-hoc networks, cognitive radio networks, cellular networks, and wireless sensor networks.

In chapter 3, secure communication in a two-hop communication system is investigated where the relay employs decode-and-forward protocol. Analysis of secrecy performance of the system model is presented where closed-form expressions of the probability of outage in secrecy capacity and probability of non-zero secrecy capacity are calculated. Then, a random phase shift scheme is presented which improves the secrecy capacity. Finally, simulation results are given which validate the theoretical contributions.

Chapter 4 is focused on the security of a multi-hop cooperative communication systems where the relays adopt decode-and-forward strategy and there are multiple illegitimate wiretappers. First, the security analysis of the system model is given. Next, the new artificial noise strategy is presented to degrade the received SNR at the illegitimate nodes, and increase the secrecy. Due to particular importance of power allocation between the friendly noise and the primary signal, power allocation solutions are proposed. Lastly, simulation results are presented to evaluate the capability of the proposed strategy to improve secrecy.

In chapter 5, the main conclusions of the thesis is summarized also potential directions for future work are suggested.

# Chapter 2

# Physical Layer Security

Using the OSI model as a reference model, security measures to protect the user's data normally takes place at the upper layers such as presentation layer. These security measures are a family of various encryption techniques including symmetric and asymmetric cryptography. The focus on upper layer security resulted in the abandonment of lower layer, physical layer, security features [35]. However, a specified level of secrecy is needed in physical layer to further utilize upper-layers security schemes [35]. Also, one cannot claim any contradictions between employing the upper-layer and physical-layer security techniques. Therefore, different layers security techniques can be adopted concurrently as they are complementary to each other. Accordingly, the combination of different levels security solutions (such as physical layer, network layer and link layer) have been investigated in recent studies [35]. In this regard, the concept of *cross-layer security* has been used to indicate the aforementioned collaboration of the layers for the purpose of security improvement [35], [36].

Physical layer security was pioneered in [37], [38] and [39]. However, more recently the interest in physical layer security was revived in the 1990s [40]. Physical-layer security schemes may be based on information theoretic techniques ([38], [41]-[42]), cooperative jamming ([43]-[45]) or diversity and beamforming approaches ([46]-[48]). In addition, combining multiple physical-layer security techniques have been used in the literature, e.g., using cooperative jamming and beamforming jointly to secure the communication [28]. In this chapter, physical-layer secrecy performance criteria are defined. Next, physical layer eavesdropping is examined. Finally, main existing security improvement approaches in physical layer for cooperative relaying systems are investigated.

## 2.1 Secrecy Performance Parameters

In this section, the parameters of secrecy performance which are examined as the secrecy criteria in the literature are introduced.

### 2.1.1 Secrecy Capacity

The fundamental metric of secrecy is termed *secrecy capacity* which is maximum achievable secrecy rate of the system and reflects maximum transmission rate from source to desired des-

tination while eavesdropper is not able to access transmitted data and decode it. This definition is formulated as the following [17, p. 62]

$$C_s = [C_m - C_w]^+, \tag{2.1}$$

where $C_m$ is the capacity of the main link and $C_w$ denotes the capacity of the illegitimate link that are, respectively, defined by

$$C_m = log_2(1 + \gamma_{sd}), \tag{2.2}$$

$$C_w = log_2(1 + \gamma_{se}), \tag{2.3}$$

in which $\gamma_{sd}$ and $\gamma_{sd}$ denote the instantaneous received SNR at the intended receiver and the illegitimate entity, respectively. Therefore, based on equation (2.1), it can be said that increasing the received SNR of the main link or decreasing the received SNR of the illegitimate link both result in improving the secrecy capacity. Accordingly, security of the communication system has been investigated considering instantaneous SNR of the legitimate and illegitimate links to examine under which conditions positive secrecy capacity is achievable [49], [50].

### 2.1.2 Probability of Non-zero Secrecy Capacity

Probability of existence of a positive secrecy capacity, also termed as *probability of non-zero secrecy capacity*, is an alternative secrecy performance parameter for communication over fading channels which is given by

$$Pr[C_s > 0] = Pr[C_m > C_w]. \tag{2.4}$$

### 2.1.3 Probability of Outage in Secrecy Capacity

*Probability of outage in secrecy capacity*, (also known as secure outage probability, i.e., SOP) indicates the likelihood of obtaining a target secrecy rate. SOP is one of the common secrecy performance criteria for communication over fading channels when there is an eavesdropper to intercept communication. This secrecy performance parameter is formulated as

$$P_{out}(R_t) = Pr[C_s < R_t], \tag{2.5}$$

where $R_t$ is the desired target secrecy rate. The outage in (2.5) can occur in any of the following cases:

- Unreliable communication which is the case where the intended receiver cannot decode a message.
- The eavesdropper is able to overhear a portion of the transmitted message.

It is worth saying that a new definition of secrecy outage has been recently pioneered in [51]. The main concern of the authors of this work is that definition (2.5) takes into account both reliability and security so any distinction between reliable communication and secure transmission cannot be recognized. The authors believe that such a definition suffers from

a shortcoming as the related outage questionably refers to the secrecy, and it may be due to reliability issues. For example, if the channel between the source and the intended destination is very weak, the transmitter is likely to delay the transmission. Considering definition (2.5), this delay will be an outage whereas transmission has not occurred. To rectify this shortcoming, the work presented in [51] has suggested another definition for the probability of outage in secrecy capacity which is formulated as

$$P_{out}(R_t) = Pr[C_w > R_b - R_t | MessageTransmission], \tag{2.6}$$

where $R_b$ denotes transmission rate of the codewords. This new definition (2.6) has the following advantages:

- It considers design parameters such as $R_b$.
- Unlike equation (2.5), in (2.6) message transmission is an initial condition of the secure outage definition.

It must be pointed out that continuous transmission may happen in the case where the transmitter is not aware of the destination's channel. Herein, the outage can be formulated as $P_{out}(R_t) = Pr[C_w > R_b - R_t]$ [52]. On the other side, if the destination channel is available, the transmitter is able to have a more proper design and to designate transmission or suspension mode, in addition to choosing the appropriate transmission rate. The aforementioned design can significantly enhance the security by degrading the probability of outage in secrecy capacity. However, SOP has been mentioned as a more worthwhile secrecy criteria compared to secrecy capacity in the literature [53].

### 2.1.4 Ergodic Secrecy Capacity

*Ergodic secrecy capacity* (ESC) indicates the average of secrecy capacity and it is formulated as [52]

$$\overline{C_s} = E\{C_s\}. \tag{2.7}$$

## 2.2 Multiple Eavesdroppers

Communication between source and destination can take place in the presence of an eavesdropper. In a more complicated case, as seen in Fig. 2.1, multiple eavesdroppers can overhear the communication. Multiple eavesdropping can be studied under two categories explained as below.

### 2.2.1 Non-colluding Eavesdroppers

In the case of non-colluding eavesdropping, there are multiple wiretappers to overhear the communication and received SNR of the illegitimate link is assumed to be the maximum of the received SNR of eavesdroppers. In other words, the illegitimate entities are mutually independent. Therefore, the received SNR is denoted by [54], [55]

$$\gamma_e = \max_{m=1}^{M} \gamma_{e_m}, \tag{2.8}$$

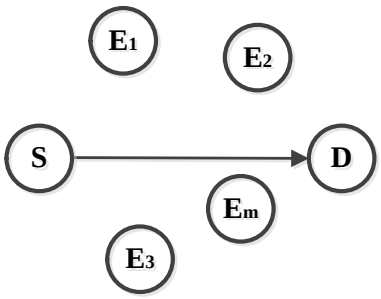


Figure 2.1: Communication in the presence of multiple eavesdroppers.

where $\gamma_{e_m}$ is the received SNR of the $m$th eavesdropper.

### 2.2.2 Colluding Eavesdroppers

In the case of colluding eavesdropping, there are multiple eavesdroppers to intercept the communication and the received SNR of the illegitimate link is the summation of the received SNR of eavesdroppers. Thus, the above relationship is reformulated as [56], [57]

$$\gamma_e = \sum_{m=1}^{M} \gamma_{e_m}. \tag{2.9}$$

## 2.3 Active and Passive Eavesdropping

Physical layer attacks can be investigated considering the capabilities that are considered for the illegitimate entities. Illegitimate nodes may have several goals. Initially, observing and monitoring communication signal to overhear the main information is one goal pursued by the attacks. From this stage forward, the attacks are categorized based on their active and passive behaviors.

### 2.3.1 Passive Attacks in the Physical Layer

Passive eavesdroppers (also known as radio eavesdroppers) are capable of monitoring the signals to detect the main transmission, decode and analyze it. Although this group of attacks are able to access the main transmission, they cannot interfere with the channel, and make any changes or modifications. Since passive attacks are silent and they do not make any apparent changes or modification, it is difficult to detect them.

### 2.3.2 Active Attacks in the Physical Layer

On the contrary, active attacks are capable of monitoring the transmission in addition to making changes and modifications to the channels, nodes and communication sessions. For example, active attacks can eliminate certain legitimate messages, modify the messages or insert faulty messages. Researches in the field have focused on different capabilities of active attacks. The authors of [58] considered the case where the active eavesdropper was a registered entity of

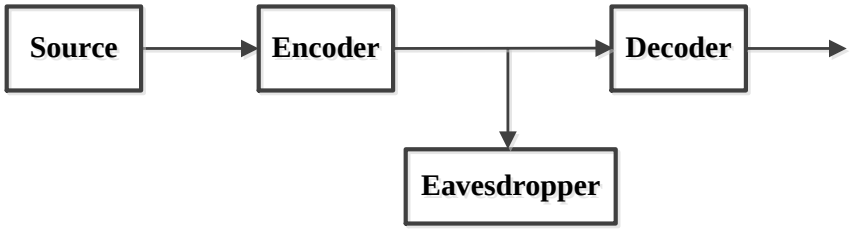


Figure 2.2: Wire-tap channel.

a cellular network and it could send signaling messages to the base station. Jamming the transmission between the source and the intended receiver via the eavesdropper was studied in [59]. Secure transmission of TDD multicell multi-user massive MIMO systems was examined in [31] where the eavesdroppers were active, and aimed at ruining channel estimation of the legitimate nodes. In addition, DoS attacks can threaten the network though different layers of the protocol stack including physical layer where the radio frequency jamming can jam the main transmission; therefore, the network cannot serve the legitimate users [5].

Note that although active eavesdroppers can significantly reduce the secrecy performance of communication systems but it is mostly easier to detect them, compared to the passive attacks, due to the silent nature of passive attacks.

## 2.4 Physical Layer Security Techniques

In this section, different physical-layer security techniques and schemes are explained through a classification that includes the following categories: information-theoretic security, beamforming techniques, artificial noise strategies, diversity approaches, coding techniques and exploiting channel characteristics for secrecy.

### 2.4.1 Information-theoretic Security

Wyner is a pioneer in the area of information-theoretic security due to his investigation of a channel model in the existence of an eavesdropper. This channel model is also known as a *wiretap channel* and is shown in Fig. 2.2 [37].

Wyner considered a discrete memoryless wire-tap channel where the information was transmitted from a legitimate node (called Alice) to an intended receiver (called Bob). The communication occurred in the presence of an illegitimate entity (called Eve) which wiretapped the channel between legitimate communication parties. The main goal is to maximize the transmission rate from the transmitter to the destination such that leakage of the information to the illegitimate entity is the least. Moreover, Shannon has first introduced the term of *perfect secrecy* in [38]. The results of these studies were later broadened to a Gaussian wire-tap channel [39], and the term *secrecy capacity* was introduced.

It must be pointed out that secure communication over fading channels are significantly important as they are helpful to analyze many practical scenarios [17]. To this end, *communication over fading channels* have attracted many researchers ( [50], [64]-[65]) as the channels

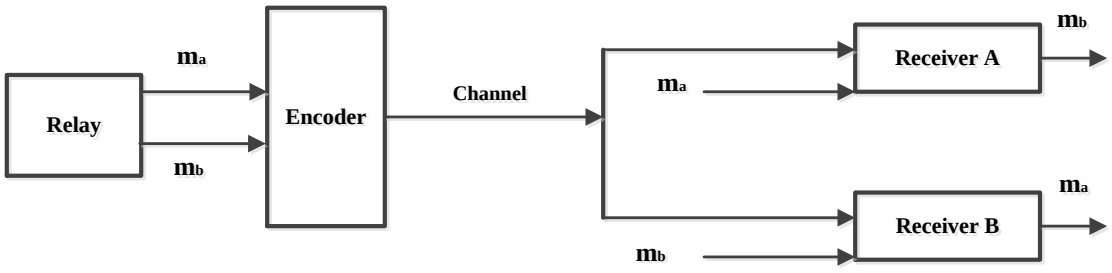


Figure 2.3: Exploiting side information in BBWC.

vary over time and it is not always possible to have access to the instantaneous channel state information (e.g., because of limited bandwidth [63]). Time-varying fading may limit the security of wireless communication systems [60]. Thus, MIMO antennas and diversity techniques were suggested to rectify this issue and enhance the secrecy [61], [62]. Also, the results of secure communication over fading channels showed that , unlike communication over Gaussian channels, a non-zero secrecy capacity is achievable even if the average SNR of the legitimate link is less than the average SNR of the illegitimate link. The reason is because fading can be beneficial in terms of secrecy such that instantaneous SNR of the main link is higher than the instantaneous SNR of the illegitimate link [50]. Furthermore, illegitimate entities can be equipped with multiple antennas to combat fading effects [61], [66].

In the year 1978, the authors of [36] have assumed a channel in which there were two receivers indicated by receiver A and receiver B, and two message types as the following.

- *Common message:* to be received by receiver A and B.
- *Confidential message:* to be received only by receiver A.

This channel was called the *broadcast channel with confidential messages (BCC)*, and since then it has been the subject of interest for many researcher. Other works have made some modifications in the aforementioned scenario and changed it to the case where there is one confidential message per receiver [67].

Following this path work, secrecy in *bidirectional wiretap channel (BBWC)* was introduced by the authors of [68]. This scenario in essence was a two-way communication system via an intermediate DF relay in the presence of an illegitimate entity. In this scenario, Node A intended to send the confidential message $m_a$ to the receiver B, and Node B intended to send the confidential message $m_b$ to the receiver A, where there was an eavesdropper which could overhear the communication. The intuition behind the presented approach is that each message can be exploited only once as a secret key to decode the other message, as seen in Fig. 2.3.

In particular, the intermediate relay can encode the two messages using the XOR operator; therefore, the coded message is given by [68]

$$\widetilde{m} = m_a \otimes m_b. \tag{2.10}$$

The coded message $\widetilde{m}$ is then sent to both receiver A and receiver B. Next, the receivers apply their original messages, termed *side information*, to decode the received message. Accordingly, the received message at receiver A is given by

$$\widetilde{m} \otimes m_a = m_a \otimes m_b \otimes m_a = m_b, \tag{2.11}$$

Similarly at receiver B, the message is as

$$\widetilde{m} \otimes m_b = m_b \otimes m_a \otimes m_b = m_a, \tag{2.12}$$

Finally, it is concluded that each of the receivers securely attain their corresponding message.

### 2.4.2 Secure Communication via Beamforming

Beamforming security approaches are based on a technique in which the main signal is sent in the desired direction such that the destination signal strength is enhanced while the illegitimate entity's received SNR is minimized. Accordingly, the received SNR of the legitimate entity is increased, but the the received SNR at the adversary node is degraded so the secrecy capacity of the system is improved. The problem of optimal beamforming to maximize the achievable secrecy rate in a dual-hop DF relaying system with the assumption of limited power constraints was studied in [69]. This work has assumed that perfect channel state information is known while this assumption is not applicable in many scenarios. Following this pathwork, the work presented in [70] has devised the beamforming for a MIMO wiretap channel where only the legitimate channels' CSI is available, but the CSI of the illegitimate node is not known. This work later extended its contributions to the sub-optimal solutions where the perfect CSI of the main link even was not available and channel estimation error was involved.

### 2.4.3 Artificial Noise

Artificial noise (AN), also known as cooperative jamming (CJ), is based on an intentional jamming signal created by legitimate helpers to confuse the eavesdropper. Consider Fig. 2.4, where the source wants to communicate with the destination in the presence of an eavesdropper. Because of the broadcast characteristic of radio propagation, the eavesdropper can wiretap the main signal so the received SNR at the illegitimate node is given by

$$\gamma_{se} = \frac{P_s \mid h_{se} \mid^2}{\sigma^2}, \tag{2.13}$$

in which $P_s$ indicates the transmit power of the source, $h_{se}$ is the channel from the source to the eavesdropper and $\sigma^2$ is the noise variance. Next, the controlled interference is created by the jammer, denoted by $J$, to mislead the eavesdropper while the desired receiver is not affected by the artificial noise. Accordingly, the eavesdropper received SNR is degraded as

$$\gamma_{se_{AN}} = \frac{P_s \mid h_{se} \mid^2}{\sigma^2 + P_j \mid h_{je} \mid^2}, \tag{2.14}$$

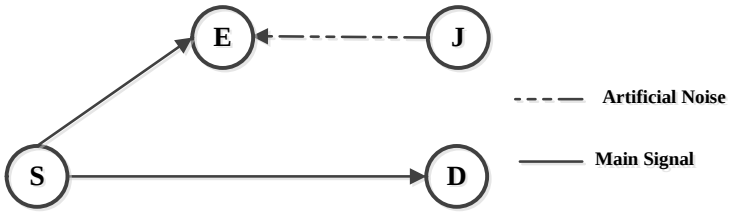


Figure 2.4: Conventional artificial noise.

where $P_j$ denotes the jamming power and $h_{jse}$ is the channel from the jammer to the eavesdropper. Comparing equations (2.13) and (2.14) shows that received SNR at the illegitimate entity is degraded. Hence, it can be concluded that secrecy capacity of the system is improved.

Artificial noise first was suggested in [71] to improve achievable secrecy of a communication system. This work showed that it is possible to obtain a positive secrecy capacity in a communication system where the illegitimate entity is closer to the transmitter compared to the intended receiver, via employing cooperative jamming. Following this framework, a number of cooperative jamming criteria including *jamming coverage* and *jamming efficiency* were introduced in [6] , where the parameter $\Delta SOP$ is defined as

$$\Delta SOP = \frac{SOP_{w/oAN}}{SOP_{AN}}, \tag{2.15}$$

in which $SOP_{w/oAN}$ and $SOP_{AN}$, respectively, denote the probability of outage in secrecy capacity without and with using artificial noise. The intentional interference can be classified into helpful and harmful jamming if $\Delta SOP \geq 1.00$ and $\Delta SOP \leq 1.00$, respectively. Using spatial sampling, jamming coverage is the total area of the helpful jamming. If a certain two-dimensional area is denoted by $A$ where the eavesdroppers can be located in $(x_e, y_e) \in A$, jamming efficiency represents the average of $\Delta SOP(x_e, y_e)$. Moreover, jamming strategies for the cases where the eavesdropper channel state information was or was not available were presented in [6]. The effect of using multiple jammers for the purpose of secrecy enhancement was also investigated, and the results showed that jamming coverage and efficiency could increase via using multiple jammers [6]. The same reference reported that increasing the transmit power can be harmful in terms of secrecy due to the closeness of the adversary nodes to the legitimate nodes. To be more specific, jamming close to the intended receiver needs accurate channel state information which is not necessarily accessible. Although cooperative jamming is known as a physical-layer security enhancement technique, the authors of [34] studied the effects of jamming on secrecy from MAC layer prospective. This work introduced *secure throughput* notion and presented jamming strategies where the objective was to enhance the jamming throughput. The results showed that being aware of the location of the jammers are very helpful to devise jamming protocols. As it was mentioned earlier in this chapter, security enhancement schemes may combine two or more physical-layer secrecy improvement techniques. In this regard, beamforming and cooperative jamming can be employed concurrently to improve the security [28], [73], [74].

The main concerns in cooperative jamming-based strategies are as following: (i) additional power consumption due to generating friendly jamming, (ii) the requirement of the helper node,

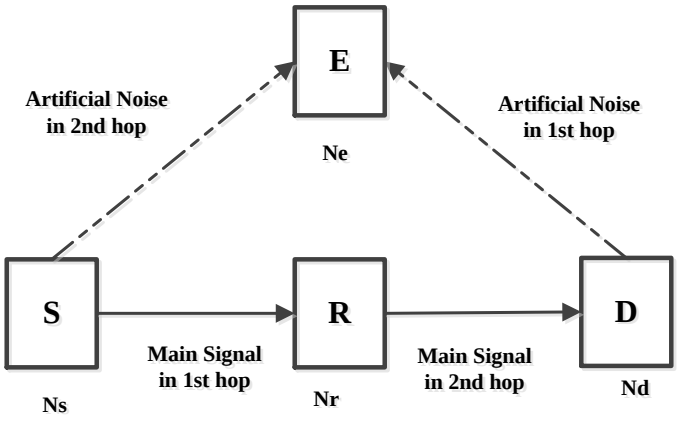


Figure 2.5: Source and destination with temporary jamming role.

and (iii) extra network overheads to coordinate between the main network and the jammer. At this point, existing solutions for the aforementioned shortcomings are briefly studied.

### Power Allocation Between Main Signal and Friendly Jamming

One of the main challenges toward employing artificial noise techniques is requirement of additional power resources. To compensate this issue, power allocation between friendly jamming and main signal has been studied in the literature such that the secrecy criterion (e.g., secrecy capacity) is maximized while power resources are limited [45], [72]. The authors of [48] were the first to assume both the secrecy and the quality of service while using the cooperative jamming. They proposed a cooperative jamming scheme which minimized the received signal-to-interference-and-noise (SINR) at the illegitimate entity in addition to ensuring a certain level of SINR at the legitimate receiver.

### Artificial Noise by Source and Receiver

Requirement of an extra node as helper to generate the jamming signal is another disadvantage of cooperative jamming strategies. Using the source and the receiver as temporary jammers for creating and sending friendly jamming was proposed in recent studies to rectify this shortcoming [73], [75].

In order to realize this methodology, the system model in Fig. 2.5 is employed where the source, equipped with $N_s$ antennas, intends to communicate with the destination, which has $N_d$ antennas, through a DF relay, with antennas $N_r$ in the presence of an eavesdropper equipped with $N_e$ antennas. In the first hop of communication, from the source to the intermediate DF relay, the receiver is used as a helper to generate the friendly interference and send it toward the eavesdropper. Next, in the second hop of transmission, from the relay to the destination, the source performs the jamming role to mislead the eavesdropper.

The authors of [28] have categorized artificial noise strategies of the aforementioned system model to following two schemes:

- Patrial cooperative jamming (PCJ): The transmitter and the destination send artificial noise simultaneously.
- Full cooperative jamming (FCJ): The transmitter and the destination do not send the intentional interference at the same time.

For example, in the fist hop of communication, the received signal at the relay and the illegitimate entity are, respectively, given by

$$y_r = \mathbf{H_{sr}}(\mathbf{T_s z_s} + \acute{\mathbf{T}}_\mathbf{s}\acute{\mathbf{z}}_\mathbf{s}) + \mathbf{H_{dr}}\acute{\mathbf{T}}_\mathbf{d}\acute{\mathbf{z}}_\mathbf{d} + \mathbf{n_r}, \tag{2.16}$$

$$y_e = \mathbf{H_{se}}(\mathbf{T_s z_s} + \acute{\mathbf{T}}_\mathbf{s}\acute{\mathbf{z}}_\mathbf{s}) + \mathbf{H_{de}}\acute{\mathbf{T}}_\mathbf{d}\acute{\mathbf{z}}_\mathbf{d} + \mathbf{n_{e,1}}, \tag{2.17}$$

where $z_i$ and $\acute{z}_i$, respectively, stand for the main signal and the artificial noise sent by node $i$, where $i \in \{s, d\}$. Also, $T_i$ and $\acute{T}_i$, respectively, indicate the beamformers of the main signal and the artificial noise. Moreover, $n_r$ is the noise at the relay, and $n_{e,1}$ is noise at the eavesdropper after the first hop of transmission. If $\acute{z}_s \neq 0$ and $\acute{z}_d \neq 0$, it is termed as FCJ; otherwise, PCJ. The results presented in [28] indicated that for the case in which the channel state information of the eavesdropper was not known, FCJ secrecy performance outperformed the PCJ strategy. The insightful work in [75], proposed a novel cooperative jamming strategy in which the intentional interference was sent from the intended receiver. Remarkably, this strategy did not depend on the channel state information of the receiver at the transmitter side. In addition, the proposed scheme did not rely on the assumption that the number of eavesdropper's antennas is less than that of the intended receiver.

### A New Way of Using Artificial Noise

It was mentioned earlier in this chapter that conventional artificial noise strategies have a number of shortcoming as following. First the requirement of the helper is costly in terms of hardware. Second, coordination between the helper and the original network is needed which increases the network overheads significantly. Third, conventional artificial noise strategies are usually limited to few applications. Such disadvantages have attracted researchers' attention to provide cost-effective and energy-efficient solutions, as the authors of [44] proposed a new way of exploiting friendly jamming which rectifies the aforementioned disadvantages. Herein, a dual-hop DF relaying system is considered in which the source aims to communicate with the destination via a DF relay in the presence of an illegitimate entity, as shown in Fig. 2.6. In this system model, the eavesdropper is able to receive signals from the first and the second hops and employ maximal ratio combining (MRC) technique.

In this scheme, all terminals have single omni-directional antenna. It is assumed that communication takes place in two phases only, i.e., direct link between the source and the destination does not exist. The transmitter of the first hop (source) or the second hop (DF relay) are capable of assigning a portion of their power for generating friendly jamming. The intentional noise is created based on a shared secret between communicating parties of the first or the second hops which is not available at eavesdropper side.

This strategy have several interesting advantages comparing with traditional cooperative jamming. First, extra hardware for the propose of jamming is not required. Second, system

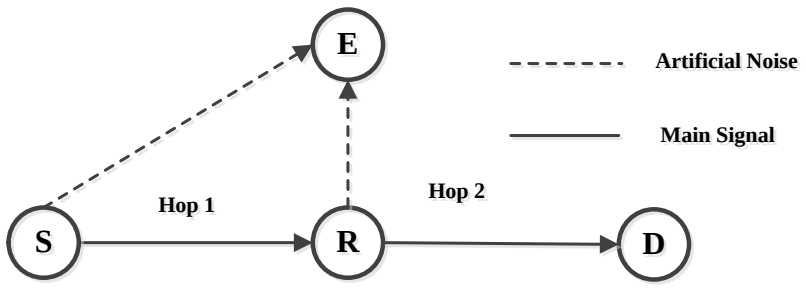


Figure 2.6: A new way of exploiting artificial noise.

complexity and network overheads are degraded as coordination between the additional node and the main network is not necessary anymore. Third, conventional artificial noise strategies are only applicable in few certain scenarios whereas the new approach can be utilized in more practical cases. Once the desired receiver of the first hop (relay) or the second hop (destination) receives the signal because they have the knowledge about the intentional noise, artificial jamming can be eliminated. On the contrary, the illegitimate entity does not have access to the the intentional jamming. Accordingly, the intentional noise misleads the eavesdropper and the received SNR of the adversary node is reduced. Based on the definition of secrecy capacity, one approach to increase the maximum achievable secrecy rate is via reduction of the received SNR at the illegitimate terminals. Thus, secrecy capacity of the system is improved.

Notably, proper power allocation in this approach have considerable effect on the performance of the presented secrecy enhancement scheme. Thus, the authors of [44] have devised an optimal power allocation in which the global channel state information including the CSI of the eavesdroppers was available. It is obvious that in many practical scenarios, the channel state information of the illegitimate nodes, or their statistics, are not accessible. Therefore, sub-optimal solutions were provided in the same reference which did not rely on channel state information of the eavesdropper.

### 2.4.4 Security Enhancement via Diversity Techniques

Primarily, diversity techniques were introduced to enhance the reliability of communication systems. However, as indicated in [6], improving the received SNR at the intended destination or degrading the received SNR at the adversary nodes, can enhance security. Thus, channel diversity is a helpful technique which can result in secrecy enhancement [46]. Notably, diversity techniques are more energy-efficient, compared to the cooperative jamming strategies because they do not require extra power resources. The following diversity approaches have been exploited in the literature to improve the security.

#### Multi-antenna Diversity

If the global CSI (CSI of the main and the eavesdropper links) is available, secrecy of communication systems can be considerably enhanced by maximizing the received SNR at the desti-

nation and minimizing the received SNR at the illegitimate entity. Consider a system model where the source intends to communicate with the receiver via relays over Rayleigh fading channels. The strategy proposed in [46] essentially was based on the definition of secrecy capacity as $C_s = [C_m - C_w]^+$, meaning that the capacity of the legitimate channel can be improved by using diversity techniques. Accordingly, if $C_r$ is increased, the total secrecy capacity of the system is improved as well. The same reference recommended using MIMO or *Virtual MIMO* in order to employ diversity techniques. In the case of virtual MIMO, multiple nodes perform the relaying role such that the received SNR at the illegitimate entity is minimized. To achieve this goal, the access control of the relays must be pre-set. Remarkable results of [46] showed that even under very low SNRs, using diversity techniques can significantly improve the achievable secrecy rate. It must be pointed out that in some practical scenarios, the channel state information of the illegitimate nodes are not known. In the former case, the CSI of the legitimate links are utilized such that the received SNR at the intended receiver is maximized; therefore, secrecy capacity of the system is in turn increased.

### Multiuser Diversity

Multiple access techniques (e.g., time devision multiple access, orthogonal frequency division multiple access) are intensively utilized in multiuser communication system to communicate with the end users. If global channel state information is available, the user channel assignment and scheduling can be effectively done such that the capacity of the main channel is maximized while the capacity of the eavesdropper link is minimized. On the other hand, if only the CSI of the main link is available, the scheduling is optimized such that the capacity of the legitimate channel is maximized. However, both of the aforementioned approaches improve the secrecy capacity to a great extent [76].

### Cooperative Diversity

Cooperative diversity reverts back to relay selection schemes. In other words, the best relay to perform the relaying role is chosen such that secrecy capacity of the system is maximized. This approach is called *relay selection with secrecy constraints* in the literature. The aforementioned relay selection strategies are categorized examining that the CSI of the eavesdropper is available or not.

Relay selection schemes have been widely investigated in recent works [77]-[80]. Previous relay selection strategies focus on reliability and performance parameters such as the link strength as the main criterion to select the relay. To describe the relay selection schemes, a two-hop DF relaying system, as seen in Fig. 2.7, is considered in which communication is carried out in the presence of an eavesdropper. In traditional relay selection schemes, the illegitimate link between the transmitters and the eavesdroppers is disregarded; thus, the instantaneous SNR of the intended receiver is employed as a relay selection criterion. Hence, the selected relay is chosen according to

$$r^* = \arg\max\{\gamma_{r_i,D}\}, \tag{2.18}$$

where $r^*$ denotes the selected relay and $\gamma_{r_i,D}$ indicates the received SNR of the link between the $i$th relay and destination. This relay selection strategy is appropriate to be used in communication environments where there is no wiretapper to overhear communication signals.

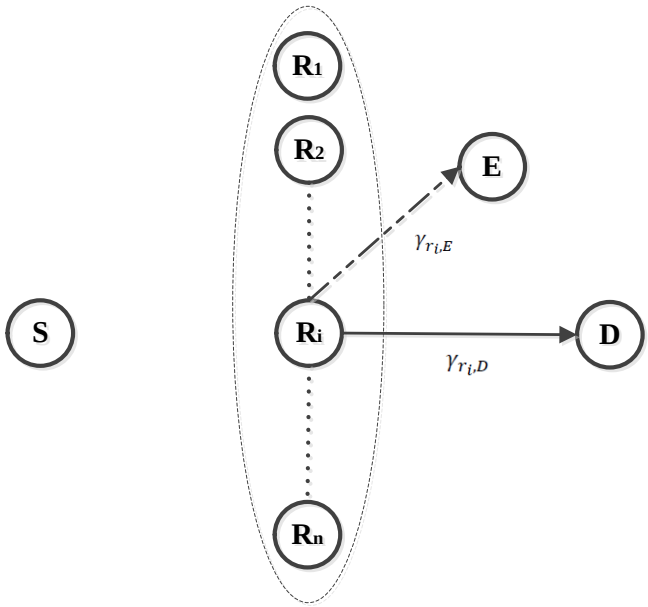


Figure 2.7: Relay selection angwith secrecy constraints.

Recently, an insightful work in [81] opened a new way of relay selection which is based on secrecy constraints. This work took into account the link between the wiretapper and the transmitter so the relay selection scheme with secrecy constraints has been updated as

$$r^* = \arg\max\{\frac{\gamma_{r_i,D}}{\gamma_{r_i,E}}\}, \tag{2.19}$$

in which $\gamma_{r_i,E}$ denotes the received SNR of the link between the $i$th relay and illegitimate entity. Based on the achievable secrecy rate definition, this strategy aims at maximizing the achievable secrecy rate of the considered system model. Furthermore, since in practice the instantaneous received SNR of the illegitimate link is intractable, a sub-optimal solution was suggested as well [81]. In particular, the sub-optimal solution was based on information about the average channel statistics and it was formulated as

$$r^* = \arg\max\{\frac{\gamma_{r_i,D}}{{\sigma^2}_{r_i,E}}\}, \tag{2.20}$$

where ${\sigma^2}_{r_i,E}$ represents an average knowledge about SNR of the link between the $i$th relay and the illegitimate entity.

Following this framework, relay selection schemes under secrecy constraints have been widely studied in the litrature [43], [81], [82]. An interesting work in [81], investigated a two-hop DF relaying system in which source intended to communicate with the eavesdropper in the presence of multiple non-colluding eavesdroppers. Consequently, the authors of [81] adopted three relay selection strategies as below:

- The first scheme suggested that the relay had to be chosen such that instantaneous received SNR at the illegitimate entity was minimized.

- The second strategy was the conventional scheme where the eavesdropper link was not included in relay selection procedure.
- In the third scheme, the maximum ratio of received SNRs of the main link to the illegitimate link is incorporated as the selection criteria.

In a more recent work [82], the relay selection was studied in a dual-hop communication system where communications occured in the presence of an eavesdropper while the relays could employ DF and AF protocols.

#### Relay Selection for Secure Communications with Artificial Noise

As previously mentioned in this chapter, artificial noise and relay selection are two techniques for security enhancement in multi-hop relaying systems. Interestingly, in a recent work [43], cooperative jamming and relay selection under secrecy constraints have been combined. In this research, the authors initially proposed a relay selection strategy for a dual-hop DF relaying communication system based on conventional relay selection strategies. Next, a relay was chosen for the purpose of jamming and confusing the wiretappers. Using the proposed relay selection schemes jointly, enhanced the security of the communication system. This work further devised relay selection strategy for the case where instantaneous channel state information of the illegitimate node was not available.

On the other hand, communication in a wiretap channel in the existence of a helper which can perform either relaying role or jamming role was studied in [83]. This study aimed at answering the question that under different conditions the helper had to perform a relaying or the jamming role in order to improve system secrecy. Therefore, the following two scenarios were investigated over path-loss and fading channels: (i) direct transmission with artificial noise, (ii) dual-hop transmission via relay.

### 2.4.5 Exploiting Channel Characteristics for Secrecy

Security improvement in physical layer can be achieved via using the channel characteristics. In this regard, different schemes have been proposed including generating the secret key based on the channel between the communicating parties, MIMO diversity and RF finger print. Since MIMO diversity have already been studied in this chapter, hereon other two methods are briefly examined.

#### Creating the Secret Key

A shared secret key between communicating nodes can be created via using the channel between the source and the intended receiver. The idea essentially comes from the fact that the channel between the communicating parties is not accessible to the illegitimate entities [84]-[86]. The authors of [85] have used this intuition to create a secret key. In this study the channel between the source and the intended receiver and the channel between the receiver and the source were assumed identical. Herein, each communicating party generated a secret key according to the reciprocal channel independently. Next, the communicating parties started a handshaking under secure conditions. If the secret keys were the same, they would be used for

security improvement for example via cryptography techniques; otherwise, the communicating parties had to start from the beginning of the procedure via another channel estimation [85].

#### RF Fingerprint

Primarily, most authentication and digital signature techniques have been used in upper layer of networking stack. However, a new trend towards using physical layer authentication has recently started where the transmitters are identified via their unique transmission characteristics [87]-[89]. This new authentication scheme is called *RF fingerprint* in the literature. In this regard, it has been suggested in [89] to use the channel response in order to differentiate between the legitimate and illegitimate entities and to verify if recent and previous messages were sent by the same node or not.

### 2.4.6 Security Enhancement via Exploiting Coding

Spread spectrum has been introduced as a coding technique to secure the communication in physical layer [5]. In spread spectrum techniques, the main signal is intentionally spread through a wide frequency bandwidth to secure it from eavesdropping, jamming, and etc. In this respect, frequency hopping spread spectrum (FHSS) is one of the proposed techniques in which the carrier's frequency changes frequently such that the unauthorized entity cannot access the carrier. Moreover, direct sequence spread spectrum (DSSS) is another technique in which the main signal is split to subsignals using pseudo noise (PN). The split signals are later transmitted over separate frequencies, and therefore the illegitimate nodes which do not have access to the frequency hopping pattern (FHP) cannot retrieve the main signal [5]. Spread spectrum techniques require smaller keys, compared to the upper-layer cryptography techniques. On the other hand, spread spectrum techniques increase the required bandwidth. Notably, the aforementioned techniques are effective solutions to mitigate jamming and physical layer DoS attacks.

## 2.5 Securing the Transmission via Untrusted Relays

The security scenarios are not only the cases where the eavesdroppers are external nodes. Indeed, there are cases in which communication between the source and destination may only be available through *untrusted relays* [35], [53], [72]. The authors of [90] and [91] have investigated the security in dual-hop communication system where the relays are untrusted. Interestingly, the results showed that for non-regenerative relays, including AF relays, achieving a positive secrecy rate is possible while for the DF relays these results are not applicable. There have been different approaches toward secure communication in networks where relays are untrusted. Hereon, some of the relevant approaches are briefly reviewed.

### 2.5.1 Securing the Transmission via Untrusted Relays Using Coding

Secure transmission over a multi-hop communication system was studied in [92] where direct link between source and destination did not exist and intermediate nodes were untrusted. In this


Figure 2.8: First hop of secure communication with untrusted relay via using cooperative jamming.

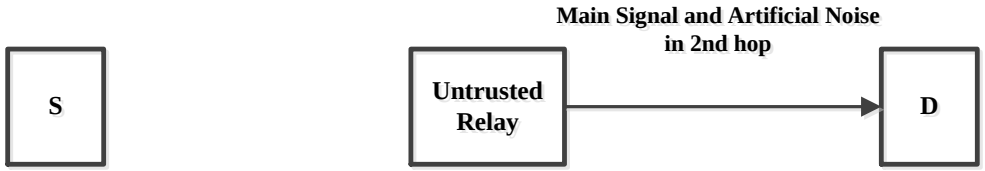


Figure 2.9: Second hop of secure communication with untrusted relay via using cooperative jamming.

paradigm, it was presumed that each node could only communicate with its adjacent neighbors and the intermediate nodes were employed for relaying. However, the results of this work implied that secure transmission between the source and the destination, despite cooperation of untrusted relays for relaying proposes, is achievable. This work focused on employing compute-and-forward protocol at the relays and using nested lattice codes.

### 2.5.2 Securing the Transmission via Untrusted Relays Using Cooperative Jamming

Another proposed strategy in existing studies to secure the communications through untrusted relays is cooperative jamming as proposed in [53]. The authors of [93] have presented a cooperative jamming strategy and corresponding secrecy performance analysis. Thereon, to examine this methodology in detail, a two-hop AF relaying system is considered where there is not any direct link between the source and the destination, and transmission from the source to the relay is realized in two phases. In the first hop of communication, as observed in Fig. 2.8, the source sends the main signal toward the untrusted AF relay while the destination sends an intentional jamming signal simultaneously toward the untrusted relay. Therefore, the received signal at the relay is given by

$$y_r = \sqrt{\rho P_t} h_{sr} x_s + \sqrt{(1-\rho) P_t} h_{dr} \acute{x_j} + n_r, \tag{2.21}$$

where the total transmission power of each hop is set to $P_t$ and $\rho$ indicates the power allocation factor between the original signal, denoted by $x_s$, and the jamming signal, denoted by $\acute{x_j}$ and

$\rho \in [0, 1]$. Herein, the total power is obtained as

$$P_t = P_s + P_j \tag{2.22}$$

in which $P_s$ and $P_j$ are the source and the jamming signal power values. The AF relay is not able to distinguish and spilt the main signal and the intentional noise. Therefore, it performs the relaying role without accessing the main transmission, as seen in Fig. 2.9. Hence, the received signal at the destination is formulated as

$$y_d = \beta h_{rd}( \sqrt{\rho P_t} h_{sr} x_s + \quad \sqrt{(1-\rho)P_t} h_{dr} \acute{x_j} + n_r) + n_d, \tag{2.23}$$

in which it is assumed that the AF relay uses $\beta$ as its amplification factor such that the sent signal by the relay is originally given by

$$x_r = \beta y_r, \tag{2.24}$$

Note that since the intentional interference was originally sent by the receiver, jamming signal is known and so can be removed at the intended receiver's side. Using equation (2.23), the received signal is retrieved as

$$\acute{y_d} = \beta h_{rd}( \sqrt{\rho P_t} h_{sr} x_s + n_r) + n_d, \tag{2.25}$$

The performance of this strategy is influenced by a number of factors. Most importantly, the power allocation between the main transmission and the intentional noise can affect the results significantly [93]. To clarify the effect of $\rho$, a single AF relay communication system was considered in which associated simulation parameters are listed in the following table.

Table 2.1: Simulation set up parameters (untrusted relay)

| Simulation Parameter | Value |
|---|---|
| Source location | (0,0) m |
| Untrusted relay location | (500,0) m |
| Destination location | (1000,0) m |
| Path loss coefficient | 3.5 |
| $\sigma^2$ | -60 dBm |

The Monte carlo simulations are corresponding to an average of $10^5$ independent trials. The results in Fig. 2.10 show that a proper power allocation is necessary to ensure that secrecy of the system is improved.

The importance of power allocation between the main signal and the artificial noise has motivated researchers in the field [72]. Herein, the authors of [72] studied ergodic secrecy capacity of a two-hop AF relaying system where the relays were untrusted. Further, it was investigated that how large-scale antenna arrays at the source or the intended receiver could affect the secrecy performance of this system. The results showed that if the source was equipped with large scale antennas, ergodic secrecy capacity only depended on the channel between the untrusted relay and the intended receiver. On the other hand, if the legitimate receiver had large antenna arrays, ergodic secrecy capacity only relied on the channel between the source and the untrusted intermediate relay.

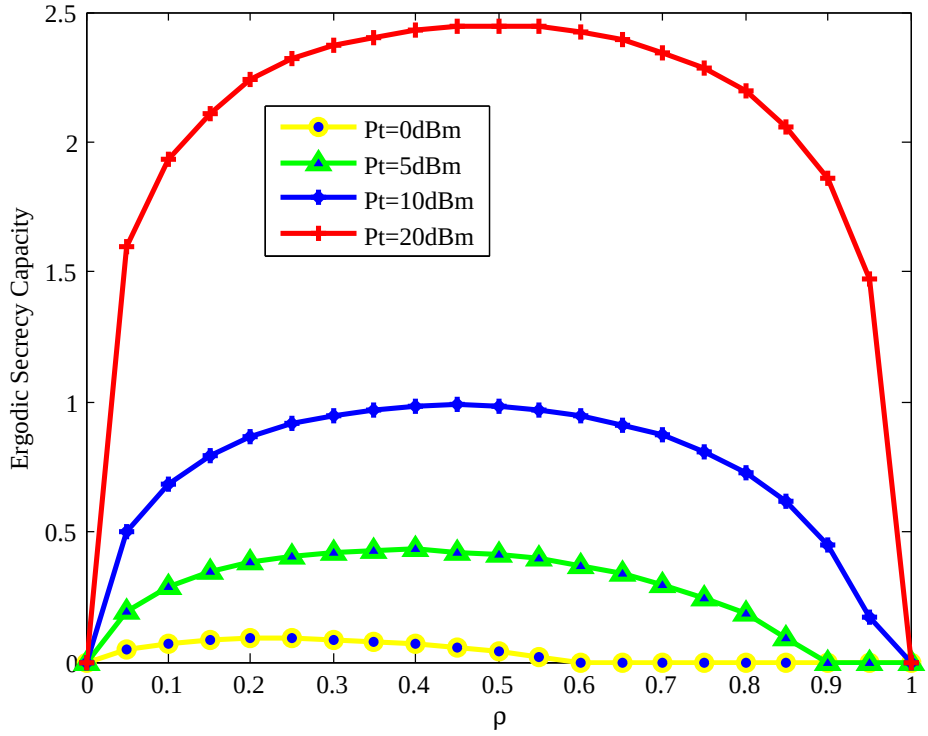


Figure 2.10: Impact of power allocation on ESC.

### 2.5.3 Securing Transmission via Untrusted Relays Using Cross-layer Approaches

If communication between source and intended receiver is only possible through untrusted relays, it is possible to secure the communication via distributing the relaying node among untruted non-collaborative relays [35]. In other words, for the source to be able to communicate with the destination, intermediate relays must perform relaying role which requires to reduce the access of each intermediate node to the entire communication.

It can be said that whenever relay $R^*$ is transmitting, other relays are presumed as potential eavesdroppers. Therefore, by distributing the relaying role among different intermediate nodes, as seen in Fig. 2.11, the physical layer security can be improved. To be more precise, if the desired transmission rate from the source to the legitimate receiver is $R_t$, the entire data stream is divided to $m$ data streams represented by $l_1, l_2, ..., l_m$ where associated transmission rates are given by $R_1, R_2, ..., R_m$ so $R_t$ can be written as

$$R_t = \sum_{i=1}^{m} R_i, \tag{2.26}$$

The authors of [35] suggested that data streams among intermediate nodes were distributed using beamforming techniques in order to minimize the access of each of intermediate entities to the entire data. Further, it was proposed to use an upper-layer security strategy via sharing the secret key to compliment the aforementioned scheme [68]. This study showed that for the

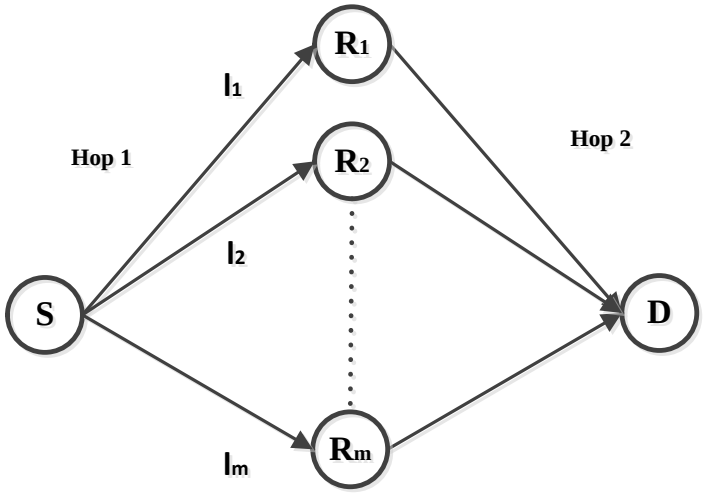


Figure 2.11: Distributing the data stream between the intermediate untrusted relays.

AF protocol, perfect information-theoretic secrecy is attainable while for the DF protocol these results are not valid. However, still for DF relays date distributing can improve the security to some extent.

### 2.5.4 Securing the Transmission via Untrusted Relays Using Beamforming

Beamforming techniques can be employed to secure the communication via untrusted relays. A two-hop AF MIMO relaying system was considered in [94] where AF relay was not trusted so had the potential to be a passive eavesdropper. Thereby, two communication scenarios were employed as follows.

- *Non-collaborative scheme* in which the intermediate node is considered as an external passive node while not performing the relaying role
- *Collaborative scheme* in which the untrusted relay retransmits the main signal using joint beamforming at the source and the relay [94]

Interestingly, the results showed that if the SNRs of source-relay link and relay-destination links were low, then the collaborative scheme outperformed better in terms of achievable secrecy rate. Moreover, the authors have shown that the aforementioned schemes lead to more secure communications in terms of secrecy capacity compared to the traditional beamforming strategies.

## 2.6 Secure Transmission with Buffer-aided Relays

Conventional relays have pre-scheduled role assignments where there is a switching between receive and transmit modes. Recent works have proposed a new relaying protocols known

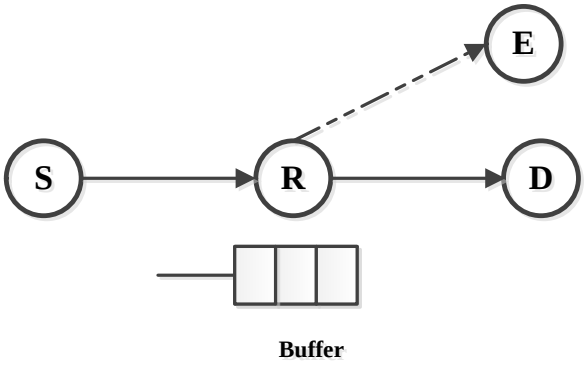


Figure 2.12: Using buffer-aided relays to improve the secrecy.

as *buffer-aided* relays where the relays are equipped with buffers while providing dynamic smart switching between the receive and transmit modes [95]-[97]. It has been proved that the introduced diversity degree has many benefits such as increasing the throughput as well as diversity gain, and signal-to-noise ratio [98], [99]. However, one of the disadvantages of buffed-aided relays is latency caused by data buffering. Interestingly, the potential advantages of adopting buffer-aided relays in terms of physical layer security was not investigated, until it was shown in [100] and [101] that adopting buffer-aided relays can improve physical layer security.

To be more specific, a two-hop communication system was considered in [100] in which all nodes were half-duplex and communication took place in the presence of an illegitimate entity which could wiretap the transmission of the second hop, as seen in Fig. 2.12. Moreover, it was assumed that the relay was equipped with a buffer, and different relay selection strategies were studied according to efficiency and security of both hops. This work investigated two cases where the channel state information of the destination is available or not. The results revealed that there is a considerable improvement in the security of the buffer-aided relay scenarios compared to the case that the relays are incapable of storing the data. However, the assumption that the eavesdropper and the destination were in the same cluster and the eavesdropper could only overhear the communication of the second hop is the limitation of this scheme.

## 2.7 Practical Scenarios of Physical Layer Security

In this section, the capabilities of physical-layer security techniques in some practical scenarios are studied. Broadcast channel with confidential message in the presence of an eavesdropper is an applicable scenario where legitimate and illegitimate entities have arbitrary locations [67]-[68]. However, physical layer security can be adopted in other scenarios partly explained in the following subsections.

### 2.7.1 Physical Layer Security in Ad-hoc Networks

The notion of *secrecy transmission capacity* has been introduced in [102] in order to specify the relevance of physical-layer security requirements and throughput of large-scale ad-hoc networks. As a contribution, it was shown that a moderate security level could be obtained via a relatively low throughput cost. On the other hand, a high security level is indeed costly in terms of throughput cost. Further results illustrated that through the use of cooperative jamming techniques, a high level of security at a lower throughput cost could be achieved. However, this method is solely applicable to a single-hop case while multi-hop scenarios are widely present in today's wireless communication systems.

### 2.7.2 Physical Layer Security in WSNs

Wireless sensor networks (WSNs) extensively expose eavesdropping. Cryptography security enhancement techniques have been already investigated in WSNs. But, the limitations of WSNs in terms of computation load and energy level have led to research efforts aiming at reducing complexity and energy consumption [32], [103]. According to the results, secrecy of WSNs can be significantly improved via physical-layer security techniques while less complexity and energy consumption are involved. In addition, it was shown that friendly jamming could enhance the security of WSNs [32].

### 2.7.3 Physical Layer Security in CRNs

Cognitive radio network (CRN) adopts an efficient way to exploit the spectrum such that the licensed spectrum is opportunistically borrowed by secondary entities, if the main user does not need it. However, CRNs introduce some security vulnerabilities in the physical layer summarized as below[104]:

- The secondary users must be able to differentiate the primary user and the illegitimate nodes.
- The accuracy of sensing information at the secondary entity affects its decisions and expose attacks.

In addition to the common eavesdropping and jamming attacks, physical layer of cognitive radio networks expose other attacks. First, primary user emulation (PUE) attack masquerades the main user, and exploits the licensed band. Therefore, the secondary entities cannot use the band. Second, objective function attack which threatens the learning engine of CRNs whose role is to adjust various parameters of the system and maximize the objective function. Third group of attacks are learning attack (LA) where the illegitimate entities send faulty information to the learning radio. Finally, Byzantine attack which injects wrong information in the spectrum sensing data so spectrum access decision cannot be accurate [104]. Furthermore, security solutions for the aforementioned attacks are presented in [104].

Moreover, the physical layer security of a CRN in the existence of multiple wiretappers was investigated in [105]. This work has presented a multiuser scheduling scheme to enhance security in communication systems against wiretappers. The results showed that the newly

presented scheme had better performance in terms of achievable secrecy rate compared to the conventional multiuser scheduling protocols.

### 2.7.4 Physical Layer Security in Cellular Networks

The majority of initial studies in physical layer are related to point-to-point scenarios or the cases where the isolated cells are considered. However, in order to adopt physical layer security in cellular networks, their impact on large-scale networks must be examined. In this regard, the authors of [106] considered a large-scale cellular network where base station and the user equipment (UE) were independently placed and Poisson point processes were used to model their spatial locations. This study reported that the best BS in terms of secrecy was not necessarily the closest one to the user. In addition, the availability of the spatial location of illegitimate users at the BS significantly improved the secrecy. A single antenna case was studied in [106] where certain nodes had the potential to be eavesdroppers while a recent work investigated a more general case in which the nodes were equipped with multiple antennas, and each node could act as an eavesdropper except the communicating parties. It was shown that optimal density of the base stations could be devised such that the mean secrecy rate of the system was maximized [107].

Table 2.2: An overview of physical-layer security techniques

| *Physical Layer Security Technique* | *Prevented Attack* | *Corresponding Security Concern* |
|---|---|---|
| Information-theoretic | Eavesdropping | Confidentiality |
| Beamforming | Eavesdropping | Confidentiality |
| Diversity | Eavesdropping | Confidentiality |
| Artificial noise | Eavesdropping | Confidentiality |
| Spread spectrum | Eavesdropping, jamming, traffic analysis | Availability, confidentiality |
| Fingerprint | Eavesdropping, masquerade, misusing resources | Authentication, confidentiality |

## 2.8 Summary

In this chapter, physical layer security was introduced and discussed. It was pointed out that the physical-layer security techniques and the upper-layer security strategies were complimentary and could be exploited simultaneously to provide secure communications. The definitions and formulations of the main secrecy performance parameters including secrecy capacity, ergodic secrecy capacity, probability of non-zero secrecy capacity and probability of outage in secrecy capacity were described. Later, communication in the presence of multiple eavesdroppers was examined, and the eavesdroppers were categorized to passive and active wiretappers based on their capabilities to make changes or modifications in the main signal. It was also highlighted

that multiple eavesdroppers could be colluding or non-colluding in the sense that they could or could not collaborate for the purpose of reducing secrecy.

Next, different physical-layer security techniques were explained with details which included information-theoretic, beamforming, artificial noise and diversity techniques. Following this framework, combination of different security techniques was proposed which included the combination of beamforming techniques and artificial noise or the artificial noise and relay selection.

Moreover, communication via untrusted relays was examined and several approaches toward achieving positive secrecy rate in such scenarios were investigated. Also, the advantages of using buffer-aided relays in terms of secrecy in physical layer was briefly studied. In addition, the capabilities of physical layer security in applicable scenarios including WSNs, CRNs, cellular networks and ad-hoc networks were highlighted in brief. Finally, an overview of existing physical-layer security schemes was presented in Table 2.2.

# Chapter 3

# Secrecy Enhancement in Two-hop DF Relaying Systems

Cooperative wireless communications via relays have been widely used to reduce energy consumption and enhance coverage and quality of service. However, the broadcast nature of wireless medium, introduces the security risks to the wireless relaying system. Therefore, security and reliability of the cooperative communication systems are needed simultaneously to meet the growing demand of secure wireless communications.

Since two-hop relaying systems are expected to be extensively utilized in the future communication systems, security of a two-hop relaying system is investigated in this chapter. For example, the long term evolution (LTE)-advanced cellular systems has presently recommended two-hop relaying as a technique to increase the coverage and mitigate the issues of cell edge for the cases when the end user is located far from the base station [112]. Relaying communications can be achieved through different protocols. Amplify-and-forward and decode-and-forward protocols are the most common protocols applied at the relays [108]. Processing time and complexity of AF relays are less, relative to DF relays, but DF relays are more robust in low to medium signal-to noise ratios (SNR) [109]-[111]. In this chapter we focus on DF strategy. In order to mitigate security risks, cooperative relaying has been investigated through different aspects among which friendly jamming must be mentioned. However, cooperative jamming mostly required additional helper and increases the network overheads. Thus, this chapter aims at providing alternative security solutions.

## 3.1 Introduction

Many existing works at physical layer security exploit conventional cooperative jamming to enhance the security [28]-[29] ,[113]. Classical cooperative jamming needs an extra helper (other than the communicating parties) to generate the jamming signal, so it is costly in terms of hardware. In addition, the coordination between the jammer and the main network raises the network overheads. Therefore, there is a need for cost-effective and energy-efficient solutions.

Herein, a novel security improvement scheme is presented in which a random phase shift is applied to the modulated data of each hop of transmission. The random phase shift is created based on a shared information between communicating entities which is not available at the

eavesdropper. Thus, the desired receiver is aware of the random phase shift and it can remove the phase shift and obtain the main signal, whereas the illegitimate node does not have access to the injected phase shift. This modification results in confusing the illegitimate nodes so the received SNR at the eavesdropper is degraded and the secrecy capacity of the system is improved. As it was mentioned, the random phase shift must be created using a shared knowledge between the communicating entities. For example the reciprocal channel between the transmitter and the intended receiver can be exploited to create the random phase shift because the illegitimate node does not have access to this channel.

It is noteworthy that due to the readily accessible channel information, the complexity of the presented secrecy improvement scheme is not high. Notably, the proposed scheme is cost-effective and it can be applied to the communication systems in which power resources are limited. The work presented in [114] is one of the first attempts to improve the secrecy via using the relays. Different approaches have targeted the secrecy of relaying systems to improve the security. Hereon, the most important recent works on the security of two-hop cooperative relaying networks are summarized as below.

In relaying systems initially, relay selections strategies have been proposed, considering the performance and reliability criteria. The study presented in [81] opened up a new aspect, as it concentrated on relay selection under secrecy performance parameters. This work considered the illegitimate link in the relay selection procedure and it aimed at maximizing the secrecy capacity. Following this framework, relay selection with secrecy constraints in the presence of an eavesdropper was studied in [115]. In the context of secure transmission with cooperative helpers, cooperative beamforming was investigated in [30] and [47].

On the other hand, although jamming initially is unwagnted, cooperative jamming has been introduced as a promising technique to improve the security of wireless communication systems where an intentional jamming can degrade the received SNR at the eavesdropper and enhance the secrecy. The jamming signals can be sent from different entities including source, relay, receiver or an extra node [113],[116]. In order to ensure that this strategy enhances the secrecy and it does not interfere the main signal transmission, power allocation between the original signal and the jamming is required. Thus, some recent works have focused on optimal and sub-optimal solutions of power allocation [44], [45]. In this regard, the work in [83] studied secure communication between a source and destination with a helper, and it explained when the helper had to jam and when it had to relay in order to achieve the best performance in terms of secrecy. The authors of [43] chose one helper among a group of available cooperative intermediate nodes to perfume the relaying role and transmit the data to the intended receiver. Next, the second helper was selected to generate the friendly jamming at the eavesdropper.

Moreover, the authors of [28] presented an interesting security enhancement strategy, based on cooperative jamming, for a dual-hop DF relaying system in the presence of an illegitimate node. However, it must be pointed out that in cooperative jamming, the coordination between the nodes results in a complexity which has to be avoided. Furthermore, the power consumption of the aforementioned strategy is considerable. Therefore, this chapter provides an alternative cost-effective solution, in terms of both energy consumption and complexity for two-hop DF relaying systems.

The problem of generating a shared secret according to a common information between the transmitter and intended receiver has been investigated in existing studies where the channel reciprocity is exploited to generate the secret key [86], [117]. However, most current ap-

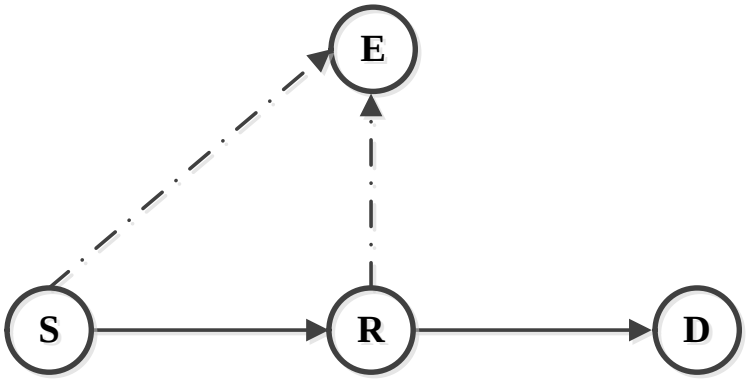


Figure 3.1: Two-hop communication system model.

proaches suggest using the generated key in cryptography algorithms. Hereupon, this chapter proposes a novel scheme to utilize the shared secret via an energy-efficient and less complex approach through physical layer. In principle, it is suggested to use a shared secret for the modification at the transmitter where the authorized receiver can detect the modification as it has access to the secret key. On the other hand, the adversary is not aware of the key and therefore its received SNR is decreased and the secrecy capacity of the system is improved.

## 3.2 System Model

Consider a two-hop decode-and-forward relay system, as shown in Figure 3.1. The system consists of a source node $S$, DF relay $R$, intended receiver $D$ and an illegitimate node $E$. It is assumed that the source has no direct link with the destination and the communication is carried out through the DF relay and in two hops. The first hop is from the source to the DF relay and the second hop performs the transmission from the relay to the intended receiver. The eavesdropper is able to overhear the communication signals of both hops, and to utilize MRC to combine the received signals from the source and the relay. All nodes in this system model are half-duplex meaning that they can receive or transmit the signal at a time.

Channels between nodes $i$ and $j$ are Rayleigh fading and denoted by $h_{ij}$ where $i, j \in \{s, r, d, e\}$. The channel fading coefficients are presumed to be constant during the transmission of each codeword but they are subject to independent and random changes once the codeword changes. It is also considered that the channel fading coefficients related to each two pair of nodes are independent. In addition, $\gamma_{ij}$ represents SNR of $ij$ link e.g., $\gamma_{sr}$ denotes the SNR of $S - R$ link.

The instantaneous received SNR of the relay at the first hop is given by

$$\gamma_{sr} = \frac{P_S \mid h_{sr} \mid^2}{\sigma^2}, \tag{3.1}$$

where $P_S$ denotes the transmit power of the source and $\sigma^2$ represents variance of the additive white Gaussian noise (AWGN) of all terminals. Similarly, the instantaneous received SNR of

the eavesdropper at the first hop can be written as

$$\gamma_{se} = \frac{P_S \mid h_{se} \mid^2}{\sigma^2}. \tag{3.2}$$

Since the fading coefficients are zero-mean complex Gaussian random variable, it can be concluded that $\gamma_{ij}$ have exponential distribution. Hence, Probability density function (PDF) and cumulative density function (CDF) of $\gamma_{sr}$ are, respectively, written as [118, p. 188]

$$p_{\gamma_{sr}}(\gamma) = \frac{1}{\overline{\gamma_{sr}}} exp(-\frac{\gamma}{\overline{\gamma_{sr}}}), \tag{3.3}$$

$$P_{\gamma_{sr}}(\gamma) = 1 - exp(-\frac{\gamma}{\overline{\gamma_{sr}}}), \tag{3.4}$$

in which $\overline{\gamma_{sr}}$ is the averaged received SNR of the relay at the first hop and it is expressed by

$$\overline{\gamma_{sr}} = \frac{P_S E\{\mid h_{sr} \mid^2\}}{\sigma^2}, \tag{3.5}$$

All over the formulations, $E\{.\}$ indicates the expectation of a random variable. Also, the instantaneous received SNR of the intended receiver and the eavesdropper in the second phase are, respectively, given by

$$\gamma_{rd} = \frac{P_R \mid h_{rd} \mid^2}{\sigma^2}, \tag{3.6}$$

$$\gamma_{re} = \frac{P_R \mid h_{re} \mid^2}{\sigma^2}, \tag{3.7}$$

in which $P_R$ represents the transmission power of the relay and CDF and PDF of $\gamma_{rd}$ are, respectively, formulated as

$$p_{\gamma_{rd}}(\gamma) = \frac{1}{\overline{\gamma_{rd}}} exp(-\frac{\gamma}{\overline{\gamma_{rd}}}), \tag{3.8}$$

$$P_{\gamma_{rd}}(\gamma) = 1 - exp(-\frac{\gamma}{\overline{\gamma_{rd}}}). \tag{3.9}$$

Hereon, $\overline{\gamma_{rd}}$ represents the averaged received SNR of the second phase and it is expressed by

$$\overline{\gamma_{rd}} = \frac{P_R E\{\mid h_{rd} \mid^2\}}{\sigma^2}. \tag{3.10}$$

## 3.3 Secrecy Performance

In this section, the secrecy performance of the system model is studied and closed-form expressions of probability of outage in secrecy capacity and probability of non-zero secrecy capacity are calculated. These secrecy analysis facilitate the realization of the security issues and it is a guide to develop security improvement schemes.

### 3.3.1 Secrecy Capacity

As mentioned in chapter 2, secrecy capacity is defined as the maximum transmission rate from the source to the intended receiver where the data is not accessible for the illegitimate nodes. Thus, it can be written as

$$C_s = [C_r - C_e]^+, \tag{3.11}$$

In this notation, $C_r$ is the capacity through the main link and $C_e$ represents the capacity of the illegitimate link. Moreover, $[x]^+$ is defined as

$$[x]^+ \triangleq \begin{cases} 0 & x \leq 0 \\ x & 0 < x \end{cases}.$$

Capacity of the main link is given by [119]

$$C_r = \frac{1}{2} min\{log_2(1+\gamma_{sr}), log_2(1+\gamma_{rd})\}, \tag{3.12}$$

in which $1/2$ is due to the fact that signal transmission is in two phases. In this system model, it has been assumed that the eavesdropper is able to combine the receives SNRs from different hops and it is capable of *joint decoding*. Thus, capacity of the eavesdropper link is given by

$$C_e = \frac{1}{2} log_2(1+\gamma_{se}+\gamma_{re}). \tag{3.13}$$

In order to facilitate the secrecy performance derivations, parameters $\gamma_T$, $\gamma_E$ and $\gamma_S$ are defined as following.

$$\gamma_T \triangleq min\,\{\gamma_{sr}, \gamma_{rd}\}, \tag{3.14}$$

$$\gamma_E \triangleq \gamma_{se} + \gamma_{re}, \tag{3.15}$$

$$\gamma_S \triangleq \frac{1+\gamma_T}{1+\gamma_E}. \tag{3.16}$$

Using these definitions, secrecy capacity of this system model is formulated as

$$C_s = \frac{1}{2}[log_2 \frac{1+\gamma_T}{1+\gamma_E}]^+ = \frac{1}{2}[log_2 \gamma_s]^+. \tag{3.17}$$

### 3.3.2 Probability of Non-zero Secrecy Capacity

It has been explained in chapter 2 that probability of existence of secrecy capacity refers to the case where the main channel capacity is stronger than the capacity of the illegitimate channel. Thus, probability of non-zero secrecy capacity of this system model can be expressed as

$$\begin{aligned} Pr[C_s > 0] &= Pr[\frac{1+\gamma_T}{1+\gamma_E} > 1] \\ &= Pr[\gamma_S > 1] \\ &= 1 - P_{\gamma_S}(1), \end{aligned} \tag{3.18}$$

where $P_{\gamma_S}(.)$ represents CDF of $\gamma_S$. Equation (3.18) is a closed-form expression for the probability of non-zero secrecy capacity in this system model. At this point $P_{\gamma_S}(.)$ is derived to utilize it for secrecy performance analysis of this work. CDF of $\gamma_S$ is given by

$$P_{\gamma_S}(\gamma) = Pr[\frac{1+\gamma_T}{1+\gamma_E} < \gamma]. \tag{3.19}$$

Therefore, (3.19) can be expressed as

$$\begin{aligned} P_{\gamma_S}(\gamma) &= Pr[\gamma_T < \gamma(1+\gamma_E) - 1] \\ &= \int_0^\infty P_{\gamma_T}(\gamma(1+\gamma_e) - 1) p_{\gamma_E}(\gamma_e) d\gamma_e. \end{aligned} \tag{3.20}$$

As it is seen in (3.20), it is needed to derive CDF of $\gamma_T$ and PDF of $\gamma_E$ to obtain the closed-form expression of $P_{\gamma_S}(.)$.

*Derivation of CDF of $\gamma_T$:*

First CDF of $\gamma_T$ is calculated as the following. Using (3.14) it can be written that

$$\begin{aligned} P_{\gamma_T}(\gamma) &= Pr[min(\gamma_{sr}, \gamma_{rd}) < \gamma] \\ &= 1 - Pr[\gamma_{sr} > \gamma, \gamma_{rd} > \gamma]. \end{aligned} \tag{3.21}$$

The obvious fact that $\gamma_{sr}$ and $\gamma_{rd}$ are independent results in

$$\begin{aligned} P_{\gamma_T}(\gamma) &= 1 - Pr[\gamma_{sr} > \gamma] Pr[\gamma_{rd} > \gamma] \\ &= 1 - (1 - P_{\gamma_{sr}}(\gamma))(1 - P_{\gamma_{rd}}(\gamma)). \end{aligned} \tag{3.22}$$

Invoking (3.4) and (3.9) in (3.22), it can be written that

$$\begin{aligned} P_{\gamma_T}(\gamma) &= 1 - exp(-\frac{\gamma}{\overline{\gamma}_{sr}}) exp(-\frac{\gamma}{\overline{\gamma}_{rd}}) \\ &= 1 - exp(-\gamma\beta), \end{aligned} \tag{3.23}$$

in which $\beta$ is given by

$$\beta \triangleq \frac{1}{\overline{\gamma}_{sr}} + \frac{1}{\overline{\gamma}_{rd}}, \tag{3.24}$$

Using (3.24) PDF of $\gamma_T$ is derived as

$$p_{\gamma_T}(\gamma) = \beta exp(-\gamma\beta). \tag{3.25}$$

*Derivation of PDF of $\gamma_E$:*

At this point, it is needed to derive PDF of $\gamma_E$. Since the received SNR of the eavesdropper at the first and second hop are exponentially distributed, related PDFs can be written as

$$p_{\gamma_{se}}(\gamma) = \frac{1}{\overline{\gamma}_{se}} exp(\frac{-\gamma}{\overline{\gamma}_{se}}), \tag{3.26}$$

$$p_{\gamma_{re}}(\gamma) = \frac{1}{\overline{\gamma}_{re}} exp(\frac{-\gamma}{\overline{\gamma}_{re}}), \tag{3.27}$$

in which the average received SNRs of the eavesdropper is the first and second hop are respectively, given by

$$\overline{\gamma_{se}} = \frac{P_S E\{| h_{se} |^2\}}{\sigma^2}, \tag{3.28}$$

$$\overline{\gamma_{re}} = \frac{P_R E\{| h_{re} |^2\}}{\sigma^2}, \tag{3.29}$$

Using the fact that $\gamma_{se}$ and $\gamma_{re}$ are independent, if $\gamma > 0$, CDF of $\gamma_E$ is given by [120, Sec. 6-45]

$$P_{\gamma_E}(\gamma) = 1 + \theta[\overline{\gamma_{re}} exp(\frac{-\gamma}{\overline{\gamma_{re}}}) - \overline{\gamma_{se}} exp(\frac{-\gamma}{\overline{\gamma_{se}}})], \tag{3.30}$$

where $\theta$ is defined as

$$\theta \triangleq \frac{1}{\overline{\gamma_{se}} - \overline{\gamma_{re}}}. \tag{3.31}$$

Hence, PDF of $\gamma_E$ is expressed by

$$p_{\gamma_E}(\gamma) = \theta[exp(\frac{-\gamma}{\overline{\gamma_{se}}}) - exp(\frac{-\gamma}{\overline{\gamma_{re}}})]. \tag{3.32}$$

*Derivation of CDF of $\gamma_S$:*
Using (3.23) and (3.48) in (3.20) results in [121, Sec. 3.310]

$$P_{\gamma_S}(\gamma) = 1 - \theta[\frac{1}{\beta\gamma + \frac{1}{\overline{\gamma_{se}}}} - \frac{1}{\beta\gamma + \frac{1}{\overline{\gamma_{re}}}}] exp(\beta - \beta\gamma). \tag{3.33}$$

### 3.3.3 Probability of Outage in Secrecy Capacity

The probability that instantaneous secrecy capacity of this system is lower than a target secrecy rate, $R_s$ refers to the probability of outage in secrecy capacity and it can be written as

$$P_{out}(R_s) = Pr[C_s < R_s]. \tag{3.34}$$

Using the total probability theorem results in [120, eq. (2-41)], [50]

$$\begin{aligned} P_{out}(R_s) = {} & Pr[C_s < R_s | \gamma_T > \gamma_E] Pr[\gamma_T > \gamma_E] \\ & + Pr[C_s < R_s | \gamma_T \leq \gamma_E] Pr[\gamma_T \leq \gamma_E], \end{aligned} \tag{3.35}$$

where it can be written that

$$Pr[\gamma_T < \gamma_E] = 1 - Pr[C_s > 0], \tag{3.36}$$

Moreover, because of the fact that $R_s > 0$, it is given that [50]

$$Pr[C_s < R_s | \gamma_T \leq \gamma_E] = 1. \tag{3.37}$$

Thus, (3.35) can be rewritten as

$$\begin{aligned} P_{out}(C_s) &= Pr[C_s < R_s | C_s > 0] Pr[C_s > 0] + Pr[C_s \leq 0] \\ &= Pr[1 < \gamma_S < 2^{2R_s}] + Pr[\gamma_S < 1] \\ &= P_{\gamma_S}(2^{2R_s}), \end{aligned} \tag{3.38}$$

where CDF of $\gamma_S$ is given by (3.33).

### 3.3.4 A Case Study: Eavesdropper without joint decoding

At this point, the differences between considered system model and the case where the illegitimate node is not able to do the joint decoding, is explanted. If the eavesdropper is not capable of joint decoding it is given that

$$C_{s,1_{w/ojd}} = [log_2 \frac{1+\gamma_{sr}}{1+\gamma_{se}}]^+, \tag{3.39}$$

$$C_{s,2_{w/ojd}} = [log_2 \frac{1+\gamma_{rd}}{1+\gamma_{re}}]^+, \tag{3.40}$$

in which $C_{s,1}$ and $C_{s,2}$, respectively, represent secrecy capacity of the first and the second hop. Accordingly, secrecy capacity of the system in this case is given by

$$C_{sw/ojd} = min\ \{C_{s,1}, C_{s,2}\}, \tag{3.41}$$

where $w/o\ jd$ subscript refers to *without joint decoding* and secrecy capacity of the system with joint decoding in the presence of an eavesdropper was earlier given in (3.17).

The rest of this chapter is based on the assumption that the illegitimate entity is able to perform joint decoding between the signals received from the first and the second phase of transmission.

## 3.4 Improving the Secrecy by Using the Phase Shift Scheme

At this point, the goal is to improve the secrecy of the considered system model via a novel energy-efficient solution. The idea behind proposed scheme is making a modification at the signal of each hop such that the authorized receiver have access to the modification, while the illegitimate node is not able to detect it. The aforementioned modification must be based on a shared information between the communicating entities which is not available at the illegitimate nodes.

To achieve this goal, a random phase shifting scheme is proposed where at each hop a phase shift is applied to the in-phase and quadrature components of the original signal, as shown in Figure 3.2. The random phase shift is denoted by $\varphi_{n,k}$ where $k \in \{1, 2\}$ and k indicates the hop of transmission.

Initially, the original signal to be transmitted is represented by $s$ and it can be written that

$$s = x + jy, \tag{3.42}$$

where $x$ and $y$ are, respectively, the in-phase and quadrature components of the original signal and $j$ indicates the imaginary part. Prior to using the secrecy enhancement scheme, the received signal at the illegitimate node in the first and the second phases are, respectively, given by

$$r_{e,1} = \sqrt{P_s} h_{se} s + n_1, \tag{3.43}$$

$$r_{e,2} = \sqrt{P_r} h_{re} s + n_2. \tag{3.44}$$

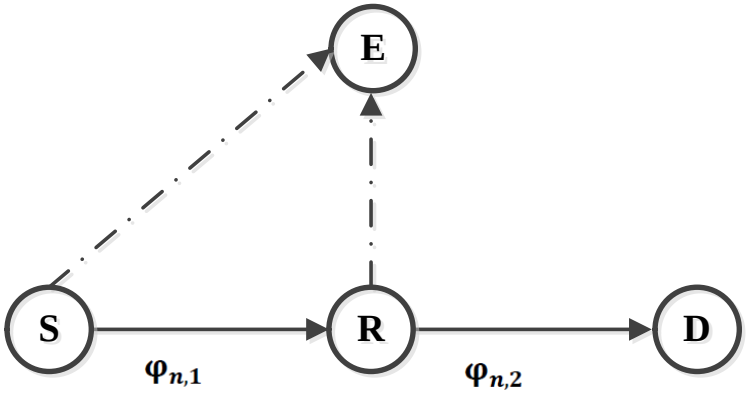


Figure 3.2: Security enhancement via using phase shift scheme.

Using the phase shifting scheme the original signal can be modified to $\acute{s}$ such that the random phase shift is applied to the modulated data of each hop and it is given that

$$\acute{s} = e^{j\varphi_{n,k}}(x + jy), \tag{3.45}$$

Once $\acute{s}$ is received, the intended receiver of the $k$th hop, which has access to $\varphi_{n,k}$, can remove the random phase shift and obtain the main signal. Notably, the eavesdropper is not aware of $\varphi_{n,k}$, so using the phase shifting scheme confuses the illegitimate entity. Thus, received SNR at the illegitimate node is degraded and secrecy capacity of the system is improved.

At this point, it must be clarified that how can the random phase shift be generated such that it is accessible for the legitimate communicating parties, but the eavesdropper is not aware of it. Some recent researches have focused on generating a shared secret between the communicating parties based on unique information that are shared between them, as this information is not available at the unauthorized entity. In this regard some existing studies have focused on generating a secret key based on reciprocal channel between the legitimate communicating entities [86]. There are two stages in order to create $\varphi_{n,k}$ which are as the following.

- Initially, it is required to estimate the channel between the communicating parties, $h_{sr}$ for the first hop or $h_{rd}$ for the second hop.
- Because of AWGN, the estimation of the channel at the communicating parties are different, so a key agreement procedure is utilized to ensure that both communicating entities have access to the same key.

Using the secrecy enhancement scheme and presuming that provision of $\varphi_{n,k}$ has been done successfully, the received signal at the illegitimate node in the first and the second phases are, respectively, given by

$$r_{e,1_{PS}} = \sqrt{P_s}h_{se}e^{j\varphi_{n,1}}s + n_1, \tag{3.46}$$

$$r_{e,2_{PS}} = \sqrt{P_r}h_{re}e^{j\varphi_{n,2}}s + n_2, \tag{3.47}$$

in which $n_1$ and $n_2$ denote AWGN of the eavesdropper respectively, in the first and the second hops and $PS$ subscript indicates using the $phase\ shift$ scheme.

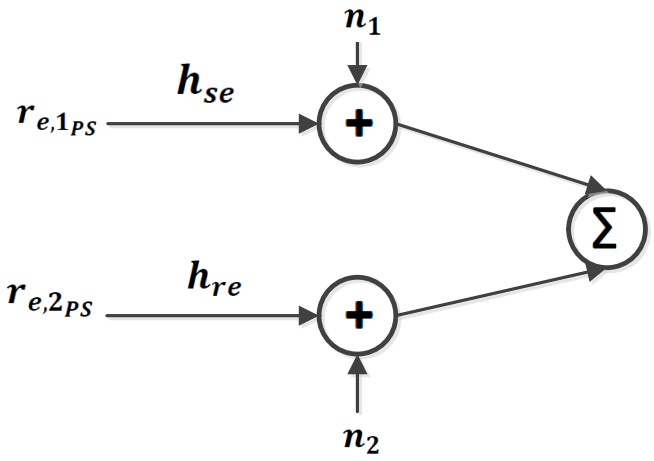


Figure 3.3: MRC at the eavesdropper.

Figure 3.3 shows MRC combining at the eavesdropper where the proposed secrecy enhancement scheme is used. Under the assumption that the eavesdropper is capable of MRC, and since the eavesdropper does not have access to $\varphi_{n,k}$, received SNR at the eavesdropper is given by

$$\gamma_{E,PS} = \frac{{P_S}^2 \mid h_{se} \mid^4 + {P_R}^2 \mid h_{re} \mid^4 + 2P_S P_R \mid h_{se} \mid^2 \mid h_{re} \mid^2 cos(\varphi_{n,1} - \varphi_{n,2})}{(P_S \mid h_{se} \mid^2 + P_R \mid h_{re} \mid^2)\sigma^2}, \tag{3.48}$$

Based on (3.15), if the proposed secrecy improvement scheme is not employed the received SNR at the illegitimate node can be written as

$$\begin{aligned} \gamma_E &= \frac{P_S \mid h_{se} \mid^2}{\sigma^2} + \frac{P_R \mid h_{re} \mid^2}{\sigma^2} \\ &= \frac{{P_S}^2 \mid h_{se} \mid^4 + {P_R}^2 \mid h_{re} \mid^4 + 2P_S P_R \mid h_{se} \mid^2 \mid h_{re} \mid^2}{(P_S \mid h_{se} \mid^2 + P_R \mid h_{re} \mid^2)\sigma^2}. \end{aligned} \tag{3.49}$$

Comparing (3.48) and (3.49), it can be concluded that $\gamma_{E,PS} < \gamma_E$. Meaning that by using the proposed secrecy improvement scheme, the received SNR of the illegitimate entity is degraded, compared to the case when phase shift scheme is not utilized.

## 3.5 Scheme Overview

It was shown that the proposed scheme degrades the received SNR at the illegitimate entity. Thus, since $C_s = (1/2)[log_2(1 + \gamma_T)/(1 + \gamma_E)]^+$, it can be written that

$$C_{s,PS} > C_s, \tag{3.50}$$

meaning that by using the proposed secrecy enhancement scheme, the instantaneous secrecy capacity of the system is improved. Furthermore, ergodic secrecy capacity of the system is given by [42]

$$\overline{C_s} = E\{C_s\}. \tag{3.51}$$

Since for two random variables of $X$ and $Y$ if $X < Y$ it can be concluded that $\overline{X} < \overline{Y}$, it is given that

$$\overline{C_s} < \overline{C_{s,PS}}. \tag{3.52}$$

Therefore, in addition to the instantaneous secrecy capacity, ergodic secrecy capacity of the system is improved.

## 3.6 Simulations and Performance Evaluation

Validity of the derivations and the proposed secrecy improvement scheme is investigated via simulations in MATLAB. A two-dimensional plane is utilized for the simulations. It is presumed that the source, relay, destination and the eavesdropper are placed at $S(-500, 0)$, $R(0, 0)$, $D(500, 0)$ and $E(d, 0)$ meters, respectively. Different values are assigned to $d$ during simulations. The global transmit power is assigned evenly between the transmitters (source and relay). It is considered that noise variance at all terminals is $-60$dBm [73]. The path loss coefficient is assumed to be 3.5. The Monte Carlo simulations are presented using an average of $10^5$ independent trials. The simulation parameters are summarized in table 3.1.

Table 3.1: Simulation set up parameters (phase shift scheme)

| Simulation Parameter | Value |
|---|---|
| Source location | (-500,0)m |
| Relay location | (0,0)m |
| Destination location | (500,0)m |
| Eavesdropper location | (0,d)m |
| $R_s$ | 0.1 |
| Path loss coefficient | 3.5 |
| $\sigma^2$ | -60dBm |

### 3.6.1 General Secrecy Evaluation

Secrecy capacity of the system with and without joint decoding capability at the eavesdropper has been simulated in Figure 3.4 where $d \in \{800, 1000, 1200\}$ meters. As Figure 3.4 illustrates joint decoding at the eavesdropper reduces secrecy capacity of the system significantly at higher transmit power levels.

Figure 3.5 depicts the probability of non-zero secrecy capacity as a function of global transmit power. It is seen that increasing the global transmit power may increase the probability of non-zero secrecy capacity if the eavesdropper is located far from the transmitters. On the contrary, if the eavesdropper is placed close to any of the transmitters, increasing the transmit power does not improve the probability of non-zero secrecy capacity. Therefore, increasing the global transmit power can have inverse effects on secrecy in terms of probability of non-zero secrecy capacity if the eavesdropper is located close to any of the transmitters. In such

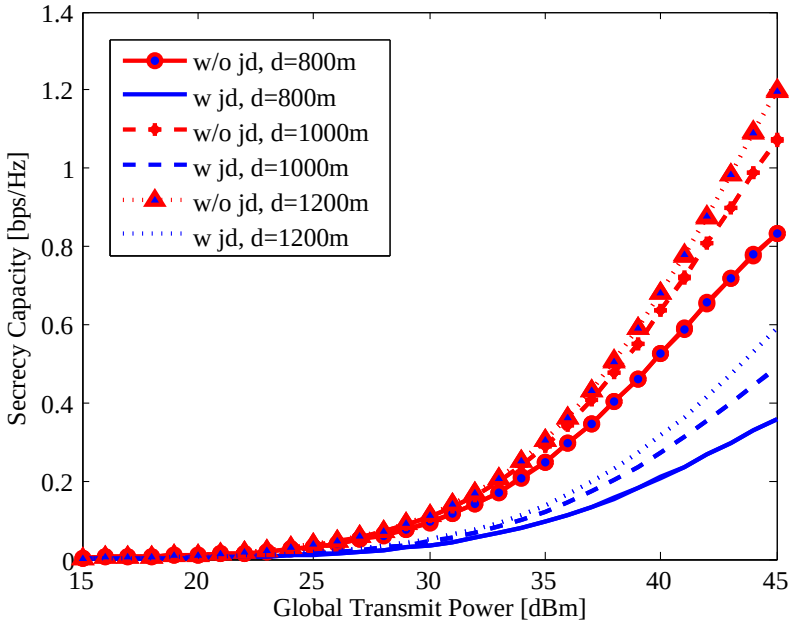


Figure 3.4: Probability of non-zero secrecy capacity versus global transmit power, with/without joint decoding at eavesdropper.

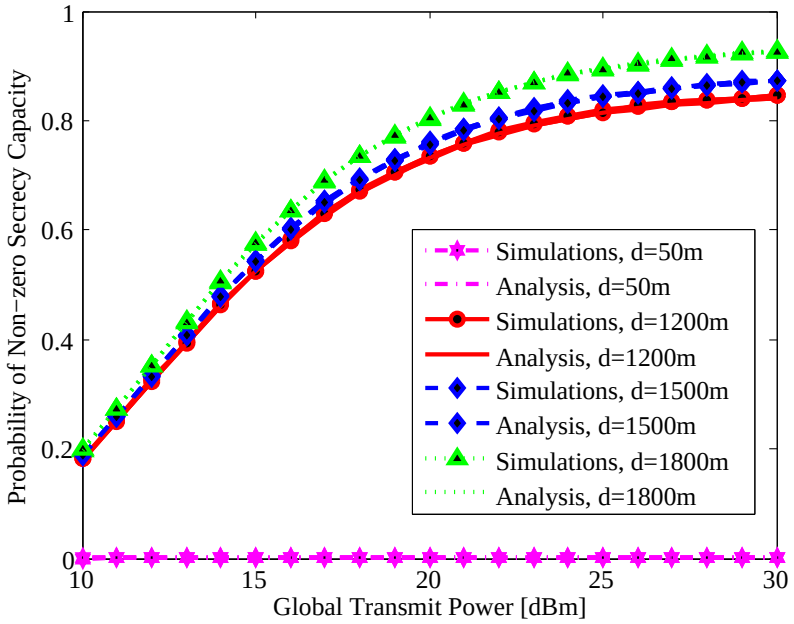


Figure 3.5: Probability of non-zero secrecy capacity versus global transmit power.

circumstances, higher transmit power results in more leakage of the signal to the illegitimate entities [122]. Figure 3.5 also shows that the simulation results agreed with the analytical results and therefore the closed-from expressions are validated.

Figure 3.6 shows the probability of outage in secrecy capacity as a function of global transit

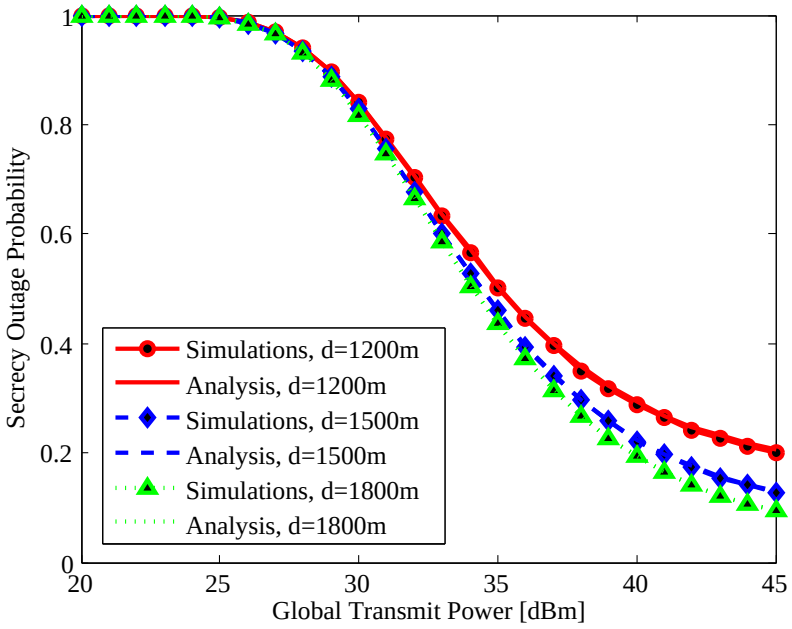


Figure 3.6: Probability of outage in secrecy capacity versus global transmit power, $R_s = 0.1$.

power. This figure illustrates that increasing the global transmit power can improve the secrecy of the system in terms of probability of outage in secrecy capacity, but as mentioned before, the effect of increasing global transmit power on secrecy also depends on the location of the eavesdropper. As if the eavesdropper is placed very close to any of the transmitters, increasing the transmit power can have adverse results on secrecy. Moreover, Figure 3.6 validates the closed-from expressions of probability of outage in secrecy capacity. It is obvious that by moving the eavesdropper to further locations secrecy of the system in terms of probability of outage in secrecy capacity and probability of non-zero secrecy capacity improves, as seen in Figure 3.5 and Figure 3.6.

### 3.6.2 Evaluation of Proposed Random Phase Shift Scheme

For the purpose of evaluating the performance of the proposed secrecy improvement scheme, it is presumed that $\varphi_{n,k}$ is a random variable with uniform distribution where

$$\varphi_{n,k} \sim U[0, 2\pi]. \tag{3.53}$$

By using the proposed scheme, as seen in Figure 3.7, ergodic secrecy capacity of the system improves significantly. To investigate the effect of the proposed scheme at higher levels of power, according to (3.17), when $P_S, P_R \to \infty$ it can be written that

$$C_s = \frac{1}{2}[log_2 \frac{\gamma_T}{\gamma_E}]^+. \tag{3.54}$$

Thus, based on (3.48) at higher levels of power, the proposed scheme always results in a better secrecy performance compared to the case where the phase shift scheme is not employed.

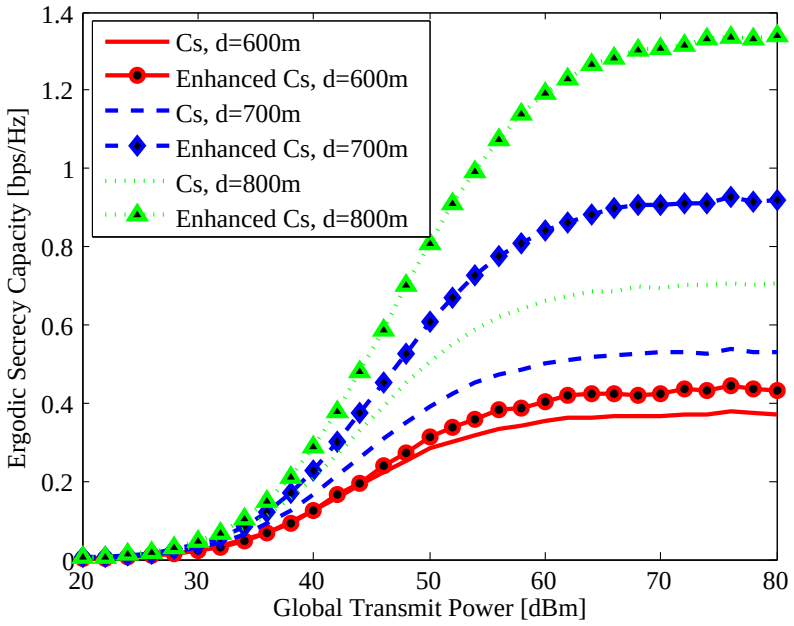


Figure 3.7: Ergodic secrecy capacity versus global transmit power.

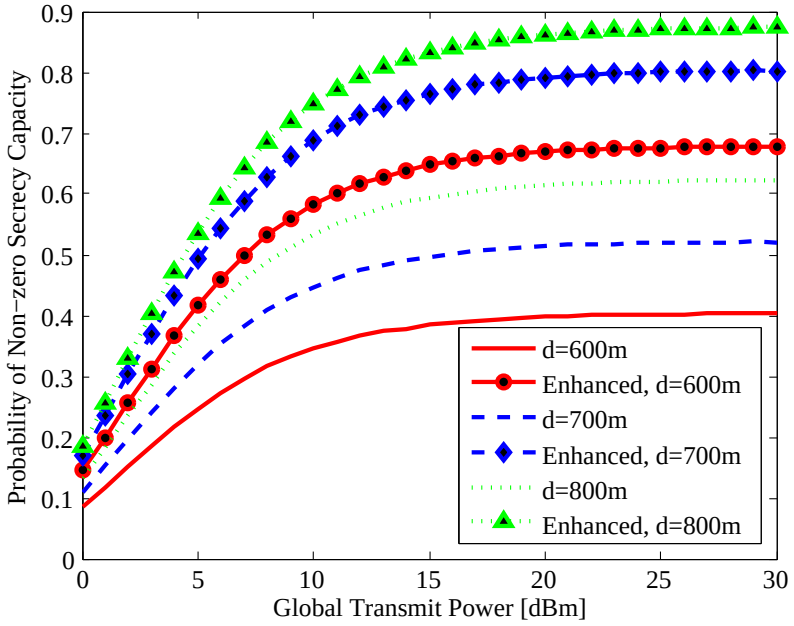


Figure 3.8: Probability of non-zero secrecy capacity versus global transmit power, phase shift scheme.

However, the secrecy capacity of the system at higher power levels has an upper bound which is due to the location of the eavesdropper, as it is seen in Figure 3.7.

Next, Figure 3.8 illustrates that the proposed secrecy enhancement scheme can improve the secrecy in terms of probability of non-zero secrecy capacity. This figure also implies the bounds on secrecy due to the location of the eavesdropper.

## 3.7 Discussion

According to the previous section, the main contributions are elaborated as the following.

- The numerical results validated the closed-form expressions of the probability of outage in secrecy capacity and the probability of non-zero secrecy capacity.
- Although increasing the transmit power can improve the secrecy, this is not always valid. The effect of increasing the power must be examined according to the location of the eavesdropper, as if the illegitimate node is close to the transmitter, increasing the transmit power does not improve the secrecy.
- The bound of secrecy capacity on high power levels refers back to the location of the eavesdropper.
- The proposed secrecy improvement scheme always outperforms the initial transmission in terms of ergodic secrecy capacity of the system.

## 3.8 Summary

In this chapter, a novel secrecy enhancement scheme was proposed to improve the ergodic secrecy capacity of a two-hop DF relaying system in which the unauthorized entity was able to overhear the communications of both hops. The closed-form expressions of the probability of non-zero secrecy capacity and probability of outage in secrecy capacity were presented.

Moreover, a random phase shift scheme was suggested to improve the security. The introduced scheme injected a random phase shift at the modulated data symbols of the hops where the related phase shift was created based on a shared information between the transmitter and desired receiver of each hop such that the adversary nodes were not aware of it. Using this scheme, the received SNR at the illegitimate node was degraded and accordingly secrecy capacity of the system was improved. The channel reciprocity between the source and relay in the first hop, or the relay and destination in the second hop could be exploited to create the random phase shift. It was shown that using this scheme boosted the ergodic secrecy capacity of the system. The proposed scheme is applicable in the systems where the power resources are limited. In addition, due to the ease of using channel reciprocity, the complexity of the presented scheme is low.

# Chapter 4

# Improving the Secrecy in Multi-hop DF Relaying Systems

In this chapter, secure transmission in a multi-hop DF relaying system over Rayleigh fading channels is investigated where the transmission is carried out in the presence of multiple non-colluding illegitimate entities. It is important to analyze the secrecy performance of the system in such a scenario in order to better understand the secrecy risks and to improve the secrecy rate of the system. Consequently, secrecy parameters of this system (e.g., probability of non-zero secrecy capacity, probability of outage in secrecy capacity) is examined.

The objective of this chapter is to present a cost-effective solution to improve the secrecy where there are multiple wiretappers which can overhear the communication. A novel secrecy improvement strategy is suggested, based on a new way of using artificial noise, and it is shown that ergodic secrecy capacity of the system can have significant improvement via exploiting this strategy . In particular, in the new way of using artificial noise, the jamming signal is generated at the transmitter based on a shared knowledge between the source and the desired receiver. Due to the importance of power allocation between friendly jamming and main signal, power allocation solutions are also presented in this chapter, to make sure that the proposed scheme have helpful results in terms of secrecy.

## 4.1 Introduction

Multi-hop communications are one of the most promising techniques in wireless communications because of their remarkable advantages, as they mitigate channel fading and shadowing and increase the coverage [123]. Reliability and performance of multi-hop communication systems have already been studied widely in the litrature [25]-[27].

However, secrecy and privacy of wireless communications is one of the main concerns of in multi-hop communication systems due to the broadcast characteristic of wireless medium. Secure communications aims at providing the information at the intended receiver while ensuring that the illegitimate and unauthorized nodes do not have access to it. In this regard, physical layer security has lately attracted a lot of research efforts[30]. To this end, the physical characteristic of the wireless channel can be used in relaying communication systems to enhance the security [114]. Specifically, it has been shown that under certain circumstances, secrecy capac-

ity of a wireless communication system can improve from zero to a positive secrecy capacity via using relays [124]. Some existing studies have focused on a simple case where communication takes place in the presence of a single illegitimate entity [6], [30],[125]. In particular, the work presented in [30] investigated the communication of a multi-hop DF relaying system in the presence of an eavesdropper and it presented an optimized relay placement scheme which maximized the secrecy capacity.

In addition, communications in the enarioes where multiple eavesdroppers are able to wiretap the transmission signal, was examined in [50] and [64]. An interesting work in [6], pointed out that degrading the received SNR at the illegitimate entities, via artificial noise, can increase the secrecy of a communication system. The basic idea of artificial noise was initially introduced by [71] and [126]. Artificial noise has also been called cooperative jamming and secure relaying in some existing studies [114],[126]. Notably, conventional way of using artificial noise needs an extra hardware to create friendly jamming signal. Moreover, the network overheads, for the purpose of coordination between the main network and the helper, is increased. Thus, many researchers have been led to alternative secrecy improvement schemes [100], [125].

Recently, authors of [44] suggested that transmitters of a two-hop communication system should allocate a portion of their available power to create friendly jamming. It was considered that the artificial noise was created according to a shared secret between the transmitter and intended receiver, but the illegitimate entity was not aware of it. This interesting strategy is cost-effective, as the extra helper is not required and the coordination between the additional node and the original network is eliminated. In this chapter, the aforementioned strategy is extended to a multi-hop DF relaying communication system. In addition, a more complex case is studied where there are multiple eavesdroppers which can wiretap the communication signal.

## 4.2 System Model

The wireless system model shown in Fig. 4.1 is considered, where the source and destination can communicate through $N-1$ intermediate DF relays. This chapter mainly deals with the case where communication takes place in the presence of $M$ non-colluding eavesdroppers. During the transmission of each codeword from one node to the other, the related channel fading coefficients are constant. However, the fading coefficients vary independently and randomly whenever the codewords change [127].

For simplicity, throughout the formulations , the source and the destination are, respectively, tagged by 0 and $N$ while $k$ denotes $k$th relay, $k = \{1, 2, ..., N-1\}$. Also, the channel related to the link from node $i$ to node $j$ is represented by $h_{ij}$ and the channel fading coefficients of each two nodes are independent from the other pairs of nodes. The practical assumption that all the nodes in this system model are half-duplex, is valid. Additionally, a similar assumption as in [92] is used, where it is presumed that the nodes can solely receive signals from their adjacent neighbors located in their most left-handed side and the most right-handed side. Hence the direct link between the source and the destination does not exist and transmission from the source to the intended receiver is performed in $N$ phases.

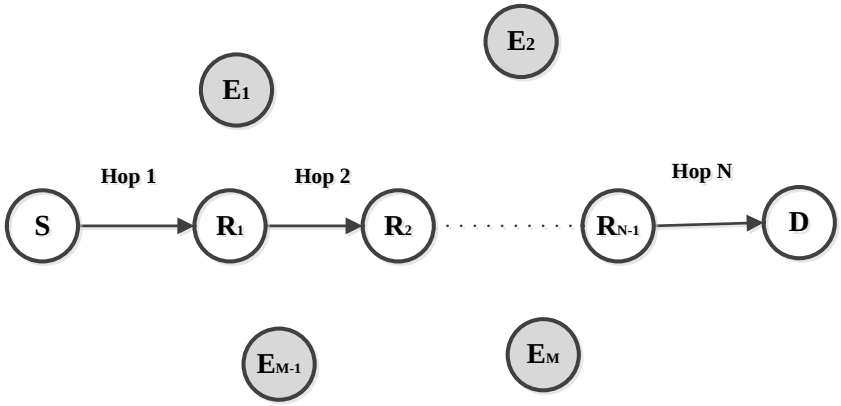


Figure 4.1: Communication through multiple DF relays in the presence of $M$ eavesdroppers.

## 4.3 Preliminaries

Based on what mentioned earlier in chapter 2, the maximal value of transmission rate from the source to the intended receiver such that the illegitimate entity cannot access the data, is termed secrecy capacity. Accordingly, secrecy capacity of $k$th hop can be written as [17, p. 62]

$$C_{s,k} = [C_{t,k} - C_{e,k}]^{+}, \tag{4.1}$$

in which $C_{t,k}$ and $C_{e,k}$, respectively, represent the capacity of the main and eavesdropper links at $k$th hop of transmission. Capacity of the main link at $k$th hop is given by

$$C_{t,k} = log_2(1 + \gamma_{t,k}), \tag{4.2}$$

in which $\gamma_{t,k}$ is the instantaneous received SNR of $k$th node at $k$th phase of transmission and it is expressed as

$$\gamma_{t,k} = \frac{P_{k-1,k} \mid h_{(k-1)k} \mid^2}{\sigma^2}, \tag{4.3}$$

where $P_{k-1,k}$ is the transmission power of $(k-1)$th node at $k$th hop of transmission.

It is presumed that $\sigma^2$ is the variance of AWGN noise at all the entities. It is considered that communication takes place over Rayleigh fading channels and fading coefficients are assumed to be zero-mean complex Gaussian random variables.

Therefore, $\gamma_{t,k}$ has exponential distribution and related PDF and CDF , respectively, are expressed by [118, p. 188]

$$p_{\gamma_{t,k}}(\gamma) = \frac{1}{\overline{\gamma_{t,k}}} exp(-\frac{\gamma}{\overline{\gamma_{t,k}}}), \tag{4.4}$$

$$P_{\gamma_{t,k}}(\gamma) = 1 - exp(-\frac{\gamma}{\overline{\gamma_{t,k}}}), \tag{4.5}$$

in which $\overline{\gamma_{t,k}}$ is the average received SNR at $k$th hop and it is given by

$$\overline{\gamma_{t,k}} = \frac{P_{k-1,k} E\{\mid h_{(k-1)k} \mid^2\}}{\sigma^2}. \tag{4.6}$$

In this chapter, it is presumed that transmission of different hops are carried out via using randomized code-books. Accordingly, the illegitimate nodes cannot jointly decode the received signals of different phases [124]. Thus, the capacity of the eavesdropper link at $k$th hop is given by

$$C_{e,k} = log_2(1 + \gamma_{e,k}), \tag{4.7}$$

where the instantaneous received SNR of the eavesdropper link at $k$th phase of transmission is represented by $\gamma_{e,k}$. Reverting back to the assumption that the multiple eavesdroppers in this system model are non-colluding, the instantaneous received SNR of the eavesdropper link at $k$th phase of transmission is given by [129]

$$\gamma_{e,k} = \max_{m=1}^{M} \gamma_{e_m,k}, \tag{4.8}$$

in which $\gamma_{e_m,k}$ is the received SNR of the $m$th eavesdropper at $k$th phase of transmission and it is given by

$$\gamma_{e_m,k} = \frac{P_{k-1,k} \mid h_{(k-1)e_m} \mid^2}{\sigma^2}. \tag{4.9}$$

Moreover, CDF of $\gamma_{e_m,k}$ is expressed by

$$P_{\gamma_{e_m,k}}(\gamma) = 1 - exp(-\frac{\gamma}{\overline{\gamma_{e_m,k}}}), \tag{4.10}$$

where at $k$th phase of transmission, the average received SNR of the $m$th illegitimate node is represented by $\overline{\gamma_{e_m,k}}$ and it is given that

$$\overline{\gamma_{e_m,k}} = \frac{P_{k-1,k} E\{\mid h_{(k-1)e_m} \mid^2\}}{\sigma^2}. \tag{4.11}$$

Assuming that secrecy decisions rely on a per hop basis, secrecy capacity of the system is given by

$$C_s = \frac{1}{N} \min_{k=1}^{N} C_{s,k}, \tag{4.12}$$

where $1/N$ refers back to the fact that transmission from the source to the intended destination is performed in $N$ phases.

## 4.4 Transmission in the Presence of Multiple Non-colluding Eavesdroppers

In this section, the analysis for the main security performance criteria of this system model are presented. Specifically, the closed-form expression of probability of non-zero secrecy capacity and probability of outage in secrecy capacity are derived and ergodic secrecy capacity of this system model is examined. Prior to any secrecy analysis, the parameters $\omega_k$ and $\omega_{e2e}$ are introduced as the following to facilitate the analysis.

$$\omega_k \triangleq \frac{1 + \gamma_{t,k}}{1 + \gamma_{e,k}}, \tag{4.13}$$

$$\omega_{e2e} \triangleq \min_{k=1}^{N} \omega_k. \tag{4.14}$$

Therefore, (4.12) can be rewritten as

$$C_s = \frac{1}{N} log_2 \omega_{e2e}, \tag{4.15}$$

Since the values of $\omega_k$ are statistically independent, CDF of $\omega_{e2e}$ is expressed by

$$\begin{aligned} P_{\Omega_{e2e}}(\omega) &= 1 - Pr[\omega_1 > \omega, ...., \omega_N > \omega] \\ &= 1 - \prod_{k=1}^{N} (1 - P_{\Omega_k}(\omega)), \end{aligned} \tag{4.16}$$

in which $P_{\Omega_k}(.)$ is CDF of $\omega_k$ and it can be written as

$$\begin{aligned} P_{\Omega_k}(\omega) &= Pr[\omega_k < \omega] \\ &= Pr[\frac{1 + \gamma_{t,k}}{1 + \gamma_{e,k}} < \omega]. \end{aligned}^2 \tag{4.17}$$

Hence, it is concluded that

$$P_{\Omega_k}(\omega) = \int_0^{\infty} P_{\gamma_{t,k}}(\omega(1 + \gamma_e) - 1) p_{\gamma_{e,k}}(\gamma_e) d\gamma_e, \tag{4.18}$$

Accordingly to (4.18), in order to derive $P_{\Omega_k}(.)$, $P_{\gamma_{t,k}}(.)$ and $p_{\gamma_{e,k}}(.)$ are required. $P_{\gamma_{t,k}}(.)$ has already been provided in (4.5), so at this point it is needed to derive PDF of $\gamma_{e,k}$.

*Derivation of $p_{\gamma_{e,k}}(.)$:*

Using (4.8), CDF of $\gamma_{e,k}$ can be written as

$$P_{\gamma_{e,k}}(\gamma) = \prod_{m=1}^{M} P_{\gamma_{e_m,k}}(\gamma). \tag{4.19}$$

Inserting (4.10) into (4.18) yields

$$\begin{aligned} P_{\gamma_{e,k}}(\gamma) &= \prod_{m=1}^{M} (1 - exp(-\frac{\gamma}{\overline{\gamma_{e_m,k}}})) \\ &= \sum_{j_1=0}^{1} \sum_{j_2=0}^{1} ... \sum_{j_M=0}^{1} (-1)^{j_1 + j_2 + ... + j_M} \times \\ & exp(\frac{-j_1\gamma}{\overline{\gamma_{e_1,k}}} + \frac{-j_2\gamma}{\overline{\gamma_{e_2,k}}} + ... + \frac{-j_M\gamma}{\overline{\gamma_{e_M,k}}}). \end{aligned} \tag{4.20}$$

Using (4.20), PDF of $\gamma_{e,k}$ is given by

$$\begin{aligned} p_{\gamma_{e,k}}(\gamma) = \sum_{j_1=0}^{1} \sum_{j_2=0}^{1} ... \sum_{j_M=0}^{1} (-1)^{j_1 + j_2 + ... + j_M} \times \\ (\frac{-j_1}{\overline{\gamma_{e_1,k}}} + \frac{-j_2}{\overline{\gamma_{e_2,k}}} + ... + \frac{-j_M}{\overline{\gamma_{e_M,k}}}) \times \\ exp(\frac{-j_1\gamma}{\overline{\gamma_{e_1,k}}} + \frac{-j_2\gamma}{\overline{\gamma_{e_2,k}}} + ... + \frac{-j_M\gamma}{\overline{\gamma_{e_M,k}}}). \end{aligned} \tag{4.21}$$

*Derivation of $P_{\Omega_k}$:*

In order to derive CDF of $\Omega_k$, (4.5) and (4.21) are substituted in (4.18). Hence it is given that

$$P_{\Omega_k}(\omega) = 1 - e^{\frac{-\omega+1}{\gamma_{t,k}}} \sum_{j_1=0}^{1}\sum_{j_2=0}^{1}...\sum_{j_M=0}^{1}(-1)^{j_1+j_2+...+j_M}\times \left(\frac{-j_1}{\gamma_{e_1,k}} + \frac{-j_2}{\gamma_{e_2,k}} + ... + \frac{-j_M}{\gamma_{e_M,k}}\right)\times \frac{1}{\left(\frac{\omega}{\gamma_{t,k}} + \frac{j_1}{\gamma_{e_1,k}} + \frac{j_2}{\gamma_{e_2,k}} + ... + \frac{j_M}{\gamma_{e_M,k}}\right)}. \tag{4.22}$$

*Derivation of $P_{\Omega_{e2e}}(\omega)$:*

Based on (4.16) and (4.22), CDF of $\Omega_{e2e}$ is given by

$$P_{\Omega_{e2e}}(\omega) = 1 - \prod_{k=1}^{N}\left[e^{\frac{-\omega+1}{\gamma_{t,k}}} \sum_{j_1=0}^{1}\sum_{j_2=0}^{1}...\sum_{j_M=0}^{1}(-1)^{j_1+j_2+...+j_M}\times \left(\frac{-j_1}{\gamma_{e_1,k}} + \frac{-j_2}{\gamma_{e_2,k}} + ... + \frac{-j_M}{\gamma_{e_M,k}}\right)\times \frac{1}{\left(\frac{\omega}{\gamma_{t,k}} + \frac{j_1}{\gamma_{e_1,k}} + \frac{j_2}{\gamma_{e_2,k}} + ... + \frac{j_M}{\gamma_{e_M,k}}\right)}\right]. \tag{4.23}$$

### 4.4.1 Probability of Non-zero Secrecy Capacity

It has been defined in chapter 2 that the probability of non-zero secrecy capacity indicates the probability that the capacity of the main channel is higher than the capacity of the eavesdropper channel. Therefore, in the considered system model it is given by

$$Pr[C_s > 0] = Pr[C_r > C_e]. \tag{4.24}$$

According to (4.15), (4.24) can be derived as

$$\begin{aligned} Pr[C_s > 0] &= Pr[\omega_{e2e} > 1] \\ &= 1 - P_{\Omega_{e2e}}(1). \end{aligned} \tag{4.25}$$

where $P_{\Omega_{e2e}}(.)$ is given by (4.23).

### 4.4.2 Probability of Outage in Secrecy Capacity

As mentioned in chapter 2, the probability that the instantaneous secrecy capacity is lower than a target secrecy rate, $R_s$, refers to the probability of outage in secrecy capacity and it is expressed by [50].

$$P_{out}(R_s) = Pr[C_s < R_s], \tag{4.26}$$

where $R_s$ represents the desired secrecy rate. Based on the total probability theorem, (4.26) is reformulated as

$$\begin{aligned} P_{out}(C_s) &= Pr[C_s < R_s | C_s > 0] Pr[C_s > 0] + Pr[C_s \leq 0] \\ &= P_{\Omega_{e2e}}(2^{N \times R_s}). \end{aligned} \tag{4.27}$$

where CDF of $\omega_{e2e}$ is expressed by (4.23).

### 4.4.3 Ergodic Secrecy Capacity

The mathematical expectation (i.e., mean or average) of maximum achievable secrecy rate implies ergodic secrecy capacity and for the considered system model, it is expressed by [72]

$$\overline{C_s} = \frac{1}{N} E\{\min_{k=1}^{N} C_{s,k_{AN}}\}. \tag{4.28}$$

ESC is a secrecy performance criterion which has been used widely in literature and this chapter to evaluate and assess the secrecy of communication systems.

## 4.5 A Case Study: Communication in the Presence of Colluding Eavesdroppers.

Although the considered system model is based on the non-colluding eavesdroppers assumption, at this point, the colluding wiretappers scenario is briefly studied to clarify the differences between collaborative and the non-collaborative eavesdroppers. As it was mentioned in chapter 2, colluding eavesdroppers is the worse case scenario in terms of secrecy, where at each hop, the eavesdroppers are able to overhear the transmitted information and perform maximal ratio combining. Thus, base on equation (2.9) the received SNR of the illegitimate link at $k$th hop can be written as [129]

$$\gamma_{e,k} = \sum\nolimits_{m=1}^{M} (\gamma_{e_m,k}), \tag{4.29}$$

where $\gamma_{e_m,k}$ is given by (4.9). Due to the fact that the fading coefficients of all channels are zero-mean complex Gaussian random variables, $\gamma_{e_m,k}$ are independent and exponentially distributed variables. Accordingly, based on (4.29) and [130], PDF of $\gamma_{e_m,k}$ can be written as

$$p_{\gamma_{e,k}}(\gamma) = [\prod_{m=1}^{M} \frac{1}{\overline{\gamma_{e_m,k}}}] \sum_{j=0}^{M} \frac{e^{\frac{-\gamma}{\overline{\gamma_{e_m,j}}}}}{\prod_{i=1, i\neq j}^{M} (\frac{1}{\overline{\gamma_{e_m,i}}} - \frac{1}{\overline{\gamma_{e_m,j}}})} \tag{4.30}$$

Henceforth, the aim is to derive the CDF of $\Omega_{e2e}$ in the presence of multiple colluding eavesdroppers. Applying (4.5) and (4.30) in (4.18) results in

$$\begin{aligned} P_{\Omega_k}(\omega) = 1 - e^{\frac{-\omega+1}{\overline{\gamma_{t,k}}}} [\prod_{m=1}^{M} \frac{1}{\overline{\gamma_{e_m,k}}}] \times \\ \sum_{j=0}^{M} (\frac{1}{\prod_{i=1, i\neq j}^{M} (\frac{1}{\overline{\gamma_{e_m,i}}} - \frac{1}{\overline{\gamma_{e_m,j}}})} \times \frac{1}{\omega + \frac{1}{\overline{\gamma_{e_m,j}}}}) \end{aligned} \tag{4.31}$$

Utilizing (4.31) in (4.16), CDF of $\omega_{e2e}$ is given by

$$P_{\Omega}(\omega) = 1 - \prod_{k=1}^{N}[e^{\frac{-\omega+1}{\overline{\gamma}_{t,k}}}[\prod_{m=1}^{M}\frac{1}{\overline{\overline{\gamma}_{e_m,k}}}]\times \sum_{j=0}^{M}(\frac{1}{\prod_{i=1,i\neq j}^{M}(\frac{1}{\overline{\overline{\gamma}_{e_m,i}}}-\frac{1}{\overline{\overline{\gamma}_{e_m,j}}})}\times\frac{1}{\omega+\frac{1}{\overline{\overline{\gamma}_{e_m,j}}}})]. \tag{4.32}$$

## 4.6 Exploiting Artificial Noise

As it was mentioned previously in chapter 2, the artificial noise in essence is an interference which is created intentionality in order to mislead the eavesdropper and therefore, degrade the received SNR at the illegitimate entity and improve the secrecy. Authors of a recent work [44], have presented a different way of using artificial noise in which the transmitter assigns a portion of its power to create friendly jamming signal, i.e., intentional jamming is generated at the transmitter and thus, an extra node is not needed.

In this chapter, the latter way of generating artificial noise is employed because of the reasons which are as the following.

- This approach does not rely on any extra entity to create the jamming signal.
- Unlike conventional artificial noise, the coordination between the additional node and the main network is not needed, which results in lower complexity.

In terms of implementation of the new approach of using artificial noise, a pseudo-random noise generator can be utilized to generate friendly jamming signal where there are finite statuses for the noise generator. Using a secure control channel, the status of the pseudo-random noise generator is sent to the intended receiver of each hop. Hence, the intended receiver can be informed about the created artificial noise so it can eliminate the intentional noise and retrieve the main signal [44].

## 4.7 Proposed Security Enhancement Scheme via Artificial Noise

In this section, a secrecy improvement scheme is presented to be employed in the multi-hop DF relaying system shown in Fig. 4.1. The proposed scheme exploits friendly jamming to enhance the secrecy by degrading the received SNR at the eavesdroppers where transmission is taking place in the presence of multiple non-colluding illegitimate nodes.

In order to extend the new approach of using artificial noise to the considered system model, it is suggested that at $k$th hop of transmission, from node $k-1$ to the node $k$, the transmitter is permitted to assign a portion of its available power to create the friendly jamming. Thus, the artificial noise is sent in addition to the main signal, and the received signal of $k$th node at $k$th phase of transmission is given by

$$y_{k,k_{AN}} = \sqrt{\alpha_k P_{t_{k-1}}} h_{(k-1)k} x_k + \sqrt{(1-\alpha_k) P_{t_{k-1}}} h_{(k-1)k} \acute{x_k} + n_k, \tag{4.33}$$

in which $x_k$ and $\acute{x_k}$, respectively, denote the main signal and the cooperative jamming signal. Moreover, $\alpha_k$ represent the power allocation factor at $k$th hop between the main signal and artificial noise, $0 \leq \alpha_k \leq 1$. Hereon, $n_k$ represents noise at the $k$th intended receiver. Similarly, the received signal of $m$th eavesdropper at $k$th phase of transmission is given by

$$y_{e_m,k} = \sqrt{\alpha_k P_{t_{k-1}}} h_{(k-1)e_m} x_k + \sqrt{(1-\alpha_k) P_{t_{k-1}}} h_{(k-1)e_m} \acute{x_k} + n_e, \tag{4.34}$$

where $n_{e_m}$ is noise of the $m$th eavesdropper at $k$th phase of transmission.

Because of the elimination of the friendly jamming at the intended receiver, the received SNR of $k$th node at $k$th phase of signal transmission can be written as

$$\gamma_{t,k_{AN}} = \frac{\alpha_k P_{t_{k-1}} \mid h_{(k-1)k} \mid^2}{\sigma^2}. \tag{4.35}$$

Using equation (4.3), (4.35) can be rewritten as

$$\gamma_{t,k_{AN}} = \alpha_k \gamma_{t,k}. \tag{4.36}$$

Since the $m$th eavesdropper is not aware of the intentional interference, its received SNR at $k$th hop can be given as

$$\gamma_{e_m,k_{AN}} = \frac{\alpha_k P_{t_{k-1}} \mid h_{(k-1)e_m} \mid^2}{\sigma^2 + (1-\alpha_k) P_{t_{k-1}} \mid h_{(k-1)e_m} \mid^2}. \tag{4.37}$$

Invoking (4.8), it can be concluded that

$$\gamma_{e,k_{AN}} = \max_{m=1}^{M} \frac{\alpha_k P_{t_{k-1}} \mid h_{(k-1)e_m} \mid^2}{\sigma^2 + (1-\alpha_k) P_{t_{k-1}} \mid h_{(k-1)e_m} \mid^2}. \tag{4.38}$$

Thus, using artificial noise, secrecy capacity of $k$th phase is given by

$$C_{s,k_{AN}} = [log_2(\frac{1+\alpha_k \gamma_{t,k}}{1+\gamma_{e,k_{AN}}})]^+. \tag{4.39}$$

Henceforth, parameters $\omega_{kAN}$ and $\omega_{AN}$ are defined to facilitate the formulations.

$$\omega_{kAN} \triangleq \frac{1+\alpha_k \gamma_{t,k}}{1+\gamma_{e,k_{AN}}}, \tag{4.40}$$

$$\omega_{AN} \triangleq \min_{k=1}^{N} \omega_{kAN}. \tag{4.41}$$

Substituting these definitions, (4.39) can be rewritten as

$$C_{s,k_{AN}} = [log_2 \omega_{kAN}]^+. \tag{4.42}$$

Accordingly, it is given that

$$2^{NC_{s,k_{AN}}} \propto \omega_{kAN}, \tag{4.43}$$

and

$$2^{NC_{sAN}} \propto \omega_{AN}. \tag{4.44}$$

Therefore, if using artificial noise-based scheme results in increasing $\min_{k=1}^{N}\omega_{kAN}$, it can be concluded that $\min\{C_{s,1_{AN}}, ...C_{s,N_{AN}}\} > \min\{C_{s,1}, ..., C_{s,N}\}$, and so $C_{sAN} > C_s$, meaning that the instantaneous secrecy capacity of the system is improved. Notably, these results can be extended to ergodic secrecy capacity. As for two random variables, $X$ and $Y$, if $X > Y$, it can be written that $E\{X\} > E\{Y\}$. Thus, it is written that $E\{C_{sAN}\} > E\{C_s\}$.

Substituting equations (4.8), (4.35) and (4.37) in (4.40) results in

$$\begin{aligned}\omega_{kAN} &= \frac{1 + \frac{\alpha_k P_t |h_{(k-1)k}|^2}{\sigma^2}}{1 + \max_{m=1}^{M} \frac{\alpha_k P_t |h_{(k-1)e_m}|^2}{\sigma^2 + (1-\alpha_k) P_t |h_{(k-1)e_m}|^2}} \\ &= \frac{1 + \alpha_k \gamma_{t,k}}{1 + \max_{m=1}^{M} \frac{\alpha_k \gamma_{e_m,k}}{1 + (1-\alpha_k)\gamma_{e_m,k}}}.\end{aligned} \tag{4.45}$$

Equation (4.45) indicates the importance of power allocation between the main signal and the friendly jamming in order to ensure that $\omega_{kAN}$ and $\omega_{AN}$ are improved.

## 4.8 Power Allocation

Presenting power allocation strategies between main signal and friendly jamming signal is the aim of this section. Notably, this problem can be solved under two circumstances as below:

- Global CSI including the channel state information of the eavesdroppers is available.
- Channel state information of the eavesdroppers is not available (neither instantaneous CSI nor its statistics).

It it presumed that available power of each transmitter is $P_t$. According to equation (4.45), the optimization problem of maximizing the achievable secrecy rate is formulated as

$$\alpha_k{}^* = \arg\max\{\omega_{kAN}(\alpha_k)\}, \tag{4.46}$$

where $\alpha_k{}^*$ represents the optimal value of power allocation. By setting the first derivative of (4.46) into zero, the optimal value of the power allocation factor is concluded as

$$\alpha_k{}^* = \frac{\gamma_{t,k} + \gamma_{t,k}(\max_{m=1}^{M}\gamma_{e_m,k}) - (\max_{m=1}^{M}\gamma_{e_m,k})}{2\gamma_{t,k}(\max_{m=1}^{M}\gamma_{e_m,k})}. \tag{4.47}$$

If $\alpha_k{}^* \in [0, 1]$, it further yields to $\alpha_k = \alpha_k{}^*$.

In addition, for the cases in which a non-zero secrecy rate is not achievable, it is given that $\alpha_k = 0$. Also in the case where friendly jamming scheme is not employed, it can be concluded that $\alpha_k = 1$, in which case the total available power is dedicated to main signal only.

Interestingly, equation (4.47) implies some noteworthy insights that are stated below:

- The optimal power allocation solution relies on instantaneous global channel state information. Notably, the channel state information is traceable for the cases in which the rate of changes in channel fading coefficients are slower than the transmission rate, e.g., in quasi-static channels. Therefore, the power allocation factors must be updated and renewed in practice, based on the rate of changes in channel fading coefficients.

- The instantaneous channel state information is not traceable in some practical scenarios. On the other hand, the statistics of the corresponding channels may be accessible [81]. In that case, it is suggested to use Jensen's inequality and specify the bounds of ergodic secrecy rate and provide the optimal power allocation solutions [44].

- Equation (4.47) requires the channel state information of the illegitimate nodes. However, mostly in practice, the CSI of the eavesdroppers or its statistics are not available.Thus, it is essential to present alternative solutions in which the knowledge of CSI of the unauthorized nodes is not required.

- A variety of factors affect the optimal value of $\alpha_k$, for example, spatial locations of the legitimate and illegitimate entities, available transmit power, and the global channel state information.

## 4.9 Sub-optimal Solution

Due to the dependency of the optimal power allocation factor on the channel state information of the eavesdroppers, there is a need for alternative sub-optimal solutions which do not rely on the CSI of the unauthorized entities. Hereon, a sub-optimal solution which does not need any knowledge about the channel state information of the illegitimate nodes is suggested. Using (4.45) and neglecting the white thermal noise at the illegitimate entities, it is given that [44]

$$\omega_{kAN} \simeq \frac{1+\frac{\alpha_k P_t |h_{(k-1)k}|^2}{\sigma^2}}{1+max_{m=1}^{M}\frac{\alpha_k P_t |h_{(k-1)e_m}|^2}{(1-\alpha_k)P_t |h_{(k-1)e_m}|^2}}. \tag{4.48}$$

Hence, (4.48) can be reformulated as

$$\omega_{kAN} \simeq \frac{1+\alpha_k \gamma_{t,k}}{1+\frac{\alpha_k}{(1-\alpha_k)}}. \tag{4.49}$$

By setting the derivative of (4.49) into zero, it can be concluded that

$$\alpha_k{}^* = \frac{\gamma_{t,k}-1}{2\gamma_{t,k}} = \frac{1}{2} - \frac{1}{2\gamma_{t,k}}. \tag{4.50}$$

Interesting, equation (4.50) implies is that when $\gamma_{t,k} \rightarrow \infty$, the power allocation factor approaches 0.5.

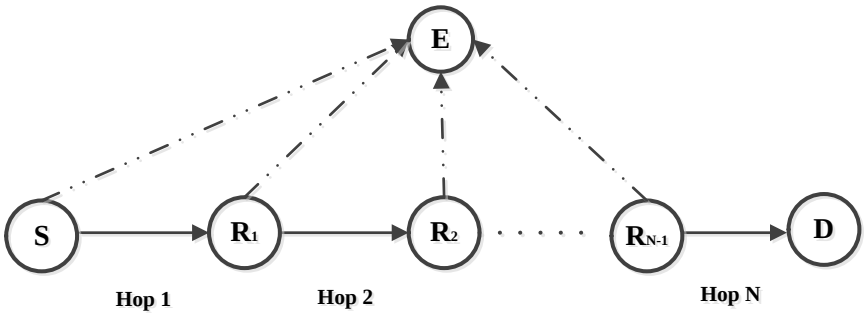


Figure 4.2: Communication via multiple DF relays in the presence of an eavesdropper.

## 4.10 A Case Study: Transmission in the Presence of an Eavesdropper

At this point, it is presumed that communication takes place in the presence of an illegitimate entity as seen in Fig. 4.2. In this case, the received SNR of the eavesdropper at $k^{th}$ phase of transmission is initially given by

$$\gamma_{e,k_{AN}} = \frac{P_{t_{k-1}} \mid h_{(k-1)e} \mid^2}{\sigma^2}. \tag{4.51}$$

Therefore, according to equation (4.37), by using the secrecy enhancement scheme, the received SNR at the eavesdropper is formulated as

$$\gamma_{e,k_{AN}} = \frac{\alpha_k P_{t_{k-1}} \mid h_{(k-1)e} \mid^2}{\sigma^2 + (1-\alpha_k) P_{t_{k-1}} \mid h_{(k-1)e} \mid^2}. \tag{4.52}$$

Hereon, defining the parameters $\theta_k$ and $\theta$ as the following facilitates the analysis.

$$\theta_k \triangleq \frac{1+\alpha_k \gamma_{t,k}}{1+\gamma_{e,k_{AN}}}, \tag{4.53}$$

$$\theta \triangleq \min_{k=1}^{N} \theta_k. \tag{4.54}$$

Hence, it is given that

$$\begin{aligned} C_{s_{AN}} &= \frac{1}{N} \min_{k=1}^{N} C_{s,k_{AN}} \\ &= \frac{1}{N} \min_{k=1}^{N} [\log_2 \frac{1+\alpha_k \gamma_{t,k}}{1+\gamma_{e,k_{AN}}}]^+ \\ &= \frac{1}{N} \min_{k=1}^{N} (\log_2 \theta_k) \\ &= \frac{1}{N} \log_2 \theta. \end{aligned} \tag{4.55}$$

Accordingly, it is given that

$$2^{NC_{s,k_{AN}}} \propto \theta_k, \tag{4.56}$$

and also

$$2^{NC_{sAN}} \propto \theta. \tag{4.57}$$

If the available global power at all the transmitters are set to $P_t$, based on (4.53), it can be written that

$$\theta_k = \frac{1 + \frac{\alpha_k P_t |h_{(k-1)k}|^2}{\sigma^2}}{1 + \frac{\alpha_k P_t |h_{(k-1)e}|^2}{\sigma^2 + (1-\alpha_k) P_t |h_{(k-1)e}|^2}}. \tag{4.58}$$

At this point, it is presumed that the total power at the transmitters are equal to $P_t$. Since the channels are quasi-static, the transmitters (source or relays) can use the channel state information and perform optimization to maximize the secrecy rate subject to the limited power resources and $\alpha_k$ bounds. According to equation (4.58), for each hop, $\theta_k$ can be reformulated as

$$\theta_k = \frac{1 + \alpha_k \gamma_{t,k}}{1 + \frac{\alpha_k \gamma_{e,k}}{1 + (1-\alpha_k)\gamma_{e,k}}}. \tag{4.59}$$

Thus, the maximization problem per hop can be formulated as

$$\begin{aligned} \max_{\alpha_k} \quad & \theta_{\mathrm{k}}(\alpha_k) \\ \text{s.t.} \quad & 0 \leq \alpha_k \leq 1. \end{aligned}$$

By setting the derivative of $\theta_k$ equal to zero, if the aforementioned constraints are met, the optimal value of $\alpha_k$ can be obtained as

$$\alpha_k^{\,*} = \frac{\gamma_{t,k} + \gamma_{t,k}\gamma_{e,k} - \gamma_{e,k}}{2\gamma_{t,k}\gamma_{e,k}}. \tag{4.60}$$

However, it is considered that $\alpha_k = 0$ if a non-zero secrecy rate is not achievable, and $\alpha_k = 1$ if artificial noise is not employed.

## 4.11 A Case Study: Security Enhancement Using Conventional Cooperative Jamming

In this case study, conventional artificial noise is used to enhance the security. In this scheme, during the $(k+1)$th hop of transmission, from the node $k$ to the node $(k+1)$, node $(k-1)$ sends the cooperative jamming signal, as shown in Fig. 4.3. However, friendly jamming signal does not affect the received signal at $(k+1)$th node, because as explained in the system model and assumed in [92], the legitimate nodes can only receive signals from the two nearest legitimate neighbors. Since the jammer is inaudible to the legitimate receiver of $k$th hop, therefore the received signal at each hop can be written as (4.3) and its PDF and CDF can be expressed by (4.4) and (4.5), respectively.

In order to enhance the secrecy of the first hop, an external jammer labeled as $(-1)$ th node is assumed at a location where it is not audible to first relay. Consequently, the received signal of $m$th eavesdropper at $(k+1)$th hop can be written as

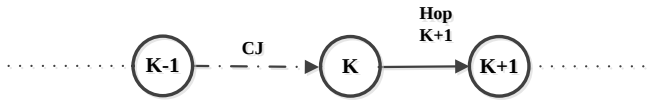


Figure 4.3: Security enhancement, using conventional cooperative jamming

$$\gamma_{e_m,k+1} = \frac{P_{t_k} \mid h_{ke_m} \mid^2}{\sigma^2 + P_{j_{k-1}} \mid h_{(k-1)e_m} \mid^2} \tag{4.61}$$

where $P_{j_{k-1}}$ is the jamming power of the (k-1)th node during (k+1)th hop of transmission.

If secrecy capacity at $k$th hop with cooperative jamming is denoted by $C_{s_{CJ},k}$, it can be written that

$$C_{s_{CJ},k} = log_2(\frac{1+\gamma_{t,k}}{1+\gamma_{e_{CJ},k}}) \tag{4.62}$$

where $\gamma_{e_{CJ},k}$ is the instantaneous received SNR of the eavesdropper at $k$th hop when cooperative jamming is utilized. If $\gamma_{e,k} > \gamma_{e_{CJ},k}$ , it can be written that $C_{s,k} < C_{s_{CJ},k}$ and $\overline{C_s} = E\{C_s\}$ [72].

Note that if the eavesdropper is located at a location where it does not receive the cooperative jamming signal while it receives the original signal, then cooperative jamming is not able to reduce the leakage of the information to the eavesdropper. On other words, in this case, the secrecy enhancement does not occur and $\gamma_{e,k} > \gamma_{e_{CJ},k}$ cannot be valid. Therefore, the new artificial noise approach has the advantage that if an eavesdropper receives the main signal, it also receives the cooperative jamming while these assumptions are not valid in conventional artificial noise which is the scenario in the current case study. In addition, if an eavesdropper is located very close to the legitimate nodes, secrecy performance results are similar to the case where the relays are untrusted DF relays, therefore, non-zero secrecy capacity is not achievable [53].

In order to achieve the end-to-end secrecy performance of the proposed system via friendly jamming, (4.61) and (4.62) are invoked in (4.12).

$$\begin{aligned} C_{s_{CJ}} &= \frac{1}{N}\min_{k=1}^{N}(C_{s_{CJ},k}) = \\ &\frac{1}{N}\min_{k=1}^{N}(log_2(\frac{1+\gamma_{t,k}}{1+\gamma_{e_{CJ},k}})) = \\ &\frac{1}{N}\min_{k=1}^{N}(log_2(\frac{1+\gamma_{t,k}}{1+\max_{m=1}^{M}\gamma_{e_m,k}})) = \\ &\frac{1}{N}\min_{k=1}^{N}\min_{m=1}^{M}(log_2(\frac{1+\gamma_{t,k}}{1+\gamma_{e_m,k}})) = \\ &\frac{1}{N}\min_{k=1}^{N}\min_{m=1}^{M}(log_2(\nu_{m,k})) \end{aligned} \tag{4.63}$$

in which $\nu_{m,k} \triangleq 1+\gamma_{t,k}/1+\gamma_{e_m,k}$. Interestingly, the end to end secrecy capacity would increase only if there is a secrecy enhancement in the hop with the least secrecy capacity.

## 4.12 Numerical Results

In this section, the validity of the presented closed-form expressions and the performance of the proposed secrecy improvement scheme are investigated. During simulations, noise variance of all terminals are $-60$ dBm [73] and the path loss coefficient is assumed to be 3.5. The source and destination are, respectively, placed at $S(0,0)$ and $D(1000,0)$ meters. The relays are distributed according to a uniform location scheme, meaning that the distance between successive authorized entities is $d = 1000/N$ meters. Therefore, it is given that $R_n(nd, 0)$ where $n \in \{1, ..., N-1\}$). The available transmit power is assigned evenly between the transmitters (source and relays). An average of $10^5$ independent trials have been used for the purpose of Monte Carlo simulations. The summary of the simulation parameters are presented in the table 4.1.

Table 4.1: Simulation set up parameters (new way of using artificial noise)

| Simulation Parameter | Value |
|---|---|
| Source location | (0,0)m |
| Relay location | (nd,0)m |
| Destination location | (1000,0)m |
| $R_s$ | 0.1 |
| Path loss coefficient | 3.5 |
| $\sigma^2$ | -60dBm |

### 4.12.1 General Secrecy Performance

In Fig. 4.4 and Fig. 4.5, first fix the location of the eavesdroppers at $E_1$ $(500, 700)$ and $E_2$ $(1000, 1700)$ meters. Then, the probability of non-zero secrecy capacity as a function of available transmit power has been simulated in Fig. 4.4. This figure illustrates that raising the transmit power results in enhancing the probability of non-zero secrecy capacity if the adversary nodes are not close to the transmitters (source, relays). On the contrary, in the cases where any illegitimate entity is located not far from the transmitters, rasing the transit power results in increasing the received SNR at the wiretappers so the secrecy of the system is degraded [122]. In addition, as pointed out in [6], enhancing the received SNR at the intended receiver can improve the secrecy of the system, as in Fig. 4.4 probability of non-zero secrecy capacity is enhanced. Moreover, the closed-form expressions of the probability of non-zero secrecy capacity which were derived earlier in this chapter are verified in here.

Fig. 4.5 shows that for the cases in which the eavesdroppers are not placed close to the transmitters, improving the global transmit power can enhance the probability of outage in secrecy capacity. Moreover, the closed-form expressions of probability of outage in secrecy capacity are validated by the simulations. Interestingly, in order to investigate the effect of global transmit power on secrecy, the spatial location of the illegitimate nodes must also be considered [125]. Fig. 4.4 and Fig. 4.5 indicate that if using the relay nodes enhances the received SNR at the desired receiver, then maximum achievable secrecy rate of the system is also improved.

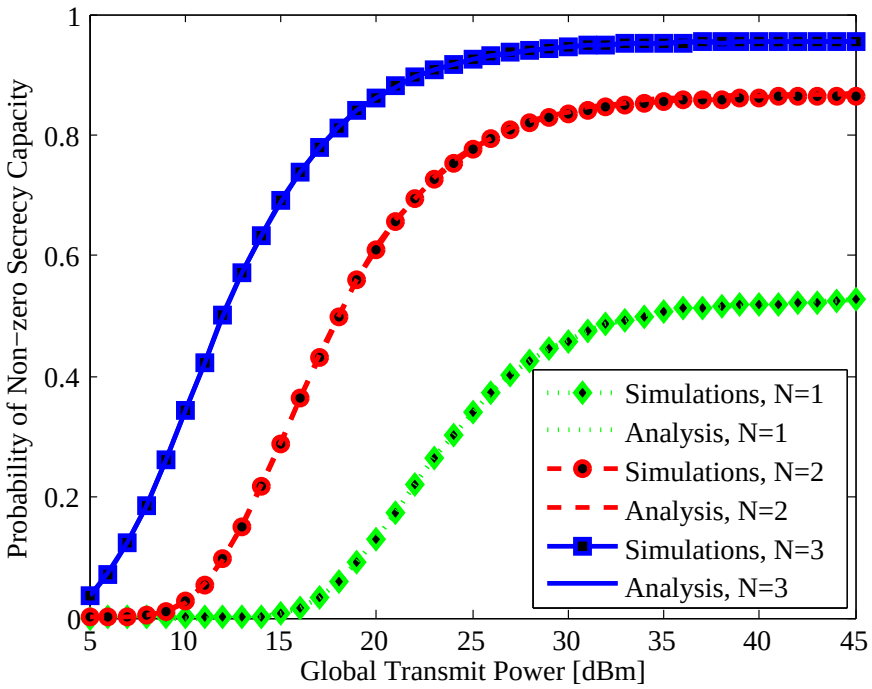


Figure 4.4: Probability of non-zero secrecy capacity versus global transmit power.

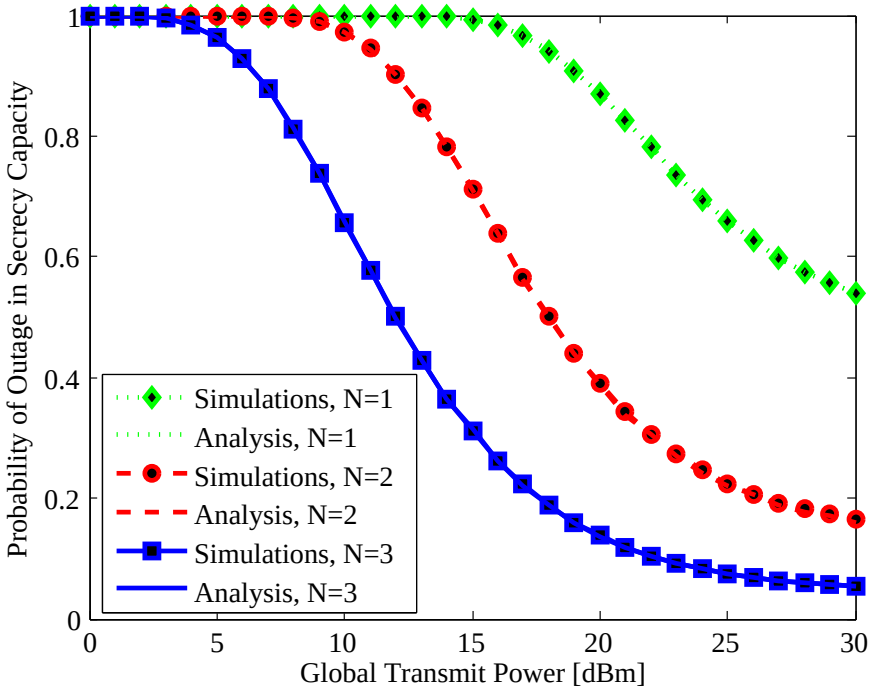


Figure 4.5: Probability of outage in secrecy capacity versus global transmit power.

### 4.12.2 Evaluation of the Proposed Secrecy Improvement Scheme

Two benchmarks are presented as below to facilitate the evaluation of the performance of the proposed secrecy enhancement scheme.

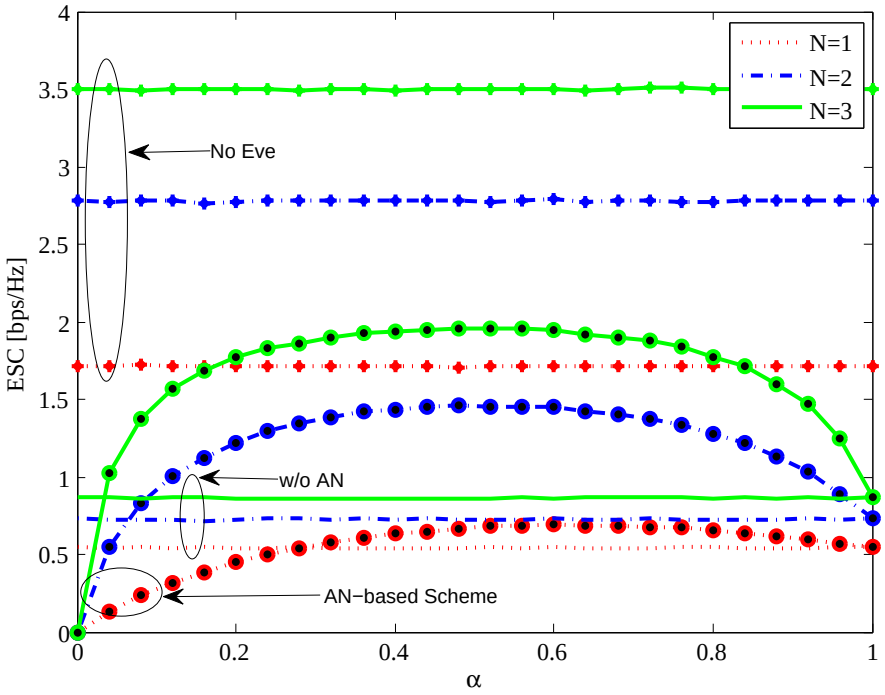


Figure 4.6: Ergodic secrecy capacity versus power allocation factor with and without AN

- ***W/O AN:*** In this case, it is considered that all the available power is used for transmission of the main signal and friendly jamming signal is not employed. This benchmark reverts back to *without artificial noise* case and therefore $w/o\ AN$ subscript has been used to indicate it.

- ***No Eve:*** In the second benchmark, it is assumed that there is no eavesdropper to wiretap the main signal. *No Eve* subscript implies this case.

Fig. 4.6 reflects the effect of power allocation among the main signal and the jamming signal. It is considered that the eavesdroppers are located at $E1(-1050, 0)$ and $E2(1150, 0)$ meters. This figure is based on an assumption that the proposed secrecy enhancement scheme has just been applied in the last hop of transmission. Moreover, the available transmit power is set to 45dBm and it has been assigned evenly between the transmitters (source and relays). This figure illustrates that one can enhance the ergodic secrecy capacity of the system via using the proposed strategy if power allocation has been devised appropriately.

Fig. 4.7 considers transmission in the presence of an eavesdropper located at $E(e, 0)$ and where the proposed AN strategy is only used in the last hop of transmission, $\alpha_N = \alpha$. This figure reveals that the optimal value of $\alpha$ is influenced by different factors such as total global power and location of the eavesdropper. It is assumed that the friendly jamming is just utilized in the last hop of transmission. In this figure the value of ESC at $\alpha = 1$ represents the case when artificial noise is not utilized.

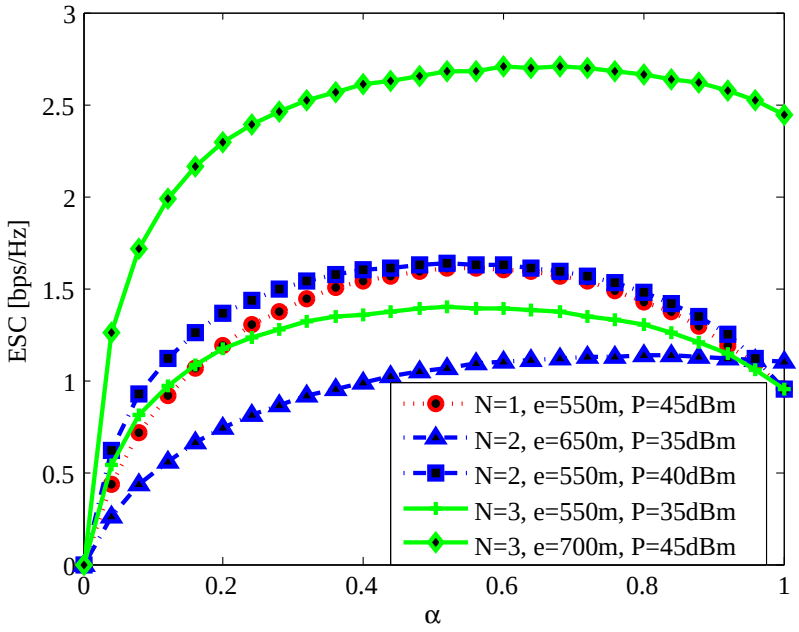


Figure 4.7: Ergodic secrecy capacity as a function of $\alpha$, $P_t$.

Ergodic secrecy capacity of the system as a function of global transmit power, with and without using the proposed friendly jamming strategy, has been shown in Fig. 4.8 where $E1(-1050, 0)$ and $E2(1150, 0)$ meters. This figure indicates that using the optimal power allocation solution can enhance the ergodic secrecy capacity of the system significantly in comparison with the case where the cooperative jamming strategy is not employed. Moreover, the two approaches to improve the secrecy rate which were indicated in [6] have been shown here. First, the received SNR at the intended receiver is enhanced via using intermediate relay nodes. Second, the received SNR of the unauthorized entities are degraded by the intentional jamming signal.

In Fig. 4.9 a single hop communication system has been considered where the location of one of the eavesdroppers is changing from $E_1(-1000, 0)$ to $E_1(1000, 0)$ meters and the other eavesdropper is placed fixed at $E_2(1500, 0)$ meters. The available transmit power of this system model is set to Pt = 45dBm. Fig. 4.9 implies that for the cases in which one of the eavesdroppers is placed not far from the transmitters, the optimal and sub-optimal solutions enhance the ESC of the system and the results of the sub-optimal solution and the optimal solution are tightened.

## 4.13 Discussion

Based on the previous section, the main results are stated below:

- The closed-form expressions of secrecy in terms of the probability of outage in secrecy capacity and the probability of non-zero secrecy capacity were validated via simulations and numerical results.

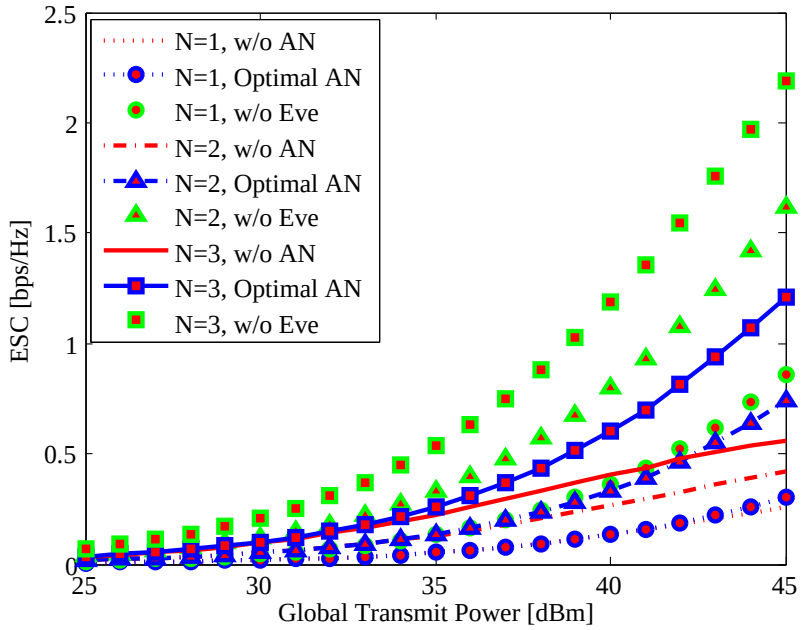


Figure 4.8: Ergodic secrecy capacity versus global transmit power with and without AN.

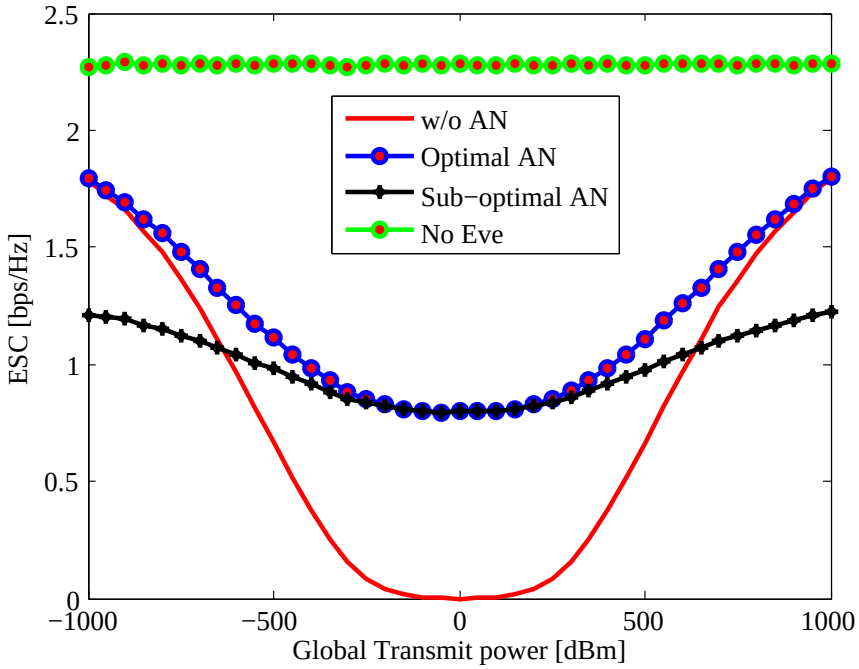


Figure 4.9: Ergodic secrecy capacity versus the location of one of the eavesdroppers.

- Having a proper power allocation between main signal and friendly jamming improved the secrecy.

- The optimal value of $\alpha$ relied on different factors such as available global power, the spatial location of the legitimate and illegitimate nodes,etc.
- The optimal solution always enhanced the ergodic secrecy capacity of the system, in comparison with the case in which the presented artificial jamming signal was not used.
- The results of the sub-optimal solution and the optimal solution are very similar if at least one of the eavesdroppers is placed close to a transmitter.

## 4.14 Summary

In this chapter, a secrecy enhancement strategy was employed which is based on friendly jamming. This chapter followed a new way of using artificial noise where the intentional jamming signal was generated at the transmitter and it was sent along with the main signal. Hence, the transmitter assigned a fraction of its power for creating the intentional noise. It must be pointed out that the new way of using artificial noise was adopted in this chapter because of considerable advantages as following. First, in the new approach, unlike conventional AN, any extra helper was not needed to generate the intentional jamming signal. Second, complexity of this solution in terms of network overheads was less, in comparison with conventional artificial noise. Accordingly, this approach was introduced as a cost-effective and energy efficient approach.

Note that power allocation between the friendly jamming and the main signal was needed to ensure that the presented scheme improves the secrecy. Thus, under the assumption that the available transmit power at the transmitters (source and relays) was limited, an optimal power allocation solution has been devised to maximize the secrecy capacity. In many applicable scenarios, the channel state information of the illegitimate entities is not available while the optimal solution required this knowledge. Thence, a sub-optimal solution was offered where the CSI of the unauthorized nodes were not necessary. It was shown that the presented optimal solution outperformed the base-line case (i.e., No AN case). In addition, the sub-optimal solution and the optimal solution results were similar if one of the illegitimate entities was close to one of the transmitters.

# Chapter 5

# Conclusion and Future Work

This chapter concludes this thesis, summarizes key results, and sheds light on open areas for future work in the context of security in cooperative communication systems.

## 5.1 Conclusion

Cooperative communications is inseparable from today's and future's development of wireless communication systems due to various advantages such as increasing the coverage and impairing fading effects. However, wireless communications through the air medium which is accessible for unauthorized and malicious entities, results in a number of security vulnerabilities. This thesis was focused on security enhancement techniques on physical layer in cooperative communications. Note that the upper layer strategies have been already studied in the literature in an extensive manner. However, there was a need to provide comprehensive security solutions through different layers of the protocol stack. Towards this goal, this thesis covered diverse physical-layer security solutions for cooperative communications including information-theoretic techniques, diversity techniques, beamforming solutions and cooperating jamming strategies, in addition to physical-layer authentication and spread spectrum. Moreover, a number of security methods were studied which multiple techniques to boost system security (e.g., combination of diversity techniques and cooperative jamming).

As highlighted in this thesis, conventional cooperative jamming strategies have some shortcomings. First, they require extra hardware to perform the jamming role which is an expensive strategy. Next, cooperation between the helper and the network results in additional network overheads and rises complexity. Furthermore, cooperative jamming strategies are not applicable to general communication systems for the purpose of security enhancement. This research presented novel remedies for the aforementioned shortcomings via proving solutions which do not depend on extra nodes. Based on what was investigated, the main contributions using the phase shift and artificial noise-based schemes, respectively proposed in chapters 3 and 4, are summarized as:

1. In chapter 3, a random phase shift scheme was presented to secure transmission in a two-hop relaying system in which the relay adopts DF protocol. To be more specific, a random phase shift was inserted to the modulated data of both phases of transmission. The phase shift was created, benefiting from a shared secret information between

communicating entities (e.g., the reciprocal channel between transmitter and intended receiver of each transmission phase can be used to create the secret key). Thus, the phase shift could not be known at the illegitimate entity. Consequently, received SNR at the unauthorized node was weakened, and growth in secrecy capacity was obtained. The most important contributions of this scheme are highlighted in the following:

- This scheme did not require the collaboration with any additional node.
- The concern about the network overheads in convectional cooperative jamming was resolved as extra helper was not incorporated.
- It was proven that the proposed solution raised the ergodic secrecy capacity and the simulation results confirmed the theoretical outcomes of the proposed solution.
- Security analysis of the system model was presented, and the probability of outage in secrecy capacity and probability of non-zero secrecy capacity were calculated as closed-form formulations.
- It was shown that increasing the transmit power did not necessarily improve the secrecy as it might cause more information leakage to the adversary nodes.
- The presented scheme is highly recommended for communication systems with lower power recourses since additional amount of power for generating friendly jamming is not required.

2. In the context of multi-hop communication systems, in chapter 4, a system model was assumed where there existed multiple non-colluding illegitimate nodes. This study extended a new method of using cooperative jamming to the considered system model where intentional interference was created at the transmitter of each hop. To be more precise, the transmitters were capable of assigning a fraction of their available power to generate friendly jamming at illegitimate entities. Major results of the proposed strategy are stated as below:

   - This novel technique of adopting cooperative jamming do not need any extra hardware, on the contrary with traditional artificial noise strategies.
   - Due to the particular importance of power allocation in cooperative jamming strategies, between the friendly jamming and the primary signal, power assignment strategies were presented. Initially, an optimal power allocation was suggested which needed the channel state information of the wiretappers. Numerical results showed that the optimal solution constantly boosted ergodic secrecy capacity.
   - Since in the majority of feasible and applicable scenarios, CSI of the wiretappers are not known, a sub-optimal solution was offered in which information about either wiretappers' CSI or their locations was not required. It was illustrated that the sub-optimal solution was helpful for the case where the illegitimate entity was located not far from the transmitter of the corresponding hop.
   - Secrecy performance of the communication system model over Rayleigh fading channels was presented and closed-form expressions of the probability of existence of a positive secrecy capacity and secure outage probability were formulated.

- It was shown that the capability of the proposed scheme for secrecy improvement depends on different factors including the location of the entities and available power.

## 5.2 Future work

Here are the suggested directions and open areas explored for future work:

1. The random phase shift scheme explained in chapter 3 can be further extended and improved in the following manners:

   - Focusing on generating random phase shift based on reciprocal channel between communicating nodes can be a good area for further studies.
   - The results of this work can be modified to communication in the presence of multiple colluding and non-colluding eavesdroppers.
   - The presented approach can also be used as a basis intuition in order to be adopted in decentralized networks such as ad-hoc networks, or centralize networks, e.g., cellular networks, as a means to improve secrecy.

2. The new cooperative jamming strategy proposed in chapter 4 can be extended or further studied in the following aspects:

   - It can be generalized to the scenarios in which there exist multiple colluding eavesdroppers that can wiretap communication.
   - The provision of the shared friendly jamming between the communicating entities can be investigated.
   - It is also suggested to explore the impact of using such a scheme on the secrecy of multi-hop AF relaying systems.

3. As mentioned in chapter 2, mobile operators have been interested in cooperative communications in recent years due to its capabilities to provide high quality services such as content aware applications, data offloading, and even the potential role of the UEs as relays to increase coverage. However, there are security concerns in UE-relaying systems which need additional research. For example: (i) It is necessary to ensure that the intermediate UE is secure for the purpose of relaying. (ii) The possibility of secure communication via untrusted UE relays is another interesting research topic. (iii) Most existing studies only consider the impact of relaying strategy on the reliability of cellular networks in order to reduce the cell edge effect and increase the quality of service. However, it is required to investigate the impact of UE-relaying on system's secrecy as well. In addition, a new research topic is designing the UE-relaying strategies which jointly meet the reliability and security requirements.

4. Most existing physical-layer studies have been proposed to mitigate the attacks which target the confidentiality of networks. However, as pointed out in chapter 2, other security requirements of wireless systems also expose attacks; therefore, future work should analyze the attacks that target authentication or availability of cooperative communication systems. As another suggestion for future work, it is notable that current studies are more concerned about passive eavesdropping attacks; however, active attacks should be more considered in the future.

5. In a different direction, randomness of the channel between communicating entities has been employed in a number of research papers to generate a secret key, and to improve security. However, there are more unique physical layer characteristics which can be utilized for secrecy improvement such as carrier frequency offset. In this regard, exploiting other exclusive physical layer characteristics can be an area for further investigation.

6. It must be expressed that the current study similar to many existing methods has mainly incorporated a physical-layer security solution for cooperative communications. And less attention has been made to examine cross-layer security solutions where physical layer and upper layers of the protocol stack collaborate efficiently through hybrid security techniques to enhance security. Therefore, cross-layer security is another open area for ongoing research.

7. Finally, it is notable that many theoretical and analytical studies have shown capabilities of physical-layer schemes to enhance security. However, practical evaluation of a potential secure approach in realistic scenarios through experiments plays a key role in final evaluation. To this end, excessive computational complexity and cost associated with hardware should be both avoided.

# Bibliography


[1] Birch, Beverley "Giants of Science - Guglielmo Marconi". Blackbirch Press, 1 edition, 2001.

[2] Andrews, Jeffrey G., Stefano Buzzi, Wan Choi, Stephen V. Hanly, Aurelie Lozano, Anthony CK Soong, and Jianzhong Charlie Zhang. "What will 5G be?." Selected Areas in Communications, IEEE Journal on 32, no. 6 (2014): 1065-1082.

[3] http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/

[4] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 1996.

[5] Shiu, Yi-Sheng, Shih Yu Chang, Hsiao-Chun Wu, Scott C-H. Huang, and Hsiao-Hwa Chen. "Physical layer security in wireless networks: a tutorial." Wireless Communications, IEEE 18, no. 2 (2011): 66-74.

[6] Vilela, Joao P., Matthieu Bloch, Joao Barros, and Steven W. McLaughlin. "Wireless secrecy regions with friendly jamming." Information Forensics and Security, IEEE Transactions on 6, no. 2 (2011): 256-266.

[7] Gupta, Vikram, Srikanth Krishnamurthy, and Michalis Faloutsos. "Denial of service attacks at the MAC layer in wireless ad hoc networks." In MILCOM 2002. Proceedings, vol. 2, pp. 1118-1123. IEEE, 2002.

[8] Sheng, Yong, Kokkiong Tan, Guanling Chen, David Kotz, and Arnett Campbell. "Detecting 802.11 MAC layer spoofing using received signal strength." In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008.

[9] Convery, Sean. "Hacking Layer 2: Fun with Ethernet Switches." Blackhat [Online Document] (2002).

[10] Tanase, Matthew. "IP spoofing: an introduction." Security Focus 11 (2003).

[11] Zou, Cliff C., Don Towsley, Weibo Gong, and Songlin Cai. "Routing worm: A fast, selective attack worm based on ip address information." In Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation, pp. 199-206. IEEE Computer Society, 2005.

[12] Zou, Yulong, Xianbin Wang, and Lajos Hanzo. "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends." arXiv preprint arXiv:1505.07919 (2015).

[13] Schuba, Christoph L., Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, and Diego Zamboni. "Analysis of a denial of service attack on TCP." In Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on, pp. 208-223. IEEE, 1997.

[14] Lee, Keunsoo, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, and Sehun Kim. "DDoS attack detection method using cluster analysis." Expert Systems with Applications 34, no. 3 (2008): 1659-1665.

[15] Ranjan, Supranamaya, Ram Swaminathan, Mustafa Uysal, and Edward W. Knightly. "DDoS-Resilient Scheduling to Counter Application Layer Attacks Under Imperfect Detection." In INFOCOM. 2006.

[16] Denning, Peter J. "Computers under attack." Intruders, Worms and Viruses Addison-Wesley, New York (1990).

[17] Bloch, Matthieu, and Joao Barros. Physical-layer security: from information theory to security engineering. Cambridge University Press, 2011.

[18] Peterson, Roger L., Rodger E. Ziemer, and David E. Borth. Introduction to spread-spectrum communications. Vol. 995. New Jersey: Prentice Hall, 1995.

[19] Omura, Jim K. Spread spectrum communications handbook. Vol. 2. New York: McGraw-Hill, 1994.

[20] Ciampa, Mark. Security + guide to network security fundamentals. Cengage Learning, 2011.

[21] Krawetz, Neal. "Introduction to network security." (2009).

[22] http://www.softpedia.com/get/Network-Tools/Protocol-Analyzers-Sniffers/Kitty-Litter-The-Anti-Sniffer.shtml

[23] Cover, Thomas M., and Abbas El Gamal. "Capacity theorems for the relay channel." Information Theory, IEEE Transactions on 25, no. 5 (1979): 572-584.

[24] Yang, Yang, Honglin Hu, Jing Xu, and Guoqiang Mao. "Relay technologies for WiMAX and LTE-advanced mobile systems." Communications Magazine, IEEE 47, no. 10 (2009): 100-105.

[25] Beaulieu, Norman C., and Samy S. Soliman. "Exact analysis of multihop amplify-and-forward relaying systems over general fading links." Communications, IEEE Transactions on 60, no. 8 (2012): 2123-2134.

[26] Farhadi, Golnaz, and Norman C. Beaulieu. "A general framework for symbol error probability analysis of wireless systems and its application in amplify-and-forward multihop relaying." Vehicular Technology, IEEE Transactions on 59, no. 3 (2010): 1505-1511.

[27] Tsiftsis, T. A., G. K. Karagiannidis, S. A. Kotsopoulos, and F-N. Pavlidou. "BER analysis of collaborative dual-hop wireless transmissions." Electronics Letters 40, no. 11 (2004): 679-681.

[28] Huang, Jing. "Cooperative jamming for secure communications in MIMO relay networks." Signal Processing, IEEE Transactions on 59, no. 10 (2011): 4871-4884.

[29] Chen, Jingchao, Rongqing Zhang, Lingyang Song, Zhu Han, and Bingli Jiao. "Joint relay and jammer selection for secure two-way relay networks." Information Forensics and Security, IEEE Transactions on 7, no. 1 (2012): 310-320.

[30] Dong, Lun, Zhu Han, Athina P. Petropulu, and H. Vincent Poor. "Improving wireless physical layer security via cooperating relays." Signal Processing, IEEE Transactions on 58, no. 3 (2010): 1875-1888.

[31] Wu, Yongpeng, Robert Schober, Derrick Wing Kwan Ng, Chengshan Xiao, and Giuseppe Caire. "Secure Massive MIMO Transmission with an Active Eavesdropper." arXiv preprint arXiv:1507.00789 (2015).

[32] Rohokale, Vandana Milind, Neeli Rashmi Prasad, and Ramjee Prasad. "Cooperative jamming for physical layer security in wireless sensor networks." In Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on, pp. 458-462. IEEE, 2012.

[33] Vilela, Joao P., Matthieu Bloch, Joao Barros, and Steven W. McLaughlin. "Friendly jamming for wireless secrecy." In Communications (ICC), 2010 IEEE International Conference on, pp. 1-6. IEEE, 2010.

[34] Vilela, Joao P., Pedro C. Pinto, and Joao Barros. "Position-based jamming for enhanced wireless secrecy." Information Forensics and Security, IEEE Transactions on 6, no. 3 (2011): 616-627.

[35] Kaliszan, Michal, Javad Mohammadi, and Slawomir Stanczak. "Cross-layer security in two-hop wireless Gaussian relay network with untrusted relays." Communications (ICC), 2013 IEEE International Conference on. IEEE, 2013.

[36] Csiszr, Imre, and Janos Korner. "Broadcast channels with confidential messages." Information Theory, IEEE Transactions on 24, no. 3 (1978): 339-348.

[37] Wyner, Aaron D. "The wire-tap channel." Bell System Technical Journal, The 54, no. 8 (1975): 1355-1387.

[38] Shannon, Claude E. "Communication theory of secrecy systems*." Bell system technical journal 28, no. 4 (1949): 656-715.

[39] Leung-Yan-Cheong, Sik K., and Martin E. Hellman. "The Gaussian wire-tap channel." Information Theory, IEEE Transactions on 24, no. 4 (1978): 451-456.

[40] Maurer, Ueli M. "Secret key agreement by public discussion from common information." Information Theory, IEEE Transactions on 39, no. 3 (1993): 733-742.

[41] Foschini, Gerard J., and Michael J. Gans. "On limits of wireless communications in a fading environment when using multiple antennas." Wireless personal communications 6, no. 3 (1998): 311-335.

[42] Bloch, Matthieu, Joo Barros, Miguel RD Rodrigues, and Steven W. McLaughlin. "Wireless information-theoretic security." Information Theory, IEEE Transactions on 54, no. 6 (2008): 2515-2534.

[43] Krikidis, Ioannis, John S. Thompson, and Steve McLaughlin. "Relay selection for secure cooperative networks with jamming." Wireless Communications, IEEE Transactions on 8, no. 10 (2009): 5003-5011.

[44] Dong, Lun, Homayoun Yousefi Zadeh, and Hamid Jafarkhani. "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper." In Communications (ICC), 2011 IEEE International Conference on, pp. 1-5. IEEE, 2011.

[45] Park, Ki-Hong, Tian Wang, and Mohamed-Slim Alouini. "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming." Selected Areas in Communications, IEEE Journal on 31, no. 9 (2013): 1741-1750.

[46] He, Fangming, Hong Man, and Wei Wang. "Maximal ratio diversity combining enhanced security." Communications Letters, IEEE 15, no. 5 (2011): 509-511.

[47] Wang, Hui-Ming, Qinye Yin, and Xiang-Gen Xia. "Distributed beamforming for physical-layer security of two-way relay networks." Signal Processing, IEEE Transactions on 60, no. 7 (2012): 3532-3545.

[48] Liao, Wei-Cheng, Tsung-Hui Chang, Wing-Kin Ma, and Chong-Yung Chi. "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach." Signal Processing, IEEE Transactions on 59, no. 3 (2011): 1202-1216.

[49] Akhtar, Auon, Aydin Behnad, and Xianbin Wang. "On the secrecy rate achievability in dual-hop amplify-and-forward relay networks." Wireless Communications Letters, IEEE 3, no. 5 (2014): 493-496.

[50] Barros, Joao, and Miguel RD Rodrigues. "Secrecy capacity of wireless channels." In Information Theory, 2006 IEEE International Symposium on, pp. 356-360. IEEE, 2006.

[51] Zhou, Xiangyun, Matthew R. McKay, Behrouz Maham, and Are Hjorungnes. "Rethinking the secrecy outage formulation: A secure transmission design perspective." arXiv preprint arXiv:1306.1346 (2013).

[52] Tang, Xiaojun, Ruoheng Liu, Predrag Spasojevi, and H. Vincent Poor. "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels." Information Theory, IEEE Transactions on 55, no. 4 (2009): 1575-1591.

[53] Huang, Jing, Arjun Mukherjee, and A. Lee Swindlehurst. "Secure communication via an untrusted non-regenerative relay in fading channels." Signal Processing, IEEE Transactions on 61, no. 10 (2013): 2536-2550.

[54] Hasna, Mazen O., and Mohamed-Slim Alouini. "Outage probability of multihop transmission over Nakagami fading channels." Communications Letters, IEEE 7, no. 5 (2003): 216-218.

[55] Liang, Yingbin, Gerhard Kramer, H. Vincent Poor, and Shlomo Shamai. "Compound wiretap channels." EURASIP Journal on Wireless Communications and Networking 2009 (2009): 5.

[56] Zhou, Xiangyun, and Matthew R. McKay. "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation." Vehicular Technology, IEEE Transactions on 59, no. 8 (2010): 3831-3842.

[57] Pinto, Pedro C., Joo Barros, and Moe Z. Win. "Wireless physical-layer security: The case of colluding eavesdroppers." In Information Theory, 2009. ISIT 2009. IEEE International Symposium on, pp. 2442-2446. IEEE, 2009.

[58] Chorti, Arsenia, Samir M. Perlaza, Zhu Han, and H. Vincent Poor. "Physical layer security in wireless networks with passive and active eavesdroppers." In Global Communications Conference (GLOBECOM), 2012 IEEE, pp. 4868-4873. IEEE, 2012.

[59] Amariucai, George T., and Shuangqing Wei. "Active eavesdropping in fast fading channels: A Block-Markov Wyner secrecy encoding scheme." In Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on, pp. 2508-2512. IEEE, 2010.

[60] Foschini, Gerard J., and Michael J. Gans. "On limits of wireless communications in a fading environment when using multiple antennas." Wireless personal communications 6, no. 3 (1998): 311-335.

[61] Oggier, Frdrique, and Babak Hassibi. "The secrecy capacity of the MIMO wiretap channel." Information Theory, IEEE Transactions on 57, no. 8 (2011): 4961-4972.

[62] Khisti, Ashish, and Gregory W. Wornell. "Secure transmission with multiple antennas I: The MISOME wiretap channel." Information Theory, IEEE Transactions on 56, no. 7 (2010): 3088-3104.

[63] Liang, Yingbin, Gerhard Kramer, H. Vincent Poor, and Shlomo Shamai. "Recent results on compound wire-tap channels." In Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on, pp. 1-5. IEEE, 2008.

[64] Sarkar, Md Zahurul I., Tharmalingam Ratnarajah, and Mathini Sellathurai. "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers." In Signals, Systems and Computers, 2009 Conference Record of the Forty-Third Asilomar Conference on, pp. 829-833. IEEE, 2009.

[65] Liang, Yingbin, H. Vincent Poor, and Shlomo Shamai. "Secure communication over fading channels." Information Theory, IEEE Transactions on 54, no. 6 (2008): 2470-2492.

[66] Oggier, Frdrique, and Babak Hassibi. "The secrecy capacity of the MIMO wiretap channel." Information Theory, IEEE Transactions on 57, no. 8 (2011): 4961-4972.

[67] Xu, Jin, and Biao Chen. "Broadcast confidential and public messages." In Information Sciences and Systems, 2008. CISS 2008. 42nd Annual Conference on, pp. 630-635. IEEE, 2008.

[68] Wyrembelski, Rafael F., Aydin Sezgin, and Holger Boche. "Secrecy in broadcast channels with receiver side information." In Signals, Systems and Computers (ASILOMAR), 2011 Conference Record of the Forty Fifth Asilomar Conference on, pp. 290-294. IEEE, 2011.

[69] Zhang, Junwei, and Mustafa Cenk Gursoy. "Collaborative relay beamforming for secrecy." In Communications (ICC), 2010 IEEE International Conference on, pp. 1-5. IEEE, 2010.

[70] Mukherjee, Amitav. "Robust beamforming for security in MIMO wiretap channels with imperfect CSI." Signal Processing, IEEE Transactions on 59, no. 1 (2011): 351-361.

[71] Goel, Satashu, and Rohit Negi. "Guaranteeing secrecy using artificial noise." Wireless Communications, IEEE Transactions on 7, no. 6 (2008): 2180-2189.

[72] Wang, Lifeng, Maged Elkashlan, Jing Huang, Nghi H. Tran, and Trung Q. Duong. "Secure transmission with optimal power allocation in untrusted relay networks." Wireless Communications Letters, IEEE 3, no. 3 (2014): 289-292.

[73] Huang, Jing. "Secure communications via cooperative jamming in two-hop relay systems." In Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, pp. 1-5. IEEE, 2010.

[74] Qin, Haohao, Xiang Chen, Yin Sun, Ming Zhao, and Jing Wang. "Optimal power allocation for joint beamforming and artificial noise design in secure wireless communications." In Communications Workshops (ICC), 2011 IEEE International Conference on, pp. 1-5. IEEE, 2011.

[75] Li, Wei, Mounir Ghogho, Bin Chen, and Chunlin Xiong. "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis." Communications Letters, IEEE 16, no. 10 (2012): 1628-1631.

[76] Vasudevan, Sudarshan, Stephan Adams, Dennis Goeckel, Zhiguo Ding, Donald Towsley, and Kin Leung. "Multi-user diversity for secrecy in wireless networks." In Information Theory and Applications Workshop (ITA), 2010, pp. 1-9. IEEE, 2010.

[77] Krikidis, Ioannis, John Thompson, Steve McLaughlin, and Norbert Goertz. "Amplify-and-forward with partial relay selection." Communications Letters, IEEE 12, no. 4 (2008): 235-237.

[78] Vicario, Jose Lopez, Albert Bel, Jose Lopez-Salcedo, and Gonzalo Seco. "Opportunistic relay selection with outdated CSI: outage probability and diversity analysis." Wireless Communications, IEEE Transactions on 8, no. 6 (2009): 2872-2876.

[79] Zhang, Wenshu, Dongliang Duan, and Liuqing Yang. "Relay selection from a battery energy efficiency perspective." In Military Communications Conference, 2009. MILCOM 2009. IEEE, pp. 1-7. IEEE, 2009.

[80] Tannious, Ramy, and Aria Nosratinia. "Spectrally-efficient relay selection with limited feedback." Selected Areas in Communications, IEEE Journal on 26, no. 8 (2008): 1419-1428.

[81] Krikidis, Ioannis. "Opportunistic relay selection for cooperative networks with secrecy constraints." Communications, IET 4, no. 15 (2010): 1787-1791.

[82] Zou, Yulong, Xianbin Wang, and Weiming Shen. "Optimal relay selection for physical-layer security in cooperative wireless networks." Selected Areas in Communications, IEEE Journal on 31, no. 10 (2013): 2099-2111.

[83] Deng, Hao, Hui-Ming Wang, Wei Guo, and Wenjie Wang. "Secrecy Transmission With a Helper: To Relay or to Jam." Information Forensics and Security, IEEE Transactions on 10, no. 2 (2015): 293-307.

[84] Lai, Lifeng, Yingbin Liang, and Wenliang Du. "Phy-based cooperative key generation in wireless networks." In Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on, pp. 662-669. IEEE, 2011.

[85] Sayeed, Akbar, and Adrian Perrig. "Secure wireless communications: Secret keys through multipath." In Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on, pp. 3013-3016. IEEE, 2008.

[86] Lai, Lifeng, Yingbin Liang, and H. Vincent Poor. "A unified framework for key agreement over wireless fading channels." Information Forensics and Security, IEEE Transactions on 7, no. 2 (2012): 480-490.

[87] Ureten, Oktay, and Nur Serinken. "Wireless security through RF fingerprinting." Electrical and Computer Engineering, Canadian Journal of 32, no. 1 (2007): 27-33.

[88] Cobb, William E., Eric W. Garcia, Michael A. Temple, Rusty O. Baldwin, and Yong C. Kim. "Physical layer identification of embedded devices using RF-DNA fingerprinting." In Military Communications Conference, 2010-MILCOM 2010, pp. 2168-2173. IEEE, 2010.

[89] Xiao, Liang, Larry J. Greenstein, Narayan B. Mandayam, and Wade Trappe. "Using the physical layer for wireless authentication in time-variant channels." Wireless Communications, IEEE Transactions on 7, no. 7 (2008): 2571-2579.

[90] He, Xiang, and Aylin Yener. "Two-hop secure communication using an untrusted relay." EURASIP Journal on Wireless Communications and Networking 2009 (2009): 9.

[91] He, Xiang, and Aylin Yener. "Cooperation with an untrusted relay: A secrecy perspective." Information Theory, IEEE Transactions on 56, no. 8 (2010): 3807-3827.

[92] He, Xiang, and Aylin Yener. "End-to-end secure multi-hop communication with untrusted relays." Wireless Communications, IEEE Transactions on 12, no. 1 (2013): 1-11.

[93] Sun, Li, Taiyi Zhang, Yubo Li, and Hao Niu. "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes." Vehicular Technology, IEEE Transactions on 61, no. 8 (2012): 3801-3807.

[94] Jeong, Cheol, Il-Min Kim, and Dong In Kim. "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system." Signal Processing, IEEE Transactions on 60, no. 1 (2012): 310-325.

[95] Khabbaz, Maurice J., Chadi M. Assi, and Wissam F. Fawaz. "Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges." Communications Surveys and Tutorials, IEEE 14, no. 2 (2012): 607-640.

[96] Psaras, Ioannis, and Lefteris Mamatas. "On demand connectivity sharing: Queuing management and load balancing for user-provided networks." Computer Networks 55, no. 2 (2011): 399-414.

[97] Nosratinia, Aria, Todd E. Hunter, and Ahmadreza Hedayat. "Cooperative communication in wireless networks." Communications Magazine, IEEE 42.10 (2004): 74-80.

[98] Zlatanov, Nikola, Aissa Ikhlef, Tarikul Islam, and Robert Schober. "Buffer-aided cooperative communications: opportunities and challenges." Communications Magazine, IEEE 52, no. 4 (2014): 146-153.

[99] Krikidis, Ioannis, Themistoklis Charalambous, and John S. Thompson. "Opportunistic relay selection for cooperative networks with buffers." In Communications (ICC), 2012 IEEE International Conference on, pp. 5578-5582. IEEE, 2012.

[100] Huang, Jing, and A. Lee Swindlehurst. "Buffer-aided relaying for two-hop secure communication." Wireless Communications, IEEE Transactions on 14, no. 1 (2015): 152-164.

[101] Lu, Xiaotao, and Rodrigo C. de Lamare. "Buffer-Aided Relay Selection for Physical-Layer Security in Wireless Networks." In WSA 2015; 19th International ITG Workshop on Smart Antennas; Proceedings of, pp. 1-5. VDE, 2015.

[102] Zhou, Xiangyun, Radha Krishna Ganti, Jeffrey G. Andrews, and Are Hjorungnes. "On the throughput cost of physical layer security in decentralized wireless networks." Wireless Communications, IEEE Transactions on 10, no. 8 (2011): 2764-277.

[103] Choi, Jinho, Jeongseok Ha, and Hyoungsuk Jeon. "Physical layer security for wireless sensor networks." In Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on, pp. 1-6. IEEE, 2013.

[104] Shu, Zhihui, Yi Qian, and Song Ci. "On physical layer security for cognitive radio networks." Network, IEEE 27, no. 3 (2013): 28-33.

[105] Zou, Yulong, Xianbin Wang, and Weiming Shen. "Physical-layer security with multiuser scheduling in cognitive radio networks." Communications, IEEE Transactions on 61, no. 12 (2013): 5103-5113.

[106] Wang, He, Xiangyun Zhou, and Mark C. Reed. "Physical layer security in cellular networks: A stochastic geometry approach." Wireless Communications, IEEE Transactions on 12, no. 6 (2013): 2776-2787.

[107] Geraci, Giovanni, Harpreet S. Dhillon, Jeffrey G. Andrews, Jinhong Yuan, and Iain B. Collings. "Physical layer security in downlink multi-antenna cellular networks." Communications, IEEE Transactions on 62, no. 6 (2014): 2006-2021.

[108] Sanguinetti, Luca, Antonio AD Amico, and Yue Rong. "A tutorial on the optimization of amplify-and-forward MIMO relay systems." Selected Areas in Communications, IEEE Journal on 30, no. 8 (2012): 1331-1346.

[109] Yu, Meng, and Jing Tiffany Li. "Is amplify-and-forward practically better than decode-and-forward or vice versa?." In Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on, vol. 3, pp. iii-365. IEEE, 2005.

[110] Souryal, Michael R., and Branimir R. Vojcic. "Performance of amplify-and-forward and decode-and-forward relaying in Rayleigh fading with turbo codes." In Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings. 2006 IEEE International Conference on, vol. 4, pp. IV-IV. IEEE, 2006.

[111] Levin, Georgy, and Sergey Loyka. "Amplify-and-Forward Versus Decode-and-Forward Relaying: Which is Better?." In International Zurich Seminar on Communications, p. 123. 2012.

[112] Zou, Yulong, Xianbin Wang, Weiming Shen, and Lajos Hanzo. "Security versus reliability analysis of opportunistic relaying." Vehicular Technology, IEEE Transactions on 63, no. 6 (2014): 2653-2661.

[113] Goeckel, Dennis, Sudarshan Vasudevan, Don Towsley, Stephan Adams, Zhiguo Ding, and Kin Leung. "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks." Selected Areas in Communications, IEEE Journal on 29, no. 10 (2011): 2067-2076.

[114] Lai, Lifeng, and Hesham El Gamal. "The relay – eavesdropper channel: Cooperation for secrecy." Information Theory, IEEE Transactions on 54, no. 9 (2008): 4005-4019.

[115] Bao, Vo Nguyen Quoc, Nguyen Linh-Trung, and Mrouane Debbah. "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers." Wireless Communications, IEEE Transactions on 12, no. 12 (2013): 6076-6085.

[116] Huang, Jing. "Cooperative jamming for secure communications in MIMO relay networks." Signal Processing, IEEE Transactions on 59, no. 10 (2011): 4871-4884.

[117] Maurer, Ueli M. "Secret key agreement by public discussion from common information." Information Theory, IEEE Transactions on 39, no. 3 (1993): 733-742.

[118] Tse, David, and Pramod Viswanath. Fundamentals of wireless communication. Cambridge university press, 2005.

[119] Laneman, J. Nicholas, David NC Tse, and Gregory W. Wornell. "Cooperative diversity in wireless networks: Efficient protocols and outage behavior." Information Theory, IEEE Transactions on 50, no. 12 (2004): 3062-3080.

[120] Papoulis, Athanasios, and S. Unnikrishna Pillai. Probability, random variables, and stochastic processes. Tata McGraw-Hill Education, 2002.

[121] I. S. Gradshteyn and I. M. Ryzhik and Alan Jeffrey, Table of Integrals, Series, and Products, 4th ed. Academic, 1980.

[122] Lee, Jeyull, Andrea Conti, Alberto Rabbachin, and Moe Z. Win. "Distributed network secrecy." Selected Areas in Communications, IEEE Journal on 31, no. 9 (2013): 1889-1900.

[123] Boyer, John, David Falconer, and Halim Yanikomeroglu. "A theoretical characterization of the multihop wireless communications channel with diversity." In Global Telecommunications Conference, 2001. GLOBECOM'01. IEEE, vol. 2, pp. 841-845. IEEE, 2001.

[124] Bao, Vo Nguyen Quoc, and N. L. Trung. "Multihop decode-and-forward relay networks: Secrecy analysis and relay position optimization." Journal on Electronics and Communication (JEC) 2, no. 1-2 (2012): 33-42.

[125] Nosrati, Elham, Xianbin Wang, and Arash Khabbazibasmenj. "Secrecy capacity enhancement in two-hop DF relaying systems in the presence of eavesdropper." In Communications (ICC), 2015 IEEE International Conference on, pp. 7365-7369. IEEE, 2015.

[126] Tekin, Ender, and Aylin Yener. "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming." Information Theory, IEEE Transactions on 54, no. 6 (2008): 2735-2751.

[127] Farhadi, Golnaz, and Norman C. Beaulieu. "Capacity of amplify-and-forward multi-hop relaying systems under adaptive transmission." Communications, IEEE Transactions on 58, no. 3 (2010): 758-763.

[128] Huang, Jing, and A. Lee Swindlehurst. ”Buffer-aided relaying for two-hop secure communication.” Wireless Communications, IEEE Transactions on 14, no. 1 (2015): 152-164.

[129] Geraci, Giovanni, Sushil Singh, Jeffrey G. Andrews, Jinhong Yuan, and Iain B. Collings. ”Secrecy rates in broadcast channels with confidential messages and external eavesdroppers.” Wireless Communications, IEEE Transactions on 13, no. 5 (2014): 2931-2943.

[130] Oguntunde, P. E., OA Odetunmibi, and AO Adejumo. ”On the Sum of exponentially distributed random variables: A convolution approach.” European Journal of Statistics and Probability 2, no. 1 (2014): 1-8.

# Curriculum Vitae

| | |
|---|---|
| **Name:** | Elham Nosrati |
| **Post-Secondary Education and Degrees:** | Western University (UWO)<br>London, ON, Canada<br>2013-2015 M.E.Sc.<br><br>Tehran Azad University<br>Tehran, Iran<br>2008-2010 M.Sc.<br><br>Karaj Azad University<br>Karaj, Iran<br>2000-2005 B.Sc. |
| **Experience:** | Teaching Assistantship<br>The University of Western Ontario<br>2013-2015<br><br>Technical Account Manager<br>VSAT Networks and Satellite Communication Systems<br>Mena Nets FZE, Dubai, UAE<br>2011-2013 |

**Publications:**

1. E. Nosrati, X. Wang, A. Khabbazibasmenj and A. M. Akhtar, ”Secrecy Enhancement via Cooperative Relays in Multi-hop Communication Systems”, Submitted to IEEE 83rd Vehicular Technology Conference (VTC2016-Spring), Nanjing, China.

2. E. Nosrati, X. Wang, A. Khabbazibasmenj, ”Secrecy Capacity Enhancement in Two-hop DF Relaying Systems in the Presence of Eavesdropper”, Presented at IEEE ICC Communication and Information Systems Security Symposium (’ICC’15 (11) CISS’), 2015, London, UK.

3. E. Nosrati, A. Kashi, Y. Darabian, N. Hashemi, ”Register Flooding Attacks Detection in IP Multimedia Subsystems by Using Adaptive z-score CUSUM Algorithm”, In Proceeding of the 5th International Conference on IT and Multimedia, IEEE, 2011, Malaysia.

4. E. Nosrati, N. Hashemi T., M. Hashemi T., ”Examining CSCF Entity Attacks Scenarios and Vulnerabilities in IP Multimedia Subsystems”, In Proceeding of the 7th International Conference on Information Assurance and Security, IEEE, 2011, Malaysia.

5. E. Nosrati, N.Hashemi, M. Hashemi, Y. Darabian, ”Comparison of EWMA and z-score Based CUSUM Algorithms Against DDoS Attacks Detection of IP Multimedia Subsystems”, In Proceeding of the 2011 IEEE International Conference on Information Theory and Security, 2011, China.

6. E. Nosrati, N. Hashemi, M. Hashemi, ”DDoS Attacks Scenario Simulation in IP Multimedia Subsystems through Flooding REGISTER messages”, In Proceeding of the 3rd International Conference on Computer and Automation Engineering, IEEE, 2011, China.