4-20-2015 12:00 AM

Novel Physical Layer Authentication Techniques for Secure Wireless Communications

Jiazi Liu, *The University of Western Ontario*

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

A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Electrical and Computer Engineering

NOVEL PHYSICAL LAYER AUTHENTICATION TECHNIQUES FOR SECURE WIRELESS COMMUNICATIONS

(Thesis format: Monograph)

by

Jiazi Liu

Graduate Program in Electrical and Computer Engineering

A thesis submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy

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

Acknowledgements

First of all, I would like to express my sincerest appreciation to my supervisor, Dr. Xianbin Wang, for his encouragement, guidance and support from the initial to the final stages during my doctoral studies. I have been lucky to have the opportunity to be Dr. Wang's student, and this work could never have been completed without his precious advice and constant supervision. I cannot describe how fruitful and enjoyable experiences I have learnt from him.

I would like to thank the members of my dissertation committee, Dr. Jean-Yves Chouinard, Dr. Han-Ping Hong, Dr. Anestis Dounavis and Dr. Vijay Parsa, for their precious time reading my thesis and valuable comments and suggestions.

My sincere thanks go to the faculty, staff and students I have met at Western University, who have helped me to complete my studies and experience a very nice and pleasant life in Canada. I would like to extend my thanks to all the colleagues in our research group for their support in all respects during my studies. I am also grateful to all my friends who cared for me and helped me to overcome the difficulties of the life.

Last but not the least, I would like to express my heartfelt thanks to my grandparents and parents. Their endless love and support have always been the source of any motivation in my life.

Abstract

Due to the open nature of radio propagation, information security in wireless communications has been facing more challenges compared to its counterpart in wired networks. Authentication, defined as an important aspect of information security, is the process of verifying the identity of transmitters to prevent against spoofing attacks. Traditionally, secure wireless communications is achieved by relying solely upon higher layer cryptographic mechanisms. However, cryptographic approaches based on complex mathematical calculations are inefficient and vulnerable to various types of attacks. Recently, researchers have shown that the unique properties of wireless channels can be exploited for authentication enhancement by providing additional security protection against spoofing attacks. Motivated by the vulnerability of existing higher-layer security techniques and the security advantages provided by exploring the physical link properties, this study proposes five novel physical layer authentication techniques to enhance the security performance of wireless systems.

In order to effectively and efficiently detect spoofing attacks in multipath fading environments, both spatial and temporal information of the signal propagation environment can be exploited to provide a comprehensive analysis for improving authentication performance. A robust channel-based authentication scheme is proposed by using the unique properties of channel impulse response (CIR) and monitoring the difference between two adjacent CIRs under a binary hypothesis testing. In fast fading environments, the reliability of CIR-based authentication is challenged by the fast channel variation. In order to solve the problem of unreliable spoofing detection, we exploit a long-range channel predictor to predict future CIRs in order to enhance the authentication performance. Multiple observations of CIR difference are used to form the final decision in the authentication process. In practice, the performance of channel-based physical layer authentication mechanisms is substantially degraded due to the large channel variation induced by the environmental changes and terminal mobility. In order to address this issue, we integrate additional multipath delay characteristics into the channel-based authentication framework, and propose an enhanced physical layer authentication scheme based on a two dimensional quantization method.

Furthermore, since the feasibility of traditional channel-based physical layer security schemes is hampered by the severe channel conditions, a novel physical layer authentication scheme is

proposed by exploiting the advantages of amplify-and-forward (AF) cooperative relaying. The essence of the proposed scheme is to select the best relay among multiple AF relays, such that the legitimate transmitter would experience better channel conditions than a spoofer. Towards this goal, two best relay selection schemes are developed based on the notion of maximizing the SNR ratios of the legitimate link to the spoofing link at the destination and relays, respectively. To evaluate the performance, we define our performance metrics based on the outage of effective SNR ratios and the probability of spoofing detection.

To prevent eavesdropping attacks in conventional orthogonal frequency division multiplexing (OFDM) systems, a continuous physical layer authentication system is developed based on an adaptive OFDM system with time-varying transmitter-receiver interaction enabled by the precoded cyclic prefix (PCP) and outlined in the final part of the dissertation. Instead of traditional CP in an OFDM system, PCP sequences are employed as guard intervals and signaling links as well, which are generated with the same temporal and spectral characteristics of data-carrying OFDM signals in order to conceal system parameters to adversaries.

Keywords: Wireless communications, physical layer authentication, CIR, channel predictor, 2-D quantization, AF cooperative relaying, best relay selection, PCP-OFDM.

Contents

List of Figures

List of Tables

List of Appendices

List of Abbreviations

Abbreviation	Description	First use
AF	Amplify-and-Forward	5
ARP	Address Resolution Protocol	14
AWGN	Additive Gaussian White Noise	146
CDF	Cumulative Distribution Function	42
CF	Compress-and-Forward	23
CFR	Channel Frequency Response	2
CFO	Carrier Frequency Offset	2
CIR	Channel Impulse Response	2
CJ	Cooperative Jamming	26
CP	Cyclic Prefix	4
CSI	Channel State Information	2
DF	Decode-and-Forward	23
DoS	Denial of Service	31
DT	Direct Transmission	104
FAR	False Alarm Rate	6
FFT	Fast Fourier Transform	27
ICI	Inter-Carrier Interference	137

IDFT	Inverse Discrete Fourier Transform	27
IEEE	Institute of Electrical and Electronics Engineers	4
IFFT	Inverse Fast Fourier Transform	27
IP	Internet Protocol	14
ISI	Inter-symbol Interference	3
LLC	Logical Link Control	14
LOS	Line-of-Sight	36
LS	Least Squares	52
LTE	Long-Term Evolution	4
MAC	Media Access Control	14
MIMO	Multiple-Input Multiple-Output	21
MISO	Multiple-Input Single-Output	21
MSE	Mean Square Error	39
OFDM	Orthogonal Frequency Division Multiplexing	3
OSI	Open Systems Interconnection	1
PCP	Precoded Cyclic Prefix	6
PD	Probability of Detection	6
PDF	Probability Density Function	79
QoS	Quality of Service	14
RF	Radio Frequency	10
RF – DNA	Radio Frequency Distinct Native Attribute	2
RIP	Routing Information Protocol	14

ROC	Receiver Operating Characteristic	43
RSS	Received Signal Strength	20
SER	Symbol Error Rate	146
SIMO	Single-Input Multiple-Output	21
SNR	Signal-to-Noise Ratio	6
TCP	Transmission Control Protocol	13
UDP	User Datagram Protocol	13
WiMax	Worldwide Interoperability for Microwave Access . . .	4
WLAN	Wireless Local Area Network	4
WSNs	Wireless Sensor Networks	17

Chapter 1

Introduction

1.1 Research Motivations and Objectives

Information security is critical for any communication systems. Compared to wired networks, wireless communication networks face more security challenges primarily due to the nature of openness [1]. Moreover, high-level security mechanisms in wired communications cannot be directly applied in wireless communication systems. Therefore, it is certainly worth investigating techniques to secure wireless communications. Traditionally, wireless security techniques are achieved by relying solely on the upper layers of the open systems interconnection (OSI) network model. However, existing higher-layer security mechanisms are designed based on the computational hardness of mathematical functions, which are not feasible for practical wireless communication systems with limited resources. Additionally, traditional cryptographic techniques are susceptible to various types of attacks and do not directly leverage the unique properties of the wireless medium to address security threats. To this end, physical layer security has drawn a lot of attention in recent years; this security is achieved based on the lowest layer of the OSI model by exploiting physical link properties to provide additional security protection [2].

In wireless communications, spoofing is a severe security threat due to the broadcast nature of radio signal propagation, in which adversaries attempt to impersonate the legitimate user within a network in order to gain illegitimate advantages [1]. In order to defend systems against spoofing attacks, the receiving end should be equipped with authentication mecha-

nisms, which provide systems with the ability of validating the identities of involved users. By exploiting the advantages of securing wireless transmissions at the physical layer, a variety of physical layer authentication schemes have been proposed by using the inherent properties of wireless channels [3–12] or the imperfections of hardware devices [13–17]. The fundamental principle behind channel-based physical layer authentication is that the spatial, spectral and temporal properties of the wireless fading channel have natural randomness and they are rapidly decorrelated between different geographic locations. As a consequence, the properties of the channel link between legitimate terminals are only available to the intended receiver but cannot be duplicated by adversaries. Additionally, radio-frequency distinct native attribute (RF-DNA) fingerprint-based physical layer authentication exploits device impairments, such as I/Q modulator imbalance and carrier frequency offset (CFO), for device discrimination. These device imperfections, which are unclonable and unforgeable to intruders, are caused by manufacturing variability. Therefore, the intrinsic characteristics of the physical layer attributes can be adopted as a way to improve the authentication performance of wireless communication systems via the physical layer.

Based on a comprehensive study of channel-based physical layer authentication, exploiting the physical layer properties of the wireless channels brings the potential to enhance authentication performance in spoofing detection. Mathematically, channel-based physical layer authentication is formulated as a binary hypothesis testing problem. As the channel state information (CSI) measurements over different links can be dramatically distinguished at the receiving end, two hypotheses are defined based on the difference of adjacent CSI measurements in time. In the presence of spoofers, the final decision is made by comparing the channel difference with a threshold in order to determine if a spoofing attack has occurred. In [6, 8, 9], the characteristics of channel frequency response (CFR) were well studied for authentication enhancement; however, the CFR analysis in the received signal fails to exploit the spatial information related to the signal propagation environment. Thus, effective, efficient and robust channel-based authentication approaches are needed to defend against spoofing attacks.

In rich scattering environments, it is noteworthy that the properties of channel impulse response (CIR) represent the spatially geographical locations of wireless terminals. Moreover, the multipath components are independent of each other, but they are highly correlated

over time. Therefore, the characteristics of CIR of a multipath fading channel represent the spatial and temporal information related to the signal propagation environment, which can be exploited to develop robust physical layer authentication schemes. However, in fast fading environments, the processing delay and outdated CIR measurements may result in large channel variation. Moreover, the variation between two successive CIRs can also be caused by the movement of mobile terminals or environmental changes. As a result, the reliability of channel-based physical layer authentication schemes is challenged by the fast channel variation. Also, the robustness of decision-making for authentication is degraded as the final decision is just based on a single observation of the channel variation. Therefore, we argue that reliable channel-based authentication approaches are needed to improve the authentication performance under a fast fading environment.

In practical wireless communication systems, it has been noticed that user mobility may affect and complicate the functioning of applications and protocols. In high mobility environments, the performance of CIR-based physical layer authentication schemes is significantly degraded due to the large channel variation induced by the environmental changes and terminal mobility. It is therefore important to enhance the performance of CIR-based authentication in high mobility environments.

Physical layer authentication techniques for wireless communications can prevent malicious attacks without upper layer data encryption. However, the reliability of traditional channel-based physical layer authentication schemes is hampered by severe channel conditions. In order to overcome this limitation, the application of multiple antennas has been explored to combat channel fading and improve the performance of secure wireless communications. However, as a result of cost and size limitations of multiple antennas, these scenarios are rarely implemented in practice. For the practical implementation of channel-based authentication systems, efficiently exploiting the advantages of multiple antenna arrays to enhance the performance of spoofing detection has yet to be investigated.

Orthogonal frequency division multiplexing (OFDM) is a multiplexing method in which data are transmitted over the equally spaced, overlapped carrier frequencies. The advantages of OFDM include: 1) It can achieve high data rates with great bandwidth efficiency and flexible underlying modulations; 2) It can easily eliminate intersymbol interference (ISI) with the

help of cyclic prefix (CP); 3) Channel equalization becomes much simpler compared to single carrier systems. Due to these advantageous features, OFDM has been included in the physical layer specifications of a large variety of wireless standards, from the well-established and widespread wireless local area network (WLAN) transmissions of the family Institute of Electrical and Electronics Engineers (IEEE) 802.11 to the more recent worldwide interoperability for microwave access (WiMax) and long-term evolution(LTE) protocols. However, conventional OFDM systems do not have inherent security features due to the distinct time and frequency characteristics of OFDM signals. In order to secure OFDM-based wireless systems, conventional higher-layer cryptographic techniques provide secrecy without considering the lower layer. The virtual physical layer transparency brings security vulnerability to the information protected by higher-layer cryptographic techniques, as the information can often be deciphered by using exhaustive trial. Consequently, an additional physical layer based security approach is necessary to enhance the security of OFDM systems.

Considering the aforementioned wireless security issues, our contributions to authentication enhancement in wireless communications are discussed in the next section.

1.2 Dissertation Contributions

The main contributions of this dissertation are summarized as follows:

- A comprehensive survey of existing wireless security techniques is illustrated and the weaknesses of the existing state-of-the-art security approaches are explained in detail. Security vulnerabilities of OFDM-based wireless networks are discussed as well. These wireless security issues were the motivation for five of the contributions of the dissertation.

- A robust physical layer authentication scheme is proposed to detect anomalous behaviors through the statistical analysis of the inherent properties of CIR difference in a time-varying multipath environment. The variation between two consecutive CIR estimates from a transmitter of interest is monitored at the receiver in order to distinguish the identities of different transmitters for authentication purposes. To minimize the impact

of noise and interference from wireless environments, we develop a new test statistic based on the difference between noise-mitigated CIRs.

- In fast fading environments, the reliability of CIR-based physical layer authentication is challenged by the fast channel variation. To address this issue, a long-range channel predictor is utilized to predict future CIRs in order to compensate for the effects of fast channel variation in the authentication performance. Moreover, by exploiting the long-range channel predictor, multiple CIR differences are calculated by the receiver in an observation window, and a final decision is formed based on the multiple observations of CIR differences in order to increase the robustness of decision-making for authentication. To find an optimal threshold in decision-making, the ratio of the threshold to the window size is optimized by minimizing the total error rate subject to false alarm constraints under different channel conditions.

- In a high mobility environment, the performance of spoofing detection for CIR-based physical layer authentication is degraded significantly due to the large variation in the channel amplitude over time. In contrast with the temporal variation of channel amplitude, another characterization of wireless channels, viz., the multipath delay spread, is relatively stationary over long time intervals [18]. More importantly, multipath delay spread profiles are distinct from one location to another if the locations are spatially separated. Therefore, we propose an enhanced CIR-based physical layer authentication scheme by integrating additional multipath delay characteristics into the CIR-based authentication framework. A two-dimensional quantization method is developed to preprocess the temporal channel variations in the dimensions of channel amplitude and path delay. Based on the quantization method, the decision rule in the authentication process is simplified.

- Motivated by the security advantages of cooperative transmissions, a novel physical layer authentication scheme is developed by exploiting the advantages of amplify-and-forward (AF) cooperative relaying. Considering multiple trusted AF relays in the scenario, only one relay is selected to provide the best end-to-end path between legitimate end nodes in the presence of a spoofer. To achieve this goal, two best relay selection schemes are

developed based on the notion of maximizing the signal-to-noise ratio (SNR) ratios of the legitimate link to the spoofing link at the destination and relays, respectively. In order to evaluate the performance of the proposed scheme, we define our performance metrics in terms of the outage probability of the effective SNR ratios and the probability of spoofing detection.

- In order to enhance the security of OFDM systems, a new continuous physical layer authentication system is proposed based on an adaptive OFDM platform by exploiting precoded cyclic prefix (PCP) instead of conventional CP to convey time-varying transmission parameters and secure the legitimate transmissions as well. The PCP sequences are generated with the same time and frequency domain characteristics as data-carrying OFDM signals in order to be concealed from eavesdroppers. By using the PCP, the transmitter can adjust its operating parameters continuously and only share the link adaptation information with legitimate receivers. Additionally, cross-layer design is utilized to continuously generate optimal PCPs according to dynamic communication conditions.

1.3 Dissertation Outline

The following details the organization of remaining chapters of this dissertation.

Chapter 2 includes a comprehensive discussion on wireless communication security, including wireless security issues and countermeasures, as well as major security requirements and security design principles. Additionally, the security vulnerabilities of wireless OFDM systems are discussed after a general introduction of OFDM technology.

In Chapter 3, a robust physical layer authentication scheme is proposed by studying the statistical analysis of the inherent properties of CIR in a time-varying multipath environment. Specifically, a new test statistic is developed based on the variation between two consecutive noise-mitigated CIRs in order to distinguish between different transmitters for authentication purpose. Based on the defined authentication test, false alarm rate (FAR) and probability of detection (PD) are theoretically derived for evaluating the performance of the proposed scheme.

To address the problem of unreliable spoofing detection caused by fast channel variation, we exploit a long-range channel predictor to predict future CIRs in order to compensate for the

negative impacts of fast channel variation in Chapter 4. By exploiting the long-range channel predictor, multiple CIR differences are achieved by the receiver in an observation window to form a final decision under a simple hypothesis testing. In order to optimize the threshold of decision-making, an optimization problem is defined based on minimizing the total error rate under false alarm constraints.

In Chapter 5, we develop an enhanced physical layer authentication scheme by integrating additional multipath delay characteristics into the CIR-based authentication framework. A two-dimensional quantization method is developed to preprocess the temporal channel variations in the dimensions of channel amplitude and path delay. More specifically, two one-bit quantizers are used in the two dimensions, respectively, to quantize the difference between adjacent channel realizations (i.e., channel amplitudes and time intervals). The quantizer output becomes identical if the difference is larger than a threshold, otherwise it is zero. By exploiting the quantization method, the decision rule for authentication test is simplified. In order to verify the performance of the proposed authentication scheme, FAR and PD are defined and their closed-form expressions are derived as well.

In Chapter 6, a novel physical layer authentication scheme is proposed based on an AF cooperative relaying system, where one best relay is selected to provide the best end-to-end path between the source and destination in the presence of a spoofer. To achieve this goal, two best relay selection schemes are developed. Specifically, the first scheme is based on the notion of maximizing the end-to-end SNR ratio of the legitimate link to the spoofing link, while the second scheme is based only on the first-hop SNR ratio in order to reduce computational complexity and resource consumption. For performance analysis, the outage of the effective SNR ratios and the probability of spoofing detection are derived.

A new continuous physical layer authentication technique with time-varying transmission parameters is investigated in Chapter 7 to enhance the security of conventional OFDM systems. A PCP sequence, which introduces an additional signaling link to carry the time-varying transmission parameters, is employed in each OFDM symbol for physical layer authentication. The new PCP sequences are generated with the same time and frequency domain characteristics as data-carrying OFDM signals to be concealed from unauthorized receivers. With the proper recovery of system parameters and interference cancellation, only legitimate users can

successfully decode the PCP sequence and obtain necessary parameters to decode OFDM data. In addition, a cross-layer design approach is introduced to continuously generate optimal PCPs according to dynamic communication conditions.

Finally, conclusions and future research directions are illustrated in Chapter 8.

Chapter 2

Security Challenges and Solutions in Wireless Communications

Advances in communications and networking technologies are rapidly making ubiquitous network connectivity a reality. Wireless networking technologies bring convenience into our lives, whereas the open nature of the wireless medium and limited options of transmission techniques have introduced many security challenges that do not exist in the wired networks. In this chapter, security issues in wireless communications are illustrated and addressed, based on a comprehensive literature survey of existing wireless security techniques. Additionally, the system modeling of OFDM is given, and the vulnerabilities of conventional OFDM systems for secure data transmission are discussed as well.

2.1 An Overview of Wireless Security Issues

2.1.1 Security Challenges of Wireless Communications

Security is an implicit part of any communication system that is relied upon for the transmission of private information. Consequently, the reliability to share secret information in the presence of malicious attackers is critically important. From a general perspective, security is concerned with unauthorized users trying to access, forge or modify messages intended for legitimate receivers. In wired networks, signals travel through the wires, which makes the wired

communications secure as long as only authorized users have access to the data. Unlike wired data communications, wireless communications is based on electromagnetic waves using radio frequencies (RF) propagating through open space, which provides the freedom of user mobility and the flexibility of data transmission, but also brings significantly more security challenges than traditional wired communications. Therefore, secure wireless communications becomes critical for wireless data transmission.

There are many factors contributing to the increasing security challenges in wireless communications. Primarily, the broadcast nature of the wireless medium makes transmitted signals available to any receiver within the transmission range, which leads to easy access to adversaries. Moreover, the mechanisms of high-level security in a wired network cannot be directly applied in wireless scenarios. Additionally, limited processing power is incurred by the limited space, cost and power constraints of wireless devices. Considering these essential limitations of wireless communications, security mechanisms for wireless systems should be developed to address increasing threats.

2.1.2 Major Security Requirements

Security aims at defending information from various malicious attacks, such as eavesdropping [2], communications jamming [20], injection and modification of data [20], traffic analysis [21], and spoofing [22]. Generally, the requirements of security can be mainly divided into six categories, i.e., confidentiality, authenticity, integrity, availability, non-repudiation and privacy. Their functions are explained as follows:

- Confidentiality: This is also known as secrecy, which means that only authorized users can access information. This level of confidentiality should be maintained while data is transmitted from source to destination within the network.

- Authenticity: This means an ability of a system to validate the identities of involved users and establish trust in provided information.

- Integrity: This means that only authorized users can modify data in authorized ways. A system should ensure completeness as well as accuracy in all its components and prevent from unauthorized modification.

- Availability: This means that authorized users can access data and resources of a system in a timely manner, which ensures the reliability of all components in a system. Failing to meet this feature can cause a denial of service.

- Non-repudiation: This means an ability of a system to prove a certain message sent by a sender or received by a receiver, an action cannot be falsely denied by either the sender or receiver.

- Privacy: This is usually addressed separately from confidentiality, which means an ability of a system to protect the identities of users and enable feasible control of one's personal information by users.

In the implementation of every security mechanism, one or several of these principles are required to assure the secrecy of communications systems. In order to address the aforementioned security issues in wireless communications, effective, efficient and robust security approaches are required. In the next section, a comprehensive literature review on existing wireless security techniques is presented from two perspectives, i.e., traditional security and physical layer security.

2.2 Traditional Wireless Security Techniques

2.2.1 Seven Layers of the OSI Model and Their Security Vulnerabilities

The OSI model was introduced by the International Standards Organization in 1978, as a first step toward the requirement of internationally standardized protocols for data communications. It defines a hierarchical architecture that logically separates networking functions required to support system-to-system communications. Consequently, each layer can be viewed as an independent module. Due to this layered architecture, network problems can be more easily solved through a divide-and-conquer methodology, and a protocol can also be theoretically substituted by another at the same layer, as can network services.

From a high-level application perspective, data is sent down the stack layer-by-layer in one station, proceeding to the bottom layer. Then it is transmitted over the physical medium to the

next station and back up the hierarchy. In what follows, the seven layers of the OSI model are illustrated (starting from the top layer) in terms of their general functionality and security vulnerabilities.

- Application layer:

  The application layer is the top layer of the OSI model and refers to the user interface supporting the end user functions. It provides a variety of high-level functions such as file transfer, access and management, virtual terminal, electronic mail and messaging handling, and common management information protocol. It also provides application access security checking and information validation.

  From the security perspective, the open-ended nature of the application layer brings various threats to the end of the stack. One of the primary threats at the application layer is that the weak security design of applications allows unauthorized users to freely use the application resources. Applications may establish identity or set privilege over untrustworthy channels. However, this "all or nothing" approach of security controls, which forces administrators to give either unlimited access or none at all, results in either excessive or insufficient access.

- Presentation layer:

  The presentation layer is responsible for converting incoming and outgoing data from one presentation format to another, where the syntax and semantics of the transmitted information are managed, making it possible for different computers to communicate with each other. More specifically, this layer provides various communications services related to information representation, such as data compression and encryption.

  Vulnerabilities at the presentation layer are mainly caused by weaknesses or shortcomings in the implementation of the presentation layer functions. In particular, format string vulnerability takes advantage of the poor handling of unexpected incoming data, which can crash applications, surrender the controls of data format and transmission, or execute arbitrary instructions. Additionally, the flaws of cryptography protocols may be exploited to circumvent the protections of privacy and authentication.

- Session layer:

  The session layer is responsible for session handling between applications by establishing, maintaining, synchronizing, controlling and terminating connections. It also provides security services, such as login passwords and exchange of user IDs, to control access to session information.

  Since the session layer is concerned with the control of access to applications, it falls prey to the weaknesses of handling passwords and authentication. In particular, password-based access is prone to attackers, who are allowed to use unlimited and undetected attempts to guess the passwords. Additionally, most of protocols at this layer lack strong authentication, as they allow lower layers to intercept their credentials.

- Transport layer:

  The transport layer is concerned with the transmission by breaking up data streams from the upper layer into packets passing to the lower layer, and reassembling the incoming data packets from the lower layer back into a coherent stream for the upper layer, without modification, loss or duplication during the transmission. This layer provides the end-to-end communications control, and the aforementioned transmission needs are achieved based on transport protocols such as transmission control protocol (TCP) and user datagram protocol (UDP). Data flow control and error checking are provided as well at this layer.

  Most transmission protocols usually do not implement strong controls to identify the source of a transmission, which leads to interruption or redirection of the flow of the transmission. For instance, UDP protocol can be trivially spoofed due to a complete lack of sequencing or state at the transport layer. In addition, the use and re-use of ports for multiple functions is another security vulnerability of the transport layer.

- Network layer:

  The network layer deals with the global network topology to handle the operation of taking packets from source to destination over multiple possible paths, where basic functions of routing and congestion control are provided. This layer typically relies on In-

ternet protocol (IP) addresses and routing tables to identify nodes and construct paths over the Internet. Address resolution protocol (ARP) is implemented to convert the IP addresses to the link layer addresses, routing information protocol (RIP) is utilized to distribute routing information within the network, and IP protocol is used to identify the transmission protocol (such as TCP or UDP) from the higher layer in order to direct the higher layer how to handle the incoming data. Additionally, if all the networks send packets at the same time, such congestion is managed by the network layer. More generally, the network layer provides the quality of service (QoS) such as transmitting time, jitter and delay.

To achieve the aforementioned goals at the network layer, protocols at this layer lack necessary protection against malicious attacks. In particular, most routing protocols have only a basic level of security, which can be exploited by spoofers propagating false network topology. Additionally, most network layer protocols lack authenticating source addresses, thereby unsecured third parties located therein can use false addresses to impersonate the source.

- Data link layer:

  The data link layer is concerned with frame transmission between two directly connected local devices, which has two sublayers, i.e., logical link control (LLC) and media access control (MAC). The main tasks of this layer are (1) to split the input bits from the physical layer into data frames so that no apparent errors can be seen by the network layer, and (2) to encapsulate the network layer data packets into frames structured based on MAC addresses whose headers contain the source and destination addresses. This layer provides error control, frame synchronization and flow control for the physical level based on the attached link-layer headers.

  Due to the insecure addressing structure and weak encryption algorithms, the data link layer is prone to several types of attacks [23]. For instance, ARP spoofing can be achieved by an attacker because the ARP protocol, as a stateless protocol, does not provide a method to a host to authenticate the peer from which the packet originated. Moreover, MAC addresses are used to uniquely identify devices in this layer; however,

they can be easily modified. Additionally, link-layer encryption has been used to protect information in transit between two points. However, a lack of authentication in the transmission link can cause vulnerability at the link when messages must be transmitted between unauthorized hosts.

- Physical layer:

  The physical layer is the lowest layer of the OSI model and responsible for transmitting raw bits across a communication medium. This layer is concerned with the actual data encoding, modulation, synchronization and transmission through the network at the electrical and physical level.

  Reviewing the flow of information through the OSI model, we can see that all of the above layers depend upon the physical layer for data delivery. Therefore, the physical layer is critical to data communications. However, it is the most vulnerable and changeable among the seven layers, as all information security assets are based on the physical security. For instance, from a networking perspective, communications can be easily stopped if one can disconnect a device from the network or physically switch it with another. Additionally, errors at the physical layer can be kept and passed through all the above layers [24].

Figure 2.1 illustrates the OSI model referred to as a layered protocol architecture, where a specific set of network functions is allocated to each layer that provides services to the upper layer and receives services from the lower layer. From the security point of view, security provision of each layer of the OSI model can be achieved independently, and secure data transmission is accomplished generally based on the use of strong authentication and data encryption at higher layers. However, these higher-layer based security solutions are vulnerable to various types of attacks. It is also noteworthy to mention that higher layers cannot be secured without secured lower layers. Therefore, secure data transmission at the lowest layer can fundamentally address the security issues in wireless communications.

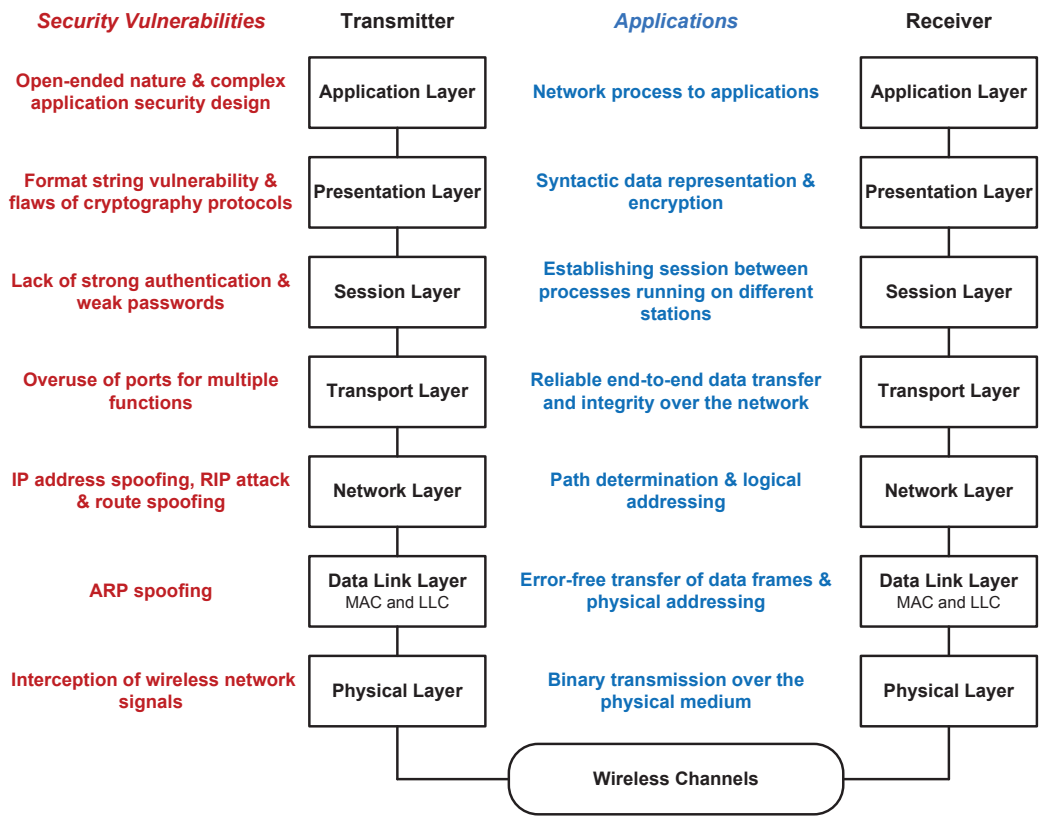

Figure 2.1: The OSI model with examples of applications and security vulnerabilities.

2.2.2 Security Limitations of Traditional Approaches

Traditionally, wireless security is achieved by relying on the upper layers of the OSI reference model. Traditional wireless security techniques can be discussed in two parts, i.e., authentication and encryption. Authentication is a policy of verifying the identity of communication partners, whereas encryption is responsible for encrypting transmitted data using an encryption key so that the data can only be decrypted by legitimate users in the presence of adversaries.

Typically, authentication relies on the MAC addresses of hardware at the link layer or IP addresses at the network layer to identify users. However, this mechanism is vulnerable for three reasons. First of all, devices can be stolen by adversaries, thereby unauthorized user can get access to the network. Moreover, MAC addresses can be changed in some hardware. A malicious device can duplicate the MAC address to spoof the legitimate user and use it to gain access to the network. This type of attacks in wireless networks is called identity-based attacks,

which is one serious threat that can be launched easily [25]. Additionally, intruders can use an IP address of a trusted user with modified packet headers to get unauthorized access to the network.

Furthermore, encryption is generally implemented at all the upper four layers, in which case the transmitted messages are encrypted based on a secret key. Encryption approaches can be classified into asymmetric-key and symmetric-key schemes [26]. Specifically, asymmetric-key encryption schemes use a public and private key-pair to perform the opposite functions by encrypting data with the public key and decrypting data with the private key. Therefore,they do not require a secure initial exchange of the secret keys between the legitimate users. On the other hand, symmetric-key encryption supposes that a secret key is privately shared between the legitimate users, and that key is used to secure the transmission against potential intruders. However, key-based encryption techniques may cause key distribution and management problems especially in large number node networks [27, 28].

Additionally, traditional higher-layer security techniques mainly rely on complex mathematical calculations that consume considerable resources. Consequently, these traditional security solutions are not feasible for wireless networks such as wireless sensor networks (WSNs) and ad hoc networks, which exploit resource-constrained nodes within the network. Moreover, traditional encryption techniques are inefficient in certain existing scenarios, as they do not directly leverage the unique properties of the wireless medium to defend against security threats [19, 26, 29].

2.3 Physical Layer Security Techniques

Physical layer security, which exploits physical link properties, is a promising paradigm to provide energy-efficient security solutions and enhance the security performance of wireless communications systems [30]. Security from the information-theoretic perspective was pioneered by Shannon [31], who introduced the definition of perfect secrecy and theoretically characterized that the fundamental ability of the physical layer can provide secure communications. In this section, a comprehensive literature survey on existing wireless security techniques at the physical layer is undertaken, and physical layer security techniques are classified

into three major categories based on the wireless channel, RF-DNA and diversity technique, respectively.

2.3.1 Wireless Channel-Based Physical Layer Security

In wireless communications, due to the presence of scatterers and reflectors in the environment, a transmitted signal undergoes multiple paths that combine constructively or destructively at the receiver. Consequently, the received signal is the superposition of multiple copies of the transmitted signal via different paths from the transmitter to the receiver, where each copy experiences differences in attenuation, phase shift and propagation delay. In a multipath propagation environment, the wireless channel can be mathematically modeled by using the method of the impulse response in the time domain,

$$h(t,\tau) = \sum_{l=0}^{L-1} \alpha_l(t) e^{\theta_l(t)} \delta(\tau - \tau_l), \tag{2.1}$$

where L is the number of multipath components. $\alpha_l(t)$, $\theta_l(t)$ and τ_l are amplitude, phase and propagation delay of the lth path, respectively.

From the expression of the multipath channel in equation (2.1), the wireless channel characterized by CIR has the following major properties:

- Reciprocity: As during the coherence time, the observed channel impulse responses at two geographically separated communicating terminals are the same.
- Correlated temporal variation: Wireless channels vary with time but the variation is usually highly correlated in time.
- Spatial decorrelation: According to the propagation theory [32], the radio channel response decorrelates rapidly in space from one transmitter-receiver pair to another if these two pairs are at least half a wavelength away.

Based on the above properties, the wireless channel has unique location-specific characteristics that are only determined by the two specific ends of the channel. Therefore, the characteristics of the wireless channels can be exploited to provide a complementary guarantee

of secure wireless communications. Additionally, exploitation of the physical link properties by the channel-based physical layer security tends to convert the open nature of the wireless medium from a security disadvantage into a security advantage.

To illustrate the general idea of channel-based physical layer security, Figure 2.2 shows a typical adversarial multipath scenario including multiple scattering surfaces, where terminals A, B and E are located in spatially different locations. It indicates that the legitimate communications between terminal A and terminal B experiences different paths from the transmission between the adversary E and terminal B. Therefore, exploiting the unique characteristics of the wireless propagation environment can discriminate among different transmitters.

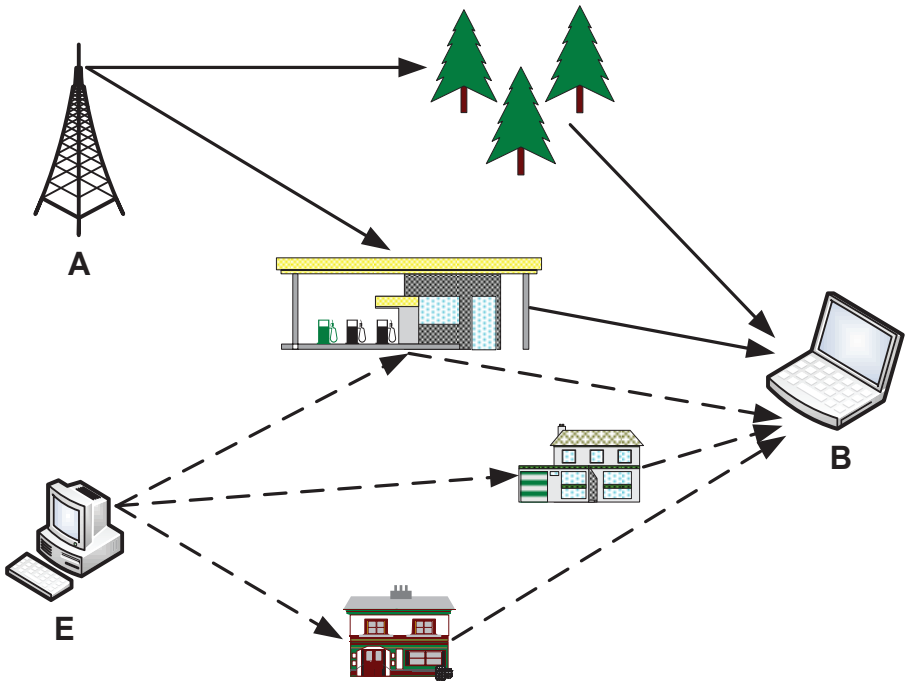

Figure 2.2: An adversarial multipath environment including multiple scattering surfaces.

A variety of channel-based physical layer security schemes have been proposed in the literature. Specifically, by exploiting the channel reciprocity in wireless communications, a multipath channel randomness-based secret key generation system was developed in [33]. Two-way training signals were employed by legitimate communicating terminals to obtain the same observations of the multipath fading channel coefficients under a static channel over two successive time slots. A secret key was generated based on the observations of the legitimate

channel; however, it is unavailable for an adversary due to the fast spatial decorrelation of multipath channels. Moreover, the received signal strength (RSS), which is a location-dependent feature associated with the transmit power and CSI, was utilized to differentiate between transmitters [4, 5]. However, such physical layer security schemes are vulnerable to intruders who can adjust transmitting power to spoof the legitimate user.

Alternatively, using the temporal and spatial properties of radio signal propagation in wireless networks, Xiao [6, 8, 34], He [9, 35] and Tugnait [10] proposed physical layer security approaches, and obtained performance enhancement in detecting spoofing attacks. In particular, Xiao explored the properties of channel difference between two consecutive CFR measurements in multipath fading environments, and not only analyzed the characteristics of channel difference from single carrier communication networks to multi-carrier wireless systems, but also extended her method from the assumption of time-invariant channel to mobile terminals. In [9], He considered both the amplitude and phase information of CFR to fully achieve authentication based on Xiao's work, and this work was expanded by using the RAKE receiver to distinguish users [35]. Following the approaches provided by Xiao, Tugnait [10] used time-domain training-based CIR to accomplish authentication instead of the CFR-based method, which considered the time-invariant channel.

2.3.2 RF-DNA Based Physical Layer Security

RF-DNA fingerprinting involves exploiting natural imperfections and unclonable variations of a unique device induced by the analog components to identify and authenticate devices at the physical layer, which cannot be changed post-production and mimicked by adversaries in a manner analogous to biometrics. Various RF characteristics, such as transient amplitude and phase, I/Q modulator imbalance and CFO, are extracted from the intrinsic physical properties of devices. These hardware impairments are observed differentially even in two devices constructed with the same manufacturing and packaging processes, and they are allowed by manufacturers as wireless transceivers as such minor imperfections are acceptable for practical implementations in the communication standards [36, 37]. Therefore, the distinct features of the RF-DNA fingerprint can be utilized to provide additional protection against identity-related

threats via the physical layer.

Many RF-DNA fingerprint-based device identification and authentication schemes have been proposed in the literature. Specifically, a RF fingerprinting system was designed to identify WiFi devices in [38] by exploiting the amplitude and phase of transient signals to enhance wireless security. Moreover, [39] investigated a RF fingerprinting approach by exploiting transient signal features for hardware-specific identification based on 802.11a OFDM signals. In [13], a stable and robust identification technique was proposed based on combining several device-specific characteristics, including the frequency offset, modulated phase offset and in-phase/quadrature-phase offset. Furthermore, a RF identification system was introduced in [40] relying on the RF characterization of integrated circuits to defend against counterfeiting. [16] proposed a novel physical layer authentication scheme by exploiting the unique bias in RF oscillators between a specific transmitter-receiver pair that is characterized by the device-dependent CFO. In [17], a physical layer authentication approach was developed by exploiting the time-varying clock offsets. Additionally, [15] investigated a device fingerprint-based estimation method by exploiting device-specific I/Q imbalance to differentiate different wireless devices.

2.3.3 Diversity Technique-Based Physical Layer Security

2.3.3.1 PHY Layer Security in Multiple-Antenna Systems

Since the capacity of single antenna systems is bounded by the Shannon limit, diversity techniques have been developed to improve system performance by using multiple replicas of transmitting signals passed over multiple channels of different characteristics. Multiple antenna techniques provide physical layer secrecy with new and exciting opportunities, and also provide extremely high spectral efficiency as well as link reliability through space diversity for wireless communications [41].

By exploiting multiple antenna array structures, secure transmissions in multiple-antenna systems were investigated in the literature [42–50], where the channel from source to legitimate destination was modeled as single-input multiple-output (SIMO) [42], multiple-input single-output (MISO) [43–45], and multiple-input multiple-output (MIMO) [46–50]. Further-

more, [51] designed a MIMO authentication system by superimposing a stealthy fingerprint on transmitted data, and also studied the tradeoffs between stealth, security and robustness. Moreover, a channel-like fingerprint signal was introduced to MIMO transmissions, where the fingerprinting was generated to mimic distortions like time-varying channel effects [52]. In a rich multipath environment, by exploiting the location-specific properties of the wireless channels, CFR-based physical layer authentication in [6] was extended to a MIMO scenario that analyzed the impact of MIMO techniques on the performance of spoofing detection based on the ability of security gain [53]. By exploiting the properties of array redundancy and channel diversity, Li *et al.* [54] developed a MIMO security scheme to effectively randomize the reception at the eavesdropper.

Innovative cross-layer designs for security enhancement combining physical layer security with upper-layer traditional security are desirable for wireless networks. In [55], a cross-layer security scheme for MIMO systems was proposed by using an extra dimension provided by MIMO systems to add artificial noise to the transmitted signals; as a result, received signals by the eavesdropper became a degraded version of legitimate signals. Additionally, [56] combined cryptographic techniques operating in higher layers with security approach exploiting redundant antennas at the physical layer to provide enhanced security performance for wireless networks.

2.3.3.2 Cooperative Relaying and Security Enhancement

MIMO systems use the technique of space diversity to improve communications performance where multiple antennas are equipped at the transmitter and receiver. However, the hardware implementation of MIMO systems is not feasible, particularly in mobile equipments, due to size, weight and cost limitations [57]. As an alternative, cooperative diversity is achieved through user cooperation, in which information is allowed to be transmitted between source and destination via other nodes in a network in order to enjoy the advantages of MIMO systems with single antenna equipped users. More specifically, cooperative communications provides the advantages of higher spatial diversity and achievable data rates, lower transmission delay and power, better frequency reuse and more adaptability to network conditions. Additionally, cooperative communications techniques exploit user cooperation to combat channel fading and

enhance the security performance of wireless networks.

A classic cooperative communications network is illustrated in Figure 2.3, which consists of one source, one destination and N nearby relay nodes. The message transmission over the direct channel between the source and the destination is called direct transmission, and the message transmission with the help of relay nodes is called cooperative transmission. Information transmission takes place in two phases. In the first phase, the message is broadcast from the source, and received by the destination and the N relays. In the second phase, a subset or all the relays process the received message then forward it to the destination based on a specific cooperation transmission protocol.

By a careful investigation of the relaying strategies, cooperative transmission protocols can be categorized into three types: the amplify-and-forward (AF) protocol in which relays amplify the source signals and then retransmit them to the destination, the decode-and-forward (DF) protocol in which relays first decode source signals and then encode and forward them to the destination, and finally the compress-and-forward (CF) protocol in which relays first maps source signals into another signals in a reduced signal space and then encode and forward them as new codewords to the destination. Depending on the network topology and the quality of the channel between the source and the relays, one protocol may perform better than the others in terms of system capacity or diversity. Generally, the AF protocol is usually preferable due to its low complexity on the relays.

The advantages of the cooperative communications come at the price of a reduced spectral efficiency. Particularly, during the second phase, the data transmission from each relay to the destination occurs through orthogonal channels, which in turn leads to the spectral inefficiency. The concept of best relay selection is an efficient and simple method to resolve this shortcoming of the cooperative communications. Specifically, instead of using all the available relays, the best relay is selected based on a specific criterion. Similar to the original cooperative communications, the best relay selection also can achieve the full diversity [58, 59]. It is worth mentioning that the best relay selection scheme can be extended to multiple relay selection schemes in which multiple relays are selected among the set of the available relays. In the case of single relay selection, only one node is selected as a cooperative relay, which minimizes the overhead due to orthogonal channels and reduces the complexity of the selection process.

Also, single relay selection has higher bandwidth efficiency and lower energy consumption compared with all-participate relaying scheme. In contrast, multiple relay selection fully exploits the available degrees of spatial diversity, and better leverages the trade-off between error performance and spectral efficiency.

In what follows, a comprehensive summary on the existing cooperative communications techniques is provided followed by introducing security enhancement in cooperation communications.

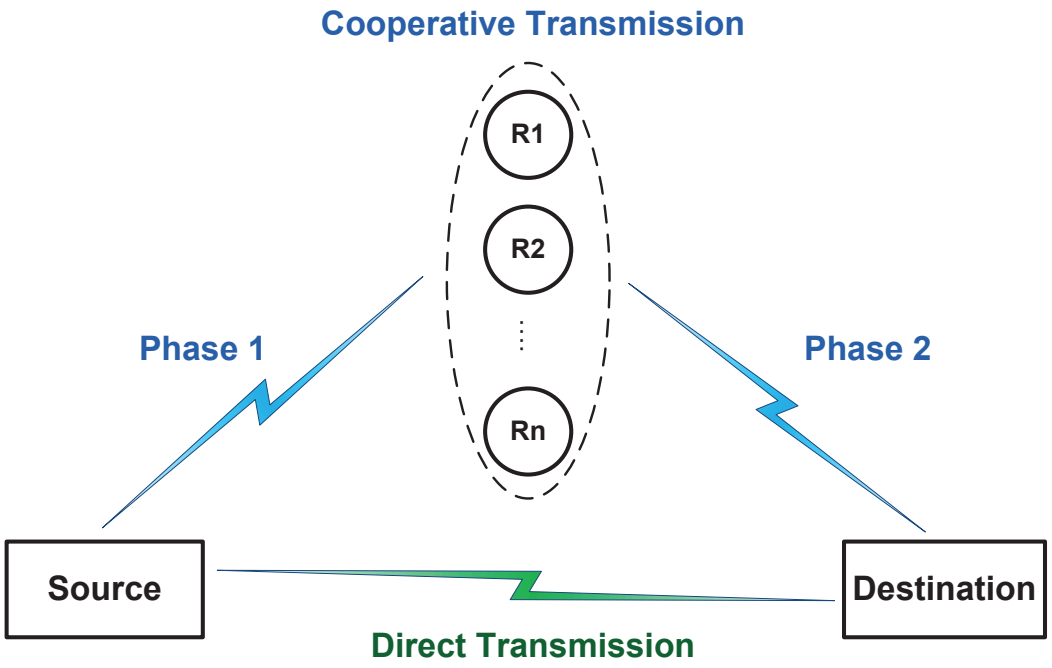

Figure 2.3: An illustration of direct transmission and cooperative transmission.

- Existing cooperative communications schemes:

  In wireless networks, cooperative mechanisms achieve space diversity with the help of relay nodes. The concept of relay channel was introduced by van der Meulen [60, 61] and studied later in [62], where a three-node relay channel, consisting of a source, relay and destination, was investigated for channel capacity analysis. To illustrate the scenario that relay nodes help a pair of terminals communicate, the model of relay channels was developed in [63]. Furthermore, wireless relay channels and their modeling, cooperative relay techniques and hardware implementations of cooperative diversity systems

were explained in [64] for different scenarios in an application perspective. Also, research work in [65] showed a survey of cooperative communication schemes and the applications of cooperative relaying schemes in LTE-advanced systems, which proved that cooperative relaying can dramatically improve the spectrum efficiency and overall system performance. Additionally, [66] introduced a distributed weighted cooperative routing algorithm where relay selection was achieved by exploiting the weights of the relays based on the residual energy and CSI of each end-to-end link. In [67], a survey of distributed relay selection schemes was presented for ad hoc cooperative wireless networks.

Alternatively, cross-layer design in cooperative wireless communications provides a significant solution for achieving energy efficiency and system reliability [68]. In [68], a new CoopMAC protocol was proposed by collaborating the physical layer with higher layers of the protocol stack to significantly improve the system robustness, throughput as well as delay, and reduce the interference with the coverage range extension. A unified cross layer technique in cooperative networks was proposed in [69] by considering the physical and network layers for resource allocation among multiple nodes to maximize the nodes utility. Additionally, a distributed cross layer technique was proposed in [70] by exploiting opportunistic relaying mechanisms to achieve QoS in the cooperative communications, where energy savings and low bit error rates can be achieved under cross-layer cooperation.

- Security enhancement in cooperative relaying:

  The feasibility of traditional physical layer security schemes is hampered by the severe channel impairment caused by multipath channel fading. Compared with the application of multiple antennas, the cooperative transmission approach is emerging as a more effective way to combat channel fading and enhance the security performance of wireless networks [71].

  In the context of secure cooperative relaying, three cooperative schemes were proposed in [72] by exploiting cooperating relays to enhance the security performance in the presence of multiple eavesdroppers. Moreover, [73] and [74] investigated the secrecy

through user cooperation for secure wireless communications. Also, a physical layer security system was designed in [75] by using collaborative relays to form a beamforming structure to achieve the goal of maximizing the secrecy rate. Furthermore, cooperative jamming(CJ) is another method by implementing cooperation to enhance physical layer security with secrecy constraints [76, 77], where each relay transmits weighted jamming signals with the purpose of degrading the eavesdropper's signal. By exploiting multi-antenna relays, two cooperative approaches were introduced in [78] for secure wireless transmissions, and a hybrid scheme was also proposed by exploiting cooperative relaying and cooperative jamming simultaneously at the relay for achieving secure transmission. Additionally, a cross-layer scheme for detecting malicious relay nodes in the cooperative communications was proposed in [79] by using adaptive signal detection at the physical layer and pseudorandom tracing symbols at the application layer simultaneously.

From the aforementioned discussions related to cooperative communications schemes and security enhancement, it can be concluded that the unique properties of the cooperative communications make it possible to develop new physical layer security strategies, which can address the drawbacks of the traditional security schemes.

2.4 Wireless OFDM System and its Security Vulnerabilities

Modern high-speed wireless communication techniques, such as the well-established and widespread WLAN transmissions of the family IEEE 802.11 [80, 81], the more recent WiMax [82] and LTE protocols [83, 84], are all standardized, developed and deployed based on the OFDM technique, due to its spectral efficiency, high achievable data rates and robust performance in multipath fading environments [85]. However, OFDM systems lack built-in security capabilities. Consequently, investigating the security weaknesses of OFDM is critical to design security mechanisms for secure existing wireless communications systems.

In what follows, a conventional OFDM system for wireless communications is introduced followed by a discussion of its security vulnerabilities.

2.4.1 OFDM Introduction and System Modeling

OFDM is a multiplexing method where data are transmitted over equally spaced and overlapped carrier frequencies, thereby providing a simple and efficient solution to deal with frequency selective channels [86]. OFDM, which was first introduced by S. B. Weinstein and P. M. Ebert in 1971 [87], allows for the multiplexing of various subchannels over the transmission medium to be obtained through the fast Fourier transform (FFT) algorithm. Mathematically, OFDM can be seen as a time-limited form of multicarrier modulation. $\{X(m)\}_{m=0}^{N-1}$ is denoted as complex symbols to be transmitted by OFDM modulation, thus, a time domain OFDM symbol consisting of N subcarriers can be expressed as

$$x(t) = \sum_{m=0}^{N-1} X(m) e^{j2\pi f_m t}, \quad 0 \le t \le T_s, \tag{2.2}$$

where f_m is the frequency of the mth subcarrier, and $f_m = m\Delta f$. T_s and Δf are denoted as the symbol duration and subcarrier space of OFDM, respectively. In order to demodulate OFDM signals at the receiver, orthogonality condition is satisfied, that is, $T_s \Delta f = 1$.

Substituting $f_m = \frac{m}{T_s}$ and $t = n\frac{T_s}{N}$ into (2.2), the transmitted OFDM symbol in the discrete-time domain can be written as

$$x(n) = \sum_{m=0}^{N-1} X(m) e^{j2\pi m \frac{n}{N}}, \quad n = 0, 1, \cdots, N-1. \tag{2.3}$$

Notice that $x(n)$ is expressed by applying inverse discrete Fourier transform (IDFT) to $X(m)$, in which IDFT can be efficiently implemented by using inverse fast Fourier transform (IFFT) for fast calculation. Figure 2.4 illustrates an OFDM symbol with five subcarriers shown in the frequency and time domain.

In order to avoid ISI and maintain subcarrier orthogonality, a CP is prefixed to time-domain OFDM symbol as a guard interval, which is a repetition of the end of the time-domain OFDM symbol. Figure 2.5 demonstrates that ISI can be eliminated between consecutive OFDM symbols when the length of multipath channel L is shorter than the guard interval.

Additionally, since CP repeats the end part of the OFDM symbol, the linear convolution of the OFDM symbol and a frequency-selective multipath channel is modeled as circular con-

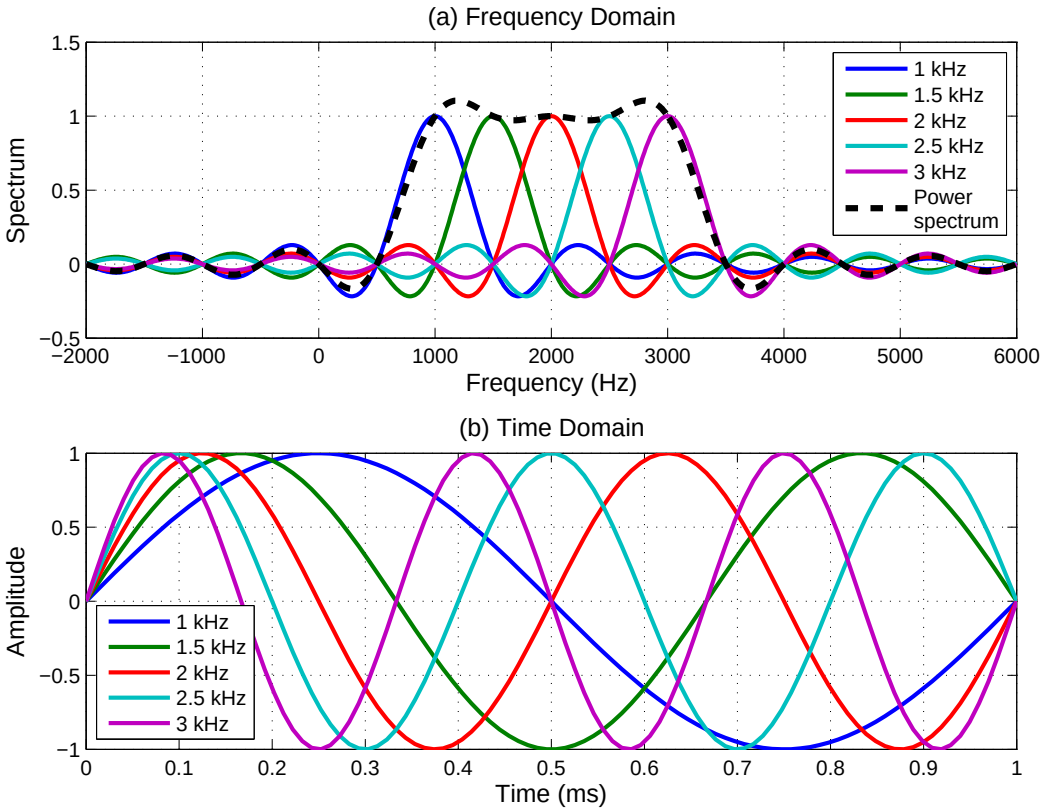

Figure 2.4: Example of an OFDM symbol.

volution. Specifically, the OFDM symbol after IFFT can be written according to the equation (2.3),

$$\mathbf{x} = [x(0), x(1), \ldots, x(N-1)]^T. \tag{2.4}$$

Prefixing the symbol with a CP of length N_{cp}, the OFDM symbol becomes

$$\begin{aligned} \tilde{\mathbf{x}} &= [\tilde{x}(-N_{cp}), \ldots, \tilde{x}(-2), \tilde{x}(-1), \tilde{x}(0), \tilde{x}(1), \ldots, \tilde{x}(N-1)]^T \\ &= [x(N-N_{cp}), \ldots, x(N-2), x(N-1), x(0), x(1), \ldots, x(N-1)]^T. \end{aligned} \tag{2.5}$$

Assume that the frequency-selective multipath channel is expressed by

$$\mathbf{h} = [h(0), h(1), \ldots, h(L-1)]^T. \tag{2.6}$$

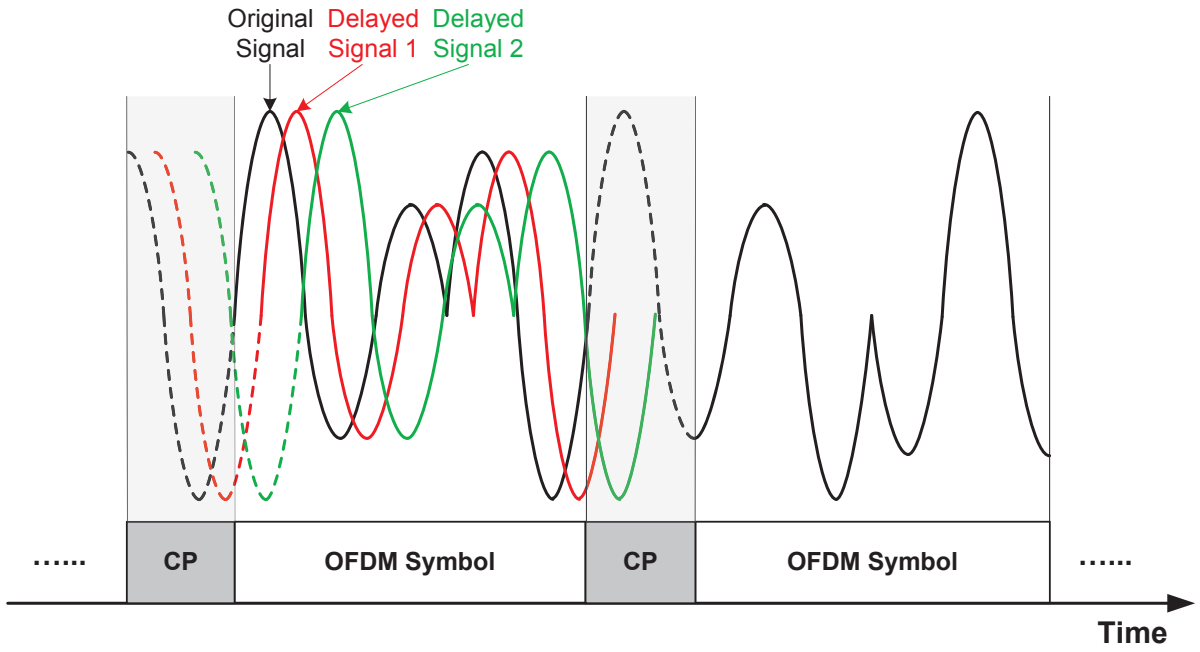

Figure 2.5: ISI cancelation.

Consequently, the received signal samples in the time domain $y(n)$ can be expressed as

$$\begin{aligned} y(n) &= \mathbf{h} * \tilde{\mathbf{x}} + w(n) \\ &= \sum_{l=0}^{L-1} h(l)\tilde{x}(n-l) + w(n), \quad -N_{cp} + 2L - 1 \leq n \leq N - 1, \end{aligned} \tag{2.7}$$

where $*$ denotes linear convolution, and $w(n)$ is zero-mean complex circular Gaussian noise with variance σ_w^2, i.e., $w(n) \sim \mathcal{N}_c(0, \sigma_w^2)$. Since $\tilde{x}(n-l)$ is equal to $x(n-l \ mod \ N)$, the convolution of the OFDM symbol and the channel becomes circular convolution. Therefore, using CP can significantly simplify the receiver design for channel estimation and equalization. Figure 2.6 shows the block diagram of an OFDM system.

From the aforementioned discussion of OFDM system, the advantages of OFDM can be summarized as follows:

- High data rate can be achieved with high bandwidth efficiency and flexible underlying modulations.
- ISI can be eliminated with the help of CP.

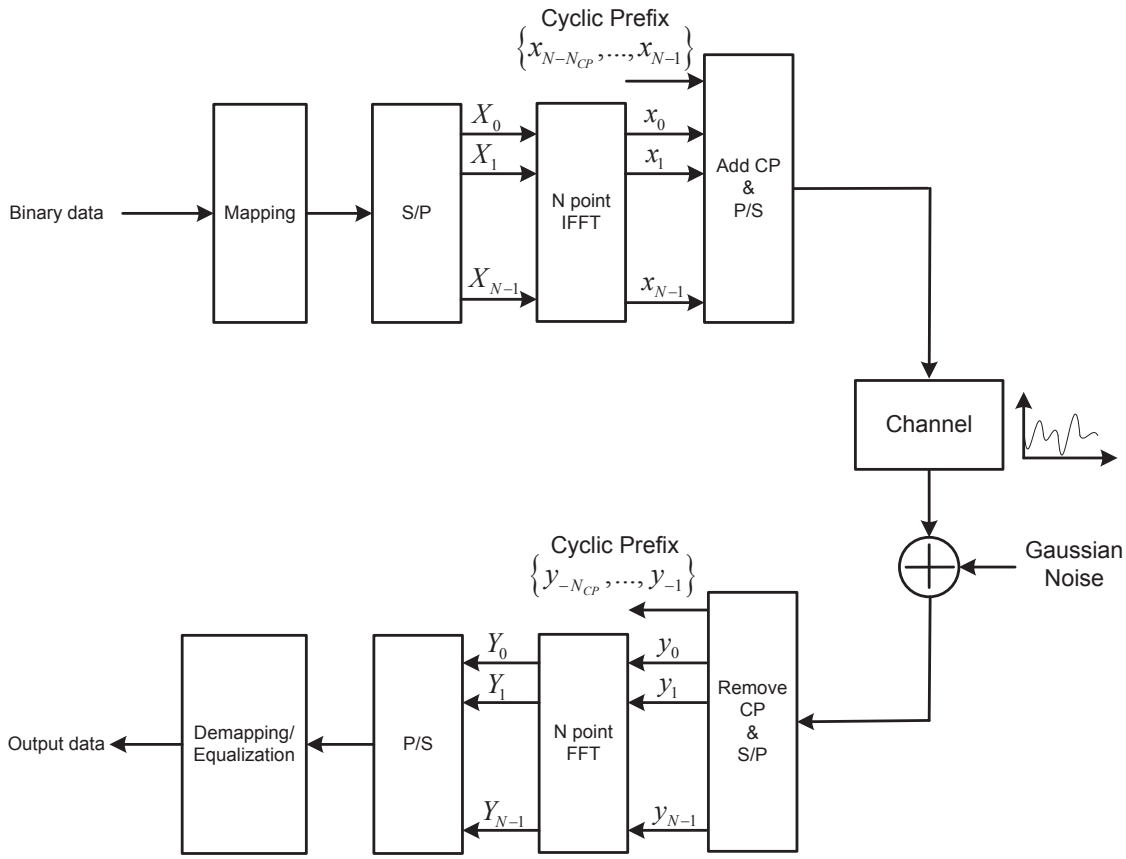

Figure 2.6: The block diagram of an OFDM system.

- Channel equalization and estimation become quite simpler because information is carried over parallel orthogonal subchannels.

2.4.2 Security Weaknesses of OFDM

OFDM has been employed in various communications systems due to its spectral efficiency, high achievable data rates and robust performance in multipath fading environments. Despite these advantageous features, OFDM signals are transparent to potential eavesdroppers, as OFDM-based communication systems lack built-in security capabilities. Typically, since OFDM employs pilot tones or preamble symbols for channel estimation, equalization and synchronization at the receiver, the implementations of OFDM are highly susceptible to signal jamming attacks [88–90]. Additionally, due to the distinct time and frequency charac-

teristics of OFDM signals, physical layer transmission parameters of OFDM signals can be blindly estimated by any user within the same network, and no prior information of the signals is required for them [91, 92]. Hence, additional encryption algorithms should be implemented in OFDM systems for data security.

In order to achieve data security in OFDM, traditionally, information encryption approaches relying on the high layers of communication stack (such as application and network layers) are used to encrypt the information with a secret key. The key is initially exchanged between the legitimate users, and the legitimate receiver uses the knowledge of the key to decrypt the message, while the eavesdropper cannot decrypt the data without the key. However, due to the improvement of terminal processing capacity, the transmitted information can be possibly decrypted by adversaries using exhaustive trials, and key distribution and management become more difficult to achieve in high-layer encryption mechanisms.

Alternatively, a few physical layer encryption techniques for OFDM systems were proposed in [93–95] based on encrypting the frequency domain symbols. Specifically, [93] proposed a physical layer security scheme by scrambling OFDM constellation symbols to encrypt the data transmission in the presence of various denial of service (DoS) attacks. The scrambling matrix is based on a key derived from a one-dimensional chaotic map. Moreover, in [94], a symmetric key physical layer encryption was developed by using non-orthogonal FDM signals to mask the OFDM signals. Additionally, a noise-enhanced encryption approach was proposed in [95] by using traditional cryptographic ciphers and adding truly random noise at the transmitter to reduce eavesdroppers' knowledge of the transmitted information.

Despite the respective contributions to secure the transmission of OFDM signals, the main limitations of these physical layer encryption systems can be summarized as follows:

- Transmission power is sacrificed to maintain the bandwidth efficiency of OFDM, which is not suitable for power constrained devices.
- The requirements for modulating symbols in OFDM are restrictive and their violation can potentially lead to information leakage to adversaries.
- The large length of key sequences for encrypting signals can potentially create problems by decreasing the speed of data transmission.

2.5 Summary

In this chapter, security challenges in wireless communications have been discussed by comparing with the wired networks. To address wireless security issues, traditional wireless security techniques relying on the higher layers of the OSI model have been studied. Due to the security weaknesses of the traditional security techniques, physical layer security is emerging as a promising paradigm by exploiting physical layer properties to complement the traditional wireless security mechanisms. A comprehensive literature survey of existing physical layer security techniques has been illustrated and these physical layer security approaches have been divided into three categories based on wireless channel, RF-DNA and diversity technique. Additionally, OFDM technology has been widely employed in modern wireless communication techniques; however, OFDM is vulnerable to adversaries due to its distinct time and frequency characteristics at the physical layer. Therefore, secure OFDM-based wireless systems is critical for secure wireless communications.

Chapter 3

Noise-Mitigated CIR-Based Physical Layer Authentication

In this Chapter, a robust physical layer authentication scheme for wireless communications is proposed by exploiting the inherent properties of CIR in a time-varying multipath environment. The variation between two consecutive CIR measurements from a transmitter of interest is utilized by the receiver in order to distinguish between different transmitters for authentication purpose.

Under a binary hypothesis testing, we develop a new test statistic based on the difference between noise-mitigated CIR estimates in order to minimize the impact of noise and interference from the wireless environment. To achieve this goal, a SNR-dependent threshold is utilized to eliminate the excessive noise in the estimated CIRs prior to conducting the authentication process. For performance analysis, FAR and PD are theoretically defined based on the developed test statistic, and an adaptive threshold for the authentication test is achieved under a constant FAR. Additionally, the proposed authentication scheme is analyzed based on an OFDM system and validated by Monte-Carlo method.

3.1 Introduction

Wireless communications face increasing challenges in combating various additional security threats comparing with traditional wireline networks, primarily due to the broadcast

and open nature of the wireless communication environment. Existing wireless security techniques are mainly focused on processing techniques in the data or protocol domains to prevent potential security threats. Due to the vulnerability of existing higher-layer wireless security mechanisms to spoofing attacks [19], new wireless security techniques exploiting the physical link properties provide additional protection for the communication process.

As a major aspect of wireless security, authentication is a process to verify the identities of terminals, and has been explored at the physical layer in recent years. Physical layer authentication methods are generally developed by formulating authentication as a hypothesis testing problem [6,8–10,34,35,96,97]. Xiao *et al.* [6,8,34,97] and He *et al.* [9,35] separately proposed authentication approaches under a binary hypothesis testing by exploring channel differences between two consecutive CFRs. Nevertheless, CFR analysis fails to exploit spatial information related to the signal propagation environment in the received signals for security enhancement purpose. Following Xiao's works, time-domain training-based CIR was used in [10] to achieve an authentication system. However, a simple time-invariant wireless environment was considered [10].

In this Chapter, we propose a physical layer authentication scheme using a channel-based hypothesis testing method to detect anomalous behaviors through the statistical analysis of the inherent properties of CIR difference in a time-varying multipath environment. Specifically, a new test statistic is developed by exploiting the noise-mitigated CIR difference and tracking the significant channel taps, where we utilize a SNR-dependent time-domain threshold to eliminate the excessive noise. To achieve effective authentication, an adaptive threshold is derived at the receiver based on the statistical properties of CIR variation and used for distinguishing the legitimate transmitter from intruders.

The rest of this Chapter is organized as follows: In Section 3.2, the system model and channel model are provided, and then the proposed CIR-based authentication scheme is presented in Section 3.3. In order to verify the proposed authentication scheme and the corresponding theoretical analysis, we illustrate numerical results in Section 3.4, and this Chapter is summarized in Section 3.5.

3.2 System Modeling

Our proposed scheme is presented under the ubiquitous "Alice-Bob-Eve" scenario shown in Figure 3.1. Here, Alice, Bob and Eve are located in spatially different positions. Alice, as the legitimate transmitter, delivers data to the intended receiver Bob, while Eve serves as an adversary attempting to impersonate the transmission from Alice. Our objective is to develop the capability for Bob to verify whether signals are from Alice or not. Since CIR reflects all the properties of a wireless channel, it indicates the spatial geometry of the wireless environment between the transmitter and the receiver. Consequently, the variation of CIR at Bob can be exploited to authenticate the identity of the transmitter (Alice or Eve). Specifically, the current CIR is compared with historical channel statistics between Alice and Bob under a binary hypothesis testing. The proposed authentication scheme and the related theoretical analysis are verified based on an OFDM system.

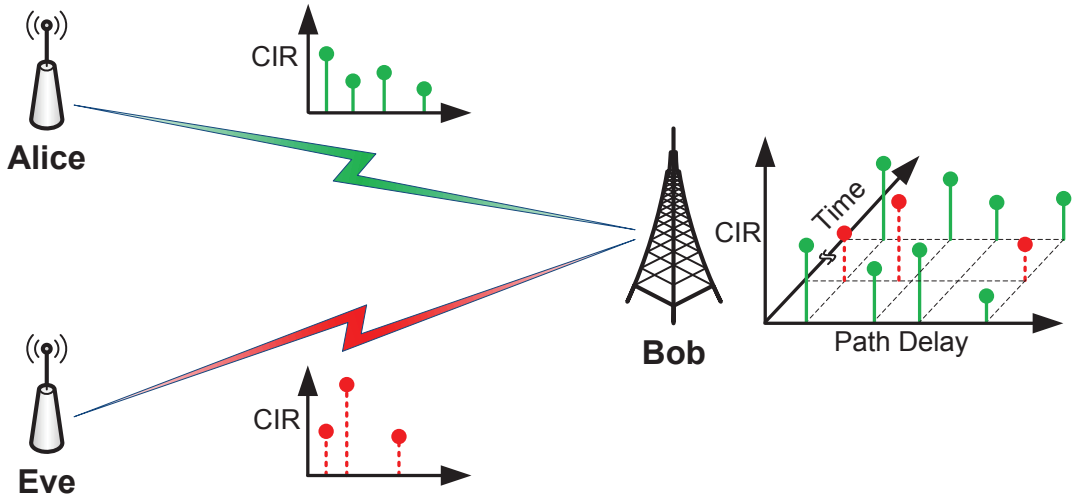

Figure 3.1: CIR-based Authentication in the "Alice-Bob-Eve" Scenario.

3.2.1 Channel Model

The wireless channel model for multipath fading environment can be expressed as

$$h(n) = \sum_{l=0}^{L-1} a_l(n)\delta(n-l), \tag{3.1}$$

where $a_l(n)$ is the channel gain of the lth multipath component at discrete time n, l represents the index of different path delay normalized to the sampling time interval, and L is the length of CIR. In a Rayleigh fading channel, at any sampling time, $a_l(n)$ can be modeled as a complex Gaussian random variable with zero mean and variance σ_l^2 , i.e., $a_l(n) \sim \mathcal{N}_c(0, \sigma_l^2)$, the paths are assumed to be statistically independent, and the average power is normalized, i.e., $\sum_{l=0}^{L-1} \sigma_l^2 = 1$.

To improve the authentication performance of the proposed technique, two types of normalization with CIR are considered [98] – time delay normalization and amplitude normalization. Time delay normalization means the time delay of the line-of-sight (LOS) multipath component is set to be zero to avoid a large timing offset between two CIRs on the same path. In addition, since there is the possibility of dramatic variation in received signal power from potential spoofers, amplitude normalization is needed to mitigate this kind of attack and achieve a robust system performance. Therefore, the measurement of normalized CIR can be obtained as $\tilde{h} = h/\| h \|$, where $\| \cdot \|$ means the Euclidean norm. In the following sections, we use h as the normalized ideal CIR for simplification.

3.2.2 Hypothesis Testing

In this subsection, we propose a physical layer authentication approach by using the properties of the CIR difference. In this new authentication scheme, the current CIR estimated by Bob in Figure 3.1 is compared with the previous CIR estimate for transmitter identification (Alice or Eve). Mathematically, a binary hypothesis testing problem can be formulated as

$$\begin{aligned} H_0 &: \hat{\mathbf{h}}_t = \hat{\mathbf{h}}_{AB} \\ H_1 &: \hat{\mathbf{h}}_t \neq \hat{\mathbf{h}}_{AB}, \end{aligned} \tag{3.2}$$

where $\hat{\mathbf{h}}_{AB}$ is the noisy version of CIR from Alice to Bob, and $\hat{\mathbf{h}}_t$ is the estimated CIR from an unknown terminal (Alice or Eve). Additionally, H_0, the null hypothesis, stands for Alice as the claimant, while the alternative hypothesis, H_1, means the terminal is someone else.

Due to the statistical independence between any two paths, the properties of a single path are analyzed here without loss of generality. Therefore, in (3.2), the noisy version of CIR on

the lth multipath component can be written as

$$\hat{h}_{t,l}(k) = h_{t,l}(k) + n_t(k) \quad , 0 \leq l \leq L-1, \tag{3.3}$$

where $\hat{h}_{t,l} = \left\{\hat{h}_{AB,l}, \hat{h}_{EB,l}\right\}$. The first term $h_{t,l}$ stands for the ideal CIR, and n_t is zero-mean white complex Gaussian noise with variance σ_N^2.

Additionally, due to the correlation of adjacent CIRs on the same path (i.e., $h_{AB,l}(k-1)$ and $h_{AB,l}(k)$), an autoregressive model of order 1 (AR-1) [8] is utilized to describe the temporal process of $h_{AB,l}(k)$,

$$h_{AB,l}(k) = \zeta h_{AB,l}(k-1) + \sqrt{(1-\zeta^2)\sigma_{A,l}^2}u_l(k-1), \quad 0 \leq l \leq L-1, \tag{3.4}$$

where the AR coefficient ζ represents the correlation of two successive CIRs which can be considered as a constant, and u_l is a zero-mean complex Gaussian random variable with variance one, which is independent of $h_{AB,l}$.

Consequently, according to the AR-1 model in (3.4), we can determine the distribution of $\mathbf{h}_{AB,l}$ as

$$\mathbf{h}_{AB,l} \sim \mathcal{N}_c\left(\underline{0}, \mathbf{\Sigma}_{M\times M}\right), \tag{3.5}$$

where

$$\mathbf{\Sigma} = \begin{bmatrix} R_{0,0} & R_{0,1} & \cdots & R_{0,(M-1)} \\ R_{1,0} & R_{1,1} & \cdots & R_{1,(M-1)} \\ \cdots & \cdots & \cdots & \cdots \\ R_{(M-1),0} & R_{(M-1),1} & \cdots & R_{(M-1),(M-1)} \end{bmatrix}, \tag{3.6}$$

and $R_{k_1,k_2} = \zeta^{|k_1-k_2|}\sigma_{A,l}^2$. M is the number of OFDM symbols in an observation window.

3.3 CIR-based Authentication

3.3.1 Noise Impact on CIR Difference Evaluation

In the following analysis, a sparse channel with a few significant multipath components on integer delays is considered. In addition, comb-type pilots are employed for CIR estimation in

an OFDM system. Let N_p be the number of pilots, which is larger than the length of ideal CIR (i.e., L) to avoid any loss of channel information. Without the knowledge of the actual CIR at the receiver, the CIR estimate based on the comb-type pilots can be expressed as

$$\hat{h}_{t,l}(k) = \begin{cases} h_{t,l}(k) + n_t(k), & if\ 0 \le l \le N_p - 1 \\ 0, & if\ N_p \le l \le N. \end{cases} \tag{3.7}$$

From the equation above, we can see that both strong and weak multipaths are corrupted by noise. Noise components are introduced at the receiver side to the original zero-valued channel taps, which will affect the determination of the true channel variation related to the significant channel taps. Thus, it is necessary to study the impact of the noise n_t in (3.7) for CIR difference evaluation due to the channel sparsity. To address this issue, first of all, the CIR difference between two consecutive estimated CIRs, which are both from the legitimate transmitter Alice, can be expressed as

$$\begin{aligned} \Delta\hat{h}_{AB} &= \sum_{l=0}^{N_p-1} \left| h_{AB,l}(k) - h_{AB,l}(k-1) + n_A(k) - n_A(k-1) \right| \\ &= \sum_{l=0}^{N_p-1} \left| \Delta h_{AB,l} + \Delta n_A \right|. \end{aligned} \tag{3.8}$$

Let us denote Q as the set of time indices for significant channel tap coefficients. The above CIR difference can be rewritten as

$$\Delta\hat{h}_{AB} = \sum_{l\in Q} \left| \Delta h_{AB,l} + \Delta n_A \right| + \sum_{l\notin Q} |\Delta n_A|. \tag{3.9}$$

The second term in (3.9) is induced totally by noise which should be eliminated. To avoid the impact of the noise on evaluating the CIR difference, we need a noise dependent threshold to mitigate the noise impact. In particular, we compare the absolute value of each tap with the threshold d_{ce}. All the insignificant taps with absolute value below the threshold are set to zeros. The general expression of the threshold-based CIR estimates corresponding to (3.7) can

be represented as

$$\hat{h}_{t,l}(k) = \begin{cases} \hat{h}_{t,l}(k), & if \ \left|\hat{h}_{t,l}(k)\right| > d_{ce} \\ 0, & if \ \left|\hat{h}_{t,l}(k)\right| \leq d_{ce}, \end{cases} \tag{3.10}$$

and the second term of the CIR difference in (3.9) is eliminated after the threshold in (3.10) is applied.

In order to determine the threshold d_{ce}, the mean square error (MSE) of estimation errors is minimized. In [99], the authors proposed a criterion for obtaining a sub-optimal threshold value without the knowledge of the channel statistics. Thus, the threshold d_{ce} can be expressed by

$$d_{ce} \approx \sqrt{\sigma_N^2 \ln\left(N_p / P_{ofa}\right)}, \tag{3.11}$$

where P_{ofa} is the overall FAR, which is assumed to be a constant parameter according to a specific security level. The numerical results in [99] also confirmed that using the sub-optimal threshold value for channel estimation can achieve same system performance as using the optimal threshold. Moreover, noise variance is needed to calculate the threshold value in (3.11). A proposed approach in [100] is utilized here for noise variance estimation, in which the redundancy introduced by the CP was exploited. Thus, the estimated noise variance can be written as

$$\sigma_N^2 = \frac{1}{2M(N_{cp}-u)} \sum_{v=0}^{M-1} \sum_{m=u}^{N_{cp}-1} \left| y(v(N+N_{cp})+m) - y(v(N+N_{cp})+N+m) \right|^2, \tag{3.12}$$

$$L \leq u \leq N_{cp} - 1,$$

where M is the number of observed OFDM symbols. Since the actual length of CIR (i.e., L) is unknown at the receiver side and it was assumed that $L \leq N_p$, L is replaced here by N_p for noise variance estimation.

3.3.2 Adaptive Threshold for Authentication

In this Chapter, the proposed CIR-based authentication method is based on the noise-mitigated CIR estimates given in (3.10). Under the binary hypothesis testing, a new test statistic

is developed based on the difference between adjacent noise-mitigated CIR estimates. That is,

$$\begin{aligned}\mathrm{T} &= \frac{1}{\rho^2}\sum_{l=0}^{N_p-1}|T_l|^2 \\ &= \frac{1}{\rho^2}\sum_{l\in Q_1\cup Q_2}\left|\hat{h}_{t,l}(k)-\hat{h}_{AB,l}(k-1)\right|^2 \\ &= \frac{1}{\rho^2}\sum_{l\in Q_1\cup Q_2}\left|h_{t,l}(k)+n_t(k)-h_{AB,l}(k-1)-n_A(k-1)\right|^2, \end{aligned} \tag{3.13}$$

where ρ^2 is the variance of the estimated CIR difference for normalization. Q_1 and Q_2 denote two sets of indices as the set Q, which are corresponding to the CIR estimates $\hat{h}_{t,l}(k)$ and $\hat{h}_{AB,l}(k-1)$ respectively.

Based on the distributions of both $\mathbf{h}_{AB,l}$ and n_t, we can derive the distributions of random variable T_l under the two hypotheses H_0 and H_1. That is,

$$\begin{aligned} H_0 &: \ T_l \sim \mathcal{N}_c(\underline{0}, \sigma^2_{H_0,l}\mathbf{I}) \\ H_1 &: \ T_l \sim \mathcal{N}_c(\mu_l\mathbf{I}, \sigma^2_{H_1,l}\mathbf{I}), \end{aligned} \tag{3.14}$$

where $\mathbf{I}$ is the identity matrix, $\mu_l = \mathrm{E}[h_{EB,l}] - \mathrm{E}[h_{AB,l}]$, $\sigma^2_{H_0,l} = 2(1-\zeta)\sigma^2_{A,l} + 2\sigma^2_N$ and $\sigma^2_{H_1,l} = \sigma^2_{E,l} + \sigma^2_{A,l} + 2\sigma^2_N$. The subscripts "$A$" and "$E$" represent the transmitters Alice and Eve respectively.

Since only significant multipath components are maintained after applying the noise-mitigated threshold on CIR estimates, the test statistic T can be further separated into three parts under the two hypotheses, respectively. Specifically, under H_0, the test statistic T is expressed by

$$\begin{aligned}\mathrm{T} &= \sum_{l\in Q_1-C}\frac{2}{\sigma^2_{A,l}+\sigma^2_N}\left|\hat{h}_{AB,l}(k)\right|^2 \\ &\quad + \sum_{l\in Q_2-C}\frac{2}{\sigma^2_{A,l}+\sigma^2_N}\left|\hat{h}_{AB,l}(k-1)\right|^2 \\ &\quad + \sum_{l\in C}\frac{2}{\sigma^2_{H_0,l}}\left|\hat{h}_{AB,l}(k)-\hat{h}_{AB,l}(k-1)\right|^2 \\ &= \mathrm{T}_{1,H_0}+\mathrm{T}_{2,H_0}+\mathrm{T}_{3,H_0}, \end{aligned} \tag{3.15}$$

where C is equal to $Q_1 \cap Q_2$. Similarly, under H_1, the test statistic T is rewritten as

$$\begin{aligned} \mathrm{T} &= \sum_{l\in Q_1-C} \frac{2}{\sigma_{E,l}^2+\sigma_N^2}\left|\hat{h}_{EB,l}(k)\right|^2 \\ &\quad + \sum_{l\in Q_2-C} \frac{2}{\sigma_{A,l}^2+\sigma_N^2}\left|\hat{h}_{AB,l}(k-1)\right|^2 \\ &\quad + \sum_{l\in C} \frac{2}{\sigma_{H_1,l}^2}\left|\hat{h}_{EB,l}(k)-\hat{h}_{AB,l}(k-1)\right|^2 \\ &= \mathrm{T}_{1,H_1}+\mathrm{T}_{2,H_1}+\mathrm{T}_{3,H_1}. \end{aligned} \tag{3.16}$$

With a closer look at the two equations above, one can find that the estimated CIR difference under two hypotheses is dominated by the first and the second terms combined, which means unexpected significant paths lead to a large CIR difference. Therefore, an adaptive threshold d_{au} is necessary for the receiver to make reliable authentication decisions.

Additionally, the distributions of the six separated parts of T given in (3.15) and (3.16) can be obtained, which follow the chi-square distribution with different degrees of freedom. That is,

$$\begin{cases} \mathrm{T}_{1,H_0} \sim \chi^2_{0,2(Q_1-C)} \\ \mathrm{T}_{1,H_1} \sim \chi^2_{0,2(Q_1-C)}, \end{cases} \tag{3.17}$$

$$\begin{cases} \mathrm{T}_{2,H_0} \sim \chi^2_{0,2(Q_2-C)} \\ \mathrm{T}_{2,H_1} \sim \chi^2_{0,2(Q_2-C)}, \end{cases} \tag{3.18}$$

and

$$\begin{cases} \mathrm{T}_{3,H_0} \sim \chi^2_{0,2C} \\ \mathrm{T}_{3,H_1} \sim \chi^2_{\lambda,2C}. \end{cases} \tag{3.19}$$

Due to the property of chi-square distribution [101] (i.e., if $X \sim \chi^2_{v1}$ and $Y \sim \chi^2_{v2}$, we have $X+Y \sim \chi^2_{v1+v2}$), the test statistic T under the two hypotheses still follow chi-square distribution, which can be expressed as

$$\begin{aligned} H_0 &: \mathrm{T} \sim \chi^2_{0,2(Q_1+Q_2-C)} \\ H_1 &: \mathrm{T} \sim \chi^2_{\lambda,2(Q_1+Q_2-C)}, \end{aligned} \tag{3.20}$$

where $\lambda = \sum_{l=0}^{C-1} \frac{2\mu_l^2}{\sigma_{E,l}^2+\sigma_{A,l}^2+2\sigma_N^2}$.

Based on the developed test statistic in (3.13), theoretical FAR P_{fa} and PD P_d can be derived

by

$$\mathrm{P}_{fa} = P(\mathrm{T} > d_{au}|H_0) = 1 - \mathrm{F}_{\chi^2_{0,2(Q_1+Q_2-C)}}(d_{au}), \tag{3.21}$$

and

$$\mathrm{P}_{d} = P(\mathrm{T} > d_{au}|H_1) = 1 - \mathrm{F}_{\chi^2_{\lambda,2(Q_1+Q_2-C)}}(d_{au}), \tag{3.22}$$

where $\mathrm{F}_{\chi^2_N}(\cdot)$ denotes the cumulative distribution function (CDF) of the chi-square distribution with the order N. For military communications, P_{fa} is normally set below 0.1. Thus, after calculating the value of $Q_1 + Q_2 - C$, the threshold d_{au} can be obtained under a given value of P_{fa}. i.e.,

$$d_{au} = \mathrm{F}^{-1}_{\chi^2_{0,2(Q_1+Q_2-C)}}(1 - \mathrm{P}_{fa}), \tag{3.23}$$

where $\mathrm{F}^{-1}(\cdot)$ is the inverse function of $\mathrm{F}(\cdot)$.

3.4 Simulation Results

3.4.1 Simulation Scenarios

In this section, simulation results are presented to confirm the effectiveness of the proposed approach. For all simulation cases, an OFDM system is employed with QPSK modulation. Comb-type pilots are inserted into each OFDM symbol for CIR estimation. Regarding the channel model, a random Rayleigh fading channel is utilized with sparse sample-spaced significant taps, uniform power delay profile, where paths on different tap positions are statistically independent with normalized average power. The particular parameters related to our simulations are list in Table 3.1.

3.4.2 Numerical Results and Discussion

In this subsection, we mainly present the simulation results to verify the theoretical analysis related to the performance of our proposed authentication system.

Table 3.1: Simulation Parameters

Subcarrier Number	1024
CP Length	256
Pilot Number	64
Significant Path Number (Alice-Bob)	6
Significant Path Number (Eve-Bob)	10

In Figure 3.2, it is shown both the theoretical and the simulated lower bound of the adaptive threshold for spoofing attack detection. Three pairs of curves of the adaptive threshold are plotted under three different FARs, which meet the requirement of low FAR for military communications. It is clear that the simulation results and the theory are approximately overlapping, especially at high SNR. The results indicate that smaller probability of rejecting signals from Alice (i.e. smaller value of FAR) needs larger threshold values, and the values of the threshold also decline while SNR rises.

Figure 3.3 shows the PD vs SNRs under three different false alarm rates. With different FAR requirements, it is observed that theoretical analysis and simulation can simultaneously achieve great performance in terms of PD. When the value of SNR reaches to 8 dB, a very high PD of 0.9 is achieved. Although low FAR affects the performance of PD, the impact is limited and the overall performance of spoofing detection remains robust.

In Figure 3.4, a Receiver Operating Characteristic (ROC) is sketched for simulated and theoretical cases at SNR of 0 dB, 5 dB and 10 dB, respectively. It is found that the theoretical analysis and simulation are approximately matching even at low FAR region for various SNR values. The performance of spoofing detection remains great even at low SNR of 5 dB.

3.5 Summary

In this Chapter, we have proposed a physical layer authentication scheme under a new hypothesis testing based on the statistical analysis of estimated CIR differences in time-varying multipath fading channels. The impacts of background noise and interference from wireless environments have been mitigated by removing the excessive noise in sparse CIRs with a SNR-dependent threshold. The FAR and PD have been theoretically derived to evaluate the performance of the proposed authentication scheme. Under a given FAR, an adaptive threshold for

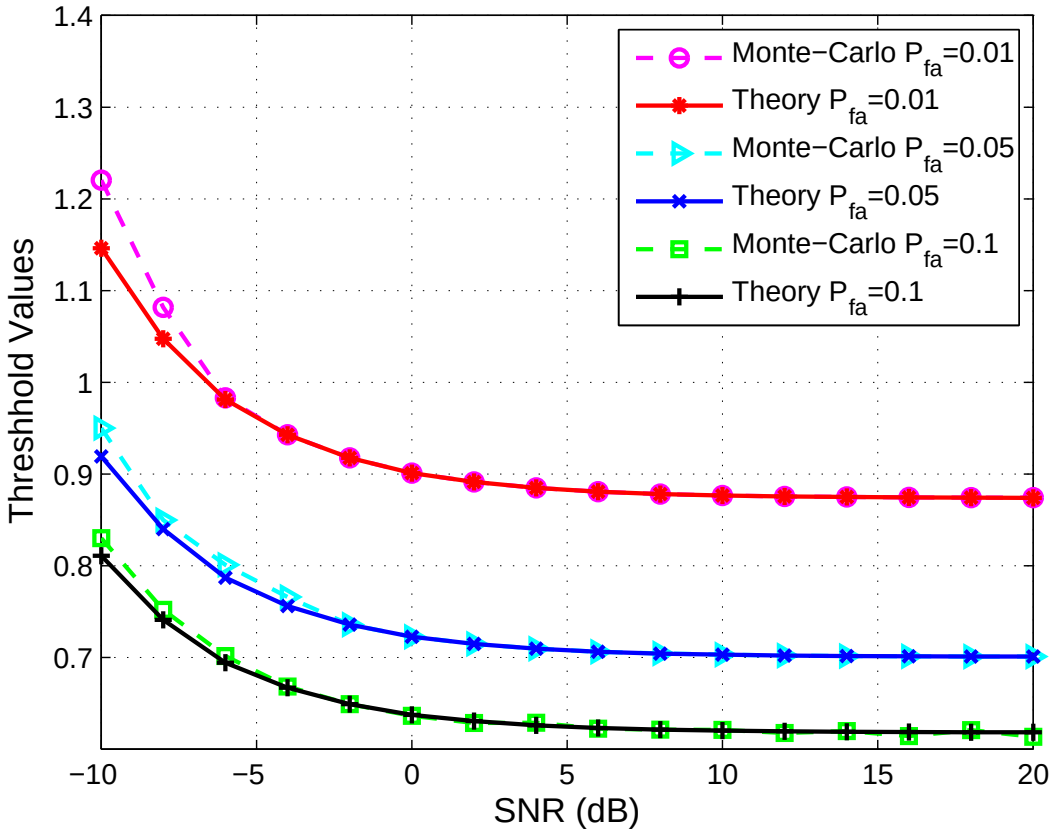

Figure 3.2: Adaptive threshold values for authentication versus SNRs under different false alarm rates.

the authentication test was achieved in different channel conditions. An OFDM system has been utilized to validate the performance of our proposed scheme. The effectiveness of the proposed CIR-based authentication scheme has been verified by using the theoretical analysis and Monte-Carlo method.

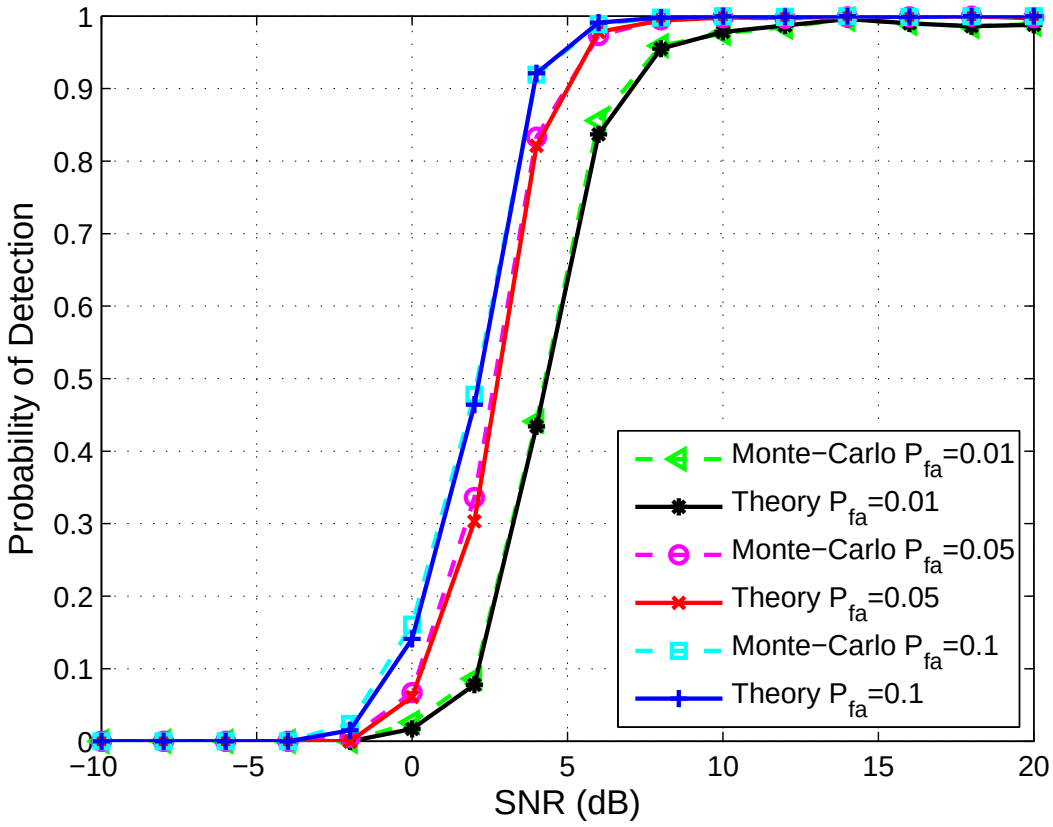

Figure 3.3: Probability of detection versus SNRs at different false alarm rates.

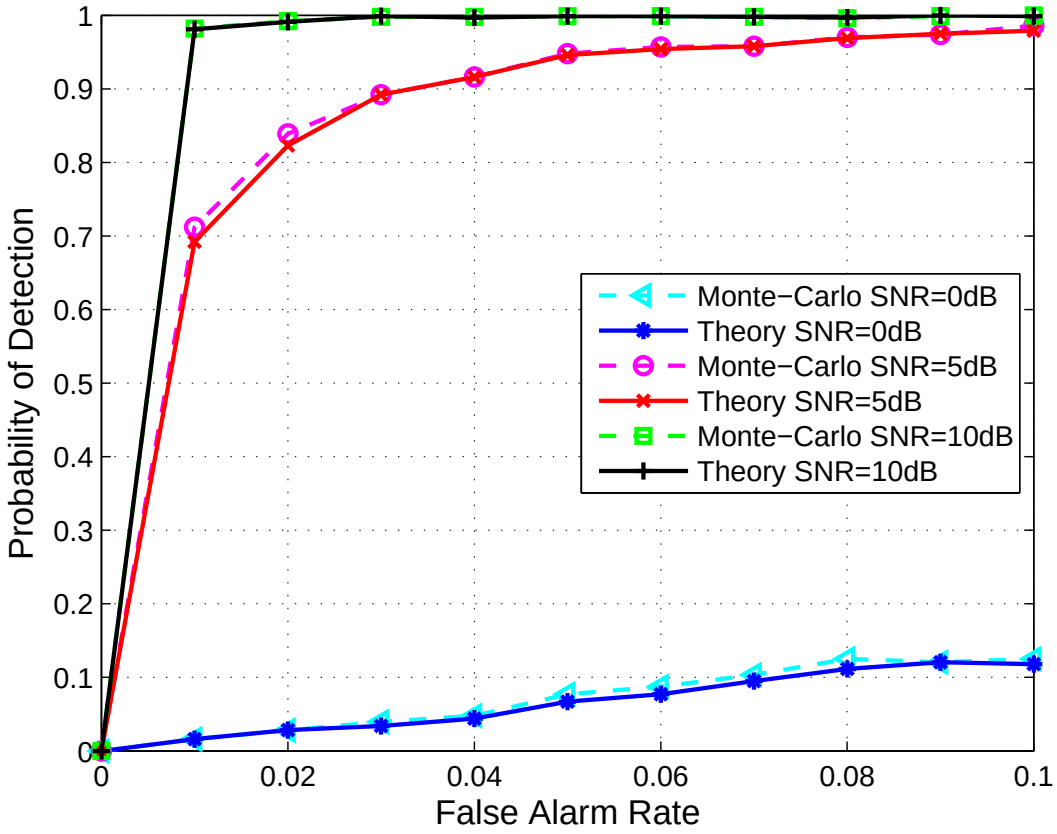

Figure 3.4: Receiver operating characteristic for the CIR-based authentication under three different SNRs.

Chapter 4

CIR-Based Authentication Enhancement Using Channel Predictor

The inherent properties of CIR, which are considered as location-specific characteristics of the physical link, have been exploited to develop a robust physical layer authentication scheme in Chapter 3. However, the reliability of CIR-based physical layer authentication is challenged by the rapid channel variation in fast fading environments. In this Chapter, we exploit a long-rang channel predictor to predict future CIRs in order to compensate for the negative effects of fast channel variation. Specifically, the predicted CIR is achieved based on the historical CIR estimates, and then it is utilized as the previous CIR measurement in the authentication process. Under a binary hypothesis testing, a test statistic is developed based on the difference between current CIR and the predicted CIR. In order to increase the robustness of authentication performance, a final decision is formed based on multiple CIR differences that are calculated by the receiver based on the long-range channel predictor. Based on the developed test statistic, theoretical FAR and PD are derived to validate the performance of the proposed authentication scheme. An optimization problem is defined based on minimizing the total error rate under false alarm constraints in order to find optimal value of the threshold for decision-making. Finally, the performance of the proposed scheme is compared with that of a traditional channel-based authentication method in simulations.

4.1 Introduction

In wireless communications, there are many emerging challenges in combating various additional security threats compared with traditional wired networks, due to the broadcast nature of the wireless medium. Typically, most existing security mechanisms are based on cryptographical techniques at the higher layers of protocol stack to prevent any potential security threats. Due to the vulnerability of existing higher-layer wireless security techniques against spoofing attacks [109], new wireless security techniques utilizing the physical link characteristics are proposed to provide an additional protection for secure data transmissions.

According to the information-theoretic security introduced by Shannon, the fundamental ability of the physical layer has been theoretically verified that it can provide secure communications in perfect secrecy. In addition, a reliable transmission in approximately perfect secrecy has been proven in [110] by introducing the concept of the wiretap channel with noise. Furthermore, the existence of channel codes can be explored to guarantee a secure communication on a broadcast channel [111]. Without clear definition of perfect authenticity in the theory of secrecy, information-theoretically secure message authentication has been initially proposed by Simmons, and a model of message authentication has been developed under a noiseless channel [112]. In [96], a generalized and simplified authentication technique has been proposed based on a binary hypothesis testing. Also, a message authentication scheme has been designed in [113] with the consideration of channel and authentication coding in a noisy environment.

More recently, the physical layer authentication is further investigated in [9, 10, 97] by exploiting the CSI. In particular, Xiao *et al.* in [97] has explored the properties of channel differences between two consecutive CFRs in a time-variant channel. Based on this work, a physical layer authentication scheme has been proposed in [9] by considering both the amplitude and phase information of CFR. Alternatively, time-domain training-based CIR has been exploited for authentication analysis in [10] under a simple time-invariant wireless channel. In realistic wireless propagation environment, the characteristics of CIR are varying over time due to the movement of terminals or the surrounded scatterers under the mobile environment, however, they are slowly time-variant. Considering a time-varying multipath fading channel, a

robust CIR-based authentication scheme is proposed in [104] by exploiting the channel variation between noise-mitigated CIRs.

In practice, the time-varying fading nature of the wireless channel is one of the main fundamental limitations in the mobile radio communications, caused by the movement of terminals or objects in the propagation environment. Therefore, the performance of channel-based authentication scenario is challenged by the environmental changes on the transmission as well as the dynamic changing topology. Particularly, the main challenges of the channel-based physical layer authentication schemes are: 1) Fast channel variation leads to outdated CIR measurements at the receiver that would negatively impact the performance of authentication; 2) Unreliable decision-making for authentication is caused by forming a final decision based on the single observation of CIR difference.

To address the aforementioned challenges, we propose an enhanced CIR-based authentication scheme in this Chapter by exploiting a long-range channel predictor to predict future CIRs based on the historical CIR estimates in order to compensate for the effects of the rapid variation of the fading channel. Moreover, to form a final decision in the authentication process, multiple CIR differences are calculated by the receiver in an observation window based on the long-range channel predictor. Theoretical FAR and PD are defined based on a new test statistic that is developed by calculating multiple CIR differences between the current CIR and one of the adjacent CIRs in the window under a binary hypothesis testing. A final decision is made to reject the null hypothesis if partial CIR differences are larger than a threshold, otherwise the null hypothesis is accepted. In order to find optimal value of the threshold in decision rule, an optimization problem is defined based on minimizing the total error rate under false alarm constraints. Lastly, the performance of the proposed schemes is evaluated by using Monte-Carlo method.

The rest of this chapter is organized as follows: In Section 4.2, the model of the proposed authentication system is illustrated, and an enhanced authentication scheme is proposed by exploiting a long-range channel predictor in Section 4.3. In order to verify the theoretical analysis of our proposed authentication schemes, we illustrate the numerical results in Section 4.4, and summarize this chapter in Section 4.5.

4.2 Authentication Model

Our proposed authentication scheme is illustrated under the "Alice-Bob-Eve" scenario shown in Figure 3.1. In this section, the CIR is modeled first and the properties of CIR are indicated as well. Moreover, our authentication problem is formulated by a binary hypothesis testing.

4.2.1 Channel Model

The continuous-time CIR of a wireless channel can be modeled as a superposition of a certain number of paths, each characterized by its amplitude and delay, that is,

$$c(t,\tau) = \sum_{l=0}^{L-1} \alpha_l e^{j2\pi f_l t} \delta(\tau - \tau_l), \tag{4.1}$$

where L is the number of channel paths, α_l is the amplitude for the l^{th} path, τ_l is the corresponding delay, and f_l is the Doppler frequency shift limited by the maximum Doppler frequency f_d. In a Rayleigh fading channel, the channel coefficient $\alpha_l e^{j2\pi f_l t}$ can be modeled as a complex Gaussian random variable with zero mean and variance σ_l^2. The paths are assumed to be statistically independent, and the average power is normalized, i.e., $\sum_{l=0}^{L-1} \sigma_l^2 = 1$. Assuming a sampling rate of $f_s = 1/T_s$, the samples of channel coefficient on the lth component can be expressed as

$$h(n,l) = \alpha_l e^{j2\pi f_l n T_s}. \tag{4.2}$$

Additionally, we assume that one channel coefficient is highly correlated with the successive one on the same path. Specifically, the AR-1 model in (3.4) is employed to describe the temporal variation between $h(n,l)$ and $h(n-1,l)$. Herein, the AR coefficient ζ represents the correlation of two successive CIRs, which is calculated by using the Jakes model [32], i.e., $\zeta = J_0(2\pi f_d T_s)$, and $J_0(\cdot)$ is the Bessel function of the first kind and zero-th order. Therefore, the discrete autocorrelation function of channels $h(n-k_1,l)$ and $h(n-k_2,l)$ is $R_{k_1,k_2} = \mathrm{E}\{h(n-k_1,l)h^*(n-k_2,l)\} = \zeta^{|k_1-k_2|}\sigma_l^2$.

In real mobile radio environments, channel parameters such as channel coefficients, Doppler

frequency shifts and path delays, and the AR coefficient are slowly time-variant. Therefore, the channel model is reasonably accurate within a finite time interval and can be assumed to be invariant in a small time window for the following authentication analysis and channel prediction.

4.2.2 Hypothesis Testing

The proposed authentication scheme is mathematically formulated as a binary hypothesis testing problem. Specifically, the current CIR estimated by Bob (i.e., $\hat{\mathbf{h}}_X(n)$) is compared with the previous estimated CIR (i.e., $\hat{\mathbf{h}}_A(n-1)$) to identify the identity of the transmitter (Alice or Eve). Thus, the binary hypothesis testing problem can be formulated as

$$\begin{aligned} H_0 &: \left|\hat{\mathbf{h}}_X(n) - \hat{\mathbf{h}}_A(n-1)\right|^2 < \delta \\ H_1 &: \left|\hat{\mathbf{h}}_X(n) - \hat{\mathbf{h}}_A(n-1)\right|^2 > \delta, \end{aligned} \tag{4.3}$$

where $\hat{\mathbf{h}}_A$ is the noisy version of CIR from Alice to Bob, and $\hat{\mathbf{h}}_X$ is the estimated CIR from an unknown terminal with $X = \{A, E\}$. Herein, the subscripts "A" and "E" represent the transmitters Alice and Eve, respectively. δ is a threshold for the authentication test to determine if an eavesdropper is present. Additionally, H_0, the null hypothesis, stands for Alice as the claimant, while the alternative hypothesis, H_1, means the terminal is someone else.

Herein the noisy version of CIR achieved by the receiver, which is the actual CIR corrupted by the noise through a wireless channel, can be expressed as

$$\hat{\mathbf{h}}_X(n) = \left[\hat{h}_X(n,1), \hat{h}_X(n,2), \cdots, \hat{h}_X(n, N_p - 1)\right]^T, \tag{4.4}$$

where

$$\hat{h}_X(n,l) = h_X(n,l) + d(n,l), \quad 0 \le l \le N_p - 1. \tag{4.5}$$

Herein, N_p is the number of estimated CIR paths, which is assumed to be larger than the length of actual CIR (i.e., L) to avoid any loss of the channel information. $d(n,l)$ is the zero-mean white complex Gaussian noise with variance σ_d^2.

We assume that the knowledge of actual CIR between two wireless terminals is unknown.

Least-squares (LS) channel estimation is employed for channel estimation. Based on the binary hypothesis testing in (4.3), the difference between two adjacent CIR estimates is mathematically formulated by

$$\begin{aligned}&\hat{h}_X(n,l) - \hat{h}_A(n-1,l)\\&= h_X(n,l) + d_X(n,l) - h_A(n-1,l) - d_A(n-1,l).\end{aligned} \tag{4.6}$$

Due to the independence of different multipath components and the assumption of uniform power delay profile of the multipath fading channel, we can just explore the properties of CIR on one single path without loss of generality. More specifically, based on the AR-1 model given in (3.4) and the distribution of d in (4.5), the distribution of the CIR difference under the two hypotheses can be derived by

$$\begin{aligned}H_0 &: \ \hat{h}_A(n,l) - \hat{h}_A(n-1,l) \sim \mathcal{N}_c(0,\sigma^2_{H_0})\\H_1 &: \ \hat{h}_E(n,l) - \hat{h}_A(n-1,l) \sim \mathcal{N}_c(0,\sigma^2_{H_1}),\end{aligned} \tag{4.7}$$

where $\mathcal{N}_c(\mu,\sigma^2)$ expresses the complex Gaussian distribution with mean μ and variance σ^2. Herein $\sigma^2_{H_0} = 2(1-\zeta)\sigma^2_A + 2\sigma^2_d$ and $\sigma^2_{H_1} = \sigma^2_E + \sigma^2_A + 2\sigma^2_d$.

4.3 Channel Prediction Based Authentication Enhancement

Indeed, channel prediction in mobile radio systems is the key element for many fading-compensation techniques, where future samples of the fading channel are estimated and used to enhance the performance of adaptive transmission systems [114]. To enable a robust authentication to overcome the negative effects of fast channel variation, channel prediction can be used to predict several symbols ahead and improve the performance of spoofing detection. In this section, an enhanced CIR-based physical layer authentication scheme is developed by exploiting a long-range channel predictor to predict future CIRs based on a series of historical CIR estimates. A statistical test is developed based on the difference between the current and the predicted CIRs. Lastly, theoretical FAR and PD are defined based on exploring multiple observations of the CIR differences for performance evaluation.

4.3.1 Noise-Mitigated CIR Estimates

In this subsection, a noise-mitigated threshold is utilized to preprocess CIR estimates in order to eliminate negative impacts of the communication noise. In practical situations, transmitted signals would be interfered by noise through a wireless channel, thereby the achieved channel response at the receiver would be corrupted by noise as well. Recalling the formula of the noisy version of CIR in (4.5), we can notice that both strong and weak paths are corrupted by noise. Therefore, the noise components, which are superimposed on the original zero-valued channel taps, can affect the determination of the actual channel difference between two CIRs on the significant paths. In order to eliminate the impact of noise, the difference between two consecutive CIR estimates is first formulated by

$$\begin{aligned} \Delta \mathrm{h} &= \sum_{l=0}^{N_p-1} \left|\hat{h}(n,l) - \hat{h}(n-1,l)\right| \\ &= \sum_{l\in Q} \left|\Delta\hat{h}_l\right| + \sum_{l\notin Q} |\Delta d_l|\,, \end{aligned} \tag{4.8}$$

where Q denotes the set of time indices for the significant multipath components between two CIRs. The first term in (4.8) is the actual CIR difference, while the second term represents the induced noise that should be eliminated. To avoid the impact of noise on evaluating the CIR difference, a noise-mitigated threshold is utilized. Particularly, the absolute value of each path is compared with a threshold β, which taps with absolute value below the threshold are set to be zeros. The threshold β is determined by minimizing the MSE of the estimation error, and the estimation error can be expressed by

$$e_{CE}(n,l) = h(n,l) - \hat{h}(n,l). \tag{4.9}$$

Therefore, the noise-mitigated threshold can be expressed by [99],

$$\beta \approx \sqrt{\sigma_d^2 \ln\left(N_p/P_{ofa}\right)}, \tag{4.10}$$

where P_{ofa} is the overall false alarm rate with a constant value under a specific security level. After the threshold is applied on the CIR estimates achieved by LS channel estimation, only

significant multipath components are obtained.

Additionally, in fast varying channels, channel estimation has the drawback of potentially yielding outdated channel state information, which can significantly degrade the authentication performance of CIR-based authentication scheme. Figure 4.1 shows the envelop of CIR for one path component under a multipath Rayleigh fading channel with two different maximum Doppler shifts. It illustrates that the envelop of channel coefficient fluctuates significantly at higher maximum Doppler shift in a long time interval, however, it can approximately seen as a constant within a finite time duration.

For instance, considering an OFDM system with 1024 subcarriers, the OFDM symbol duration is calculated by multiplying the number of total subcarriers with the sampling period. Thus, the symbol duration in this case is 1.024 ms. From Figure 4.1, during transmitting one OFDM symbol, the envelop of CIR is not changed at $f_d = 10$ Hz, while it is slightly decreased by 1 dB at $f_d = 100$ Hz. However, in the duration of transmitting 10 OFDM symbols, the variation of CIR envelop is slightly 1 dB at $f_d = 10$ Hz, while it can reach to 11 dB at $f_d = 100$ Hz. Therefore, under high-speed movement of terminals, the outdated CIR estimate dramatically effects the authentication analysis based on exploiting the channel variation.

In order to overcome the issue caused by the fast channel variation, a long-range channel predictor is exploited and introduced in the next subsection.

4.3.2 Channel Predictor based on CIR estimates

A linear channel predictor [115] is employed here by linearly combining the past CIR estimates to predict the future CIRs. The MSE of the prediction error is minimized to achieve the predictor coefficient. In particular, the predicted CIR on the lth path and the prediction error can be written respectively as

$$\tilde{h}_A(n,l) = \sum_{i=1}^{G} w(i,l)\hat{h}_A(n-i,l), \tag{4.11}$$

and

$$e_{CP}(n,l) = \hat{h}_A(n,l) - \tilde{h}_A(n,l), \tag{4.12}$$

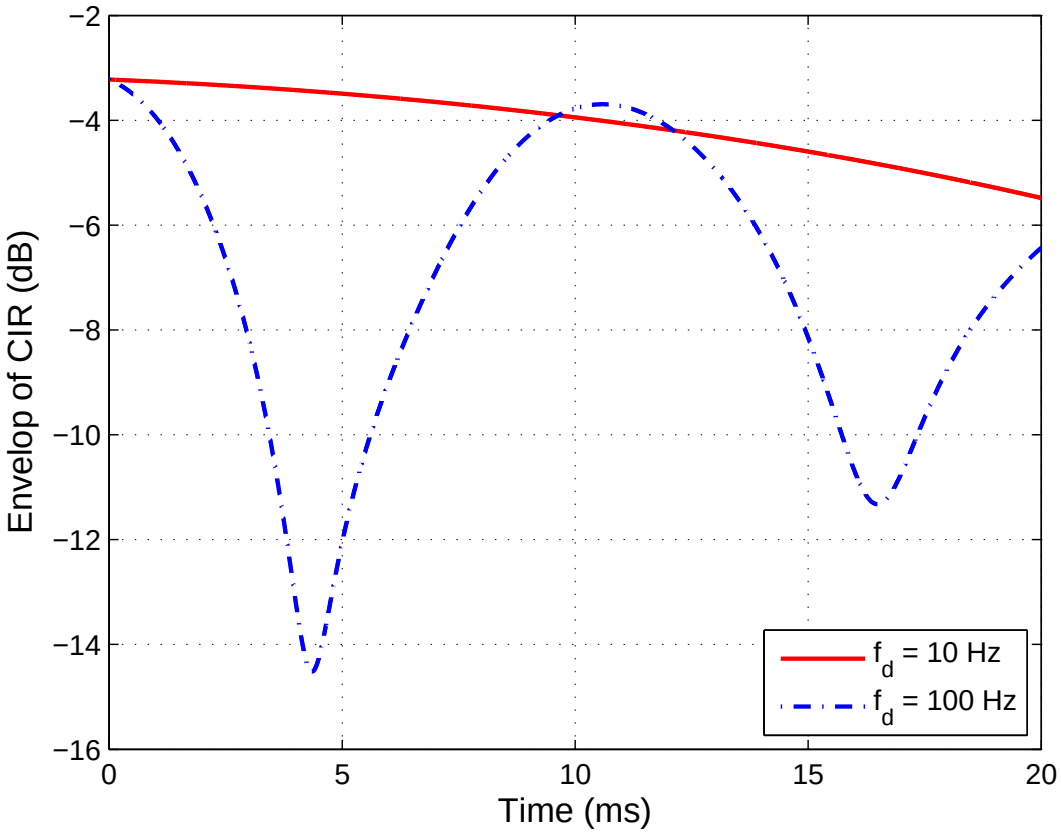

Figure 4.1: The envelope of CIR for one path component in the multipath Rayleigh fading channel under two different maximum Doppler frequencies. The sampling rate $f_s = 1MHz$.

where G is the number of past CIR estimates used for channel prediction. The optimal predictor coefficient of the lth multipath component is denoted as $W(l) = [w(1,l), w(2,l), \ldots, w(G,l)]^T$, which is obtained by minimizing the prediction MSE. Thus, the MSE of the prediction error can be minimized and expressed by

$$\arg\min \text{MSE} = \min_{w} \left[\frac{1}{N_p} \sum_{l=0}^{N_p-1} \text{E}\left\{ |e_{CP}(n,l)|^2 \right\} \right]. \tag{4.13}$$

Consequently, the prediction coefficient vector can be derived by solving the Yule-Walker equations [116], resulting in

$$W(l) = (\mathbf{R}_{hh}^{(l)})^{-1} \mathbf{r}_{hh}^{(l)}, \tag{4.14}$$

where

$$\mathbf{R}_{hh}^{(l)} = \begin{bmatrix} \tilde{R}_{1,1} & \tilde{R}_{1,2}^{*} & \cdots & \tilde{R}_{1,G}^{*} \\ \tilde{R}_{2,1} & \tilde{R}_{2,2} & \cdots & \tilde{R}_{2,G}^{*} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{R}_{G,1} & \tilde{R}_{G,2} & \cdots & \tilde{R}_{G,G} \end{bmatrix}, \tag{4.15}$$

and

$$\mathbf{r}_{hh}^{(l)} = [r_1, r_2, \cdots, r_G]^{\mathbf{T}}. \tag{4.16}$$

$\mathbf{R}_{hh}^{(l)}$ is the $G \times G$ correlation matrix between historical CIR estimates for the lth multipath component, and $\mathbf{r}_{hh}^{(l)}$ is the $G \times 1$ cross-correlation vector between the past and future CIR estimates on the lth path. Since ideal correlation functions are unknown at the receiver and have slowly time variations in practice, they can be derived from these noise-corrupted channel observations (i.e., achieved historical CIR estimates). That is,

$$\begin{aligned} \tilde{R}_{i,i'} &= \mathrm{E}\left\{\hat{h}_A(n-i,l)\hat{h}_A^{*}(n-i',l)\right\} \\ &\approx \frac{1}{M}\sum_{m=0}^{M-1}\hat{h}_A(n-m-i,l)\hat{h}_A^{*}(n-m-i',l), \end{aligned} \tag{4.17}$$

and

$$\begin{aligned} r_i &= \mathrm{E}\left\{\hat{h}(n-i,l)\hat{h}_A^{*}(n,l)\right\} \\ &\approx \frac{1}{M}\sum_{m=0}^{M-1}\hat{h}_A(n-m-i,l)\hat{h}_A^{*}(n-m,l), \end{aligned} \tag{4.18}$$

where $i, i' = 1, 2, \cdots, G$. Consequently, based on the analysis of CIR predictor above, a long-range CIR prediction can be derived as [117]

$$\tilde{h}_A(n+\Delta,l) = \sum_{i=1}^{\Delta} w(i,l)\tilde{h}_A(n+\Delta-i,l) + \sum_{i=\Delta+1}^{G} w(i,l)\hat{h}_A(n+\Delta-i,l), \tag{4.19}$$

where Δ is the prediction range and $\Delta \geq 0$. Equation (4.19) shows an iterative process to predict CIR estimates in a long range, and the predicted CIR estimates are also used for the future CIR prediction. Additionally, the vector of predictor coefficient $W(l)$ should be updated

and derived based on the equation (4.14).

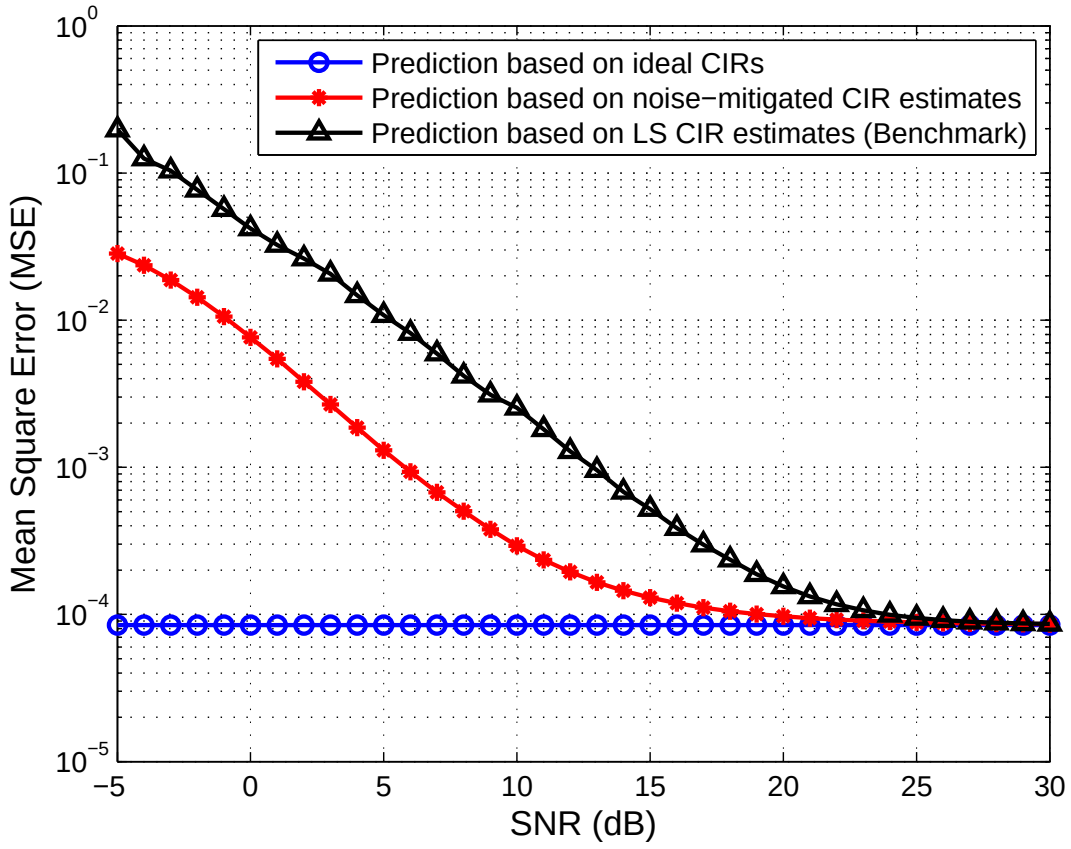

Figure 4.2: MSE of the total error versus SNR values under three different scenarios.

By using the equations (3.4) and (4.5), the predicted CIR $\tilde{h}_A$ follows a complex Gaussian distribution. The expected value and the variance of $\tilde{h}_A$ are derived, respectively, by

$$\begin{aligned}\tilde{\mu}_l &= \mathrm{E}\left\{\sum_{i=1}^{G} w(i,l)\hat{h}_A(n-i,l)\right\} \\ &= \sum_{i=1}^{G} w(i,l)\mathrm{E}\Big\{h_A(n-i,l) + d(n-i,l)\Big\} \\ &= 0, \end{aligned} \tag{4.20}$$

and

$$\begin{aligned}
\tilde{\sigma}_l^2 &= \mathrm{Var}\left\{\sum_{i=1}^{G} w(i,l)\hat{h}_A(n-i,l)\right\} \\
&= \mathrm{Var}\Big\{w(1,l)\hat{h}_A(n-1,l) + \cdots + w(G-2,l)\hat{h}_A(n-G+2,l) \\
&\quad + w(G-1,l)\hat{h}_A(n-G+1,l) + w(G,l)\hat{h}_A(n-G,l)\Big\} \\
&= \mathrm{Var}\Big\{w(1,l)\hat{h}_A(n-1,l) + \cdots + w(G-2,l)\Big[\zeta^2 h_A(n-G,l) + \zeta\sqrt{(1-\zeta^2)\sigma_A^2}u(n-G,l) \\
&\quad + \sqrt{(1-\zeta^2)\sigma_A^2}u(n-G+1,l) + d(n-G+2,l)\Big] \\
&\quad + w(G-1,l)\Big[\zeta h_A(n-G,l) + \sqrt{(1-\zeta^2)\sigma_A^2}u(n-G,l) + d(n-G+1,l)\Big] \\
&\quad + w(G,l)\Big[h_A(n-G,l) + d(n-G,l)\Big]\Big\} \\
&= (\sigma_A^2 + \sigma_d^2)\sum_{i=1}^{G}|w(i,l)|^2 + \sum_{1\le i<i'\le G} 2w(i,l)w^*(i',l)(\zeta^{|i-i'|}\sigma_A^2 + \sigma_d^2).
\end{aligned} \tag{4.21}$$

Due to the presence of channel estimation error in (4.9) and channel prediction error in (4.12), the total error between the actual CIR and the predicted CIR should be studied on evaluating the impact of these negative errors on the CIR variation. Thus, the total error can be written by

$$e_{Total}(n,l) = e_{CE}(n,l) + e_{CP}(n,l) = h(n,l) - \tilde{h}(n,l). \tag{4.22}$$

The MSE of the total error is plotted in Figure 4.2 under three different scenarios. Specifically, the blue line with circle marker (labeled "Prediction based on ideal CIRs") refers to a lowerbound of the MSE of the total error. Herein, the total error is only the prediction error, and the MSE of the total error is -41 dB in a wide range of SNR values. Additionally, the black curve with triangle marker (labeled "Prediction based on LS CIR estimates (Benchmark)") represents a upperbound of the MSE of the total error, which is corresponding to the benchmark scheme. Furthermore, the red line with asterisk marker (labeled "Prediction based on noise-mitigated CIR estimates") indicates the performance of MSE according to the scheme proposed in this subsection. When the value of SNR is equal to -5 dB, the performance of the red curve is approximately 7 dB better than that of the upperbound. Overall, a comparison of

these three curves illustrates that the CIR variation is not significantly affected by the presence of estimation error and prediction error at a reasonable SNR value (i.e., larger than 10 dB).

4.3.3 Authentication Analysis Using Channel Predictor

Since the CIR estimated by the receiver would be outdated because of the processing delay in high mobility environments, we compare the current CIR estimate with the predicted one. Thus, a new statistical test is developed as

$$\begin{aligned} \mathrm{T_s} &= \sum_{l=0}^{N_p-1} \left|\hat{h}_X(n,l) - \tilde{h}_A(n,l)\right|^2, \\ &= \sum_{l\in Q} \left|\hat{h}_X(n,l) - \sum_{i=1}^{G} \omega(i,l)\hat{h}_A(n-i,l)\right|^2. \end{aligned} \tag{4.23}$$

Using the derived results in equations (4.20) and (4.21), the distributions of the statistical test under the two hypotheses can be derived, respectively, by

$$\begin{aligned} H_0 &: \ \mathrm{T_s} \sim \Gamma(Q, \tilde{\sigma}^2_{H_0}) \\ H_1 &: \ \mathrm{T_s} \sim \Gamma(Q, \tilde{\sigma}^2_{H_1}), \end{aligned} \tag{4.24}$$

where $\tilde{\sigma}^2_{H_0} = (\sigma^2_A + \sigma^2_d) + \tilde{\sigma}^2_l - 2\sum_{i=1}^{G} |w(i,l)|(\zeta^i\sigma^2_A + \sigma^2_d)$ and $\tilde{\sigma}^2_{H_1} = (\sigma^2_E + \sigma^2_d) + \tilde{\sigma}^2_l$.

Based on the distributions of $\mathrm{T_s}$ in (4.24), the theoretical FAR $\mathrm{P}_{fa,1}$ and PD $\mathrm{P}_{d,1}$ can be derived by

$$\mathrm{P}_{fa,1} = P_r(\mathrm{T_s} > \delta_1 | H_0) = \sum_{i=0}^{Q-1} \frac{1}{i!}\left(\frac{\delta_1}{\tilde{\sigma}^2_{H_0}}\right)^i e^{-\frac{\delta_1}{\tilde{\sigma}^2_{H_0}}}, \tag{4.25}$$

and

$$\mathrm{P}_{d,1} = P_r(\mathrm{T_s} > \delta_1 | H_1) = \sum_{i=0}^{Q-1} \frac{1}{i!}\left(\frac{\delta_1}{\tilde{\sigma}^2_{H_1}}\right)^i e^{-\frac{\delta_1}{\tilde{\sigma}^2_{H_1}}}, \tag{4.26}$$

where δ_1 is the threshold of decision-making for authentication. After determining the value of Q, δ_1 can be calculated under a given value of $\mathrm{P}_{fa,1}$. It can be noticed that δ_1 is an adaptive threshold varying with different values of Q.

4.3.4 Multiple Observations of CIR Difference

Traditionally, the final authentication decision is formed under the binary hypothesis testing by individually comparing the current CIR with the previous one, which is to determine if an eavesdropper interrupts the communication link. However, due to the presence of noise and the movement of terminals, the robustness of spoofing detection is severely degraded by various channel fading conditions. Therefore, we propose a new binary hypothesis testing based on multiple observations of CIR difference to form the final decision. Specifically, we assume that the total number of CIR differences used for the decision-making is Z, if at least K-out-of-Z CIR differences are larger than a threshold δ, the receiver determines a spoofing attack is occurred, otherwise no eavesdropper is present. Thus, the authentication test can be formulated by

$$\begin{aligned} H_0 &: \sum_j \mathbf{I}\left[\mathrm{T}_{s,j} > \delta\right] \leq K \\ H_1 &: \sum_j \mathbf{I}\left[\mathrm{T}_{s,j} > \delta\right] > K, \end{aligned} \tag{4.27}$$

where $j = -\frac{Z}{2}, \cdots, -2, -1, 1, 2, \cdots, \frac{Z}{2}$. $\mathbf{I}$ is a characteristic function, and $\mathbf{I}[x]$ is equal to one if the statement x is true, otherwise equals zero. Herein $\mathrm{T}_{s,j}$ is defined as a statistical test corresponding to the jth CIR difference, which is expressed by

$$\mathrm{T}_{s,j} = \begin{cases} \sum_{l \in Q} \left|\hat{h}_X(n,l) - \hat{h}_A(n+j,l)\right|^2, & if\ j = -1, -2, \cdots, -\dfrac{Z}{2}, \\ \sum_{l \in Q} \left|\hat{h}_X(n,l) - \tilde{h}_A(n+j,l)\right|^2, & if\ j = 1, 2, \cdots, \dfrac{Z}{2}, \end{cases} \tag{4.28}$$

where $\hat{h}_A$ is the historical CIR estimate from Alice, and $\tilde{h}_A$ is the predicted CIR that is achieved based on the proposed long-range channel predictor. Figure 4.3 shows the procedure of achieving multiple CIR differences, which indicates that the CIR differences Δh are individually calculated between the current CIR and one of its adjacent CIRs (i.e., one of historical CIRs or predicted CIRs) in a window size Z.

Based on the AR model, we can further derive the distributions of the statistical test $\mathrm{T}_{s,j}$ under the two hypotheses. In particular, when $j = -1, -2, \cdots, -\frac{Z}{2}$, the statistical test is defined as a sum of the squares of the difference between current estimated CIR and the historical CIR

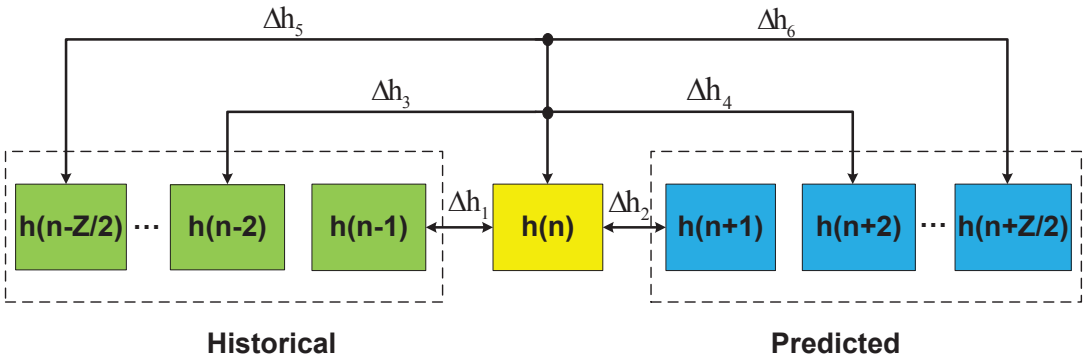

Figure 4.3: The procedure of achieving multiple CIR differences.

estimate for the lth path. Therefore, the statistical test $\mathrm{T}_{s,j}$ follows Gamma distribution. That is,

$$\begin{aligned} H_0 &: \ \mathrm{T}_{s,j} \sim \Gamma(Q, \sigma^2_{H_0,j}) \\ H_1 &: \ \mathrm{T}_{s,j} \sim \Gamma(Q, \sigma^2_{H_1}), \end{aligned} \tag{4.29}$$

where $\sigma^2_{H_0,j} = 2(1-\zeta^{|j|})\sigma^2_A + 2\sigma^2_d$. By using the distributions in (4.29), the probabilities that the statistical test $\mathrm{T}_{s,j}$ is larger than a threshold δ_2 under the two hypotheses, can be derived, respectively, as

$$\mathrm{P}_{fa,2} = P_r(\mathrm{T}_{s,j} > \delta_2 | H_0) = \sum_{i=0}^{Q-1} \frac{1}{i!}\left(\frac{\delta_2}{\sigma^2_{H_0,j}}\right)^i e^{-\frac{\delta_2}{\sigma^2_{H_0,j}}}, \tag{4.30}$$

and

$$\mathrm{P}_{d,2} = P_r(\mathrm{T}_{s,j} > \delta_2 | H_1) = \sum_{i=0}^{Q-1} \frac{1}{i!}\left(\frac{\delta_2}{\sigma^2_{H_1}}\right)^i e^{-\frac{\delta_2}{\sigma^2_{H_1}}}. \tag{4.31}$$

Similarly, when $j = 1, 2, \cdots, \frac{Z}{2}$, we can achieve the distributions of the statistical test $\mathrm{T}_{s,j}$ based on the derived results in (4.24). That is,

$$\begin{aligned} H_0 &: \ \mathrm{T}_{s,j} \sim \Gamma(Q, \tilde{\sigma}^2_{H_0,j}) \\ H_1 &: \ \mathrm{T}_{s,j} \sim \Gamma(Q, \tilde{\sigma}^2_{H_1}). \end{aligned} \tag{4.32}$$

For simplification, we assume that only one past CIR estimate is used for predicting the future one. Therefore, the variance $\tilde{\sigma}^2_{H_0,j}$ is $\tilde{\sigma}^2_{H_0,j} = \sigma^2_A(\zeta - |\omega(1,l)|^{j+1})^2 + (1-\zeta^2)\sigma^2_A + \sigma^2_d(1-|\omega(1,l)|^{j+1})^2$.

Based on the distributions in (4.32), the probabilities that the statistical test $\mathrm{T}_{s,j}$ is larger than a threshold δ_3 under the two hypotheses, can be derived, respectively, as

$$\mathrm{P}_{fa,3} = P_r(\mathrm{T}_{s,j} > \delta_3 | H_0) = \sum_{i=0}^{Q-1} \frac{1}{i!}\Big(\frac{\delta_3}{\tilde{\sigma}^2_{H_0,j}}\Big)^i e^{-\frac{\delta_3}{\tilde{\sigma}^2_{H_0,j}}}, \tag{4.33}$$

and

$$\mathrm{P}_{d,3} = P_r(\mathrm{T}_{s,j} > \delta_3 | H_1) = \sum_{i=0}^{Q-1} \frac{1}{i!}\Big(\frac{\delta_3}{\tilde{\sigma}^2_{H_1}}\Big)^i e^{-\frac{\delta_3}{\tilde{\sigma}^2_{H_1}}}. \tag{4.34}$$

Consequently, under the developed hypothesis testing given in (4.27), theoretical FAR and PD can be defined, respectively, by

$$\mathrm{P}_{fa} = \sum_{k=K+1}^{Z} P_r\Big(\sum_{j=-\frac{Z}{2}}^{-1} \mathbf{I}[\mathrm{T}_{s,j} > \delta] + \sum_{j=1}^{\frac{Z}{2}} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = k | H_0 \Big), \tag{4.35}$$

and

$$\mathrm{P}_{d} = 1 - \sum_{k=0}^{K} P_r\Big(\sum_{j=-\frac{Z}{2}}^{-1} \mathbf{I}[\mathrm{T}_{s,j} > \delta] + \sum_{j=1}^{\frac{Z}{2}} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = k | H_1 \Big). \tag{4.36}$$

Under the hypothesis H_0, the closed-form expression for the FAR in equation (4.35) cannot be easily derived, because the probability $\mathrm{P}_{fa,2}$ in (4.30) is not identical when different value of j is chosen, as is the probability $\mathrm{P}_{fa,3}$ in (4.33). Fortunately, the closed-form expression for the PD in (4.36) can be derived by using the results (4.31) and (4.34). More specifically, when the

value of K is between 0 and $\frac{Z}{2}$ (i.e., $0 \leq K \leq \frac{Z}{2}$), the PD can be further expressed by

$$\begin{aligned}
\mathrm{P}_d = 1 - \sum_{k=0}^{K} \Big\{ & P_r\Big(\sum_{j=-\frac{Z}{2}}^{-1} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = 0, \sum_{j=1}^{\frac{Z}{2}} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = k | H_0 \Big) \\
& + P_r\Big(\sum_{j=-\frac{Z}{2}}^{-1} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = 1, \sum_{j=1}^{\frac{Z}{2}} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = k-1 | H_0 \Big) \\
& + \cdots + P_r\Big(\sum_{j=-\frac{Z}{2}}^{-1} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = k, \sum_{j=1}^{\frac{Z}{2}} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = 0 | H_0 \Big) \Big\} \\
= 1 - \sum_{k=0}^{K} \Big\{ & \sum_{v=0}^{k} \binom{\frac{Z}{2}}{v} (\mathrm{P}_{d,2})^v (1-\mathrm{P}_{d,2})^{\frac{Z}{2}-v} \times \binom{\frac{Z}{2}}{k-v} (\mathrm{P}_{d,3})^{k-v} (1-\mathrm{P}_{d,3})^{\frac{Z}{2}-k+v} \Big\}.
\end{aligned} \tag{4.37}$$

If the value of K is between $\frac{Z}{2}+1$ and Z (i.e., $\frac{Z}{2}+1 \leq K \leq Z$), the PD can be rewritten by

$$\begin{aligned}
\mathrm{P}_d = \sum_{k=K+1}^{Z} \Big\{ & P_r\Big(\sum_{j=-\frac{Z}{2}}^{-1} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = \frac{Z}{2}, \sum_{j=1}^{\frac{Z}{2}} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = k - \frac{Z}{2} | H_0 \Big) \\
& + P_r\Big(\sum_{j=-\frac{Z}{2}}^{-1} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = \frac{Z}{2} - 1, \sum_{j=1}^{\frac{Z}{2}} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = k - \frac{Z}{2} + 1 | H_0 \Big) \\
& + \cdots + P_r\Big(\sum_{j=-\frac{Z}{2}}^{-1} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = k - \frac{Z}{2}, \sum_{j=1}^{\frac{Z}{2}} \mathbf{I}[\mathrm{T}_{s,j} > \delta] = \frac{Z}{2} | H_0 \Big) \Big\} \\
= \sum_{k=K+1}^{Z} \Big\{ & \sum_{v=k-\frac{Z}{2}}^{\frac{Z}{2}} \binom{\frac{Z}{2}}{k-v} (\mathrm{P}_{d,2})^{k-v} (1-\mathrm{P}_{d,2})^{\frac{Z}{2}-k+v} \times \binom{\frac{Z}{2}}{v} (\mathrm{P}_{d,3})^{v} (1-\mathrm{P}_{d,3})^{\frac{Z}{2}-v} \Big\}.
\end{aligned} \tag{4.38}$$

Therefore, the total error rate can be expressed by summing the false alarm rate (or a Type I error) and the missed detection rate (or a Type II error), that is,

$$\mathrm{P}_T = \mathrm{P}_{fa} + (1 - \mathrm{P}_d)\,. \tag{4.39}$$

4.3.5 Parameter Optimization

Comparing multiple observations with the single observation of CIR difference, there should be a tradeoff between the robustness of spoofing detection and the computational complexity

as well as the latency of decision-making. In order to leverage between these aspects, a parameter η is defined as the ratio of the threshold K to the observation window size Z, i.e., $\eta = \frac{K}{Z}$. The value of η is optimized based on minimizing the total error rate subject to false alarm constraints. Mathematically, the optimization problem can be expressed by

$$\begin{aligned} &\eta_{opt} = \min_{\eta} \{\mathrm{P}_T\} = \min_{\eta} \left\{\mathrm{P}_{fa} + (1 - \mathrm{P}_d)\right\}, \\ &s.t.\ \ 0 < \mathrm{P}_{fa,2}, \mathrm{P}_{fa,3} \leq 0.1. \end{aligned} \tag{4.40}$$

Suppose the number of total CIR differences Z is fixed, the optimal value of K can be found using exhaustive search method in the simulations.

4.4 Simulation Results

4.4.1 Simulation Scenarios

In this section, the effectiveness of the proposed authentication scheme is verified by numerical simulation. Specifically, an OFDM system is employed with QPSK modulation in all simulation cases, and LS channel estimation is utilized for achieving CIR estimates based on embedded comb-type pilots with the length of N_p in the transmitted OFDM symbols.

As for the channel model, a multipath Rayleigh fading channel is modeled with sparse sample-spaced significant taps and uniform power delay profile, and different path components are statistically independent to each other with normalized average power. Additionally, since Alice, Eve and Bob are located in spatially different locations in the communication networks, the channel between Eve and Bob is assumed with different number of path components and path positions from the channel link between Alice and Bob. The particular parameters related to our simulations are list in Table 3.1.

4.4.2 Numerical Results and Discussion

In this subsection, the performance of the proposed authentication scheme is verified and compared with that of the benchmark scheme. In the simulations, “scheme 1” and “scheme 2”

refer to the channel predictor-based authentication based on single CIR difference and multiple CIR differences, respectively.

In Figure 4.4, it is shown the PD versus different SNR values at $P_{fa} = 0.1$. As it can be seen from this figure, a spoofing attack can be successfully detected with a probability of one in the two schemes when the SNR is higher than 5 dB. Moreover, compared with "scheme 1", "scheme 2" performs better at low SNR.

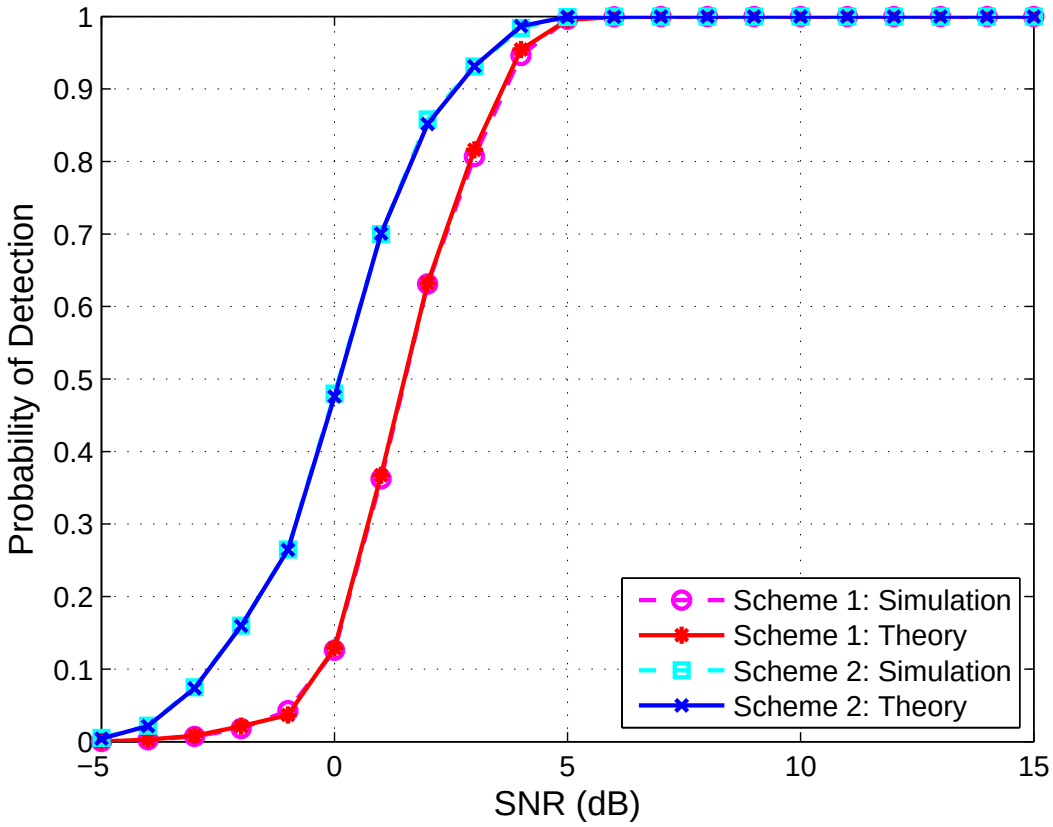

Figure 4.4: Probability of detection versus SNRs at $P_{fa} = 0.1$.

In Figure 4.5, the ROC is sketched at low SNR of 5 dB for the two schemes. As expected, the probability of spoofing detection increases when the value of FAR increases. Moreover, it can be seen from this figure that the performance of "scheme 2" is better than that of "scheme 1" at low FAR values.

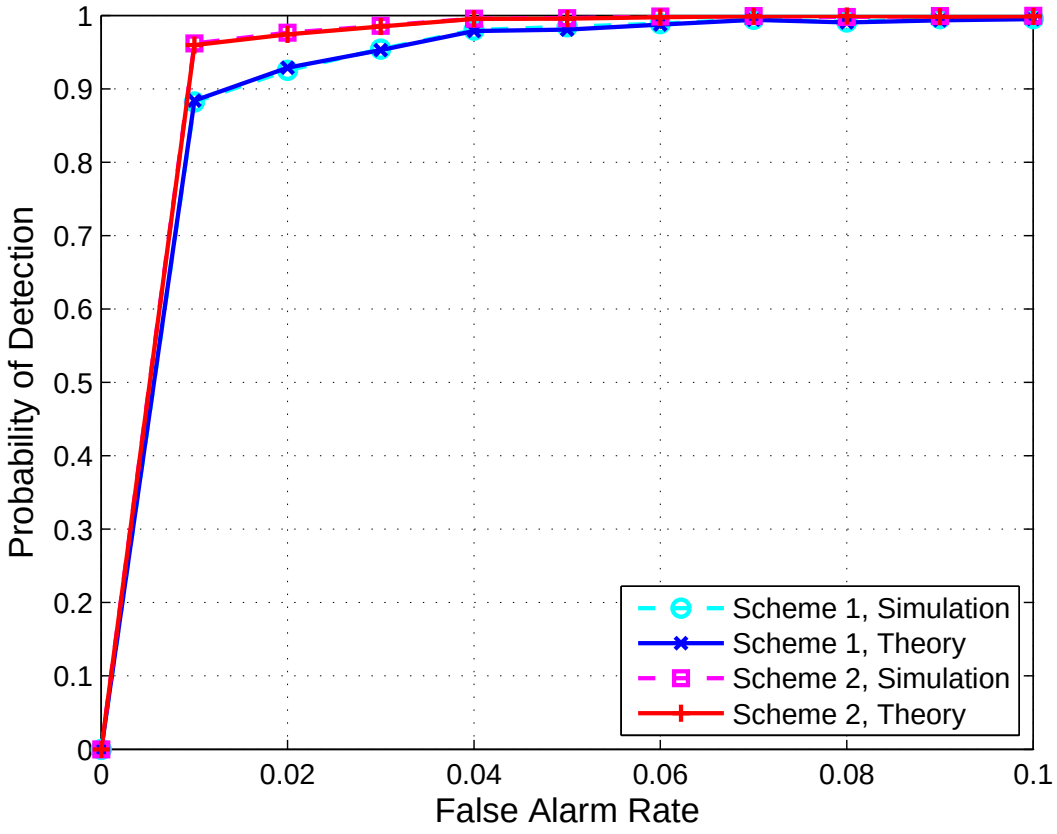

Figure 4.5: Receiver operating characteristic (ROC) at SNR of 5dB.

4.5 Summary

In this chapter, we have proposed an enhanced CIR-based physical layer authentication schemes by exploiting a long-range channel predictor. Initially, a noise-mitigated threshold has been utilized to eliminate the noise components of the CIR estimates, so that, the significant multipath components were obtained and further exploited for the authentication analysis. In addition, a channel prediction method has been employed by predicting future CIRs based on the historical CIR estimates in order to overcome the effects of fast channel fading. Furthermore, based on the long-range channel predictor, multiple channel differences were observed simultaneously between the current CIR and one of its adjacent CIRs in an observation window. After that, the final decision in the authentication process was formed by exploiting the multiple CIR differences based on a new binary hypothesis testing. An optimization prob-

lem has been defined in order to find the optimal value of the threshold by minimizing the total error rate subject to constraints of false alarm. Finally, simulation results have shown the effectiveness of the proposed authentication enhancement scheme.

Chapter 5

CIR-Based Authentication Enhancement Using 2-D Quantization

In real mobile radio environments, the performance of spoofing detection for CIR-based physical layer authentication is degraded significantly due to the large variation in the channel amplitude over time. In contrast with the temporal variation of channel amplitude, the multipath delay spread is relatively stationary over long time intervals [18]. More importantly, multipath delay spread profiles also represent the distinct properties of the wireless channels, which can be exploited to distinguish between spatially separated users.

In this Chapter, a novel physical layer authentication enhancement scheme is proposed by integrating additional multipath delay characteristics of wireless channels into the CIR-based physical layer authentication framework. In order to simplify the decision rule for authentication, a two-dimensional quantization method is developed to preprocess the channel variations. More specifically, two one-bit quantizers are used to quantize the temporal channel variations in the dimensions of channel amplitude and path delay, respectively. Under a simple hypothesis testing, a new test statistic is developed based on the sum of outputs of the two quantizers. For performance analysis, theoretical FAR and PD are defined based on the developed test statistic, and their closed-form expressions are derived as well. In order to evaluate the performance of the proposed scheme, Monte-Carlo method is utilized and the numerical results are compared with the closed-form derivations. Additionally, an optimization problem is defined to find the optimal parameters for the proposed authentication technique by using exhaustive

search method in the simulations.

5.1 Introduction

In wireless communications, the broadcast nature of the wireless channels brings significant challenges for security provisioning between legitimate transmitters and receivers. Spoofing is one important aspect of security threats, in which adversaries attempt to impersonate the legitimate transceiver within a network in order to gain illegitimate advantages [1]. In order to defend systems against spoofing attacks, the receiving end should be equipped with authentication mechanisms which provide systems with the ability of validating the identities of involved transmitting users. Traditionally, authentication mechanisms are accomplished by exchanging secret keys between authorized users, and the keys are generated based on complex mathematical calculations. However, the computational complexity causes a practical problem associated with key distribution and scalability. Additionally, traditional authentication techniques rely solely on the upper layers of the open systems interconnection (OSI) network model, thereby the lack of physical layer protection makes them vulnerable against adversaries. In order to address these shortcomings of the traditional authentication mechanisms, physical layer authentication is emerging as a new promising technique by exploiting the physical link properties to provide additional security protection [2].

The fundamental principle behind physical layer authentication is to exploit the channel characteristics such as channel reciprocity, spatial decorrelation and temporal correlation, in order to discriminate between transmitters placed at different positions. A variety of physical layer authentication schemes have been proposed in [3, 8–12, 34, 53, 103, 104] by exploiting the properties of wireless channels under various system models and different assumptions of the available knowledge of channel state information (CSI). In order to achieve authentication schemes which are applicable in practical systems, these approaches have also taken into account the environmental changes and/or the mobility of terminals in their design. The results presented in the literature have shown performance effectiveness of spoofing detection for various cases.

In Chapter 3, we developed a robust physical layer authentication scheme by exploiting

the inherent properties of CIR under a time-varying multipath fading channel. Nevertheless, in high mobility environments, the performance of spoofing detection is degraded significantly due to the fast variations in the channel amplitude over time. In contrast with the temporal variation of channel amplitude, another characterization of wireless channels, i.e., the multipath delay spread, is relatively stationary over long time intervals [18]. More importantly, multipath delay spread profiles are distinct from one location to another if the locations are spatially separated. In [105], an enhanced physical layer authentication scheme was proposed by integrating the multipath delay characteristics into the channel-based authentication framework. As in [105], each channel amplitude and path delay was quantized, respectively, into multiple number of levels in order to reduce the impact of rapid channel variation. However, the use of multi-level quantization increases the computational complexity. Moreover, the other shortcoming of the method proposed in [105] is its non-robust performance in the case of large channel variations. Particularly, this approach exploits the total difference between quantized channel realizations (i.e., channel amplitude and delay) over two consecutive time intervals. However, large channel variation induced by the movement of terminals and environmental changes contributes the major part of the channel difference, which results in a non-robust decision-making for authentication.

In this Chapter, we propose a novel channel-based physical layer authentication enhancement scheme by exploiting the inherent properties of channel amplitude and multipath time delay spread. Due to the temporal correlation and spatial decorrelation of multipath channels, the variations of channel amplitude and time delay are exploited to discriminate between the legitimate transmitter and the spoofer. In order to simplify the decision rule for authentication, a two-dimensional quantization algorithm is developed to preprocess the channel variations. Particularly, two one-bit quantizers are used on the difference of adjacent channel amplitudes over time and the difference between two successive time intervals of path delays, respectively. Under a simple hypothesis testing, a new test statistic is developed based on the outputs of the two one-bit quantizers. For performance analysis, the closed-form expressions for FAR and PD are derived. The performance of the proposed scheme is validated in the simulations. In order to find optimal parameters that satisfying our optimization problem, exhaustive search method is utilized in the simulations.

The rest of this Chapter is organized as follows: In Section 5.2, we provide the channel model of the proposed authentication system, and a simple hypothesis testing based on a two-dimensional quantization is described as well. Based on the developed authentication model, the performance of the two-dimensional quantization scheme is analyzed under two hypotheses in Section 5.3. The closed-form expressions for FAR and PD are derived in Section 5.4, and an optimization problem is defined as well. In order to verify the statistical analysis, a benchmark method is introduced and then numerical results are illustrated in Section 5.5. Lastly, this paper is summarized in Section 5.6.

5.2 System Model

In our scenario, we consider the ubiquitous "Alice-Bob-Eve" model, where Eve serves as a spoofer attempting to impersonate the legitimate transmitter Alice and inject messages into the legitimate transmission from Alice to the intended receiver Bob. We assume that two messages are received by Bob at two successive time slots. The first message is sent from Alice while the second message is sent from an uncertain transmitter Alice or Eve. The objective of physical layer authentication is exploiting the physical layer information obtained by Bob to determine if the second message is still sent from Alice. Suppose Alice, Bob and Eve are geographically located at different positions. According to propagation theory [32], the characteristics of the propagation channel between Alice and Bob is independent of that of the channel between Eve and Bob due to the rapid spatial decorrelation. Additionally, in real mobile radio environments, the wireless channel is varying significantly with time. However, the channel parameters, such as channel coefficient and path delays, vary slowly on a symbol-by-symbol basis. In other words, the channel coefficient and path delay are highly correlated to their counterparts at adjacent time instant, respectively. Therefore, this spatial decorrelation and temporal correlation properties of wireless channels can be used to distinguish Alice from Eve.

Next, a time-varying multipath channel model is first introduced, and then the temporal channel variation is modeled on a symbol-by-symbol basis. Additionally, we assume that only noisy version of CSI is available at Bob and it can be obtained using various channel estimation

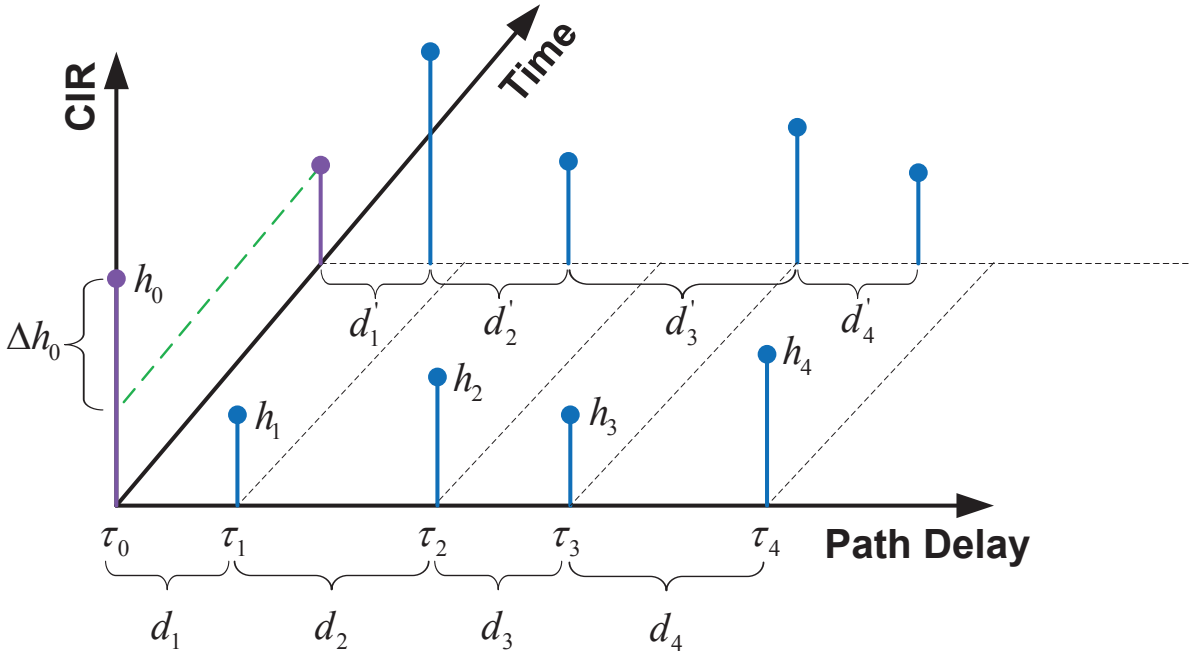

Figure 5.1: Channel model and channel variations in the dimensions of amplitude and time delay.

techniques [106]. The modeling of channel estimates is described, and a binary hypothesis is built based on a two dimensional quantization method.

5.2.1 Channel Model and Variations

Figure 5.1 shows our multipath channel model consisting of time-varying amplitude and propagation delay. It is a discrete-time representation of the CIR model of a time-varying multipath channel [107]. More specifically, the discrete-time CIR can be modeled as a superposition of a certain number of paths, each characterized by its amplitude and delay, that is,

$$c(n,\tau) = \sum_{l=0}^{L-1} h_l(n)\delta(\tau - \tau_l(n)), \tag{5.1}$$

where L is the total number of channel paths; h_l is the complex channel amplitude for the lth path; τ is the delay spread index, and τ_l is the corresponding propagation delay with $\tau_0 < \tau_1 < \cdots < \tau_{L-1}$. $\delta(\cdot)$ is the Dirac delta function. In a Rayleigh fading channel, the channel coefficient h_l can be modeled as a complex Gaussian random variable with zero mean and variance $\sigma^2_{h_l}$.

The paths are assumed to be statistically independent, and the average power is normalized, i.e., $\sum_{l=0}^{L-1} \sigma_{h_l}^2 = 1$. For simplifying the analysis, we assume that $\sigma_{h_0}^2 = \sigma_{h_1}^2 = \cdots = \sigma_{h_{L-1}}^2 = \sigma_h^2$.

Moreover, the propagation delay is described by Poisson process that models the arrival times of multipath components. Thus, the time interval between each pair of adjacent delays has an exponential distribution with parameter λ, which is defined by

$$d_i(n) \triangleq \tau_i(n) - \tau_{i-1}(n), \qquad i = 1, 2, \ldots, L-1. \tag{5.2}$$

It is important to note that the random variables $\{d_1, d_2, \cdots, d_{L-1}\}$ are assumed to be statistically independent to each other.

In real mobile radio environments, the temporal channel variation varies slowly on a symbol-by-symbol basis, although the motion of scatterers and terminals in the signal propagation environment results in time-varying multipath channels. In other words, the channel coefficients and propagation delays have the characteristics of high temporal correlation. Mathematically, the temporal variation of the channel coefficient h_l can be well described by an autoregressive model of order 1 (AR-1) [34], which is expressed by

$$h_l(n+1) = \zeta h_l(n) + \sqrt{(1-\zeta^2)\sigma_h^2}u(n), \tag{5.3}$$

where the AR coefficient ζ represents the correlation of two successive CIRs; and u is a zero-mean complex Gaussian random variable with variance one, which is independent of h_l.

Additionally, the temporal variation between adjacent propagation delays has not yet been statistically studied to the best of our knowledge. In this Chapter, considering the distribution of the interval between two time delays (which is exponentially distributed), we first model the ith time interval d_i defined in equation (5.2) as a sum of the squares of two independent normally distributed random variables. That is,

$$d_i(n) = (d_{R,i}(n))^2 + (d_{I,i}(n))^2, \tag{5.4}$$

where $d_{R,i}$ and $d_{I,i}$ are two independent normal random variables with mean zero and equal variance σ_d^2, i.e., $d_{R,i}, d_{I,i} \sim \mathrm{N}(0, \sigma_d^2)$. Therefore, d_i has an exponential distribution with parameter

$\lambda = \frac{1}{2\sigma_d^2}$, i.e., $d_i \sim \text{Exp}(\frac{1}{2\sigma_d^2})$.

Based on the developed model of the time interval d_i in equation (5.4), the time-variant propagation delay can be simply described by using the autoregressive models to model the two independent random variables $d_{R,i}$ and $d_{I,i}$. More specifically, the AR-1 model is also employed here to describe the temporal process of $d_{R,i}$ and $d_{I,i}$, respectively. Mathematically, they are formulated by

$$d_{R,i}(n+1) = \rho d_{R,i}(n) + \sqrt{(1-\rho^2)\sigma_d^2} v_R(n), \tag{5.5}$$

and

$$d_{I,i}(n+1) = \rho d_{I,i}(n) + \sqrt{(1-\rho^2)\sigma_d^2} v_I(n). \tag{5.6}$$

where ρ is an AR coefficient. v_R and v_I are two independent zero-mean complex Gaussian random variables with equal variance one, which are independent of $d_{R,i}$ and $d_{I,i}$.

5.2.2 Channel Estimates

In our scenario, we assume that only noisy version of CIR is available at Bob. Bob can obtain estimated CIR from the received messages based on channel estimation techniques. According to our channel model, a channel vector is obtained at Bob that consists of L independent channel coefficients $\{h_l, l = 0, 1, \ldots, L-1\}$ and $L-1$ independent time intervals $\{d_i, i = 1, 2, \ldots, L-1\}$.

To model the channel coefficient estimates at time instant n, we assume each channel coefficient is corrupted by an additive complex Gaussian noise. Thus, the lth channel coefficient estimate $\hat{h}_l$ is formulated as a sum of its actual value and a noise component. That is,

$$\hat{h}_l(n) \triangleq h_l(n) + w(n), \qquad l = 0, 1, \ldots, L-1. \tag{5.7}$$

where w is the complex Gaussian noise with mean zero and variance σ_w^2.

Moreover, using the same modeling of the time interval in equation (5.4), the time interval

estimate at time instant n can be expressed by

$$\hat{d}_i(n) \triangleq (\hat{d}_{R,i}(n))^2 + (\hat{d}_{I,i}(n))^2, \qquad i = 1, 2, \ldots, L-1. \tag{5.8}$$

where $\hat{d}_{R,i}$ and $\hat{d}_{I,i}$ are the estimation versions corresponding to $d_{R,i}$ and $d_{I,i}$, respectively. Considering the contributions of estimation errors, $\hat{d}_{R,i}$ and $\hat{d}_{I,i}$ are modeled by

$$\hat{d}_{R,i}(n) \triangleq d_{R,i}(n) + w_{R,i}(n), \tag{5.9}$$

and

$$\hat{d}_{I,i}(n) \triangleq d_{I,i}(n) + w_{I,i}(n), \tag{5.10}$$

where $w_{R,i}$ and $w_{I,i}$ are independent estimation errors that are both normally distributed with mean zero and equal variance $\frac{\sigma_w^2}{2}$. Since $d_{R,i}$ and $d_{I,i}$ are two independent normal random variables, it can be concluded that the sum of two independent normal random variables $\hat{d}_{R,i}$ and $\hat{d}_{I,i}$ are also independent normally distributed with mean zero and variance $\sigma_d^2 + \sigma_w^2/2$, i.e., $\hat{d}_{R,i}, \hat{d}_{I,i} \sim \mathrm{N}(0, \sigma_d^2 + \sigma_w^2/2)$. Therefore, the distribution of the time interval estimate $\hat{d}_i$ can be derived, which has an exponential distribution with parameter $\lambda' = \frac{1}{2\sigma_d^2+\sigma_w^2}$, i.e., $\hat{d}_i \sim \mathrm{Exp}(\frac{1}{2\sigma_d^2+\sigma_w^2})$.

In our scenario, the received message at Bob is either from the legitimate transmitter Alice or the spoofer Eve. As noted, the channel estimate from the previous received message is confirmed by Bob, which is achieved from the legitimate link. In order to distinguish Alice from Eve in the following sections, we define the subscripts "A" and "E" to represent the different transmitters Alice and Eve throughout this Chapter.

5.2.3 Hypothesis Testing based on 2-D Quantization

In this subsection, our proposed physical layer authentication scheme is formulated as a simple hypothesis testing problem, where a two-dimensional quantization approach is developed to simplify the decision rule for authentication. Specifically, two one-bit quantizers are utilized to quantize the differences between adjacent channel realizations in the dimensions of channel amplitude and time intervals. Mathematically, two random variables S_T and S_Z are

defined as the sum of outputs of one-bit quantizers Q_T and Q_Z, respectively. That is,

$$S_T \triangleq \sum_{l=0}^{L-1} O_{T,l}, \tag{5.11}$$

and

$$S_Z \triangleq \sum_{i=1}^{L-1} O_{Z,i}, \tag{5.12}$$

where

$$\begin{aligned} O_{T,l} &\triangleq Q_T\left[|T_l(n+1) - \hat{h}_{A,l}(n)|^2\right] \\ &= \begin{cases} 0, & |T_l(n+1) - \hat{h}_{A,l}(n)|^2 \le \delta_T, \\ 1, & otherwise, \end{cases} \end{aligned} \tag{5.13}$$

and

$$\begin{aligned} O_{Z,i} &\triangleq Q_Z\left[|Z_i(n+1) - \hat{d}_{A,i}(n)|\right] \\ &= \begin{cases} 0, & |Z_i(n+1) - \hat{d}_{A,i}(n)| \le \delta_Z, \\ 1, & otherwise. \end{cases} \end{aligned} \tag{5.14}$$

Herein, $Q_T[X]$ and $Q_Z[X]$ are two one-bit quantizers. For the lth component, $Q_T[X]$ produces $O_{T,l} = 1$ if input argument X is larger than a threshold δ_T, otherwise $O_{T,l} = 0$. Similarly, for the ith time interval, $Q_Z[X]$ produces $O_{Z,i} = 1$ if X is larger than a threshold δ_Z, otherwise $O_{Z,i} = 0$. The two thresholds δ_T and δ_Z have positive values. Thus, the values of S_T and S_Z can be easily determined, respectively, i.e., $0 \le S_T \le L$ and $0 \le S_Z \le L-1$. Moreover, $T_l(n+1)$ and $Z_i(n+1)$ are the current estimated channel coefficient and time interval from the legitimate

or spoofing link, while $\hat{h}_{A,l}(n)$ and $\hat{d}_{A,i}(n)$ are their counterparts achieved previously from the legitimate link.

Based on the developed two-dimensional quantization scheme, an authentication decision is made under a simple binary hypothesis testing. That is,

$$\begin{aligned} H_0 &: S \triangleq S_T + S_Z \leq K \\ H_1 &: S \triangleq S_T + S_Z > K, \end{aligned} \tag{5.15}$$

where S is the sum of the values of S_T and S_Z, and K is a non-negative integer between 0 and $(2L-1)$. H_0, the null hypothesis, stands for Alice as the claimant, while the alternative hypothesis, H_1, means the terminal is Eve.

5.3 Statistical Analysis of 2-D Quantization under Two Hypotheses

In this section, the proposed two-dimensional quantization scheme is statistically analyzed under a binary hypothesis testing. In order to achieve the distributions of the outputs of two binary quantizers under two hypotheses, we first need to find the distributions of the two quantizer inputs.

5.3.1 Under Hypothesis H_0

Under hypothesis H_0, the current channel measurements at Bob are still achieved from the legitimate link. Accordingly, the inputs to the two quantizers given in (5.13) and (5.14) are expressed, respectively, by

$$\Lambda_{T,H_0} \triangleq |\hat{h}_{A,l}(n+1) - \hat{h}_{A,l}(n)|^2, \tag{5.16}$$

and

$$\Lambda_{Z,H_0} \triangleq |\hat{d}_{A,i}(n+1) - \hat{d}_{A,i}(n)|. \tag{5.17}$$

To achieve the distribution of random variable Λ_{T,H_0}, we first derive the distribution of input argument of the absolute square operator in (5.16). It is defined by

$$\begin{aligned}\Delta h_{AA} &\triangleq \hat{h}_{A,l}(n+1) - \hat{h}_{A,l}(n) \\ &= (\zeta - 1)h_{A,l}(n) + \sqrt{(1-\zeta^2)\sigma^2_{h_A}}\,u(n) \\ &\quad + w_l(n+1) - w_l(n). \end{aligned} \tag{5.18}$$

Since random variables $h_{A,l}$, w_l and u have complex Gaussian distribution with mean zero, Δh_{AA} has zero-mean complex Gaussian distribution with variance $2(1-\zeta)\sigma^2_{h_A} + 2\sigma^2_w$. Consequently, the absolute square of Δh_A follows exponential distribution, that is

$$\Lambda_{T,H_0} = |\Delta h_{AA}|^2 \sim \text{Exp}\Big(\frac{1}{2(1-\zeta)\sigma^2_{h_A} + 2\sigma^2_w}\Big). \tag{5.19}$$

Similarly, in order to achieve the distribution of Λ_{Z,H_0}, we first define the input argument of the absolute value operator in equation (5.17) as Δd_{AA} and derive its distribution. That is,

$$\begin{aligned}\Delta d_{AA} &\triangleq \hat{d}_{A,i}(n+1) - \hat{d}_{A,i}(n) \\ &= (\hat{d}_{A,R,i}(n+1))^2 + (\hat{d}_{A,I,i}(n+1))^2 - (\hat{d}_{A,R,i}(n))^2 - (\hat{d}_{A,I,i}(n))^2 \\ &= (\underbrace{\hat{d}_{A,R,i}(n+1) - \hat{d}_{A,R,i}(n)}_{G_1}) \times (\underbrace{\hat{d}_{A,R,i}(n+1) + \hat{d}_{A,R,i}(n)}_{G_2}) \\ &\quad + (\underbrace{\hat{d}_{A,I,i}(n+1) - \hat{d}_{A,I,i}(n)}_{G_3}) \times (\underbrace{\hat{d}_{A,I,i}(n+1) + \hat{d}_{A,I,i}(n)}_{G_4}). \end{aligned} \tag{5.20}$$

Since $\hat{d}_{A,R,i}$ and $\hat{d}_{A,I,i}$ are two independent normal random variables with mean zero and variance $\sigma^2_d + \sigma^2_w/2$, random variables G_1, G_2, G_3 and G_4 have zero-mean normal distribution with difference variances $\sigma^2_{G_1}$, $\sigma^2_{G_2}$, $\sigma^2_{G_3}$ and $\sigma^2_{G_4}$, respectively. Based on the expressions given in equations (5.5), (5.6), (5.9) and (5.10), the variances $\sigma^2_{G_1}$, $\sigma^2_{G_2}$, $\sigma^2_{G_3}$ and $\sigma^2_{G_4}$ can be derived, respectively, by

$$\sigma^2_{G_1} = \sigma^2_{G_3} = 2\sigma^2_{d_A}(1-\rho) + \sigma^2_w, \tag{5.21}$$

and

$$\sigma^2_{G_2} = \sigma^2_{G_4} = 2\sigma^2_{d_A}(1+\rho) + \sigma^2_w. \tag{5.22}$$

As $d_{A,R,i}$ and $d_{A,I,i}$ are normally distributed with zero mean and same variance, we can obtain that the expectations $\mathrm{E}\{G_1 \cdot G_2\}$ and $\mathrm{E}\{G_3 \cdot G_4\}$ are both zeros. Additionally, it is noticed that the correlation coefficient between random variables G_1 and G_2 is equal to that between G_3 and G_4. Using $\mathrm{E}\{G_1 \cdot G_2\} = \mathrm{E}\{G_3 \cdot G_4\} = 0$, it is concluded that G_1, G_2, G_3 and G_4 are independent from each other.

Using the variances of G_1, G_2, G_3 and G_4 derived in equations (5.21) and (5.22), the function Δd_{AA} in equation (5.20) can be further expressed by

$$\begin{aligned}
\Delta d_{AA} &= G_1 \cdot G_2 + G_3 \cdot G_4 \\
&= \sqrt{4\sigma^4_{d_A}(1-\rho^2) + 4\sigma^2_{d_A}\sigma^2_w + \sigma^4_w} \\
&\quad \times \Bigg[\underbrace{\frac{G_1}{\sqrt{2\sigma^2_{d_A}(1-\rho) + \sigma^2_w}}}_{X_1} \times \underbrace{\frac{G_2}{\sqrt{2\sigma^2_{d_A}(1+\rho) + \sigma^2_w}}}_{X_2} \\
&\quad + \underbrace{\frac{G_3}{\sqrt{2\sigma^2_{d_A}(1-\rho) + \sigma^2_w}}}_{X_3} \times \underbrace{\frac{G_4}{\sqrt{2\sigma^2_{d_A}(1+\rho) + \sigma^2_w}}}_{X_3} \Bigg].
\end{aligned} \tag{5.23}$$

Note that X_1, X_2, X_3 and X_4 are four independent Gaussian random variables with mean zero and variance one. Based on the distribution given in [108, eq.(6.5)], the probability density function (PDF) of random variable $X_1X_2 + X_3X_4$ can be derived by

$$f_{X_1X_2+X_3X_4}(x) = \frac{1}{2}e^{-\frac{|x|}{2}} = \begin{cases} \frac{1}{2}e^{\frac{x}{2}}, & x < 0, \\ \\ \frac{1}{2}e^{-\frac{x}{2}}, & x \geq 0. \end{cases} \tag{5.24}$$

Using the distribution given in equation (5.24), we can conclude that Δd_{AA} has a Laplace

distribution, and the absolute of Δd_{AA} follows exponential distribution. That is,

$$\Delta d_{AA} \sim \text{Laplace}\Big(0,\ \sqrt{4\sigma_{d_A}^4(1-\rho^2) + 4\sigma_{d_A}^2\sigma_w^2 + \sigma_w^4}\Big), \tag{5.25}$$

and

$$\Lambda_{Z,H_0} = |\Delta d_{AA}| \sim \text{Exp}\Big(\frac{1}{\sqrt{4\sigma_{d_A}^4(1-\rho^2) + 4\sigma_{d_A}^2\sigma_w^2 + \sigma_w^4}}\Big). \tag{5.26}$$

To sum up, under hypothesis H_0, random variables Λ_{T,H_0} and Λ_{Z,H_0} are both exponentially distritbuted with different parameters. That is,

$$\Lambda_{T,H_0} \sim \text{Exp}\Big(\frac{1}{2(1-\zeta)\sigma_{h_A}^2 + 2\sigma_w^2}\Big), \tag{5.27}$$

$$\Lambda_{Z,H_0} \sim \text{Exp}\Big(\frac{1}{\sqrt{4\sigma_{d_A}^4(1-\rho^2) + 4\sigma_{d_A}^2\sigma_w^2 + \sigma_w^4}}\Big). \tag{5.28}$$

Based on the obtained distributions in equations (5.27) and (5.28), under hypothesis H_0, the probabilities that two quantizers have one output value can be derived, respectively, by

$$\begin{aligned} P_{T,H_0} &\triangleq P(Q_T[|T_l(n+1) - \hat{h}_{A,l}(n)|^2] = 1|H_0) \\ &= P(\Lambda_{T,H_0} > \delta_T) \\ &= e^{-\frac{\delta_T}{2(1-\zeta)\sigma_{h_A}^2 + 2\sigma_w^2}}, \end{aligned} \tag{5.29}$$

and

$$\begin{aligned} P_{Z,H_0} &\triangleq P(Q_Z[|Z_i(n+1) - \hat{d}_{A,i}(n)|^2] = 1|H_0) \\ &= P(\Lambda_{Z,H_0} > \delta_Z) \\ &= e^{-\frac{\delta_Z}{\sqrt{4\sigma_{d_A}^4(1-\rho^2) + 4\sigma_{d_A}^2\sigma_w^2 + \sigma_w^4}}}. \end{aligned} \tag{5.30}$$

Consequently, the probabilities that two quantizers have zero output values can be ex-

pressed as well, respectively, by

$$\begin{aligned} &P(Q_T[|T_l(n+1)-\hat{h}_{A,l}(n)|^2]=0|H_0) \\ &= 1 - P_{T,H_0} \\ &= 1 - e^{-\frac{\delta_T}{2(1-\zeta)\sigma^2_{\hat{h}_A}+2\sigma^2_w}}, \end{aligned} \tag{5.31}$$

and

$$\begin{aligned} &P(Q_Z[|Z_i(n+1)-\hat{d}_{A,i}(n)|^2]=0|H_0) \\ &= 1 - P_{Z,H_0} \\ &= 1 - e^{-\frac{\delta_Z}{\sqrt{4\sigma^4_{d_A}(1-\rho^2)+4\sigma^2_{d_A}\sigma^2_w+\sigma^4_w}}}. \end{aligned} \tag{5.32}$$

5.3.2 Under Hypothesis H_1

Under hypothesis H_1, the current received signal at Bob is from the spoofer Eve. First of all, we also define two new random variables to express the differences of successive channel coefficients and time intervals, respectively. That is,

$$\Lambda_{T,H_1} \triangleq |\hat{h}_{E,l}(n+1) - \hat{h}_{A,l}(n)|^2, \tag{5.33}$$

and

$$\Lambda_{Z,H_1} \triangleq |\hat{d}_{E,i}(n+1) - \hat{d}_{A,i}(n)|, \tag{5.34}$$

where $\hat{h}_{E,l}$ is denoted as the lth channel coefficient from Eve, and $\hat{d}_{E,i}$ is the ith time interval estimate from Eve.

To achieve the distribution of Λ_{T,H_1}, we first derive the distribution of the input argument

of the absolute square operator in (5.33). It is defined by

$$\begin{aligned}\Delta h_{EA} &\triangleq \hat{h}_{E,l}(n+1) - \hat{h}_{A,l}(n) \\ &= h_{E,l}(n+1) - h_{A,l}(n) + w_l(n+1) - w_l(n). \end{aligned} \tag{5.35}$$

since $h_{E,l}$, $h_{A,l}$ and w_l are independent zero mean complex Gaussian random variables, Δh_{EA} also has zero mean complex Gaussian distribution with variance $\sigma^2_{h_E} + \sigma^2_{h_A} + 2\sigma^2_w$. Thus, we can easily obtain that the square absolute of Δh_E follows exponential distribution, that is,

$$\Lambda_{T,H_1} = |\Delta h_{EA}|^2 \sim \text{Exp}\Big(\frac{1}{\sigma^2_{h_E} + \sigma^2_{h_A} + 2\sigma^2_w}\Big). \tag{5.36}$$

Similarly, in order to achieve the distribution of Λ_{Z,H_1}, we first define the input argument of the absolute value operator in equation (5.34) as Δd_{AE} and derive its distribution. That is,

$$\begin{aligned}\Delta d_{EA} &\triangleq \hat{d}_{E,i}(n+1) - \hat{d}_{A,i}(n) \\ &= \hat{d}^2_{E,R,i}(n+1) + \hat{d}^2_{E,I,i}(n+1) - \hat{d}^2_{A,R,i}(n) - \hat{d}^2_{A,I,i}(n) \\ &= (\hat{d}_{E,R,i}(n+1) - \hat{d}_{A,R,i}(n)) \times (\hat{d}_{E,R,i}(n+1) + \hat{d}_{A,R,i}(n)) \\ &\quad + (\hat{d}_{E,I,i}(n+1) - \hat{d}_{A,I,i}(n)) \times (\hat{d}_{E,I,i}(n+1) + \hat{d}_{A,I,i}(n)), \end{aligned} \tag{5.37}$$

since $\hat{d}_{E,i}$ and $\hat{d}_{A,i}$ are independent exponential random variables, we can obtain the distribution of Δd_{EA} based on the results in subsection 5.3.1. Hence, the absolute of Δd_{EA} also has exponential distribution, that is,

$$\Lambda_{Z,H_1} = |\Delta d_{EA}| \sim \text{Exp}\Big(\frac{1}{\sigma^2_{d_E} + \sigma^2_{d_A} + \sigma^2_w}\Big). \tag{5.38}$$

To sum up, under hypothesis H_1, the absolute square of difference of channel coefficients and the absolute of difference of time intervals are both exponentially distritbuted with different

parameters. That is,

$$\Lambda_{T,H_1} \sim \text{Exp}\Big(\frac{1}{\sigma^2_{h_E} + \sigma^2_{h_A} + 2\sigma^2_w}\Big), \tag{5.39}$$

$$\Lambda_{Z,H_1} \sim \text{Exp}\Big(\frac{1}{\sigma^2_{d_E} + \sigma^2_{d_A} + \sigma^2_w}\Big). \tag{5.40}$$

Using the achieved results in equations (5.39) and (5.40), under hypothesis H_1, the probabilities that two quantizers have one output values can be derived, respectively, by

$$\begin{aligned} P_{T,H_1} &\triangleq P(Q_T[|T_l(n+1) - \hat{h}_{A,l}(n)|^2] = 1|H_1) \\ &= P(|\hat{h}_{E,l}(n+1) - \hat{h}_{A,l}(n)|^2 > \delta_T) \\ &= e^{-\frac{\delta_T}{\sigma^2_{h_E} + \sigma^2_{h_A} + 2\sigma^2_w}}. \end{aligned} \tag{5.41}$$

and

$$\begin{aligned} P_{Z,H_1} &\triangleq P(Q_Z[|Z_i(n+1) - \hat{d}_{A,i}(n)|^2] = 1|H_1) \\ &= P(|\hat{d}_{E,i}(n+1) - \hat{d}_{A,i}(n)| > \delta_Z) \\ &= e^{-\frac{\delta_Z}{\sigma^2_{d_E} + \sigma^2_{d_A} + \sigma^2_w}}. \end{aligned} \tag{5.42}$$

Consequently, the probabilities that two quantizers have zero output values can be expressed, respectively, by

$$\begin{aligned} &P(Q_T[|T_l(n+1) - \hat{h}_{A,l}(n)|^2] = 1|H_1) \\ &\quad = 1 - P_{T,H_1} \\ &\quad = 1 - e^{-\frac{\delta_T}{\sigma^2_{h_E} + \sigma^2_{h_A} + 2\sigma^2_w}}. \end{aligned} \tag{5.43}$$

and

$$\begin{aligned} &P(Q_Z[|Z_i(n+1)-\hat{d}_{A,i}(n)|^2]=1|H_1) \\ &\quad = 1 - P_{Z,H_1} \\ &\quad = 1 - e^{-\frac{\delta_Z}{\sigma^2_{d_E}+\sigma^2_{d_A}+\sigma^2_w}}. \end{aligned} \tag{5.44}$$

5.4 Performance Analysis for Authentication

In this section, the performance in terms of FAR and PD are analyzed and their closed-form expressions are derived as well. In order to find optimal parameters, an optimization problem is defined and the optimal values are obtained by using exhaustive search method.

5.4.1 Derivation of FAR and PD

To analyze the authentication performance, we define FAR and PD based on our defined binary hypothesis testing given in (5.15). In particular, FAR and PD are defined, respectively, by

$$\begin{aligned} P_{fa} &\triangleq P(S > K|H_0) \\ &= P(S = K+1 \; or \; S = K+2 \; or \; \cdots \; S = 2L-1|H_0) \\ &= P(S = K+1|H_0) + P(S = K+2|H_0) \\ &\quad + \cdots + P(S = 2L-1|H_0) \\ &= \sum_{k=K+1}^{2L-1} P(S = k|H_0), \end{aligned} \tag{5.45}$$

and

$$\begin{aligned}
P_d &\triangleq P(S > K|H_1) \\
&= 1 - P(S \leq K|H_1) \\
&= 1 - P(S = 0 \; or \; S = 1 \; or \; \cdots \; S = K|H_1) \\
&= 1 - \Big[P(S = 0|H_1) + P(S = 1|H_1) \\
&\quad + \cdots + P(S = K|H_1)\Big] \\
&= 1 - \sum_{k=0}^{K} P(S = k|H_1). \qquad (5.46)
\end{aligned}$$

In order to derive FAR and PD shown in equations (5.45) and (5.46), we can use the results given in equations (A.3) and (A.4) from Appendix A. In our case, the probabilities P_T and P_Z in equations (A.3) and (A.4) are expressed based on different equations under the two hypotheses H_0 and H_1. In particular, P_{T,H_0} and P_{Z,H_0} in equations (5.29) and (5.30) are used in the derivation of FAR, while P_{T,H_1} and P_{Z,H_1} in (5.41) and (5.42) are used in the derivation of PD.

According to Appendix A, we also consider two cases for the derivations of FAR and PD based on different value of K. Specifically, in the case that K is smaller than $L-1$, the FAR and PD can be further derived, respectively, by

$$\begin{aligned}
P_{fa} &= \sum_{k=K+1}^{2L-1} P(S = k|H_0) \\
&= \sum_{k=K+1}^{L-1} P(S = k|H_0) + \sum_{k=L}^{2L-1} P(S = k|H_0) \\
&= \sum_{k=K+1}^{L-1} \sum_{v=0}^{k} \binom{L}{v} (P_{T,H_0})^v (1 - P_{T,H_0})^{L-v} \\
&\quad \times \binom{L-1}{k-v} (P_{Z,H_0})^{k-v} (1 - P_{Z,H_0})^{L-1-k+v} \\
&\quad + \sum_{k=L}^{2L-1} \sum_{v=k-L}^{L-1} \binom{L}{k-v} (P_{T,H_0})^{k-v} (1 - P_{T,H_0})^{L-k+v} \\
&\quad \times \binom{L-1}{v} (P_{Z,H_0})^{v} (1 - P_{Z,H_0})^{L-1-v}, \qquad (5.47)
\end{aligned}$$

and

$$\begin{aligned} P_d &= 1 - \sum_{k=0}^{K} P(S = k|H_1) \\ &= 1 - \sum_{k=0}^{K} \sum_{v=0}^{k} \binom{L}{v} (P_{T,H_1})^v (1 - P_{T,H_1})^{L-v} \\ &\quad \times \binom{L-1}{k-v} (P_{Z,H_1})^{k-v} (1 - P_{Z,H_1})^{L-1-k+v}. \end{aligned} \tag{5.48}$$

Additionally, when K is equal or larger than $L-1$, the closed-form expressions for the FAR and PD are expressed, respectively, by

$$\begin{aligned} P_{fa} &= \sum_{k=K+1}^{2L-1} P(S = k|H_0) \\ &= \sum_{k=K+1}^{2L-1} \sum_{v=k-L}^{L-1} \binom{L}{k-v} (P_{T,H_0})^{k-v} (1 - P_{T,H_0})^{L-k+v} \\ &\quad \times \binom{L-1}{v} (P_{Z,H_0})^v (1 - P_{Z,H_0})^{L-1-v}, \end{aligned} \tag{5.49}$$

and

$$\begin{aligned} P_d &= 1 - \sum_{k=0}^{K} P(S = k|H_1) \\ &= 1 - \left\{ \sum_{k=0}^{L-1} P(S = k|H_1) + \sum_{k=L}^{K} P(S = k|H_1) \right\} \\ &= 1 - \left\{ \sum_{k=0}^{L-1} \sum_{v=0}^{k} \binom{L}{v} (P_{T,H_1})^v (1 - P_{T,H_1})^{L-v} \right. \\ &\quad \times \binom{L-1}{k-v} (P_{Z,H_1})^{k-v} (1 - P_{Z,H_1})^{L-1-k+v} \\ &\quad + \sum_{k=L}^{K} \sum_{v=k-L}^{L-1} \binom{L}{k-v} (P_{T,H_1})^{k-v} (1 - P_{T,H_1})^{L-k+v} \\ &\quad \left. \times \binom{L-1}{v} (P_{Z,H_1})^v (1 - P_{Z,H_1})^{L-1-v} \right\}. \end{aligned} \tag{5.50}$$

5.4.2 Parameter Optimization

As it can be seen from the derived equations of FAR and PD in subsection 5.4.1, we need to choose the parameters properly so that a high PD and low FAR can be achieved simultaneously. Towards this goal, the objective is to find the values of δ_T, δ_Z and K which maximize the PD subject to a false alarm constraint at the receiver Bob. Mathematically, our optimization problem can be expressed by

$$\begin{aligned} \max \quad & P_d \\ \text{subject to} \quad & P_{fa} \leq \theta \\ & \delta_T, \delta_Z \geq 0 \\ & 0 \leq K < 2L - 1, \end{aligned} \tag{5.51}$$

where θ is a constant value between 0 and 1. Generally, FAR P_{fa} is normally set below 0.1 for secure wireless communications. Two subfigures in Fig. 5.2 show the PD and FAR, respectively, under various threshold values of δ_T and δ_Z, where the value of threshold K is fixed. As it can be seen from this figure, PD and FAR are both increasing when the values of δ_T and δ_Z decrease. Therefore, we can first fix the value of θ, the optimal values δ_T^*, δ_Z^*, and K^* can be found by using exhaustive search method in the simulations.

5.5 Benchmark Method and Simulation Results

In this section, in order to evaluate the proposed scheme, a benchmark method is developed and its performance in detecting spoofers is analyzed as well. For achieving optimized performance in spoofing detection, exhaustive search method is used to find the optimal values of parameters in the simulations. Additionally, numerical results are given to verify the theoretical analysis and show the effectiveness of the proposed authentication scheme.

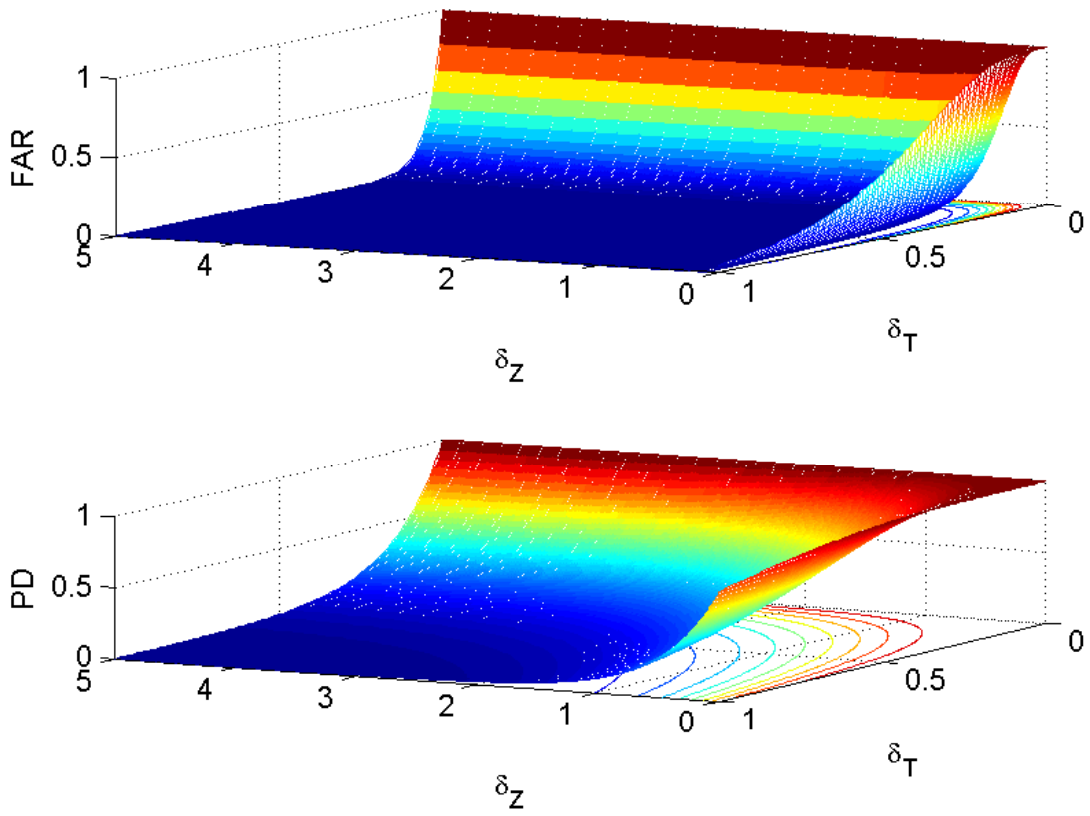

Figure 5.2: Probability of detection and false alarm rate under various threshold values of δ_T and δ_Z, respectively.

5.5.1 Performance Analysis for Benchmark Method

In this subsection, a benchmark scheme is developed for performance comparison in spoofing detection. The benchmark method is also formulated as a binary hypothesis testing problem. Mathematically, a test statistic for the benchmark scheme is developed based only on the difference of adjacent channel coefficients, that is,

$$S_B \triangleq \sum_{l=0}^{L-1} O_{B,l}, \tag{5.52}$$

where

$$\begin{aligned} O_{B,l} &\triangleq Q_B\left[|T_l(n+1) - \hat{h}_{A,l}(n)|^2\right] \\ &= \begin{cases} 0, & |T_l(n+1) - \hat{h}_{A,l}(n)|^2 \leq \delta_B, \\ \\ 1, & otherwise, \end{cases} \end{aligned} \tag{5.53}$$

Similarly, $Q_B[X]$ is an one-bit quantizer that produces $O_{B,l} = 1$ if X is larger than a threshold δ_B, otherwise $O_{B,l} = 0$. Based on the developed test statistic, an authentication decision is made under a binary hypothesis testing, that is,

$$\begin{aligned} H_0 &: S_B \leq K_B \\ H_1 &: S_B > K_B, \end{aligned} \tag{5.54}$$

where K_B is a threshold of the decision making for authentication in the benchmark scheme, and it is a non-negative integer between 0 and L. H_0, the null hypothesis, stands for Alice as the claimant, while the alternative hypothesis, H_1, means the terminal is Eve.

Based on the derived distributions in equations (5.27) and (5.39), under the two hypotheses,

the probabilities that the quantizer $Q_B[\cdot]$ has one output value can be derived, respectively, by

$$\begin{aligned} P_{B,H_0} &\triangleq P(Q_B[|T_l(n+1) - \hat{h}_l^A(n)|^2] = 1|H_0) \\ &= P(|\hat{h}_l^A(n+1) - \hat{h}_l^A(n)|^2 > \delta_T) \\ &= e^{-\frac{\delta_B}{2(1-\zeta)\sigma_{h_A}^2 + 2\sigma_w^2}}, \end{aligned} \tag{5.55}$$

and

$$\begin{aligned} P_{B,H_1} &\triangleq P(Q_B[|T_l(n+1) - \hat{h}_l^A(n)|^2] = 1|H_1) \\ &= P(|\hat{h}_l^E(n+1) - \hat{h}_l^A(n)|^2 > \delta_T) \\ &= e^{-\frac{\delta_B}{\sigma_{h_E}^2 + \sigma_{h_A}^2 + 2\sigma_w^2}}. \end{aligned} \tag{5.56}$$

Consequently, under the two hypotheses, the probabilities that the quantizer has zero output values can be expressed, respectively, by

$$\begin{aligned} &P(Q_B[|T_l(n+1) - \hat{h}_l^A(n)|^2] = 0|H_0) \\ &= 1 - P_{B,H_0} \\ &= 1 - e^{-\frac{\delta_B}{2(1-\zeta)\sigma_{h_A}^2 + 2\sigma_w^2}}, \end{aligned} \tag{5.57}$$

and

$$\begin{aligned} &P(Q_B[|T_l(n+1) - \hat{h}_l^A(n)|^2] = 0|H_1) \\ &= 1 - P_{B,H_1} \\ &= 1 - e^{-\frac{\delta_B}{\sigma_{h_E}^2 + \sigma_{h_A}^2 + 2\sigma_w^2}}. \end{aligned} \tag{5.58}$$

By using the derived result (A.1) in Appendix A, PD and FAR are defined and derived,

respectively, by

$$\begin{aligned} P_{fa} &\triangleq P(\tilde{\Lambda} > \delta_B | H_0) \\ &= \sum_{k=K_B+1}^{L} P(\tilde{\Lambda} = k | H_0) \\ &= \sum_{k=K_B+1}^{L} \binom{L}{k} (P_{B,H_0})^k (1 - P_{B,H_0})^{L-k}, \end{aligned} \tag{5.59}$$

and

$$\begin{aligned} P_d &\triangleq P(\tilde{\Lambda} > \delta_B | H_1) \\ &= \sum_{k=K_B+1}^{L} P(\tilde{\Lambda} = k | H_1) \\ &= \sum_{k=K_B+1}^{L} \binom{L}{k} (P_{B,H_1})^k (1 - P_{B,H_1})^{L-k}. \end{aligned} \tag{5.60}$$

In order to achieve optimized performance, the optimal values of δ_B and K_B can be determined by maximizing the PD subject to a false alarm constraint at Bob. Mathematically, the optimization problem corresponding to the benchmark method can be expressed by

$$\begin{aligned} \max \quad & P_d \\ \text{subject to} \quad & P_{fa} \leq \theta \\ & \delta_B \geq 0 \\ & 0 \leq K_B < L. \end{aligned} \tag{5.61}$$

The optimal values of δ_B and K_B, i.e., δ_B^* and K_B^*, can be found as well by using exhaustive search method in the simulations.

5.5.2 Numerical results

In this subsection, numerical simulations are used to verify the effectiveness of the proposed authentication scheme, and the performance of the proposed scheme is compared with

Table 5.1: Optimal values of parameters under different values of θ

θ	SNR=5dB					SNR=10dB				
	δ_T^*	δ_Z^*	δ_B^*	K^*	K_B^*	δ_T^*	δ_Z^*	δ_B^*	K^*	K_B^*
0.01	2.54	3.61	2.44	1	1	1.04	1.80	0.96	1	1
0.02	2.30	3.26	2.19	1	1	0.94	1.65	0.86	1	1
0.03	2.14	3.15	2.03	1	1	0.87	1.61	0.80	1	1
0.04	2.05	2.94	1.92	1	1	0.83	1.54	0.76	1	1
0.05	1.94	2.98	1.84	1	1	0.81	1.43	0.72	1	1
0.06	1.93	2.63	1.77	1	1	0.79	1.36	0.70	1	1
0.07	1.84	2.69	1.71	1	1	0.76	1.35	0.67	1	1
0.08	1.79	2.62	1.65	1	1	0.75	1.28	0.65	1	1
0.09	1.78	2.43	1.61	1	1	0.73	1.26	0.63	1	1
0.1	1.70	2.53	1.56	1	1	0.70	1.28	1.09	1	0

that of the benchmark method. In order to study the effect of propagation delays in authentication performance, we assume that the two correlation coefficients are $\zeta = 0.8$ and $\rho = 0.99$ throughout the simulations. Additionally, the number of channel paths L is fixed to be 5. For Monte-Carlo experiments, 10^6 independent trails are used to obtain the average results.

We first use the exhaustive search method to find the optimal values of parameters based on the optimization problems defined in (5.51) and (5.61), respectively. Table 5.1 and Table 5.2 show the optimal values of different thresholds under various values of θ and SNR, respectively. As it can be seen from the two tables, the optimal values are varying under different θ and SNRs. In table 5.1, it indicates that the optimal values δ_T^*, δ_Z^* and δ_B^* gradually decrease when the value of θ becomes larger. From Table 5.2, the values of δ_T^*, δ_Z^* and δ_B^* are also decreasing when SNR increases. As observed in Table 5.1 and Table 5.2, optimal value K^* is always 1 while the value of K_B^* becomes smaller at lager θ or SNR.

Figure 5.3 illustrates the FAR for different values of θ under the correspondingly calculated optimal values of thresholds. As for the proposed and benchmark schemes, the values of FAR is approximately equal to the values of θ, as it was expected. In Figure 5.4, it shows the FAR versus different SNRs based on the correspondingly optimized threshold values. As expected, the value of FAR is approximately equal to θ when SNR value is changing. Figures 5.3 and 5.4 indicate that the PD is maximized while the false alarm constraint is approximately met with equality.

Figure 5.5 shows the PD versus various values of θ under two different SNRs. As expected,

Table 5.2: Optimal values of parameters under different SNRs

SNR (dB)	$\theta = 0.05$					$\theta = 0.1$				
	δ_T^*	δ_Z^*	δ_B^*	K^*	K_B^*	δ_T^*	δ_Z^*	δ_B^*	K^*	K_B^*
4	2.39	3.39	2.26	1	1	2.09	2.90	1.92	1	1
6	1.64	2.36	1.50	1	1	1.40	2.18	1.28	1	1
8	1.12	1.86	1.03	1	1	0.99	1.58	0.87	1	1
10	0.81	1.43	0.72	1	1	0.70	1.28	1.09	1	0
12	0.59	1.23	0.95	1	0	0.53	1.02	0.80	1	0
14	0.46	1.05	0.74	1	0	0.42	0.85	0.62	1	0
16	0.38	0.91	0.60	1	0	0.33	0.81	0.51	1	0
18	0.33	0.82	0.52	1	0	0.29	0.71	0.44	1	0
20	0.30	0.75	0.46	1	0	0.27	0.63	0.39	1	0

the derived close-form expressions of PD are overlapping with the Monte-Carlo simulation results. As it can be seen from this figure, the proposed scheme outperforms the benchmark method. When the value of θ is fixed to be 0.1 and SNR is 10 dB, the probability of spoofing detection can reach to 0.65 in the proposed scheme that is 0.06 higher than that of the benchmark method.

In Figure 5.6, the PD is plotted for various SNRs under two different values of θ. The closed-form expressions of the proposed and benchmark schemes are overlapping with the Monte-Carlo simulation results, respectively. As observed, the proposed scheme outperforms the benchmark method especially at higher SNRs. Additionally, the performance in the case of $\theta = 0.1$ is better than that under $\theta = 0.05$, which can also be concluded from Figure 5.5.

5.6 Summary

In this Chapter, a novel channel-based physical layer authentication enhancement scheme has been proposed by exploiting the inherent two-dimensional properties of multipath fading channels. Specifically, the characteristics of channel amplitude and multipath time delay spread are integrated in order to enhance the authentication performance in the presence of spoofers. A two dimensional quantization algorithm has been proposed to preprocess the channel variations. Particularly, two one-bit quantizers were adopted to quantize the temporal channel variations in the dimensions of channel amplitude and time delay, respectively. By exploiting

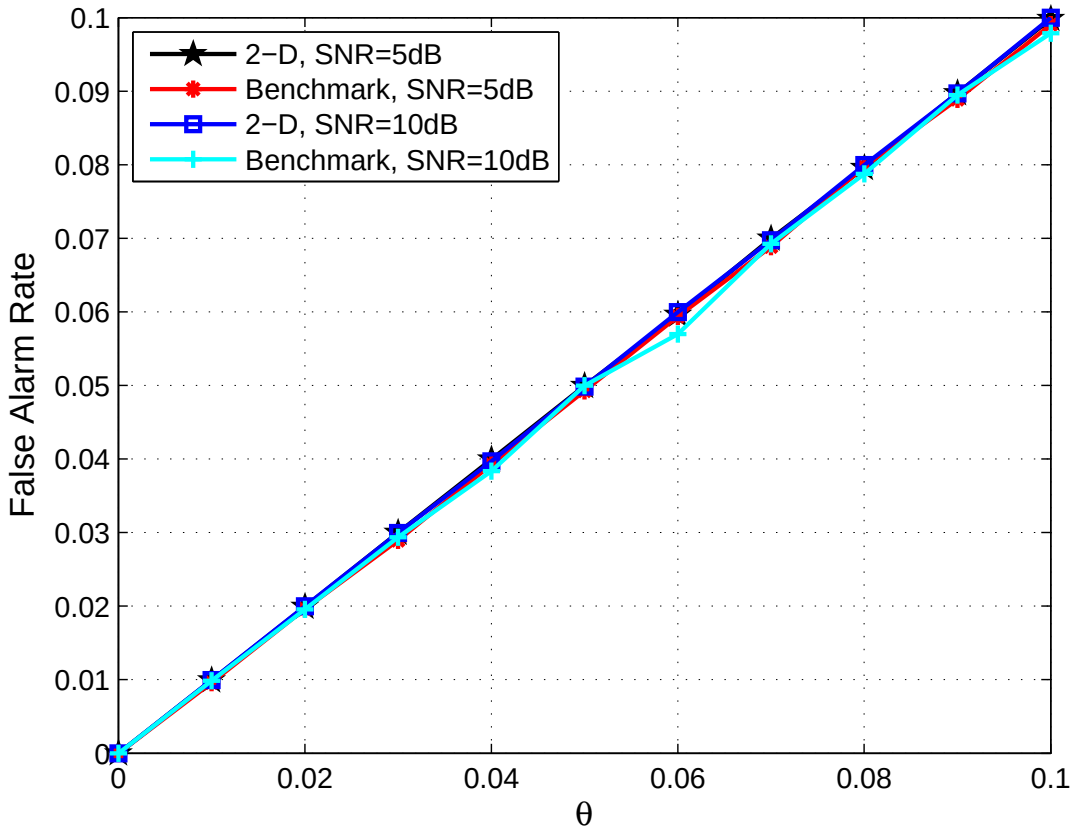

Figure 5.3: False alarm rate versus different values of θ under the optimized threshold values.

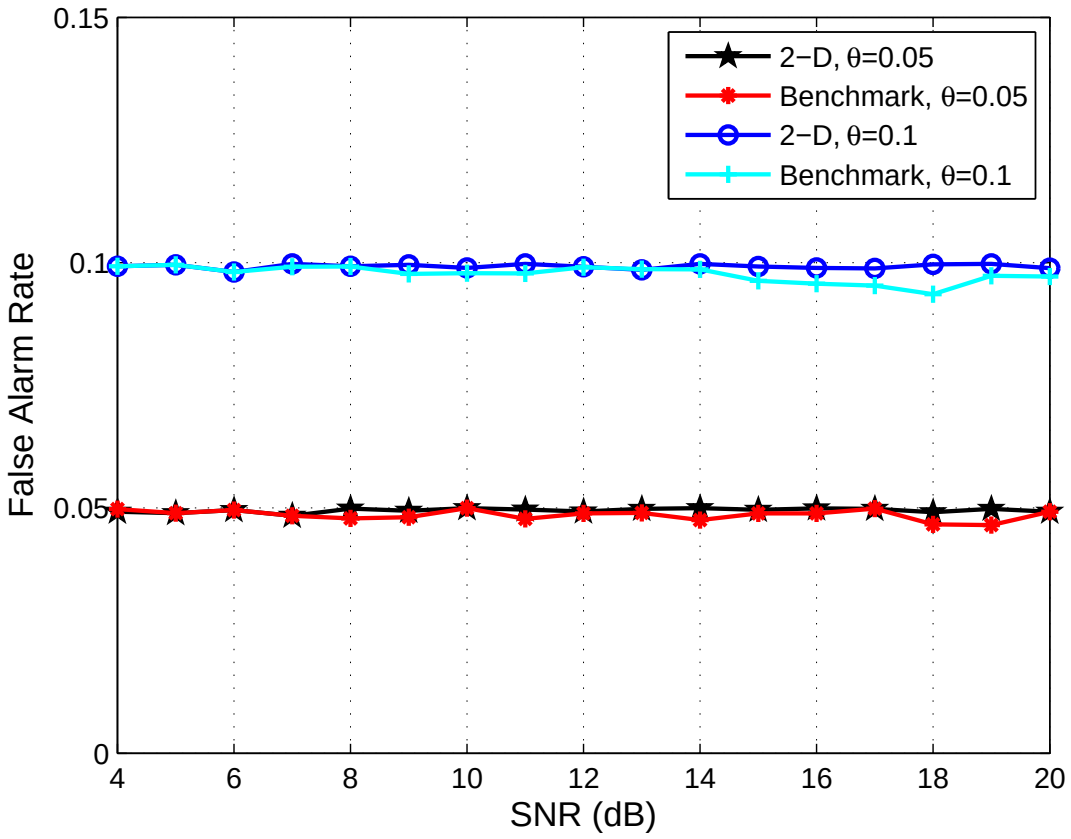

Figure 5.4: False alarm rate versus different SNRs under the optimized threshold values.

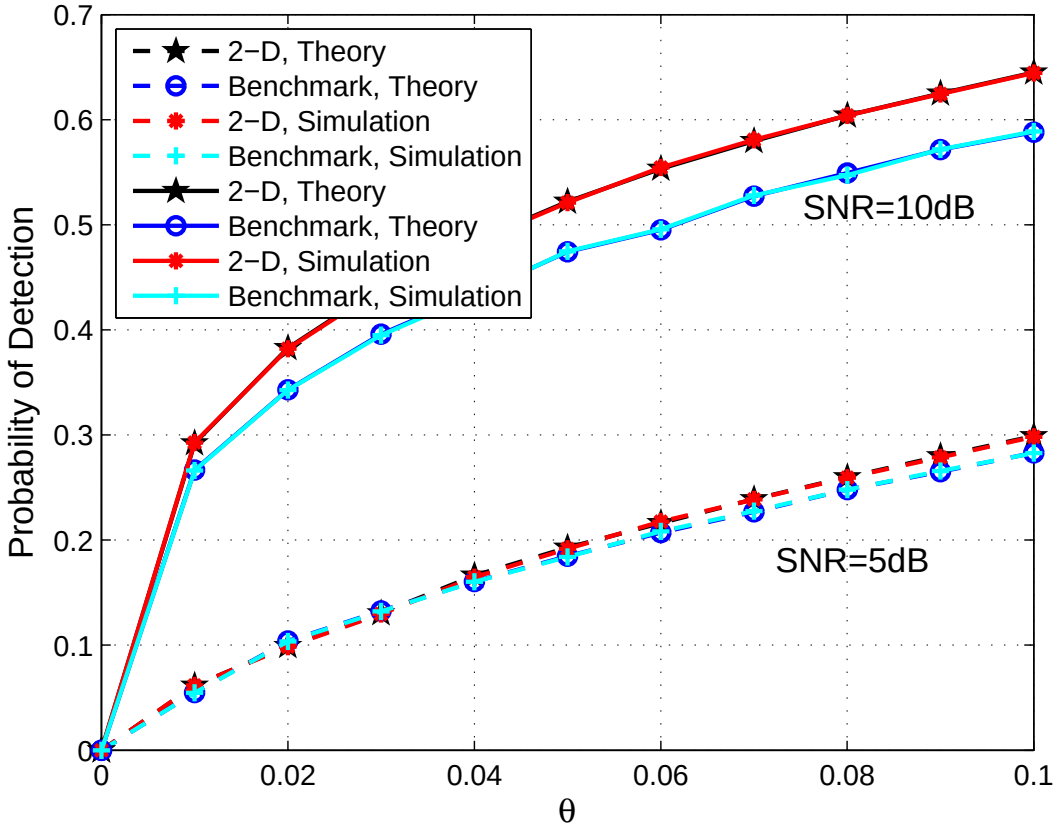

Figure 5.5: Probability of detection versus different values of θ under the comparison of theory and Monte Carlo.

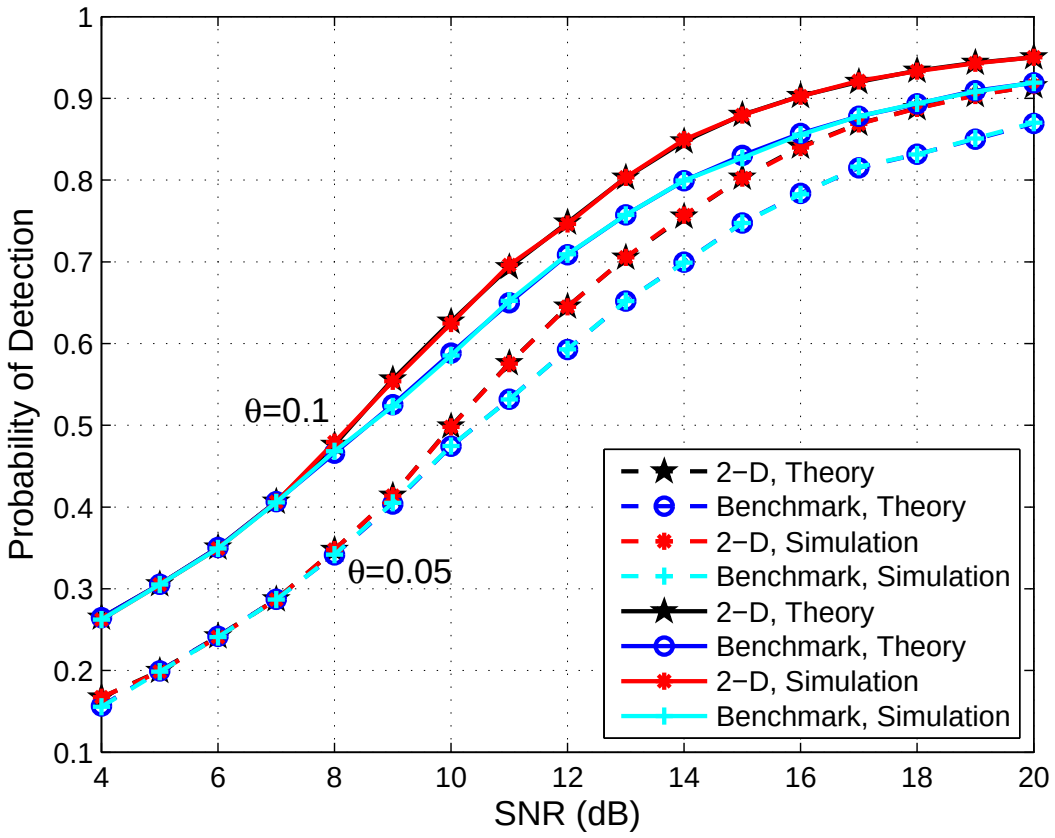

Figure 5.6: Probability of detection versus different SNRs under the comparison of theory and Monte Carlo.

the one-bit quantizers, the proposed authentication scheme has been formulated as a simpler hypothesis testing problem. For performance analysis, FAR and PD have been defined and their closed-form expressions have been derived as well. To assess the performance of the proposed authentication scheme, Monte-Carlo method has been used and the numerical results were compared with the theoretical derivations. Additionally, the optimal parameters of the proposed authentication technique were determined by utilizing exhaustive search method.

Chapter 6

Channel-based Authentication Enhancement Using AF Cooperative Relays

Traditional channel-based physical layer authentication techniques suffer from the problem of unreliable spoofing detection at low SNR. To address this issue, we propose a novel physical layer authentication scheme by exploiting the advantages of AF cooperative relaying in this Chapter. The essence of proposed scheme is to select the best relay among multiple AF relays, such that legitimate transmitter would experience better channel conditions than a spoofer. To achieve this goal, two best relay selection schemes are developed by maximizing the SNR ratios of the legitimate link to the spoofing link at the destination and relays, respectively. In the sequel, we derive closed-form expressions for the outage probabilities of effective SNR ratios at the destination. Additionally, our proposed authentication scheme is formulated as a hypothesis testing problem in order to discriminate the legitimate transmitter from the spoofer. A new test statistic is developed based on normalized channel difference between two adjacent end-to-end channel estimates at the destination. The performance of the proposed authentication scheme is compared with that of a direct transmission scheme. According to numerical results, the proposed scheme outperforms the benchmark method in terms of outage and spoofing detection.

6.1 Introduction

One major objective of information security is to protect information and systems from various malicious attacks. Authentication is a critical aspect of information security, which provides the process of verifying the identity of transmitters to prevent against spoofing attacks. In wireless communications, spoofing attack is one of the most serious security threats due to the absence of physical connections between a transmitter-receiver pair [19]. In order to address this issue, traditional cryptographic techniques have been established based on the exchange of secret keys between legitimate users. Generally, cryptographic algorithms are designed by relying on the computational hardness of mathematical functions. However, the computational complexity leads to a practical issue associated with key distribution and scalability. Additionally, traditional authentication approaches have been developed mainly based on the higher layers of protocol stack, which are vulnerable against adversaries due to the lack of physical layer protection. Due to these shortcomings, physical layer authentication has attracted significant attention in recent years, which is emerging as a new promising paradigm by exploiting the inherent characteristics of wireless channels for additional security protection [102].

A variety of channel-based physical layer authentication schemes has been proposed in the literature [8–10, 34, 104] by comparing adjacent channel estimates under a binary hypothesis testing in order to discriminate legitimate transmitter from potential adversaries. However, the detection performance of traditional channel-based physical layer authentication mechanisms is severely degraded under low SNR condition. In order to overcome this issue, multiple antenna techniques have been utilized [53]. By using multiple antennas, the dimension of signal space is increased, which in turn, results in improvements in authentication performance. However, as a result of cost and size limitations of multiple antennas, these scenarios are rarely implemented in practice.

Alternatively, cooperative relaying is another promising solution to the aforementioned issue of the existing channel-based authentication schemes. It is accomplished via user cooperation at the physical layer, through which signals are allowed to be transmitted between source and destination with the help of other nodes. Different variety of improving physical layer security through cooperating relays have been proposed in the literature [72, 73, 76, 118–126].

These approaches considered various design problems under different assumptions of CSI. Exploiting the advantages of cooperative relaying, researchers have showed improvements in physical layer security in terms of preventing eavesdropping attacks. However, the benefits of cooperative communications have not yet been fully utilized for physical layer protection against spoofing attacks to the best of our knowledge. Inspired by previous work that adopted user cooperation in physical layer security and its promised advantages, we develop a novel channel-based physical layer authentication scheme using cooperative relays in this Chapter.

Among those aforementioned relay-assisted physical layer security schemes, three cooperative transmission protocols are primarily considered, which are AF, DF and CJ. Specifically, the AF scheme is designed in which relays simply amplify the source signals and then retransmit them to the destination. In the DF scheme, relays first decode the source signals and then encode and forward them to the destination. As for the CJ scheme, the source transmits the data signal while all relays transmit jamming signals to interfere with eavesdroppers. Compared with DF and CJ, the AF relay scheme is more preferable for channel-based physical layer authentication due to its low-complexity processing at the relay nodes and destination as well. In this Chapter, we focus on the AF scheme.

Additionally, in order to obtain an efficient and practical physical layer authentication scheme through cooperative relays, relay selection is of significant importance. It refers to the process of choosing only one or more than one relay to help transmit messages between the source and destination. Accordingly, relay selection strategies can be generally classified into two categories, i.e., multiple-relay selection and single-relay selection. Compared to the multiple-relay selection, the single-relay selection is preferable in various scenarios [58, 59, 127]. Based on the selection of only one relay out of multiple available ones, single-relay selection schemes provide the best path between the source and destination. Although only one relay participates in the cooperative transmission, full order diversity can be achieved and the overhead is minimized due to orthogonal channels. Among existing best relay selection strategies for AF relaying systems, the instantaneous end-to-end SNR, which is seen as a well-defined system parameter, was widely utilized as a relay selection criterion [59]. However, in resource-constrained systems such as ad-hoc and sensor networks, only partial knowledge of the channel links is available to nodes. In [127], Krikidis *et al.* proposed a relay selection

algorithm based only on the instantaneous SNR of the channel link between the source and relays.

In this Chapter, a novel channel-based physical layer authentication scheme is proposed based on an AF cooperative relaying system. Only one relay out of multiple AF relays is chosen to provide the best end-to-end path between two legitimate end nodes in the presence of a spoofer. To achieve this goal, two best relay selection schemes are developed based on the notion of maximizing the instantaneous SNR ratios of the legitimate link to the spoofing link at the destination and relays, respectively. More specifically, in the first scheme, the best relay node is selected based on the maximum end-to-end SNR ratio. In order to reduce the computational complexity and resource consumption, the second scheme is developed based only on the first-hop instantaneous SNR ratio. For statistical analysis, we derive closed-form expressions for the outage probabilities of these two effective SNR ratios at the destination, respectively. Additionally, our proposed authentication scheme is formulated as a binary hypothesis testing problem, and a new test statistic is developed based on the normalized channel difference between two adjacent end-to-end channel estimates at the destination. The performance of our proposed authentication scheme is compared with that of a direct transmission scheme in terms of outage and spoofing detection.

The rest of this Chapter is organized as follows: In Section 6.2, the system model based on an AF cooperative relaying is described, and the benchmark scheme is explained as well. Section 6.3 illustrates the proposed best relay selection schemes. The closed-form expressions for the two outage probabilities are derived in Section 6.4, and the performance of spoofing detection is analyzed as well. In order to verify the statistical analysis, we illustrate the numerical results in Section 6.5, and summarize this Chapter in Section 6.6.

6.2 System Model Based on AF Cooperative Relaying

The proposed physical layer authentication using AF cooperative relays is shown in Figure 6.1, which consists of one legitimate transmitter (Alice), one destination (Bob) and M trusted available relay nodes in the presence of one spoofer (Eve). All nodes are located in spatially different positions and equipped with single antenna. From Figure 6.1, Alice delivers data

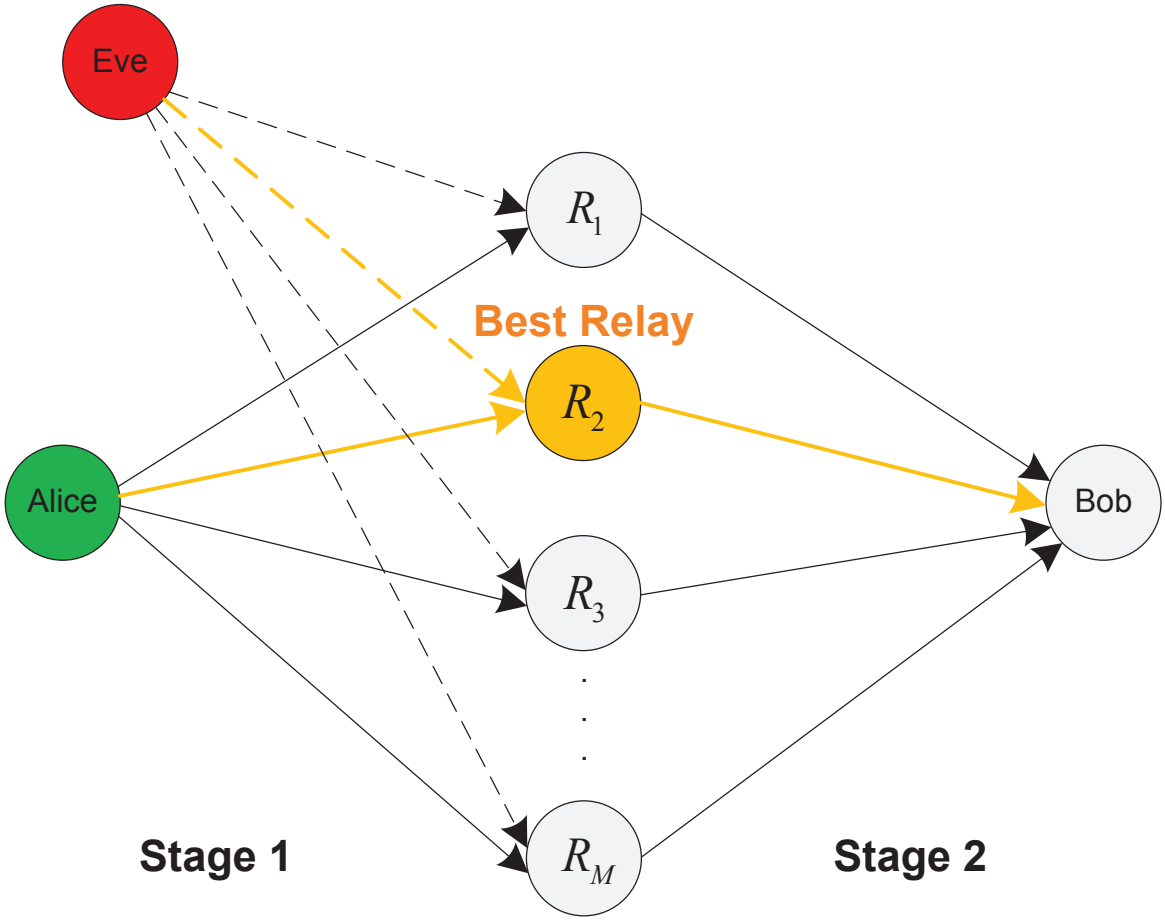

Figure 6.1: Our cooperative system with multiple relays under the "Alice-Bob-Eve" scenario. The best relay is selected based on the proposed relay selection schemes.

through the selected best relay to the intended receiver Bob. However, Eve serves as a spoofer attempting to impersonate the transmission from Alice, and sends spoofing signals to Bob via the best relay over different time slot. In order to study the performance of physical layer authentication through cooperative relays, we assume severe channel conditions between Alice and Bob. Also, we assume that Eve has the knowledge of the transmission protocol between Alice and Bob.

It is noteworthy to mention that traditional channel-based physical layer authentication is achieved based on channel temporal correlation in the legitimate link and spatial decorrelation between the legitimate and spoofing channels. In our scenario, we assume that the spacing between any nodes is large enough, thereby the wireless links between different nodes are

independent to each other. Also, the channel coefficient of each single-hop link is highly correlated over time and the temporal correlation can be described by an autoregressive model of order 1 (AR-1). Based on these two facts, Eve can be discriminated from Alice at Bob by comparing current channel estimate with the previous one. Mathematically, traditional channel-based physical layer authentication scheme can be formulated as a binary hypothesis testing problem. That is,

$$\begin{aligned} H_0 &: \hat{h}(n) = \hat{h}(n-1) \\ H_1 &: \hat{h}(n) \neq \hat{h}(n-1), \end{aligned} \tag{6.1}$$

where H_0, the null hypothesis, stands for Alice as the source, while the alternative hypothesis, H_1, means the source is the spoofer Eve. Moreover, $\hat{h}(n-1)$ and $\hat{h}(n)$ are both channel coefficient estimates at Bob, which are achieved from the previous and current symbols, respectively.

Next, a benchmark scheme is first described, and then our AF cooperative relaying scheme is explained. Particularly, the direct transmission scheme is employed as the benchmark scheme, in which the source transmits signals directly to the destination without the help of relays. Additionally, the designs of AF schemes can be found in [72, 118, 126, 128], however, our system model and problem description are different from these existing schemes.

6.2.1 Direct Transmission (DT)

In this subsection, the direct transmission (DT) scheme is described as the benchmark scheme. Specifically, the transmitted signal x with unit power (i.e., $E\{|x|^2\} = 1$ where $E\{\cdot\}$ denotes the expectation operator) is received directly by Bob, and the received signals at Bob from Alice/Eve can be written, respectively, by

$$y_{AB} = \sqrt{P_A + P_R} h_{AB} x + n_{AB}, \tag{6.2}$$

and

$$y_{EB} = \sqrt{P_E + P_R} h_{EB} x + n_{EB}, \tag{6.3}$$

where y_{AB} and y_{EB} are the received signals at Bob from Alice and Eve, respectively. Correspondingly, h_{AB} and h_{EB} are actual channel coefficients of the legitimate and spoofing links, respectively. Over a Rayleigh fading channel, h_{AB} and h_{EB} can be modeled as complex Gaussian random variables with zero mean and different variances σ^2_{AB} and σ^2_{EB}, respectively. Moreover, n_{AB} and n_{EB} are zero-mean complex Gaussian noises with equal variance $\tilde{\sigma}^2_n$. Additionally, P_A, P_E and P_R are the transmit powers of Alice, Eve and relays, respectively.

Based on the expressions of the received signals at Bob, the instantaneous SNRs of the legitimate and spoofing links can be expressed, respectively, by

$$\gamma_{AB} \triangleq \frac{(P_A + P_R)|h_{AB}|^2}{\tilde{\sigma}^2_n}, \tag{6.4}$$

and

$$\gamma_{EB} \triangleq \frac{(P_E + P_R)|h_{EB}|^2}{\tilde{\sigma}^2_n}. \tag{6.5}$$

Since the channel coefficients h_{AB} and h_{EB} are both modeled as zero-mean complex Gaussian random variables with different variances, the corresponding SNRs γ_{AB} and γ_{EB} are exponentially distributed with different values of parameter λ. Herein, λ is denoted as the reciprocal of the averaged SNR. The averaged values of γ_{AB} and γ_{EB} can be calculated, respectively, i.e., $\bar{\gamma}_{AB} \triangleq \frac{(P_A+P_R)\sigma^2_{AB}}{\tilde{\sigma}^2_n}$ and $\bar{\gamma}_{EB} \triangleq \frac{(P_E+P_R)\sigma^2_{EB}}{\tilde{\sigma}^2_n}$.

6.2.2 Amplify-and-Forward (AF)

As it can be seen from Figure 6.1, our AF-based cooperative transmission is conducted in two stages. In stage one, the source (Alice or Eve) broadcasts signal x to M relays at the first transmission slot. From different sources Alice/Eve, the received signals at the ith relay R_i can be expressed, respectively, by

$$y_{AR_i} = \sqrt{P_A} h_{AR_i} x + n_{AR_i}, \tag{6.6}$$

and

$$y_{ER_i} = \sqrt{P_E} h_{ER_i} x + n_{ER_i}, \tag{6.7}$$

where y_{AR_i} and y_{ER_i} are the received signals at relay R_i from Alice and Eve, respectively. Correspondingly, h_{AR_i} and h_{ER_i} are the actual channel coefficients of the links between the relay R_i and Alice/Eve, respectively. The channel coefficients h_{AR_i} and h_{ER_i} follow zero-mean complex Gaussian distributions with different variances $\sigma^2_{AR_i}$ and $\sigma^2_{ER_i}$, respectively. Additionally, n_{AR_i} and n_{ER_i} represent zero-mean complex Gaussian noises with equal variance σ^2_n.

Consequently, the instantaneous SNRs of the links between the relay R_i and different sources Alice/Eve can be expressed, respectively, by

$$\gamma_{AR_i} \triangleq \frac{P_A|h_{AR_i}|^2}{\sigma^2_n}, \tag{6.8}$$

and

$$\gamma_{ER_i} \triangleq \frac{P_E|h_{ER_i}|^2}{\sigma^2_n}. \tag{6.9}$$

Herein, the instantaneous SNRs γ_{AR_i} and γ_{ER_i} are also exponentially distributed with different parameters. Accordingly, the averaged values of γ_{AR_i} and γ_{ER_i} are derived by $\bar{\gamma}_{AR_i} \triangleq P_A\sigma^2_{AR_i}/\sigma^2_n$ and $\bar{\gamma}_{ER_i} \triangleq P_E\sigma^2_{ER_i}/\sigma^2_n$, respectively.

In stage two, the selected relay forwards the received signal to Bob at the second transmission slot. We assume that relays forward their signals over orthogonal channels, and forwarded signal from each relay to the destination is the multiplication of the received signal with an amplification factor K. Considering different sources Alice or Eve, K is defined, respectively, by

$$K_{AR_i} = \sqrt{\frac{1}{P_A\sigma^2_{AR_i} + \sigma^2_n}}, \tag{6.10}$$

and

$$K_{ER_i} = \sqrt{\frac{1}{P_E\sigma^2_{ER_i} + \sigma^2_n}}, \tag{6.11}$$

where K_{AR_i} and K_{ER_i} are the amplification factors applied on the received signals at relay R_i from Alice or Eve, respectively.

Consequently, the received signals at the destination Bob from Alice/Eve can be expressed,

respectively, as

$$\begin{aligned} y_{AR_iB} &= \sqrt{P_R} h_{R_iB} K_{AR_i} y_{AR_i} + n_{R_iB} \\ &= \sqrt{P_A P_R} K_{AR_i} h_{AR_i} h_{R_iB} x + \underbrace{\sqrt{P_R} K_{AR_i} h_{R_iB} n_{AR_i} + n_{R_iB}}_{n_D}, \end{aligned} \tag{6.12}$$

and

$$\begin{aligned} y_{ER_iB} &= \sqrt{P_R} h_{R_iB} K_{ER_i} y_{ER_i} + n_{R_iB} \\ &= \sqrt{P_E P_R} K_{ER_i} h_{ER_i} h_{R_iB} x + \underbrace{\sqrt{P_R} K_{ER_i} h_{R_iB} n_{ER_i} + n_{R_iB}}_{n_D}, \end{aligned} \tag{6.13}$$

where y_{AR_iB} and y_{ER_iB} are the received signals by Bob from different sources Alice/Eve through the relay R_i. Correspondingly, h_{R_iB} is the actual channel coefficient of the link between the relay R_i and Bob, which is modeled as a complex Gaussian random variable with zero mean and variance $\sigma^2_{R_iB}$. Also, n_{R_iB} is a zero-mean complex Gaussian noise with variance σ^2_n. In addition, n_D is the effective noise.

Consequently, based on the expressions of the received signals at Bob, the instantaneous end-to-end SNRs of the legitimate and spoofing links through the relay R_i can be derived, respectively, by

$$\gamma_{AR_iB} \triangleq \frac{P_A |h_{AR_i}|^2}{\sigma^2_n} \cdot \frac{P_R |h_{R_iB}|^2}{P_R |h_{R_iB}|^2 + (P_A \sigma^2_{AR_i} + \sigma^2_n)}, \tag{6.14}$$

and

$$\gamma_{ER_iB} \triangleq \frac{P_E |h_{ER_i}|^2}{\sigma^2_n} \cdot \frac{P_R |h_{R_iB}|^2}{P_R |h_{R_iB}|^2 + (P_E \sigma^2_{ER_i} + \sigma^2_n)}. \tag{6.15}$$

The essence of our proposed authentication scheme using AF cooperative relays is to select the best relay such that Alice would experience better channel conditions than Eve. Towards this goal, we propose two best relay selection schemes in the next section.

6.3 Best Relay Selection

In this section, two best relay selection schemes are developed. The best relay node is chosen based on the notion of maximizing the instantaneous SNR ratios of the legitimate link

to the spoofing link at the destination and relays, respectively. The instantaneous SNR ratios are derived based on the defined system model in the previous section.

More specifically, our first relay selection scheme is developed based on the instantaneous end-to-end SNR ratio of the legitimate link to the spoofing link at the destination through the ith relay node. By using the instantaneous end-to-end SNRs given in (6.14) and (6.15), the instantaneous end-to-end SNR ratio Γ_i is expressed by

$$\begin{aligned}\Gamma_i &= \frac{\gamma_{AR_iB}}{\gamma_{ER_iB}} \\ &= \frac{P_A|h_{AR_i}|^2}{P_E|h_{ER_i}|^2} \cdot \frac{P_R|h_{R_iB}|^2 + (P_E\sigma^2_{ER_i} + \sigma^2_n)}{P_R|h_{R_iB}|^2 + (P_A\sigma^2_{AR_i} + \sigma^2_n)}.\end{aligned} \tag{6.16}$$

However, taking into account all end-to-end links for the best relay selection increases the operational complexity and leads to a high resource consumption as well. Thus, the second relay selection scheme is developed based only on the knowledge of the first-hop link between the relays and different sources Alice/Eve. In our second relay selection scheme, the instantaneous first-hop SNR ratio Z_i is derived by using the instantaneous SNRs given in (6.8) and (6.9). That is,

$$\begin{aligned}Z_i &= \frac{\gamma_{AR_i}}{\gamma_{ER_i}} \\ &= \frac{P_A|h_{AR_i}|^2}{P_E|h_{ER_i}|^2}.\end{aligned} \tag{6.17}$$

Since the instantaneous SNRs γ_{AR_i} and γ_{ER_i} are exponentially distributed and they are independent to each other, the probability density function (PDF) and cumulative distribution function (CDF) of the instantaneous first-hop SNR ratio Z_i can be derived, respectively, by

$$f_{Z_i}(z) = \frac{\bar{\gamma}_{AR_i}\bar{\gamma}_{ER_i}}{(z\bar{\gamma}_{ER_i} + \bar{\gamma}_{AR_i})^2}, \tag{6.18}$$

and

$$F_{Z_i}(z) = P(Z_i \leq z) = \frac{z\bar{\gamma}_{ER_i}}{z\bar{\gamma}_{ER_i} + \bar{\gamma}_{AR_i}}. \tag{6.19}$$

It is interesting to note that the instantaneous end-to-end SNR ratio through the ith relay,

i.e., $\Gamma_i, i = 1, \cdots, M$, is related to the instantaneous first-hop SNR ratio at the ith relay, i.e., $Z_i, i = 1, \cdots, M$, through the following equation,

$$\Gamma_i = Z_i \cdot W_i, \tag{6.20}$$

where W_i is defined by

$$W_i = \frac{P_R|h_{R_iB}|^2 + (P_E\sigma^2_{ER_i} + \sigma^2_n)}{P_R|h_{R_iB}|^2 + (P_A\sigma^2_{AR_i} + \sigma^2_n)}. \tag{6.21}$$

In order to analyze the performance of the proposed relay selection schemes, we define an effective end-to-end SNR ratio as our performance metrics. Particularly, in the first relay selection scheme, the best relay is the one for which the end-to-end SNR ratio is maximum. Mathematically, the effective end-to-end SNR ratio of the first relay selection scheme is expressed by

$$S_{EF} = \Gamma_k \quad \text{where} \quad k = \arg\max_i \Gamma_i. \tag{6.22}$$

On the other hand, the best relay in the second scheme is the one for which the first-hop SNR ratio is maximum. Accordingly, the effective end-to-end SNR ratio of the second relay selection scheme is formulated by

$$S_{EF} = \Gamma_k \quad \text{where} \quad k = \arg\max_i Z_i. \tag{6.23}$$

In the next section, the performance of the proposed authentication scheme based on developed relay selection approaches is analyzed in terms of outage and spoofing detection, respectively.

6.4 Performance Analysis

In this section, the performances of outage and spoofing detection are analyzed respectively. The outage of effective end-to-end SNR ratios is defined based on equations in (6.22) and (6.23), and the closed-form expressions of the two outage probabilities are derived accordingly. Additionally, the authentication performance in terms of FAR and PD is defined and discussed as well.

6.4.1 Outage Analysis of First Relay Selection Scheme

In our scenario, the outage probability is defined as a probability of the effective end-to-end SNR ratio below a threshold δ. Mathematically, the outage probability of the first relay selection scheme can be formulated as

$$\begin{aligned} P_{out} &\triangleq P(S_{EF} \leq \delta) \\ &= P\left(\max\{\Gamma_1, \Gamma_2, \ldots, \Gamma_M\} \leq \delta\right) \\ &= \prod_{i=1}^{M} P(\Gamma_i \leq \delta), \end{aligned} \tag{6.24}$$

where S_{EF} is the effective end-to-end SNR ratio of the first scheme that is defined in (6.22). From the equation (6.24), the outage probability can be achieved based on the CDF of random variable Γ_i. Using the definition of Γ_i in equation (6.16), the CDF of Γ_i can be expressed by

$$\begin{aligned} F_{\Gamma_i}(z) &\triangleq P(\Gamma_i \leq z) \\ &= P\left(\frac{P_A|h_{AR_i}|^2}{P_E|h_{ER_i}|^2} \cdot \frac{P_R|h_{R_iB}|^2 + (P_E\sigma^2_{ER_i} + \sigma_n^2)}{P_R|h_{R_iB}|^2 + (P_A\sigma^2_{AR_i} + \sigma_n^2)} \leq z\right) \\ &= P\left(\frac{P_A|h_{AR_i}|^2}{P_E|h_{ER_i}|^2} \leq z\frac{P_R|h_{R_iB}|^2 + (P_A\sigma^2_{AR_i} + \sigma_n^2)}{P_R|h_{R_iB}|^2 + (P_E\sigma^2_{ER_i} + \sigma_n^2)}\right). \end{aligned} \tag{6.25}$$

Using the derived CDF of the SNR ratio Z_i given in equation (6.19), $F_{\Gamma_i}(z)$ in (6.25) can be further expressed as

$$\begin{aligned} F_{\Gamma_i}(z) &= E_{h_{R_iB}}\left\{\frac{z\frac{P_R|h_{R_iB}|^2 + (P_A\sigma^2_{AR_i} + \sigma_n^2)}{P_R|h_{R_iB}|^2 + (P_E\sigma^2_{ER_i} + \sigma_n^2)}\bar{\gamma}_{ER_i}}{z\frac{P_R|h_{R_iB}|^2 + (P_A\sigma^2_{AR_i} + \sigma_n^2)}{P_R|h_{R_iB}|^2 + (P_E\sigma^2_{ER_i} + \sigma_n^2)}\bar{\gamma}_{ER_i} + \bar{\gamma}_{AR_i}}\right\} \\ &= E_{h_{R_iB}}\left\{\frac{z\bar{\gamma}_{ER_i}}{z\bar{\gamma}_{ER_i} + \bar{\gamma}_{AR_i}} \cdot \frac{|h_{R_iB}|^2 + G_i}{|h_{R_iB}|^2 + L_i}\right\}, \end{aligned} \tag{6.26}$$

where G_i as well as L_i are defined for simplicity, respectively, as

$$G_i \triangleq \frac{1}{P_R}(P_A\sigma^2_{AR_i} + \sigma_n^2), \tag{6.27}$$

and

$$L_i \triangleq \frac{1}{P_R}\Big(\frac{P_A\sigma^2_{AR_i}+\sigma^2_n}{z\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}z\bar{\gamma}_{ER_i}+\frac{P_E\sigma^2_{ER_i}+\sigma^2_n}{z\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}\bar{\gamma}_{AR_i}\Big). \tag{6.28}$$

Since the power of absolute value of channel coefficient $|h_{R_iB}|^2$ is exponentially distributed, equation (6.26) can be further simplified as

$$\begin{aligned} F_{\Gamma_i}(z) &= \frac{z\bar{\gamma}_{ER_i}}{z\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}\Big(1+E_{h_{R_iB}}\Big\{\frac{(G_i-L_i)}{|h_{R_iB}|^2+L_i}\Big\}\Big) \\ &= \frac{z\bar{\gamma}_{ER_i}}{z\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}\Big(1+\int_0^\infty \frac{(G_i-L_i)}{(x+L_i)\sigma^2_{R_iB}}e^{-\frac{x}{\sigma^2_{R_iB}}}dx\Big). \end{aligned} \tag{6.29}$$

The integral term inside the equation (6.29) can be expressed in terms of exponential integral function, i.e., $\mathrm{Ei}(x) = -\int_{-x}^{\infty}\frac{1}{t}e^{-t}dt$, as follows

$$\begin{aligned} &\int_0^\infty \frac{(G_i-L_i)}{(x+L_i)\sigma^2_{R_iB}}e^{-\frac{x}{\sigma^2_{R_iB}}}dx \\ &\quad= \frac{G_i-L_i}{\sigma^2_{R_iB}}\int_{\frac{L_i}{\sigma^2_{R_iB}}}^\infty \frac{1}{t}e^{-(t-\frac{L_i}{\sigma^2_{R_iB}})}dt \\ &\quad= -\frac{(G_i-L_i)e^{L_i/\sigma^2_{R_iB}}}{\sigma^2_{R_iB}}\mathrm{Ei}\Big(-\frac{L_i}{\sigma^2_{R_iB}}\Big). \end{aligned} \tag{6.30}$$

Using the expression of the integral term in (6.30), the CDF of Γ_i can be expressed in closed form as

$$F_{\Gamma_i}(z) = \frac{z\bar{\gamma}_{ER_i}}{z\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}\cdot\left[1-\frac{(G_i-L_i)e^{\frac{L_i}{\sigma^2_{R_iB}}}}{\sigma^2_{R_iB}}\mathrm{Ei}\Big(-\frac{L_i}{\sigma^2_{R_iB}}\Big)\right]. \tag{6.31}$$

By substituting the CDF of Γ_i in equation (6.24), the closed form expression of the outage probability can be expressed by

$$P_{out} = \prod_{i=1}^{M}\frac{\delta\bar{\gamma}_{ER_i}}{\delta\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}\cdot\left[1-\frac{(G_i-L_i)e^{\frac{L_i}{\sigma^2_{R_iB}}}}{\sigma^2_{R_iB}}\mathrm{Ei}\Big(-\frac{L_i}{\sigma^2_{R_iB}}\Big)\right]. \tag{6.32}$$

6.4.2 Outage Analysis of Second Relay Selection Scheme

In this subsection, we derive the outage probability of the second relay selection scheme. In the second relay selection scheme, the relay with the largest end-to-end SNR ratio is not always chosen due to the lack of CSI of the links between relays and Bob. Using the law of total probability, outage probability in this case can be expressed as

$$\begin{aligned} P_{out} &\triangleq P(S_{EF} \leq \delta) \\ &= \sum_{k=1}^{M} P(S_{EF} \leq \delta | k = \arg\max_i Z_i) P(k = \arg\max_i Z_i) \\ &= \sum_{k=1}^{M} P(\Gamma_k \leq \delta | k = \arg\max_i Z_i) P(k = \arg\max_i Z_i) \\ &= \sum_{k=1}^{M} P(\Gamma_k \leq \delta \text{ and } k = \arg\max_i Z_i), \end{aligned} \tag{6.33}$$

where S_{EF} is the effective end-to-end SNR ratio of the second scheme that is defined in (6.23). Replacing Γ_k with $Z_k W_k$ according to the equation (6.20), the outage probability above can be equivalently expressed as

$$\begin{aligned} P_{out} &= \sum_{k=1}^{M} P(Z_k W_k \leq \delta \text{ and } k = \arg\max_i Z_i) \\ &= \sum_{k=1}^{M} P(Z_k W_k \leq \delta \text{ and } Z_k \geq Z_i, i \neq k) \\ &= \sum_{k=1}^{M} E_{Z_k}\Big\{ P(W_k \leq \frac{\delta}{Z_k} \text{ and } Z_k \geq Z_i, i \neq k | Z_k) \Big\}. \end{aligned} \tag{6.34}$$

The last line in the chain of equations (6.34) is achieved by fixing the random variable Z_k in the kth summand of the second line and then finding statistical expectation with respect to Z_k in the kth summand. Due to the fact that all the random variables $Z_i, i = 1, \cdots, M$ and $W_i, i = 1, \cdots, M$ are statistically independent, the outage probability in (6.34) can be simplified

as

$$P_{out} = \sum_{k=1}^{M} E_{Z_k}\Big\{ \prod_{i=1,i\neq k}^{M} P(Z_i \leq Z_k)\cdot P(W_k \leq \frac{\delta}{Z_k}|Z_k)\Big\}$$
$$= \sum_{k=1}^{M} E_{Z_k}\Big\{ \prod_{i=1,i\neq k}^{M} \frac{Z_k\bar{\gamma}_{ER_i}}{Z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}\cdot P(W_k \leq \frac{\delta}{Z_k}|Z_k)\Big\}. \tag{6.35}$$

Let $\mathcal{S}$ denote the subset of M relays for which the average channel power between Alice and relay is better than that between Eve and the relay, i.e., $P_A\sigma^2_{AR_i} > P_E\sigma^2_{ER_i}$, and $\bar{\mathcal{S}}$ denote its complement. Additionally, the CDF of the random variable $W_i, i = 1,\cdots,M$ has been derived in the Appendix A. As a consequence, the outage probability in (6.35) can be recast by using the derived results in the Appendix A. That is,

$$\begin{aligned}
P_{out} &= \sum_{k\in\mathcal{S}} E_{Z_k}\Big\{ \prod_{i=1,i\neq k}^{M} \frac{Z_k\bar{\gamma}_{ER_i}}{Z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}\cdot P(W_k \leq \frac{\delta}{Z_k}|Z_k)\Big\} + \sum_{k\in\bar{\mathcal{S}}} E_{Z_k}\Big\{ \prod_{i=1,i\neq k}^{M} \frac{Z_k\bar{\gamma}_{ER_i}}{Z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}\cdot P(W_k \leq \frac{\delta}{Z_k}|Z_k)\Big\} \\
&= \sum_{k\in\mathcal{S}} \underbrace{\int_0^{\frac{\delta(P_A\sigma^2_{AR_k}+\sigma^2_n)}{P_E\sigma^2_{ER_k}+\sigma^2_n}} \prod_{i=1,i\neq k}^{M} \frac{z_k\bar{\gamma}_{ER_i}}{z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}} \times \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2} dz_k}_{I_{1,k}} \\
&\quad - \sum_{k\in\mathcal{S}} \underbrace{\int_{\delta}^{\frac{\delta(P_A\sigma^2_{AR_k}+\sigma^2_n)}{P_E\sigma^2_{ER_k}+\sigma^2_n}} \prod_{i=1,i\neq k}^{M} \frac{z_k\bar{\gamma}_{ER_i}}{z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}} \times \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2} e^{-\frac{\frac{\delta}{z_k}(P_A\sigma^2_{AR_k}+\sigma^2_n)-(P_E\sigma^2_{ER_k}+\sigma^2_n)}{(1-\frac{\delta}{z_k})\sigma^2_{R_k}BP^2_R}} dz_k}_{I_{2,k}} \\
&\quad + \sum_{k\in\bar{\mathcal{S}}} \underbrace{\int_{\frac{\delta(P_A\sigma^2_{AR_k}+\sigma^2_n)}{P_E\sigma^2_{ER_k}+\sigma^2_n}}^{\delta} \prod_{i=1,i\neq k}^{M} \frac{z_k\bar{\gamma}_{ER_i}}{z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}} \times \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2} e^{-\frac{\frac{\delta}{z_k}(P_A\sigma^2_{AR_k}+\sigma^2_n)-(P_E\sigma^2_{ER_k}+\sigma^2_n)}{(1-\frac{\delta}{z_k})\sigma^2_{R_k}BP^2_R}} dz_k}_{I_{3,k}} \\
&\quad + \sum_{k\in\bar{\mathcal{S}}} \underbrace{\int_0^{\frac{\delta(P_A\sigma^2_{AR_k}+\sigma^2_n)}{P_E\sigma^2_{ER_k}+\sigma^2_n}} \prod_{i=1,i\neq k}^{M} \frac{z_k\bar{\gamma}_{ER_i}}{z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}} \times \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2} dz_k}_{I_{4,k}}.
\end{aligned} \tag{6.36}$$

In order to find a closed-form solution for outage probability in (6.36), we first find the

fractional decomposition of the following function, that is,

$$\begin{aligned} f_k(z_k) &\triangleq \prod_{i=1,i\neq k}^{M} \frac{z_k\bar{\gamma}_{ER_i}}{z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}} \times \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2} \\ &\triangleq \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2} \\ &\quad + \frac{\prod_{i=1,i\neq k}^{M}(z_k\bar{\gamma}_{ER_i}) - \prod_{i=1,i\neq k}^{M}(z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i})}{\prod_{i=1,i\neq k}^{M}(z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i})} \cdot \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2}. \end{aligned} \tag{6.37}$$

Since the degree of the polynomial in the denominator of the multiplicative term in the second line of (6.37) is less than that of the polynomial in the numerator of the same term, using partial fraction decompositions, it can be easily decomposed as

$$\frac{\prod_{i=1,i\neq k}^{M}(z_k\bar{\gamma}_{ER_i}) - \prod_{i=1,i\neq k}^{M}(z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i})}{\prod_{i=1,i\neq k}^{M}(z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i})} = \sum_{i=1,i\neq k}^{M} \frac{a_{k,i}}{z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}, \tag{6.38}$$

where $a_{k,i}$ is defined for simplicity as

$$a_{k,i} \triangleq \frac{\prod_{l=1,l\neq k}^{M}(-\frac{\bar{\gamma}_{AR_i}}{\bar{\gamma}_{ER_i}}\bar{\gamma}_{ER_l})}{\prod_{l=1,l\neq k,l\neq i}^{M}(-\frac{\bar{\gamma}_{AR_i}}{\bar{\gamma}_{ER_i}}\bar{\gamma}_{ER_l}+\bar{\gamma}_{AR_l})}. \tag{6.39}$$

By substituting (6.38) in (6.37), the function $f_k(z_k)$ can be equivalently expressed as

$$\begin{aligned} f_k(z_k) &= \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2} \\ &\quad + \sum_{i=1,i\neq k}^{M} \frac{a_{k,i}}{z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}} \times \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2}. \end{aligned} \tag{6.40}$$

By using the equation (6.40), $I_{1,k}$ and $I_{4,k}$ in the equation (6.36) can be derived in closed

form. It is interesting to note that the closed-form expression for $I_{4,k}$ is same as that for $I_{1,k}$. Therefore, $I_{1,k}$ and $I_{4,k}$ can be derived by

$$\begin{aligned}
I_{1,k} = I_{4,k} &= \int_0^{v_k} f_k(z_k) dz_k \\
&= \frac{1}{\bar{\gamma}_{ER_k}} \times \frac{-\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{z_k\bar{\gamma}_{ER_k} + \bar{\gamma}_{AR_k}}\Bigg]_0^{v_k} \\
&\quad + \sum_{i=1,i\neq k}^{M} \frac{\frac{\bar{\gamma}_{AR_k}}{\bar{\gamma}_{ER_k}} \times \frac{a_{k,i}}{\bar{\gamma}_{ER_i}}}{(\frac{\bar{\gamma}_{AR_k}}{\bar{\gamma}_{ER_k}} - \frac{\bar{\gamma}_{AR_i}}{\bar{\gamma}_{ER_i}})^2} \ln\left(\frac{z_k + \frac{\bar{\gamma}_{AR_i}}{\bar{\gamma}_{ER_i}}}{z_k + \frac{\bar{\gamma}_{AR_k}}{\bar{\gamma}_{ER_k}}}\right)\Bigg]_0^{v_k} \\
&\quad - \sum_{i=1,i\neq k}^{M} \frac{\frac{\bar{\gamma}_{AR_k}}{\bar{\gamma}_{ER_k}} \times \frac{a_{k,i}}{\bar{\gamma}_{ER_i}}}{(\frac{\bar{\gamma}_{AR_i}}{\bar{\gamma}_{ER_i}} - \frac{\bar{\gamma}_{AR_k}}{\bar{\gamma}_{ER_k}})} \times \frac{1}{z_k + \frac{\bar{\gamma}_{AR_k}}{\bar{\gamma}_{ER_k}}}\Bigg]_0^{v_k} \\
&= 1 - \frac{\varphi_k - \delta}{v_k + \varphi_k - \delta} + \sum_{i=1,i\neq k}^{M} \frac{a_{k,i}(\varphi_k - \delta)}{\bar{\gamma}_{ER_i}(\varphi_i - \varphi_k)^2} \times \ln\left(\frac{(\varphi_k - \delta)(v_k + \varphi_i - \delta)}{(\varphi_i - \delta)(v_k + \varphi_k - \delta)}\right) \\
&\quad - \sum_{i=1,i\neq k}^{M} \frac{a_{k,i}(\varphi_k - \delta)}{\bar{\gamma}_{ER_i}(\varphi_i - \varphi_k)}\left(\frac{1}{v_k + \varphi_k - \delta} - \frac{1}{\varphi_k - \delta}\right),
\end{aligned} \tag{6.41}$$

where v_k and φ_i are defined for simplicity, respectively, as

$$v_k \triangleq \frac{\delta(P_A\sigma^2_{AR_k} + \sigma_n^2)}{P_E\sigma^2_{ER_k} + \sigma_n^2}, \tag{6.42}$$

and

$$\varphi_i \triangleq \delta + \frac{\bar{\gamma}_{AR_i}}{\bar{\gamma}_{ER_i}}. \tag{6.43}$$

In what follows, we will find closed-form expressions for $I_{2,k}$ and $I_{3,k}$, respectively. Similarly, using the decomposed function $f_k(z_k)$ in (6.40), $I_{2,k}$ can be expressed as

$$\begin{aligned}
I_{2,k} &= \int_\delta^{v_k} f_k(z_k) \cdot e^{-\frac{\frac{\alpha_k}{z_k} - \beta_k}{1 - \frac{\delta}{z_k}}} dz_k \\
&= e^{\beta_k} \int_\delta^{v_k} \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k} + \bar{\gamma}_{AR_k})^2} e^{\frac{\beta_k\delta - \alpha_k}{z_k - \delta}} dz_k \\
&\quad + e^{\beta_k} \sum_{i=1,i\neq k}^{M} \int_\delta^{v_k} \frac{a_{k,i}}{z_k\bar{\gamma}_{ER_i} + \bar{\gamma}_{AR_i}} \times \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k} + \bar{\gamma}_{AR_k})^2} e^{\frac{\beta_k\delta - \alpha_k}{z_k - \delta}} dz_k,
\end{aligned} \tag{6.44}$$

where α_k and β_k are defined for simplicity, respectively, as

$$\alpha_k \triangleq \frac{\delta(P_A\sigma^2_{AR_k} + \sigma^2_n)}{P^2_R\sigma^2_{R_kB}}, \tag{6.45}$$

and

$$\beta_k \triangleq \frac{P_E\sigma^2_{ER_k} + \sigma^2_n}{P^2_R\sigma^2_{R_kB}}. \tag{6.46}$$

Using the change of the variable $t = z_k - \delta$, the first term of $I_{2,k}$ in (6.44) can be simplified and derived based on the result in (C.3) in the Appendix B. That is,

$$\begin{aligned}
&\int_{\delta}^{v_k} \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k} + \bar{\gamma}_{AR_k})^2} e^{\frac{\beta_k\delta-\alpha_k}{z_k-\delta}} dz_k \\
&= \int_0^{v_k-\delta} \frac{\varphi_k - \delta}{(t+\varphi_k)^2} e^{\frac{\beta_k\delta-\alpha_k}{t}} dt \\
&= \frac{(\varphi_k-\delta)}{\varphi_k} e^{\frac{\alpha_k-\beta_k\delta}{\varphi_k}} \left[\frac{\alpha_k - \beta_k\delta}{\varphi_k} \cdot \mathrm{Ei}\left(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_k-\delta)}{\varphi_k(v_k-\delta)} \right) \right. \\
&\quad \left. + \frac{v_k-\delta}{v_k+\varphi_k-\delta} \cdot e^{\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_k-\delta)}{\varphi_k(v_k-\delta)}} \right],
\end{aligned} \tag{6.47}$$

where $v_k > \delta$ and $(\beta_k\delta - \alpha_k) < 0$.

Moreover, using the changes of the variables $t = z_k - \delta$ and $s = \frac{1}{t}$, the second term of $I_{2,k}$ in (6.44) can be equivalently recast and derived based on the integrals [129, eq.(3.352.2)]

and [129, eq.(3.353.1)]. That is,

$$\begin{aligned}
&\sum_{i=1,i\neq k}^{M}\int_{\delta}^{v_k}\frac{a_{k,i}}{z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}}\cdot\frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}e^{\frac{\beta_k\delta-\alpha_k}{z_k-\delta}}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2}dz_k\\
&=\sum_{i=1,i\neq k}^{M}\int_{0}^{v_k-\delta}\frac{\frac{a_{k,i}}{\bar{\gamma}_{ER_i}}}{t+\varphi_i}\cdot\frac{\varphi_k-\delta}{(t+\varphi_k)^2}e^{\frac{\beta_k\delta-\alpha_k}{t}}dt\\
&=\sum_{i=1,i\neq k}^{M}\int_{\frac{1}{v_k-\delta}}^{\infty}\frac{\frac{a_{k,i}}{\bar{\gamma}_{ER_i}}s}{1+\varphi_i s}\cdot\frac{\varphi_k-\delta}{(1+\varphi_k s)^2}e^{(\beta_k\delta-\alpha_k)s}ds\\
&=\sum_{i=1,i\neq k}^{M}\frac{(\varphi_k-\delta)a_{k,i}}{\bar{\gamma}_{ER_i}}\Big[\int_{\frac{1}{v_k-\delta}}^{\infty}\frac{\frac{-\varphi_i}{(\varphi_i-\varphi_k)^2}}{1+\varphi_i s}e^{(\beta_k\delta-\alpha_k)s}ds\\
&+\int_{\frac{1}{v_k-\delta}}^{\infty}\frac{\frac{\varphi_k}{(\varphi_k-\varphi_i)^2}}{1+\varphi_k s}e^{(\beta_k\delta-\alpha_k)s}ds+\int_{\frac{1}{v_k-\delta}}^{\infty}\frac{\frac{-1}{(\varphi_k-\varphi_i)}}{(1+\varphi_k s)^2}e^{(\beta_k\delta-\alpha_k)s}ds\Big]\\
&=\sum_{i=1,i\neq k}^{M}\frac{(\varphi_k-\delta)a_{k,i}}{\bar{\gamma}_{ER_i}}\Big\{\frac{e^{\frac{\alpha_k-\beta_k\delta}{\varphi_i}}}{(\varphi_i-\varphi_k)^2}\mathrm{Ei}\Big(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_i-\delta)}{\varphi_i(v_k-\delta)}\Big)\\
&-\frac{1}{(\varphi_k-\varphi_i)^2}e^{\frac{\alpha_k-\beta_k\delta}{\varphi_k}}\mathrm{Ei}\Big(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_k-\delta)}{\varphi_k(v_k-\delta)}\Big)\\
&+\frac{1}{\varphi_k^2(\varphi_i-\varphi_k)}\Big[\frac{\varphi_k(v_k-\delta)}{v_k+\varphi_k-\delta}\cdot e^{\frac{\alpha_k-\beta_k\delta}{\delta-v_k}}+(\alpha_k-\beta_k\delta)e^{\frac{\alpha_k-\beta_k\delta}{\varphi_k}}\mathrm{Ei}\Big(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_k-\delta)}{\varphi_k(v_k-\delta)}\Big)\Big]\Big\}. \quad (6.48)
\end{aligned}$$

By combining the derived results shown in equations (6.47) and (6.48), the closed-form expression for $I_{2,k}$ can be written as

$$\begin{aligned}
I_{2,k}=e^{\beta_k}\Big\{&\frac{(\varphi_k-\delta)}{\varphi_k}e^{\frac{\alpha_k-\beta_k\delta}{\varphi_k}}\Big[\frac{\alpha_k-\beta_k\delta}{\varphi_k}\mathrm{Ei}\Big(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_k-\delta)}{\varphi_k(v_k-\delta)}\Big)+\frac{e^{\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_k-\delta)}{\varphi_k(v_k-\delta)}}}{1+\frac{\varphi_k}{v_k-\delta}}\Big]\\
&+\sum_{i=1,i\neq k}^{M}\frac{(\varphi_k-\delta)a_{k,i}}{\bar{\gamma}_{ER_i}}\Big[\frac{e^{\frac{\alpha_k-\beta_k\delta}{\varphi_i}}}{(\varphi_i-\varphi_k)^2}\mathrm{Ei}\Big(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_i-\delta)}{\varphi_i(v_k-\delta)}\Big)\\
&-\frac{e^{\frac{\alpha_k-\beta_k\delta}{\varphi_k}}}{(\varphi_k-\varphi_i)^2}\mathrm{Ei}\Big(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_k-\delta)}{\varphi_k(v_k-\delta)}\Big)\\
&+\frac{1}{\varphi_k^2(\varphi_i-\varphi_k)}\Big(\frac{\varphi_k(v_k-\delta)}{v_k+\varphi_k-\delta}\cdot e^{\frac{\alpha_k-\beta_k\delta}{\delta-v_k}}+(\alpha_k-\beta_k\delta)e^{\frac{\alpha_k-\beta_k\delta}{\varphi_k}}\\
&\times\mathrm{Ei}\Big(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_k-\delta)}{\varphi_k(v_k-\delta)}\Big)\Big)\Big]\Big\}, \quad (6.49)
\end{aligned}$$

where $v_k>\delta$ and $(\beta_k\delta-\alpha_k)<0$.

Similarly, using the decomposed function $f_k(z_k)$ in (6.40) and changes of the variables $t=$

$\delta - z_k$ as well as $s = \frac{1}{t}$, $I_{3,k}$ can be derived by

$$\begin{aligned}
I_{3,k} &= \int_{v_k}^{\delta} f_k(z_k) \cdot e^{-\frac{\frac{\alpha_k}{z_k}-\beta_k}{1-\frac{\delta}{z_k}}} dz_k \\
&= e^{\beta_k}\Bigg\{ \int_{v_k}^{\delta} \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2} e^{\frac{\beta_k\delta-\alpha_k}{z_k-\delta}} dz_k + \sum_{i=1,i\neq k}^{M} \int_{v_k}^{\delta} \frac{a_{k,i}}{z_k\bar{\gamma}_{ER_i}+\bar{\gamma}_{AR_i}} \cdot \frac{\bar{\gamma}_{AR_k}\bar{\gamma}_{ER_k} e^{\frac{\beta_k\delta-\alpha_k}{z_k-\delta}}}{(z_k\bar{\gamma}_{ER_k}+\bar{\gamma}_{AR_k})^2} dz_k \Bigg\} \\
&= e^{\beta_k}\Bigg\{ \int_{0}^{\delta-v_k} \frac{\varphi_k-\delta}{(t-\varphi_k)^2} e^{\frac{\alpha_k-\beta_k\delta}{t}} dt + \sum_{i=1,i\neq k}^{M} \int_{0}^{\delta-v_k} \frac{\frac{a_{k,i}}{\bar{\gamma}_{ER_i}}}{\varphi_i - t} \cdot \frac{\varphi_k-\delta}{(t-\varphi_k)^2} e^{\frac{\alpha_k-\beta_k\delta}{t}} dt \Bigg\} \\
&= e^{\beta_k}\Bigg\{ \frac{\varphi_k-\delta}{\varphi_k^2} \int_{\frac{1}{\delta-v_k}}^{\infty} \frac{1}{(s-\frac{1}{\varphi_k})^2} e^{-(\beta_k\delta-\alpha_k)s} ds + \sum_{i=1,i\neq k}^{M} \int_{\frac{1}{\delta-v_k}}^{\infty} \frac{\frac{a_{k,i}}{\bar{\gamma}_{ER_i}} s}{\varphi_i s - 1} \cdot \frac{\varphi_k-\delta}{(\varphi_k s-1)^2} e^{(\alpha_k-\beta_k\delta)s} ds \Bigg\}.
\end{aligned} \tag{6.50}$$

Using the same integrals given in [129, eq.(3.352.2)] and [129, eq.(3.353.1)], the closed-form expression for $I_{3,k}$ can be written by

$$\begin{aligned}
I_{3,k} = e^{\beta_k}\Bigg\{ & \frac{\varphi_k-\delta}{\varphi_k^2}\Bigg[\frac{\varphi_k(\delta-v_k)}{v_k+\varphi_k-\delta} e^{\frac{\beta_k\delta-\alpha_k}{v_k-\delta}} \\
& + (\beta_k\delta-\alpha_k) e^{\frac{\alpha_k-\beta_k\delta}{\varphi_k}} \mathrm{Ei}\Big(\frac{(\alpha_k-\beta_k\delta)(v_k+\varphi_k-\delta)}{\varphi_k(\delta-v_k)} \Big) \Bigg] \\
& + \sum_{i=1,i\neq k}^{M} \frac{(\varphi_k-\delta)a_{k,i}}{\bar{\gamma}_{ER_i}} \Bigg[\frac{-e^{\frac{\alpha_k-\beta_k\delta}{\varphi_i}}}{(\varphi_i-\varphi_k)^2} \mathrm{Ei}\Big(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_i-\delta)}{\varphi_i(v_k-\delta)} \Big) \\
& \quad + \frac{e^{\frac{\alpha_k-\beta_k\delta}{\varphi_k}}}{(\varphi_k-\varphi_i)^2} \mathrm{Ei}\Big(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_k-\delta)}{\varphi_k(v_k-\delta)} \Big) \\
& \quad - \frac{1}{\varphi_k^2(\varphi_i-\varphi_k)} \Bigg(\frac{\varphi_k(v_k-\delta)}{v_k+\varphi_k-\delta} \cdot e^{\frac{\alpha_k-\beta_k\delta}{\delta-v_k}} + (\alpha_k-\beta_k\delta) e^{\frac{\alpha_k-\beta_k\delta}{\varphi_k}} \\
& \quad \times \mathrm{Ei}\Big(\frac{(\beta_k\delta-\alpha_k)(v_k+\varphi_k-\delta)}{\varphi_k(v_k-\delta)} \Big) \Bigg) \Bigg] \Bigg\},
\end{aligned} \tag{6.51}$$

where $v_k < \delta$ and $(\alpha_k - \beta_k\delta) < 0$.

Since $I_{1,k}$ and $I_{4,k}$ have same closed-form expression, the outage probability in equation (6.36) can be simplified by using only terms $I_{1,k}$ (6.41), $I_{2,k}$ (6.49) and $I_{3,k}$ (6.51). Consequently, the closed-form expression of the outage probability for the second scheme can be expressed

by

$$P_{out} = \sum_{k\in\mathcal{S}} I_{1,k} - \sum_{k\in\mathcal{S}} I_{2,k} + \sum_{k\in\bar{\mathcal{S}}} I_{3,k} + \sum_{k\in\bar{\mathcal{S}}} I_{1,k}. \tag{6.52}$$

Figure 6.2 illustrates the outage probabilities of two proposed relay selection schemes versus the transmit power ratio of Alice to Eve (i.e., $\frac{P_A}{P_E}$) under the comparison of the closed-form expressions and Monte-Carlo experiments. In this figure, AF1 and AF2 represent the proposed first and second relay selection schemes, respectively. As expected, the closed-form expressions of two outage probabilities given in equations (6.32) and (6.52) coincide with the corresponding Monte-Carlo results. Additionally, the performance of AF1 is slightly better than that of AF2 when $\frac{P_A}{P_E}$ is larger than 2 dB. Although AF1 performs slightly better than AF2 in terms of outage probability, AF2 provides great performance with lower complexity and resource consumption.

6.4.3 Authentication Analysis

In this subsection, the authentication performance in terms of FAR and PD is defined and analyzed. Basically, channel-based physical layer authentication is achieved based on the channel temporal correlation in the legitimate link and spatial decorrelation between different links. In our proposed authentication scheme based on AF cooperative relaying, a new test statistic is developed in order to discriminate Alice from Eve under the binary hypothesis testing defined in equation (6.1). More specifically, the test statistic T_{AF} is defined based on the normalized channel difference between two adjacent end-to-end channel estimates at the destination. That is,

$$T_{AF} \triangleq \frac{|\hat{h}_X(n) - \hat{h}_{AR^bB}(n-1)|^2}{|\hat{h}_{AR^bB}(n-1)|^2}, \tag{6.53}$$

where $\hat{h}_X(n) = \{\hat{h}_{AR^bB}(n), \hat{h}_{ER^bB}(n)\}$ is defined as current end-to-end channel coefficient estimate of the link between an unknown transmitter (Alice or Eve) and Bob through relay R^b. Herein, the subscript R^b represents the selected best relay R^b which is determined and updated based on our proposed relay selection schemes. Also, $\hat{h}_{AR^bB}(n-1)$ is previous end-to-end channel coefficient estimate of the legitimate link via the best relay R^b.

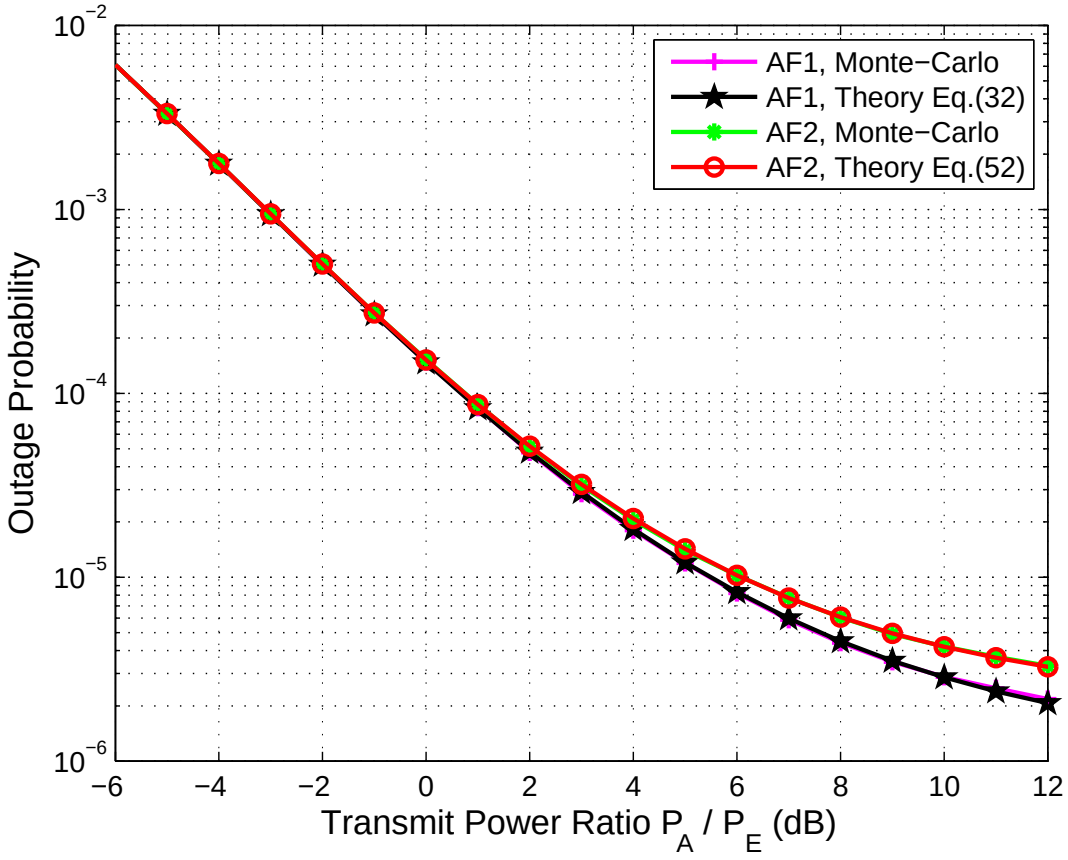

Figure 6.2: Comparison of outage probabilities based on closed-form expressions and Monte-Carlo simulations.

Furthermore, the end-to-end channel coefficient estimates $\hat{h}_{AR^bB}$ and $\hat{h}_{ER^bB}$ can be modeled as a sum of the actual value and a noise component, respectively. That is,

$$\hat{h}_{AR^bB}(n) \triangleq h_{AR^b}(n)h_{R^bB}(n) + \varepsilon_{AR^bB}(n), \tag{6.54}$$

and

$$\hat{h}_{ER^bB}(n) \triangleq h_{ER^b}(n)h_{R^bB}(n) + \varepsilon_{ER^bB}(n), \tag{6.55}$$

where ε_{AR^bB} and ε_{ER^bB} are the estimation errors. Based on LS channel estimation [106], the variances of ε_{AR^bB} and ε_{ER^bB} are derived, respectively, by

$$\sigma^2_{\varepsilon_{AR^bB}} \triangleq \frac{\sigma_n^2\sigma^2_{R^bB}}{P_A} + \frac{\sigma_n^2(P_A\sigma^2_{AR^b} + \sigma_n^2)}{P_AP_R}, \tag{6.56}$$

and

$$\sigma^2_{\varepsilon_{ER^bB}} \triangleq \frac{\sigma_n^2\sigma^2_{R^bB}}{P_E} + \frac{\sigma_n^2(P_E\sigma^2_{ER^b} + \sigma_n^2)}{P_EP_R}, \tag{6.57}$$

where $\sigma^2_{R^bB}$ is the variance of the channel link between the selected best relay and Bob.

Since the performance of the proposed authentication scheme is evaluated by comparing with that of the direct transmission scheme, a test statistic is developed for the direct transmission scheme as well. Specifically, the test statistic is defined based on the normalized channel difference between adjacent channel coefficient estimates. Mathematically, the test statistic T_{DT} is expressed by

$$T_{DT} \triangleq \frac{|\hat{h}_X(n) - \hat{h}_{AB}(n-1)|^2}{|\hat{h}_{AB}(n-1)|^2}, \tag{6.58}$$

where $\hat{h}_X(n) \triangleq \{\hat{h}_{AB}(n), \hat{h}_{EB}(n)\}$. Herein, $\hat{h}_{AB}$ and $\hat{h}_{EB}$ are the estimated channel coefficients of the legitimate and spoofing links, respectively. Similarly, the channel coefficient estimates can be modeled, respectively, by

$$\hat{h}_{AB}(n) \triangleq h_{AB}(n) + \varepsilon_{AB}(n), \tag{6.59}$$

and

$$\hat{h}_{EB}(n) \triangleq h_{EB}(n) + \varepsilon_{EB}(n), \tag{6.60}$$

where ε_{AB} and ε_{EB} are the estimation errors, which are independent to each other. Based on LS channel estimation, the variances of ε_{AB} and ε_{EB} can be expressed, respectively, by

$$\sigma^2_{\varepsilon_{AB}} \triangleq \frac{1}{(P_A + P_R)\sigma^2_{AB}}, \tag{6.61}$$

and

$$\sigma^2_{\varepsilon_{EB}} \triangleq \frac{1}{(P_E + P_R)\sigma^2_{EB}}. \tag{6.62}$$

According to the developed test statistics T_{AF} in (6.53) and T_{DT} in (6.58), FAR and PD can be defined, respectively, by

$$P_{fa} \triangleq P(T > \delta_{au}|H_0), \tag{6.63}$$

and

$$P_d \triangleq P(T > \delta_{au}|H_1), \tag{6.64}$$

where $T \triangleq \{T_{AF}, T_{DT}\}$. Herein, δ_{au} is the threshold for decision making of authentication. Generally, FAR is normally set below 0.1 for secure wireless communications. Consequently, the threshold δ_{au} can be calculated by using the Monte-Carlo method under a given value of FAR. Based on the achieved threshold value, PD can be calculated based on Monte-Carlo simulations as well.

6.5 Simulation Results

In this section, the performance of our proposed authentication scheme based on cooperative AF relay system is evaluated using the numerical results. In our scenario, one legitimate

transmitter (Alice) communicates with the intended receiver (Bob) through M trusted relay nodes in the presence of one spoofer (Eve). A two-dimensional coordinate system is considered in the simulations, and for simplicity, Alice, Eve, Bob and relays are located at different intervals along a horizontal line. The Alice-relay distances are assumed to be smaller than the Eve-relay distances. In order to study the effects of distances, the channel coefficients between any two nodes are modeled by using frequency non-selective Rayleigh fading with a path loss exponent, i.e., $h_{ij} \sim N_c(0, d_{ij}^{-\nu})$. Herein, d_{ij} is the Euclidean distance between nodes i and j, and ν is the path loss exponent that is assumed to be a constant throughout the simulations. In our simulations, we fix Alice and Bob locations at $(0, 0)$ and $(10, 0)$, respectively. Moreover, the transmit powers of the relays and Eve are fixed to one. Additionally, Noise variance σ_n^2 is assumed to equal to -40 dB, and the path loss is $\nu = 3$. For Monte-Carlo experiments, 10^6 independent trails are used to obtain the average results.

In order to compare the authentication performance based on our proposed AF cooperative schemes against the direct transmission scheme, two examples are considered by studying the effects of Alice-Eve distance and the number of available relays, respectively. In the simulations, AF1 and AF2 represent the proposed authentication schemes based on the first and second relay selection methods, respectively, while DT is corresponding to the direct transmission scheme.

6.5.1 Example 1 : Effect of Alice-Eve distance

In *Example* 1, we will study the effect of distances between Alice and Eve on the performances of outage and spoofing detection, respectively. Particularly, four available relays are considered and fixed at the locations $(5, 0)$, $(5, 1)$, $(5, 2)$ and $(5, 3)$, respectively. The position of Eve is moved from $(-1, 0)$ to $(-10, 0)$. Figure 6.3 illustrates the outage probability of the effective SNR ratio versus the distances between Alice and Eve under different values of transmit power ratio. It shows that the outage probabilities under three schemes are decreasing dramatically when Eve is moving away from Alice. As expected, the outage performances for our proposed schemes AF1 and AF2 are significantly better than that for DT under different values of transmit power ratio. Additionally, comparing AF2 with AF1, AF2 performs worse

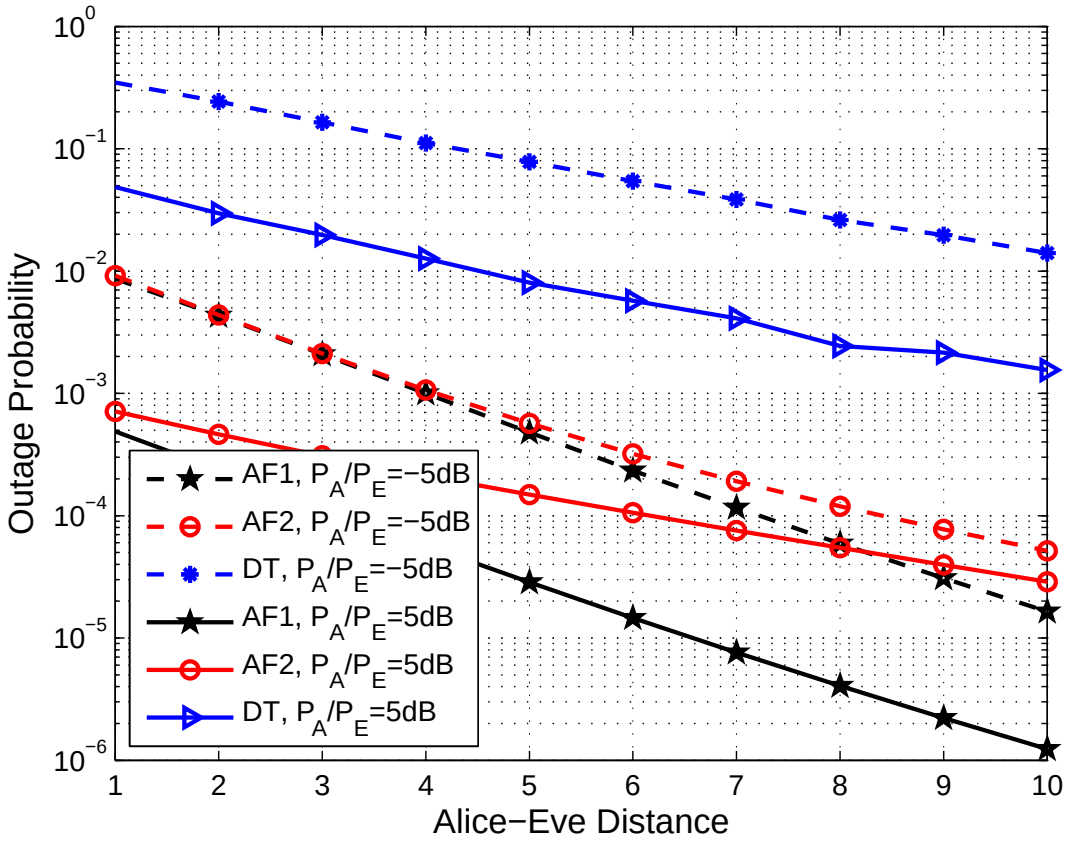

Figure 6.3: Outage probabilities versus Alice-Eve distance under different values of transmit power ratio.

than AF1 when Eve is at a farther position to Alice, but the outage probability of AF2 is lower than -30 dB under different Alice-Eve distances.

Figure 6.4 shows the probability of spoofing detection versus the distances between Alice and Eve under different values of transmit power ratio. As expected, the probability of spoofing detection under three schemes increases when the position of Eve is moving away from Alice. The performance of the proposed two schemes is significantly better than that in the direct transmission especially at lower transmit power ratio. Additionally, AF1 performs best among three schemes, and the proposed schemes are much better than DT when Eve is close to Alice. The PD of AF2 is higher than 0.8 at different Alice-Eve distances. In Figure 6.5, we fix the value of transmit power ratio to be 5 dB, and study the spoofing detection for different Alice-Eve distances under two values of FAR. As expected, the PD of three schemes increases

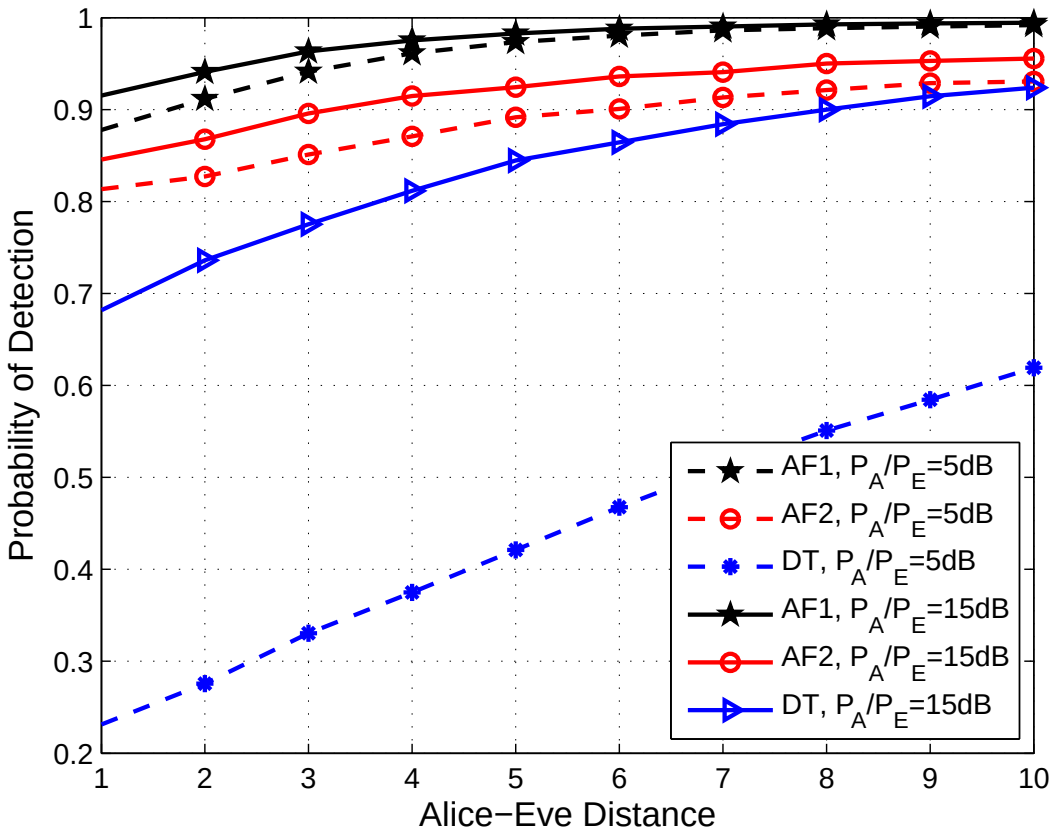

Figure 6.4: PD versus Alice-Eve distance under different values of transmit power ratio.

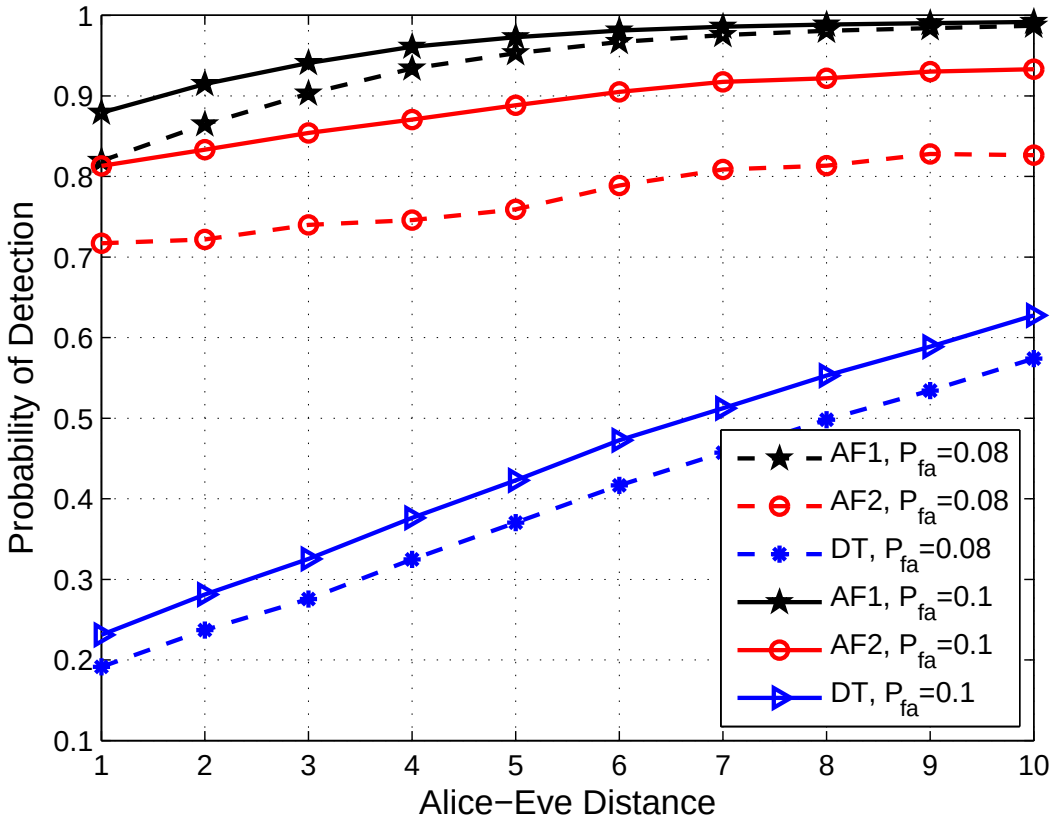

Figure 6.5: PD versus Alice-Eve distance under different values of FAR.

correspondingly under higher value of FAR. In our proposed two schemes, the probability of spoofing detection is always larger than 0.7. However, for DT, the probability is just 0.2 when the Alice-Eve distance equals to 1.

6.5.2 Example 2 : Effect of the number of available relays

In this example, we will study the effect of the number of available relays on the analysis of outage probability and probability of spoofing detection. To achieve this, we consider six available relays in our scenario which are placed in order at $(5, 0)$, $(5, 1)$, $(5, 2)$, $(5, 3)$, $(5, 4)$ and $(5, 5)$, respectively. Moreover, the position of Eve is fixed at $(-5, 0)$. The performance of the outage for the effective SNR ratio is depicted in Figure 6.6 versus the number of available relays. Note that the number of N available relays in *Example* 2 are set based on the first N relays, where $N = 1, 2, \ldots, 6$.

Figure 6.6 shows the outage probability for the number of available relays under different values of transmit power ratio. As expected, the outage probability of DT is independent of the number of relays. As it can be seen from this figure, the outage probability dramatically decreases with the increasing number of available relays under two proposed schemes. When more available relays are considered, AF1 and AF2 both perform much better than DT. At higher transmit power ratio, the outage probability of AF1 decreases to 10^{-4} when the number of available relays is $N = 6$, which is 21 dB lower than that of DT, and also 10 dB lower than that of AF2.

In Figure 6.7, the transmit power ratio is fixed at 5 dB. This figure illustrates the spoofing detection for the number of available relays under two different values of FAR. As expected, the probability of spoofing detection for DT is independent of the number of available relays, and the values are approximately 0.38 at $P_{fa} = 0.08$ and 0.42 at $P_{fa} = 0.1$, respectively. As for the two proposed schemes, the PD increases when the number of available relays becomes larger. When the number of relays is $N = 6$ and the FAR is $P_{fa} = 0.1$, the PD can reach to 0.98 and 0.89 in AF1 and AF2, respectively. Even at lower FAR value, the PD is still larger than 0.7 under our proposed schemes where N is no smaller than 3.

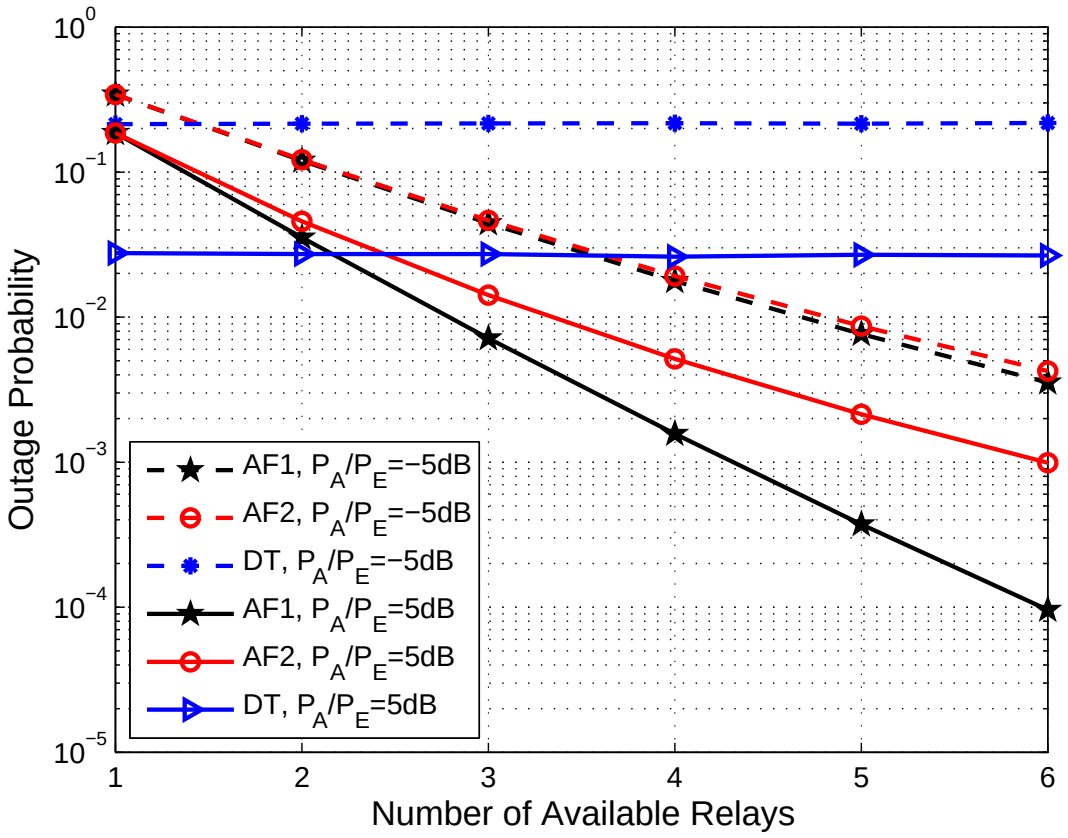

Figure 6.6: Outage probability versus the number of available relays under different values of transmit power ratio.

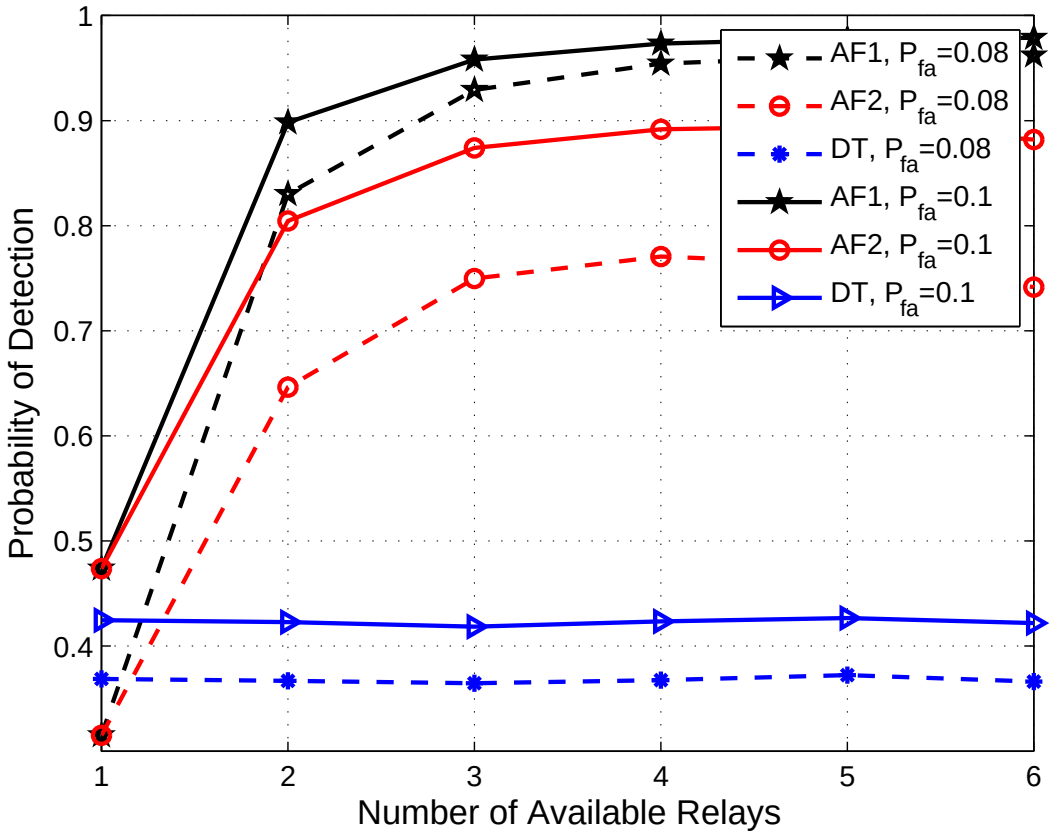

Figure 6.7: PD versus the number of available relays under different FAR values.

6.6 Summary

In this Chapter, we have proposed a novel channel-based physical layer authentication scheme based on an AF cooperative relaying system. To achieve our goal, the best relay was chosen to provide the best end-to-end path between two legitimate communication ends in the presence of a spoofer. Specifically, two relay selection schemes have been proposed by maximizing the SNR ratios of the legitimate link to the spoofing link at the destination and relays, respectively. For statistical analysis, we defined our performance metrics in terms of the outage of effective SNR ratios and probability of spoofing detection. One of the main contributions was that the closed-form expressions for the two outage probabilities have been derived. Under a binary hypothesis testing, a new test statistic has been developed to analyze the performance of spoofing detection. By using Monte-Carlo method, the performance of the proposed scheme

was evaluated and compared with that of the direct transmission scheme. Numerical results have shown the effectiveness on the improvement in performance of the proposed scheme.

Chapter 7

Continuous Physical Layer Authentication Using PCP-OFDM System

Traditional authentication techniques for wireless communications are facing great challenges, due to the open radio propagation environment and limited options of transmission techniques. In this Chapter, a new continuous physical layer authentication system based on an adaptive OFDM platform is proposed to enhance the security of tractional OFDM systems. A PCP sequence, which introduces an additional signaling link to carry the time-varying transmission parameters, is employed in each OFDM symbol for authentication purpose. Moreover, PCP sequences are generated with the same time and frequency domain characteristics as data-carrying OFDM signals in order to conceal the system parameters from adversaries. With the proper recovery of system parameters and interference cancellation, only legitimate users can successfully decode the PCP sequence and recover necessary parameters for demodulating OFDM data. In addition, a cross-layer optimization approach, which trade-offs between the stealth, system robustness and transmitting efficiency, is introduced to continuously generate optimal PCPs according to dynamic communication conditions. Finally, numerical simulation is employed to evaluate the performance of our proposed authentication system.

7.1 Introduction

Wireless communications is facing additional issues and new challenges in defending against various types of security risks compared with traditional wired networks [130, 131]. One major challenge for secure wireless networks is the broadcast nature of radio propagation due to the lack of direct physical connection between the transmitter and receiver. Moreover, limited options of transmission techniques at the physical layer brings potential security issues. To address wireless security issues, traditionally, cryptographic techniques relying on the higher layers of the protocol stack provide an effective solution based on complex mathematical calculations [31, 132]. However, due to the physical layer transparency, information protected by these traditional security approaches can often be deciphered using exhaustive trial. Therefore, they are inefficient and vulnerable to various malicious attacks. Recently, the physical properties of the wireless transmission are recognized as a powerful and under-utilized source to provide additional security protection and enhance security performance of wireless communications systems.

Alternatively, OFDM has been adopted in various latest wireless and telecommunications standards, due to its spectral efficiency, high achievable data rates, and robust performance in multipath fading environments. However, OFDM signals are transparent to potential adversaries, as OFDM-based communications systems lack built-in security capabilities. More specifically, since OFDM employs pilot tones or preamble symbols for channel estimation, equalization and synchronization at the receiver, the implementations of OFDM are highly susceptible to signal jamming attacks [88–90]. Additionally, due to the distinct time and frequency characteristics of OFDM signals, physical layer transmission parameters of OFDM signals can be blindly estimated by any user within the same network, and no prior information of the signals is required for them [91, 92]. Consequently, secure OFDM-based transmission is critical for designing wireless security mechanisms.

In this Chapter, we propose a new continuous physical layer authentication system based on PCP-OFDM, where PCP is introduced to replace the traditional CP and bring an additional signaling link at the physical layer to convey current system parameters and the identity of different transceivers [133, 134]. Specifically, transmitter can use the PCP sequences to adjust

its operating parameters continuously and share the link adaptation information with the legitimate receiver. PCPs are generated with the same time and frequency domain characteristics as the OFDM data-carrying symbols, thus, they are concealed to unauthorized users. For the analysis of system performance pertaining to security and efficiency, the stealth, system robustness and transmitting efficiency are considered. The stealth of a communications system describes how covert the authentication scheme is to prevent against eavesdropping users [7], while the system robustness is defined how reliable the signal can be recovered by the legitimate receiver. The performance trade-off between stealth, system robustness and efficiency is investigated from a cross-layer view. An optimization method is developed to adapt the system parameters continuously. Eventually, numerical simulation is employed to evaluate the performance of our proposed authentication system.

The rest of this Chapter is organized as follows. In Section 7.2 and 7.3, the design of our proposed continuous physical-layer authentication using the PCP-OFDM system is illustrated. In Section 7.4, performance analysis in terms of stealth and robustness is investigated, followed by a cross-layer optimization method. Numerical results of MATLAB simulation are discussed in Section 7.5 to validate the proposed authentication scheme. This Chapter is then summarized in Section 7.6.

7.2 Transmitter Design of Continuous Physical Layer Authentication System

Figures 7.1 shows the transmitter block diagram of our proposed continuous physical layer authentication system based on PCP-OFDM. Compared with the traditional OFDM system shown in Figure 2.6 in Chapter 2, PCP-OFDM employs PCP instead of traditional CP [133], which introduces an additional signaling link to convey time-varying physical layer parameters such as modulation method and number of subcarriers. In our proposed authentication system, a notable difference is an authentication module which is used to continuously direct the adjustment of the physical layer parameters. The adjustment decision is made based on a cross-layer optimization that considers the tradeoffs between the stealth, system robustness and

transmitting efficiency. The overall system optimization will be introduced later in Section 7.4.

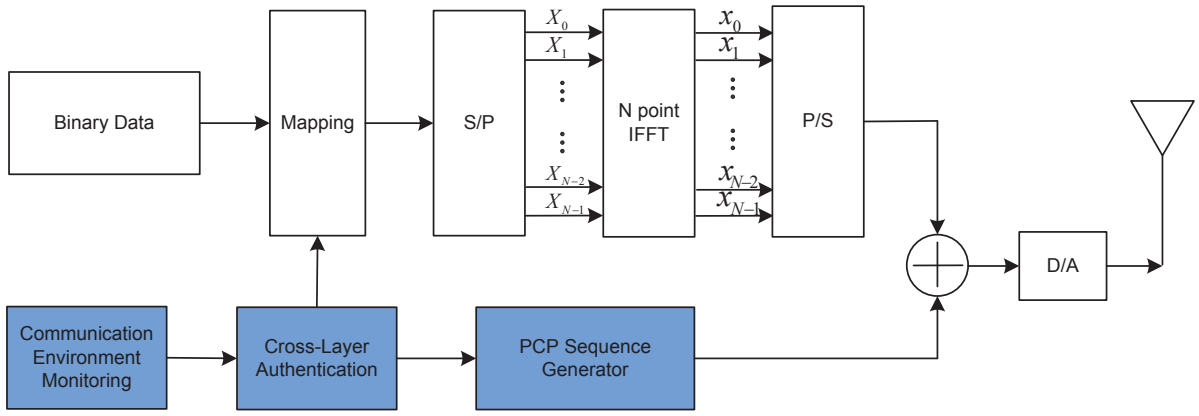

Figure 7.1: Transmitter block diagram of the proposed continuous authentication system.

7.2.1 PCP-OFDM Transmitter

The transmitter of PCP-OFDM system is designed as same as that of the traditional OFDM system, except the prefixed part. As for the data-carrying part, We consider one OFDM data symbol consisting of N subcarriers, and source data are grouped and mapped into $\mathbf{X} = [X(0), X(1), \ldots, X(N-1)]^T$. With inverse discrete Fourier transformation, the transmitted data symbol $\mathbf{x} = [x(0), x(1), \ldots, x(N-1)]^T$ in the discrete time domain can be written by

$$x(n) = \sqrt{\frac{1}{N}} \sum_{m=0}^{N-1} X(m) e^{j2\pi m \frac{n}{N}}, \quad n = 0, 1, \cdots, N-1. \tag{7.1}$$

Before transmitting an OFDM symbol, PCP is generated and inserted as prefix with size of P. As a result, two adjacent PCP-OFDM symbols with total length of $N + 2P$ can be expressed by

$$\tilde{\mathbf{x}} = [c_{p1}(0), c_{p1}(1), \ldots, c_{p1}(P-1), x(0), x(1), \ldots, x(N-1), c_{p2}(0), c_{p2}(1), \ldots, c_{p2}(P-1)]^T \tag{7.2}$$

where $\mathbf{c}_{p1} = [c_{p1}(0), c_{p1}(1), \ldots, c_{p1}(P-1)]^T$ and $\mathbf{c}_{p2} = [c_{p2}(0), c_{p2}(1), \ldots, c_{p2}(P-1)]^T$ are two PCP sequences preceded and succeeded to the data symbol, repectively. They are identical if there is no change of the operating parameters, otherwise they are different. Additionally, to

completely mitigate the impact of ISI, we assume that the length of PCP (i.e., P) has to be longer than the channel delay spread.

7.2.2 PCP Generation

To avoid distinct time and frequency characteristics between PCPs and OFDM data, herein PCP sequences are generated using an OFDM modulator. Specifically, an N-length sequence with P sparse input, $\mathbf{C}_p = [C_p(0), C_p(1), \ldots, C_p(N-1)]^T$, passes through an OFDM modulator, and only the first P samples of $\mathbf{C}_p$ are used to generate a P-length PCP sequence $\mathbf{c}_p = [c_p(0), c_p(1), \ldots, c_p(P-1)]^T$. That is,

$$c_p(k) = \lambda \sqrt{\frac{1}{P}} \sum_{m=0}^{P-1} C_p(m) e^{j2\pi m \frac{k}{P}}, \quad k = 0, 1, \cdots, P-1, \tag{7.3}$$

where the parameter $\lambda = \sqrt{N/P}$ is the normalization factor to maintain the generated PCP with same power as the OFDM data, and it is assumed to be an integer.

Figure 7.2 illustrates the sparse input $\mathbf{C}_p$ passed through the OFDM modulator [135]. Herein a random frequency shift of $l = \text{random}[0, N/P - 1]$ is employed to differentiate PCPs such that no distinct frequency domain features is introduced. Therefore, two random PCP sequences in the frequency domain are orthogonal to each other, which represent adaptive transmission parameters for continuous authentication. Take two random PCP sequences in the frequency domain $\mathbf{C}_{p1} = [C_{p1}(0), C_{p1}(1), \ldots, C_{p1}(P-1)]^T$ and $\mathbf{C}_{p2} = [C_{p2}(0), C_{p2}(1), \ldots, C_{p2}(P-1)]^T$ as an example. Due to the orthogonality of $\mathbf{C}_{p1}$ and $\mathbf{C}_{p2}$, we have

$$\mathbf{C}_{p1}^H \mathbf{C}_{p2} = \frac{1}{P} \sum_{k=0}^{P-1} C_{p1}(k) C_{p2}^*(k) = 0. \quad where \quad p1 \neq p2. \tag{7.4}$$

Accordingly, two PCP sequences in the time domain $\mathbf{c}_{p1}$ and $\mathbf{c}_{p2}$ in equation (7.2) can be

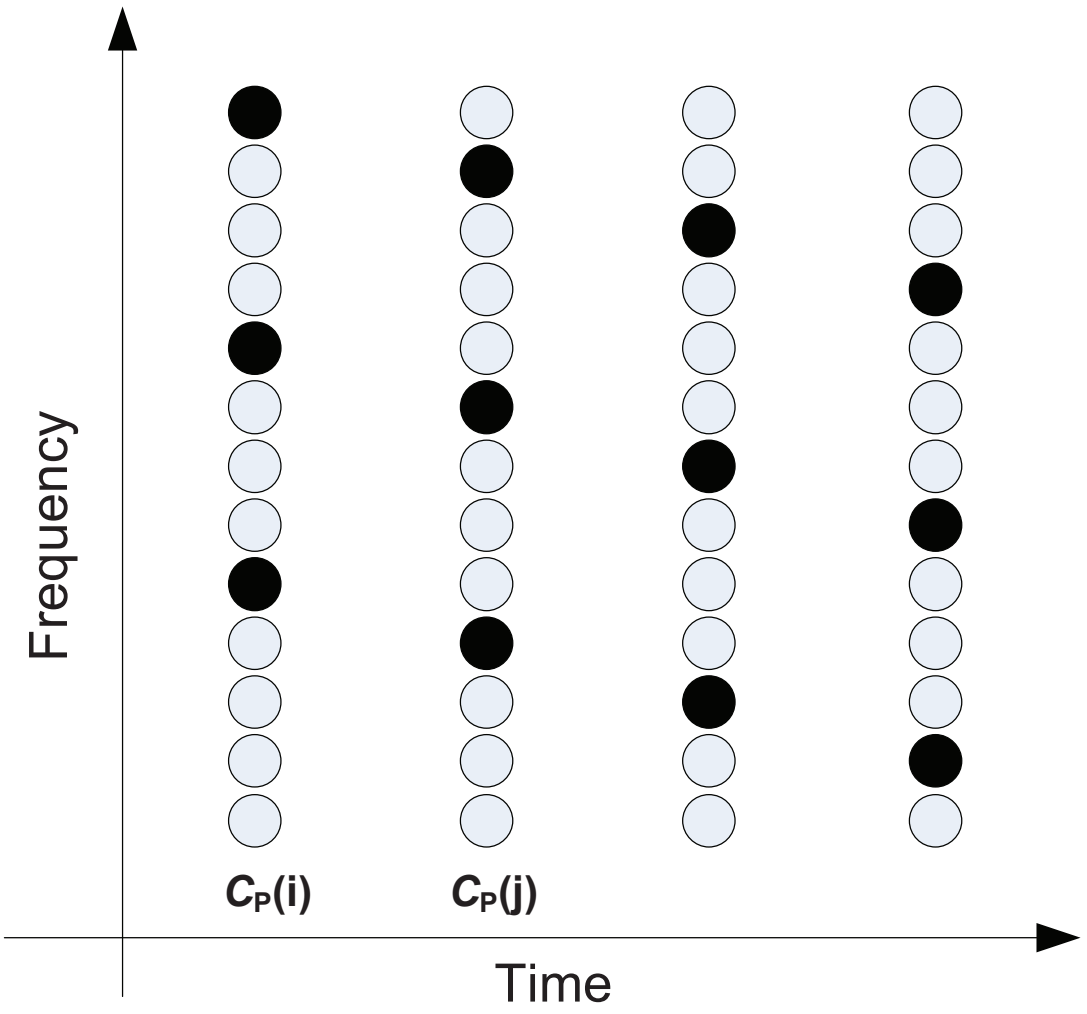

Figure 7.2: Sparse input to OFDM modulator used for PCP sequence generation.

generated based on the equation (7.3),

$$c_{p1}(k) = \lambda \sqrt{\frac{1}{P}} \sum_{m=0}^{P-1} C_{p1}(m) e^{j2\pi m \frac{k}{P}}, \tag{7.5}$$

$$c_{p2}(k) = \lambda \sqrt{\frac{1}{P}} \sum_{m=0}^{P-1} C_{p2}(m) e^{j2\pi m \frac{k}{P}}. \tag{7.6}$$

Consequently, according to the equation (7.4), the orthogonality of $\mathbf{c}_{p1}$ and $\mathbf{c}_{p2}$ can be

proved by

$$
\begin{aligned}
\mathbf{c}_{p1}^{H}\mathbf{c}_{p2} &= \frac{1}{P}\sum_{k=0}^{P-1} c_{p1}(k)c_{p2}^{*}(k) \\
&= \frac{\lambda^2}{P^2}\sum_{k=0}^{P-1}\left(\sum_{m_1=0}^{P-1} C_{p1}(m_1)e^{j2\pi m_1\frac{k}{P}}\right)\cdot\left(\sum_{m_2=0}^{P-1} C_{p2}^{*}(m_2)e^{-j2\pi m_2\frac{k}{P}}\right) \\
&= \frac{\lambda^2}{P^2}\sum_{m_1=0}^{P-1}\sum_{m_2=0}^{P-1} C_{p1}(m_1)C_{p2}^{*}(m_2)\sum_{k=0}^{P-1}\left(e^{j2\pi m_1\frac{k}{P}}\cdot e^{-j2\pi m_2\frac{k}{P}}\right) \\
&= \begin{cases} \dfrac{\lambda^2}{P^2}\displaystyle\sum_{m_1=0}^{P-1} C_{p1}(m_1)C_{p2}^{*}(m_1)\cdot P = 0, & if\ m_1 = m_2, \\ \dfrac{\lambda^2}{P^2}\displaystyle\sum_{m_1=0}^{P-1}\sum_{m_2=0}^{P-1} C_{p1}(m_1)C_{p2}^{*}(m_2)\cdot 0 = 0, & if\ m_1 \neq m_2. \end{cases}
\end{aligned}
\tag{7.7}
$$

Equation (7.7) indicates that two random PCP sequences are orthogonal to each other in both the frequency and time domains simultaneously. The orthogonality of two random PCP sequences guarantees successful detection of PCP sequences at the receiver.

7.3 Receiver Design of Continuous Physical Layer Authentication System

Figures 7.3 shows the receiver block diagram of our proposed continuous authentication system using PCP-OFDM. Compared with traditional OFDM receiver, a frequency-domain equalization and time-domain interference cancellation are used. Additionally, the PCP detection is discussed and the correct detection rate is derived in this section.

7.3.1 PCP-OFDM Receiver

In multipath fading environments, due to the channel dispersive nature, the desired OFDM data symbol and two adjacent PCP sequences are overlapped within the duration of one received OFDM symbol. As a result, ISI and inter-carrier interference (ICI) are introduced, where ISI is from the adjacent symbols and ICI is from the current symbol. Herein, we consider a typical scenario of static multipath channel for PCP-OFDM receiver design, and the

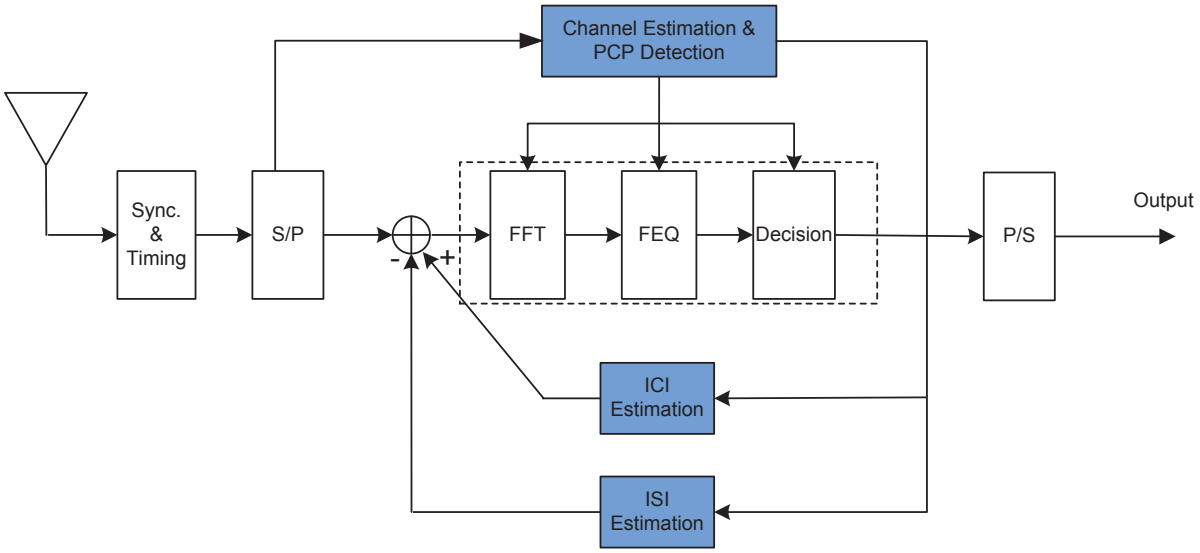

Figure 7.3: Receiver block diagram of the proposed continuous authentication system.

channel vector with length of L is defined by

$$\mathbf{h} = [h_0, h_1, \ldots, h_{L-1}]^T. \tag{7.8}$$

Consequently, transmitting the signal given in equation (7.2), the received signal $\mathbf{y}$ in the time domain can be written by

$$\mathbf{y} = \mathbf{h} * \tilde{\mathbf{x}} + \mathbf{w}, \tag{7.9}$$

where $*$ denotes cyclic convolution, and $\mathbf{w}$ is an additive white Gaussian noise vector with the size of $(N + 2P + L - 1)$.

For the analysis of interference cancellation, we define two zero padded PCP sequences in an observation period of N-samples [133]. That is,

$$\mathbf{R}_{c_{p1}} = [\underbrace{0, \ldots 0}_{(N-L+1)\text{Samples}}, \underbrace{\mathbf{c}_{p1}(P-L+1), \ldots, \mathbf{c}_{p1}(P-1)}_{(L-1)\text{Samples}}]^T, \tag{7.10}$$

$$\mathbf{R}_{c_{p2}} = [\underbrace{\mathbf{c}_{p2}(0), \ldots \mathbf{c}_{p2}(L-2)}_{(L-1)\text{Samples}}, \underbrace{0, \ldots, 0}_{(N-L+1)\text{Samples}}]^T. \tag{7.11}$$

Based on our previous work in [133,134,136], three $N \times N$ matrices, i.e., $\mathbf{C}$, $\mathbf{C}_T$, and $\mathbf{C}_H$, are used to reconstructed ISI and ICI. More specifically, the first matrix $\mathbf{C}$ represents the channel seen by the OFDM symbol, i.e,

$$\mathbf{C} = \begin{bmatrix} h_0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ h_1 & h_0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & 0 \\ h_{L-1} & h_{L-2} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_{L-1} & \cdots & h_1 & h_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & h_{L-1} & \cdots & h_0 \end{bmatrix}. \tag{7.12}$$

As for the succeeding symbol, the second matrix $\mathbf{C}_T$ is the tail of the channel response which leads to ISI, i.e.,

$$\mathbf{C}_T = \begin{bmatrix} 0 & \cdots & 0 & h_{L-1} & h_{L-2} & \cdots & h_1 \\ 0 & \cdots & 0 & 0 & h_{L-1} & \cdots & h_2 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & h_{L-1} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}. \tag{7.13}$$

The third matrix $\mathbf{C}_H$ represents head response of the channel for ICI interference cancellation, i.e.,

$$\mathbf{C}_H = \begin{bmatrix} h_0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ h_1 & h_0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & 0 \\ h_{L-2} & h_{L-3} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}. \tag{7.14}$$

Additionally, two signal vectors $\mathbf{y}_1$ and $\mathbf{y}_2$ are defined and constructed from the received signal $\mathbf{y} = [y(0), \ldots, y(P-1), y(P), \ldots, y(P+N-1), y(P+N), \ldots, y(P+N+L-2), \ldots, y(2P+N+L-1)]$ for ISI and ICI cancellation. In particular, $\mathbf{y}_1$ expresses the received OFDM data symbol in the observation period of N-samples, while $\mathbf{y}_2$ contains the remaining tail from the OFDM data symbol and the components from the succeeding PCP. That is,

$$\begin{aligned} \mathbf{y}_1 &= [y(P),\ \ldots,\ y(P+N-1)]^T \\ &= \mathbf{C}\mathbf{x} + \mathbf{C}_T\mathbf{R}_{c_{p1}} + \mathbf{w}_N, \end{aligned} \tag{7.15}$$

and

$$\begin{aligned} \mathbf{y}_2 &= \underbrace{[y(P+N)\ ,\ \ldots\ y(P+N+L-2),}_{(L-1)\text{Samples}}\ \underbrace{0,\ \ldots,\ 0]^T}_{(N-L+1)\text{Samples}} \\ &= \mathbf{C}_T\mathbf{x} + \mathbf{C}_H\mathbf{R}_{c_{p2}} + \mathbf{w}_N. \end{aligned} \tag{7.16}$$

where $\mathbf{w}_N$ is the noise vector applied on the samples.

Consequently, ISI term can be removed by subtracting the preceding PCP (i.e., $\mathbf{C}_T\mathbf{R}_{c_{p1}}$) from $\mathbf{y}_1$, while ICI term (i.e., $\mathbf{C}_T\mathbf{x}$) can be achieved by subtracting $\mathbf{C}_H\mathbf{R}_{c_{p2}}$ from $\mathbf{y}_2$.

Using the two signal vectors, the ideal signal for demodulation can be expressed by [133]

$$\mathbf{y}_{Ideal} = \mathbf{y}_1 - \mathbf{C}_T\mathbf{R}c_{p1} + \mathbf{y}_2 - \mathbf{C}_H\mathbf{R}c_{p2}. \tag{7.17}$$

Note that the "ideal" channel matrix can be achieved by adding two matrices $\mathbf{C}$ and $\mathbf{C}_T$, i.e.,

$$\mathbf{C} + \mathbf{C}_T = \mathbf{C}_{cycl}, \tag{7.18}$$

where $\mathbf{C}_{cycl}$ is the ideal channel matrix resulted in a cyclic convolution between the transmitted signal and the channel.

If the channel estimate is accurate, (7.17) can be expressed by

$$\mathbf{y}_{Ideal} = \mathbf{C}_{cycl}\mathbf{x} + \mathbf{w}_N. \tag{7.19}$$

In the traditional CP-OFDM system, $\mathbf{C}_{cycl}$ can be diagonalized by $N \times N$ (I)FFT matric [137], i.e.,

$$\mathbf{C}_{cycl} = \mathbf{F}_N^H \mathbf{D}_N(\mathbf{H}_N)\mathbf{F}_N, \tag{7.20}$$

where $\mathbf{F}_N$ is the FFT matrix and $\mathbf{F}_N^H$ is the IFFT matrix. $\mathbf{D}_N(\mathbf{H}_N)$ is the $N \times N$ diagonal matrix with the channel frequency response as its diagonal elements. For the equalization, applying a FFT matrix on the equation (7.19) results to

$$\begin{aligned} \mathbf{F}_N \mathbf{y}_{Ideal} &= \mathbf{F}_N \{\mathbf{F}_N^H \mathbf{D}_N(\mathbf{H}_N)\mathbf{F}_N\}\mathbf{F}_N^H \mathbf{X} + \mathbf{w}_N \\ &= \mathbf{D}_N\left(\mathbf{H}'_N\right)\mathbf{X}', \end{aligned} \tag{7.21}$$

where $\mathbf{H}'_N$ is the estimated channel frequency response.

Finally, the zero-forcing demodulation process could be completed by

$$\mathbf{X}' = \mathbf{D}_N^{-1}(\mathbf{H}'_N)\{\mathbf{F}_N \mathbf{y}_{Ideal}\}. \tag{7.22}$$

7.3.2 PCP Detection

For authenticated user, PCP detection must be achieved to recover necessary transmission parameters for OFDM demodulation. As proved before, PCP sequences are orthogonal with each other in order to guarantee successful detection. Therefore, PCP can be detected by correlating the received PCP with M_P orthogonal PCP candidates in a local library at the receiver side. The one resulted in a correlation peak is recognized as the transmitted PCP. Herein, perfect timing, phase and frequency synchronization is assumed. Specifically, the correlation function can be mathematically expressed by

$$R(m) = \sum_{k=0}^{P-1} y_p(k)\ c_{p,m}^*(k), \tag{7.23}$$

where y_p is the received PCP, and $c_{p,m}$ is the mth locally generated PCP sequences.

For simplifying the analysis of PCP detection, a white Gaussian channel is used. Therefore,

equation (7.23) can be written by

$$\begin{aligned} R(m) &= \sum_{k=0}^{P-1} (c_p(k) + w_p(k))\, c^*_{p,m}(k) \\ &= \sum_{k=0}^{P-1} c_p(k) c^*_{p,m}(k) + w_p(k) c^*_{p,m}(k). \end{aligned} \tag{7.24}$$

where w_p is the zero-mean white complex Gaussian noise with variance σ_w^2.

It is worth mentioning that, the correlation between two random PCP sequences is

$$\sum_{k=0}^{P-1} c_{p,i}(k) c^*_{p,j}(k) = \begin{cases} P, & if\ i = j, \\ 0, & if\ i \neq j. \end{cases} \tag{7.25}$$

Consequently, the correlation peak of equation (7.24) can be derived by

$$R(m) = \begin{cases} P + n_1, & if\ i = j, \\ 0 + n_2, & if\ i \neq j. \end{cases} \tag{7.26}$$

where n_1 is the interference to the auto-correlation function, and n_2 is the interference to the cross-correlation between the received PCP and the rest of $(M_P - 1)$ PCP sequences. Both are complex Gaussian distributed with zero mean and variance $\sigma_n^2 = P\sigma_w^2$, and they are statistically independent to each other.

Therefore, PCP can be successfully detected by the receiver if

$$|P + n_1| > |n_2|. \tag{7.27}$$

Based on the equation in (7.27), the correct detection rate of each test in the PCP detection

can be expressed by

$$\begin{aligned} Pr_{c_p,m} = Pr(|P+n_1| > |n_2|) &= Pr\left(\frac{|n_2|^2}{2} < \frac{|P+n_1|^2}{2}\right) \\ &= \mathbf{E}\left\{1 - e^{-\frac{\lambda}{2}|P+n_1|^2}\right\} \\ &= 1 - \mathbf{E}_{n_{1,R},n_{1,I}}\left\{e^{-\frac{\lambda}{2}[(n_{1,R}+P)^2+n_{1,I}^2]}\right\} \\ &= 1 - \mathbf{E}_{n_{1,R}}\left\{e^{-\frac{1}{2}\lambda(n_{1,R}+P)^2}\right\} \cdot \mathbf{E}_{n_{1,I}}\left\{e^{-\frac{1}{2}\lambda n_{1,I}^2}\right\}, \end{aligned} \tag{7.28}$$

where n_1 is written as $n_1 = n_{1,R} + j\, n_{1,I}$, where $n_{1,R}$ and $n_{1,I}$ are statistically independent, and both are following zero-mean Normal distribution, i.e., $n_{1,R}, n_{1,I} \sim N(0, \sigma^2)$ with $\sigma^2 = \frac{\sigma_n^2}{2}$. Additionally, $\lambda = \frac{2}{\sigma_n^2}$.

According to the law of the unconscious statistician, the expectation of a measurable function $g(X)$ of a random variable X given the PDF function $f_X(x)$, can be written by $\mathbf{E}\{g(X)\} = \int_{-\infty}^{\infty} g(x) f_X(x) dx$. Therefore, two expected values in equation (7.28) can be derived as follows, i.e.,

$$\begin{aligned} &\mathbf{E}_{n_{1,R}}\left\{e^{-\frac{1}{2}\lambda(n_{1,R}+P)^2}\right\} \\ &= \int_{-\infty}^{\infty} e^{-\frac{1}{2}\lambda(n_{1,R}+P)^2} \cdot \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{n_{1,R}^2}{2\sigma^2}} dn_{1,R} \\ &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\left(\frac{\lambda}{2}(n_{1,R}^2+2Pn_{1,R}+P^2)+\frac{n_{1,R}^2}{2\sigma^2}\right)} dn_{1,R} \\ &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\left(\frac{\lambda}{2}+\frac{1}{2\sigma^2}\right)\left(n_{1,R}^2+2\frac{P\lambda}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}n_{1,R}+\frac{\lambda P^2}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}\right)} dn_{1,R} \\ &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\left(\frac{\lambda}{2}+\frac{1}{2\sigma^2}\right)\left[\left(n_{1,R}+\frac{P\lambda}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}\right)^2+\frac{\lambda P^2}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}-\left(\frac{P\lambda}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}\right)^2\right]} dn_{1,R} \\ &= \frac{\sqrt{2\pi\frac{1}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}}}{\sqrt{2\pi\sigma^2}} e^{-\left(\frac{\lambda}{2}+\frac{1}{2\sigma^2}\right)\left[\frac{\lambda P^2}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}-\left(\frac{P\lambda}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}\right)^2\right]} \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\frac{1}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}}} e^{-\frac{\left(n_{1,R}+\frac{P\lambda}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}\right)^2}{2\cdot\frac{1}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}}} dn_{1,R} \\ &= \sqrt{\frac{1}{\lambda\sigma^2+1}} e^{-\frac{\lambda P^2}{2(\lambda\sigma^2+1)}}, \end{aligned} \tag{7.29}$$

and

$$\begin{aligned}
&\mathbf{E}_{n_{1,R}}\left\{e^{-\frac{1}{2}\lambda n_{1,I}^2}\right\} \\
&= \int_{-\infty}^{\infty} e^{-\frac{1}{2}\lambda n_{1,I}^2} \cdot \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{n_{1,I}^2}{2\sigma^2}} dn_{1,I} \\
&= \frac{\sqrt{2\pi\frac{1}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}}}{\sqrt{2\pi\sigma^2}} \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\frac{1}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}}} e^{-\frac{n_{1,I}^2}{2\cdot\frac{1}{2(\frac{\lambda}{2}+\frac{1}{2\sigma^2})}}} dn_{1,I} \\
&= \sqrt{\frac{1}{\lambda\sigma^2+1}}.
\end{aligned} \tag{7.30}$$

Therefore, the correct detection rate in equation (7.28) can be derived by

$$\begin{aligned}
Pr_{c_p,m} &= 1 - \frac{1}{\lambda\sigma^2+1} e^{-\frac{\lambda P^2}{2(\lambda\sigma^2+1)}} \\
&= 1 - \frac{1}{2} e^{-\frac{P}{2\sigma_w^2}}.
\end{aligned} \tag{7.31}$$

7.4 Performance Analysis for Cross Layer Authentication

In this section, a cross-layer authentication system is designed to derive the optimal PCP parameters under dynamic network conditions. In the proposed system, security is achieved by continuously adapting the configuration of the physical layer with the assistance of time-varying PCP sequences. To optimize the overall system performance, three important factors need to be considered, that is,

a) Stealth performance, i.e., the stealth of PCP sequences;

b) System robustness performance, i.e., the correct detection rate of PCP-OFDM system;

c) Cross-layer optimization, i.e., co-design PCP signaling link and OFDM system.

7.4.1 Stealth Performance

From the perspective of an eavesdropper, an illegal receiver will try to recover all the information from the PCP-OFDM signal blindly. Since the transmission parameters are carried by PCP in the proposed system, an adversary will naturally try to recover the PCP information

first.

Since the PCP sequence and the following OFDM data are all generated by using the same OFDM modulator, thereby both have the identical time and frequency characteristics. More specifically, large number of orthogonal random sequences are used to generate PCP sequence c_p. According to central limit theorem, both the real and imaginary part of PCP sequence are approximately following Normal distribution with zero mean and variance $\frac{\sigma_{cp}^2}{2}$, i.e., $c_{p,R}, c_{p,I} \sim N(0, \frac{\sigma_{cp}^2}{2})$. As a result, the envelope of PCP sequence $|c_p|$ approximately follows Rayleigh distribution, i.e., $|c_p| \sim Rayleigh(\sqrt{\frac{\sigma_{cp}^2}{2}})$.

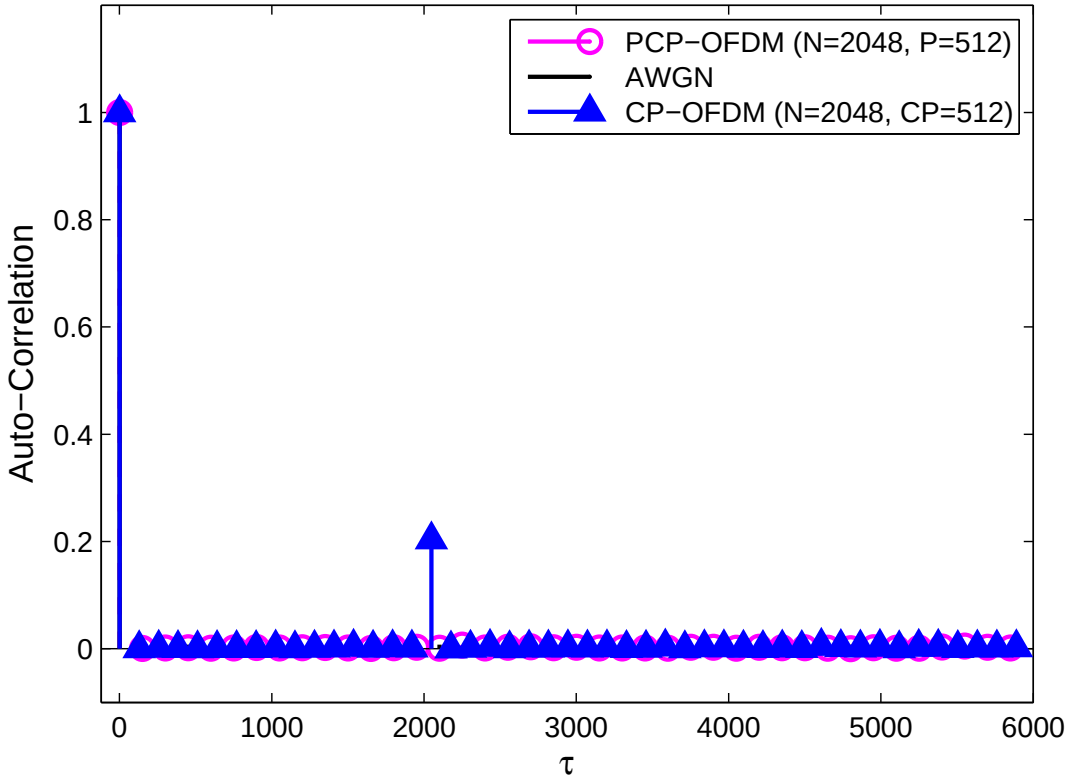

Figure 7.4: Auto-correlation of PCP-OFDM, CP-OFDM and AWGN.

Furthermore, the statistic characteristics of PCP-OFDM can also be analyzed by observing the autocorrelation function. Due to the periodic replication structure in CP-OFDM, the auto-correlation of CP-OFDM signal in time domain would have two peaks, one locates at $\tau_1 = 0$, the other locates at $\tau_2 = N$. Based on the difference $|\tau_1 - \tau_2|$, the useful symbol boundary of

CP-OFDM could be detected. In contrast, the autocorrelation of PCP-OFDM is very similar to the additive white Gaussian noise (AWGN), which has only one peak at $\tau = 0$. Figure 7.4 illustrates the auto-correlation of PCP-OFDM, CP-OFDM and AWGN. Obviously, as depicted in Figure 7.4, even if the PCP-OFDM signals can be detected by detection methods such as energy detection, it is extremely difficult to detect the symbol boundary of the signals.

7.4.2 System Robustness Performance

The robustness of the PCP-OFDM system can be evaluated by two factors, i.e. detection error rate for the PCP signalling link, and the symbol error rate (SER) for the data carrying part. Therefore, the overall system robustness can be modeled by

$$E(P, M_P) = 1 - \Big[Pr_{e,c_p} + (1 - Pr_{e,c_p})Pr_{e,s}\Big], \tag{7.32}$$

where Pr_{e,c_p} is the overall PCP detection error rate, and $Pr_{e,s}$ is the SER of OFDM data carrying signal.

Specifically, the overall PCP detection error rate Pr_{e,c_p} can be expressed by

$$Pr_{e,c_p} = 1 - Pr_{c_p}, \tag{7.33}$$

where Pr_{c_p} is the overall PCP correct detection rate. According to the equation (7.27), the overall PCP correct detection rate Pr_{c_p} is defined by

$$\begin{aligned} Pr_{c_p} &= Pr\Big(|P + N_1| > |N_2| \quad and \quad |P + N_1| > |N_3| \quad and \quad \cdots \quad |P + N_1| > |N_{M_p}|\Big) \\ &= Pr\Big(|P + N_1| > \max(|N_2|, |N_3|, \ldots, |N_{M_p}|)\Big) \\ &= Pr\Big(|P + N_1|^2 > \underbrace{\max(|N_2|^2, |N_3|^2, \ldots, |N_{M_p}|^2)}_{fz}\Big). \end{aligned} \tag{7.34}$$

Herein, the CDF of function $f_Z = \max(|N_2|^2, |N_3|^2, \ldots, |N_{M_p}|^2)$ can be derived by

$$\begin{aligned} F_Z(z) &= Pr\Big(\max(|N_2|^2, |N_3|^2, \ldots, |N_{M_p}|^2) \le z \Big) \\ &= Pr\Big(|N_2|^2 \le z \quad and \quad |N_3|^2 \le z \quad and \quad \cdots \quad |N_{M_p}|^2 \le z \Big) \\ &= Pr\Big(|N_2|^2 \le z \Big) \cdot Pr\Big(|N_3|^2 \le z \Big) \cdots Pr\Big(|N_{M_p}|^2 \le z \Big) \\ &= \left(1 - e^{-\frac{\lambda}{2} z} \right)^{M_p - 1} \\ &= \sum_{i=0}^{M_p - 1} \binom{M_p - 1}{i} \cdot (-1)^i \cdot e^{-\frac{\lambda}{2} z \cdot i}. \end{aligned} \tag{7.35}$$

Using the derived CDF of f_Z above, the overall PCP correct detection rate in equation (7.34) can be further derived by

$$\begin{aligned} Pr_{c_p} &= \mathbf{E}\Big\{ \sum_{i=0}^{M_p - 1} \binom{M_p - 1}{i} \cdot (-1)^i \cdot e^{-\frac{\lambda}{2} |P + N_1|^2 \cdot i} \Big\} \\ &= \mathbf{E}\Big\{ 1 - \binom{M_p - 1}{1} \cdot (-1)^1 \cdot e^{-\frac{\lambda}{2} |P + N_1|^2} + \binom{M_p - 1}{2} \cdot (-1)^2 \cdot e^{-2\frac{\lambda}{2} |P + N_1|^2} \\ &\quad + \cdots + 1 \cdot (-1)^{M_p - 1} \cdot e^{-(M_p - 1)\frac{\lambda}{2} |P + N_1|^2} \Big\}. \end{aligned} \tag{7.36}$$

According to the equation (7.28) and derived results given in (7.31), we can achieve that

$$\begin{aligned} \mathbf{E}\Big\{ e^{-i\frac{\lambda}{2} |P + N_1|^2} \Big\} &= \mathbf{E}_{N_{1,R}}\Big\{ e^{-i\frac{\lambda}{2} (N_{1,R} + P)^2} \Big\} \cdot \mathbf{E}_{N_{1,I}}\Big\{ e^{-i\frac{\lambda}{2} N_{1,I}^2} \Big\} \\ &= \frac{1}{(i+1)} e^{-\frac{i \cdot P}{(i+1)\sigma_w^2}}. \end{aligned} \tag{7.37}$$

Consequently, the close-form expression of the overall PCP correct detection rate can be

derived by

$$\begin{aligned} Pr_{c_p} &= 1 - \left\{ \binom{M_p-1}{1} \cdot (-1)^1 \cdot \mathbf{E}\left\{ e^{-\frac{\lambda}{2}|P+N_1|^2} \right\} + \binom{M_p-1}{2} \cdot (-1)^2 \cdot \mathbf{E}\left\{ e^{-2\frac{\lambda}{2}|P+N_1|^2} \right\} \right. \\ &\quad \left. + \cdots + 1 \cdot (-1)^{M_p-1} \cdot \mathbf{E}\left\{ e^{-(M_p-1)\frac{\lambda}{2}|P+N_1|^2} \right\} \right\} \\ &= 1 - \left\{ \binom{M_p-1}{1} \cdot (-1)^1 \cdot \frac{1}{2} e^{-\frac{P}{2\sigma_w^2}} + \binom{M_p-1}{2} \cdot (-1)^2 \cdot \frac{1}{3} e^{-\frac{2P}{3\sigma_w^2}} \right. \\ &\quad \left. + \cdots + 1 \cdot (-1)^{M_p-1} \cdot \frac{1}{M_p} e^{-\frac{(M_p-1)P}{M_p\,\sigma_w^2}} \right\}. \end{aligned} \tag{7.38}$$

Additionally, based on different modulation method, the SER of OFDM data carrying signal can be evaluated numerically.

7.4.3 Cross-layer Optimization

In our proposed cross-layer authentication scheme, the PCP sequence is changing continuously to enhance the authentication performance of PCP-OFDM system. The PCP changing should guarantee the communications performance as well. Therefore, the performances in terms of robustness and transmitting efficiency, which are both affected by introducing of PCP, are used as important metrics to direct the PCP changing. Denoting that the set of all available PCP configurations at time t is

$$\Omega_t = \{(P_1, M_{P1}), (P_2, M_{P2}), (P_3, M_{P3}), (P_4, M_{P4}), ...\}. \tag{7.39}$$

To implement continuous authentication, transmitter needs to change the configuration of PCP continuously. We denote that the probability of using the configuration (P_i, M_{Pi}) is Pr_{ci}, thus, $\{Pr_{c1}, Pr_{c2}, Pr_{c3}, Pr_{c4}, ...\}$ is the probability set corresponding to the PCP configuration set. In order to maintain the best system performance, it is necessary for the transmitter to find the optimal transmission policy from all available scenarios. The optimization process can be

formulated by

$$U(t) = \max\left\{\sum_i Pr_{ci}\left(E_N^t(P_i, M_{Pi}) + R_D \cdot \frac{N}{P_i + N}\right)\right\},$$
$$s.t. \quad \sum_i Pr_{ci} = 1 \quad and \quad Pr_{ci} \geq 0, \tag{7.40}$$

where R_D is the received data rate of PCP-OFDM signal. $E_N^t(P_i, M_{Pi})$ is the normalized robustness performance of PCP with the ith configuration at time t, defined by

$$E_N^t(P_i, M_{Pi}) = \frac{E^t(P_i, M_{Pi}) - \min\limits_{\Omega_t}(\mathbf{E})}{\max\limits_{\Omega_t}(\mathbf{E}) - \min\limits_{\Omega_t}(\mathbf{E})}, \tag{7.41}$$

where $\mathbf{E} = \{E(P_1, M_{P1}), E(P_2, M_{P2}), E(P_3, M_{P3}), E(P_4, M_{P4}), \ldots\}$.

Based on the equation (7.40), the proposed system can adapt its operating parameters continuously and share system adaptation information with the legitimate receiver using the physical layer PCP signaling link.

7.5 Simulation Results

In this section, simulation results are presented to confirm the effectiveness of our proposed authentication system. Herein, the traditional CP-OFDM is employed in the comparison of system performance. More specifically, PCP-OFDM symbols are generated based on our design of transmitter in Figure 7.1, where the numbers of data subcarriers and the corresponding lengths of PCP are $N = \{128, 256, 512\}$ and $P = \{32, 64, 128\}$, respectively. The OFDM signals are modulated with 4-QAM modulation, and CP has same length as PCP sequences in the same case. Moreover, the size of local PCP library (M_p) is 31 in the simulations. Additionally, Three different channel mode, one AWGN channel, and two multipath Rayleigh fading channels are used. Under a sampling frequency of 10 MHz, one multipath channel has a length of 3 with the maximum Doppler shift 10 Hz, and the length of the other multipath channel is 5 with the maximum Doppler shift 100 Hz.

The error rate of PCP detection is illustrated under different lengths of PCP sequences in

Figure 7.5. Since data recovery at the receiver in our proposed system relies on correct PCP detection, low error rate of PCP detection was expected. As it can be seen from Figure 7.5, low error probability of PCP detection is achieved in the range of low SNR values, and larger size of PCP sequence can perform even lower error probability. In addition, this Figure shows that the closed-form exprsseion of PCP detection error rate derived in equations (7.33) and (7.38) coincides with the corresponding Monte-Carlo results as it was expected.

Figure 7.6 shows the overall error detection probability with different lengths of PCP under a multipath fading channel, and the performance of our proposed system is compared with that of the traditional CP-OFDM system. For fairness, the size of CP is adjusted accordingly as the length of PCP is changing based on the cross-layer optimization process. This figure shows that the overall error detection rate is not affected by changing the lengths of guard interval (i.e., the lengths of CP or PCP). Additionally, traditional CP-OFDM system performs slightly better in overall error detection than our proposed system when SNR is larger than 10 dB, but similar to CP-OFDM, our proposed system provides robust system performance under a multipath fading channel.

Figure 7.7 illustrates the overall error detection rate under three different channels. As a comparison, the error probability of the traditional CP-OFDM system is numerically evaluated as well. Herein, the size of PCP sequence is fixed to be 128. As it can be seen from Figure 7.7, when the SNR value is increasing, the performance in the overall error detection for PCP-OFDM and CP-OFDM decreases exponentially under an AWGN channel, while the performance approximates to a linear decrease under multipath Rayleigh fading channels. Additionally, under the AWGN channel, the overall error probability of PCP-OFDM performs similar to that of the traditional CP-OFDM. The performance difference between PCP-OFDM and CP-OFDM is negligible under multipath fading channels.

7.6 Summary

A new continuous physical layer authentication based on a novel adaptive OFDM system with time-varying transmission parameters has been proposed in this Chapter. In the proposed system, continuous authentication has been achieved through the transmission parameter adap-

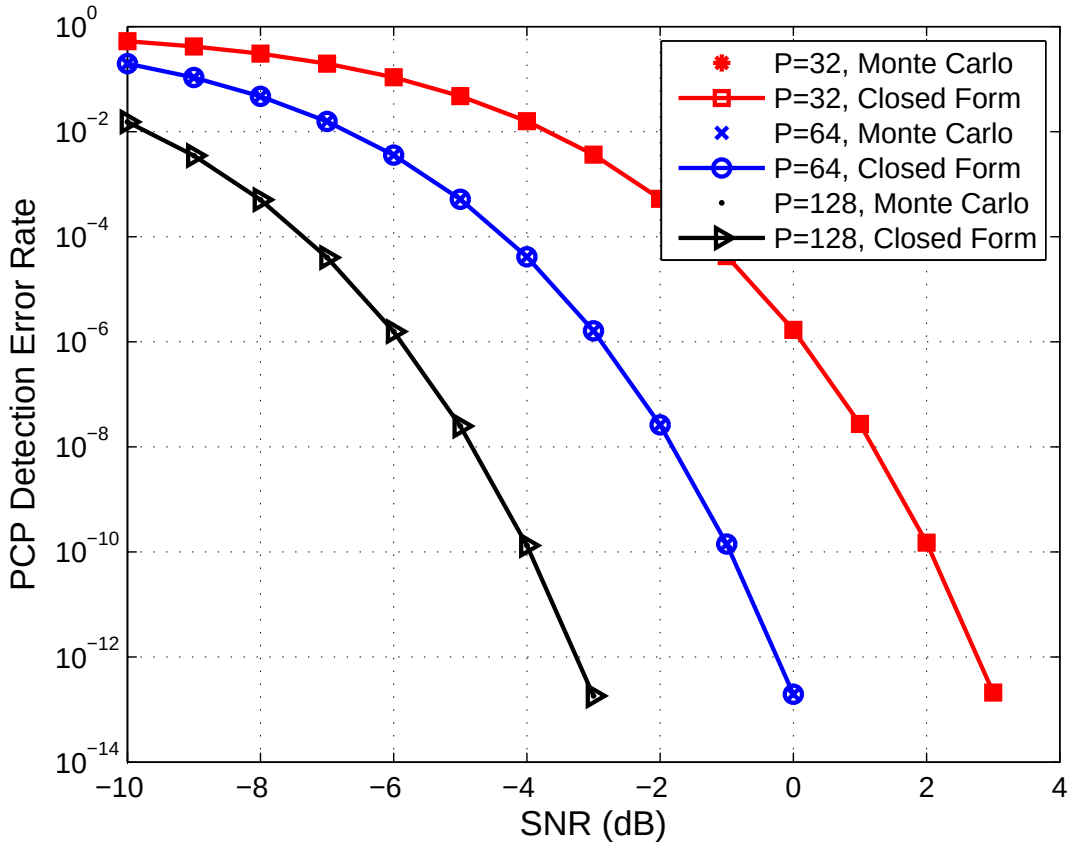

Figure 7.5: PCP detection error rate under different lengths of PCP.

tation, which was enabled by the additional signalling link between the transmitter and receiver. The PCP sequences were designed with the same time and frequency domain characteristics to avoid detection by adversary. By using PCP, time-varying physical layer transmission parameters of an OFDM system can therefore be securely transmitted between the legitimate users. The robustness, stealth and system capacity of the proposed PCP-OFDM system have been analyzed in this Chapter. Lastly, the security performance of the proposed PCP-OFDM system has been verified through numerical simulations.

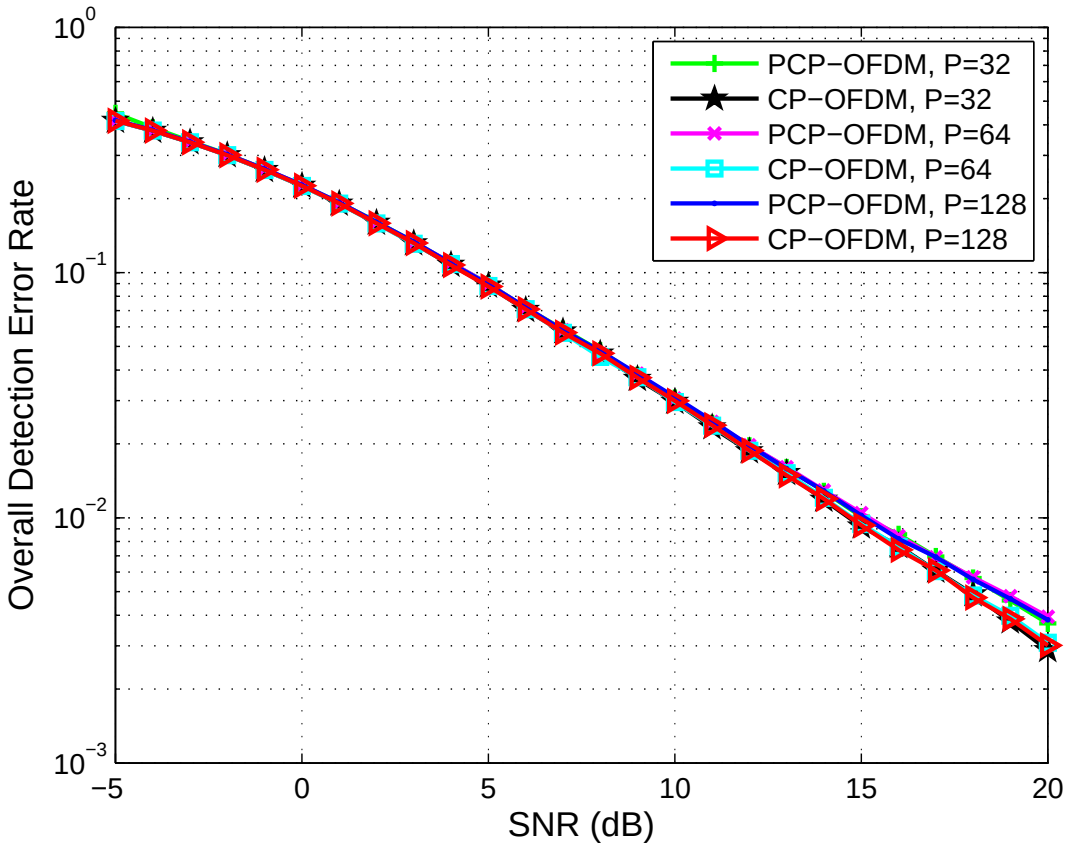

Figure 7.6: Overall detection error rate under different lengths of PCP.

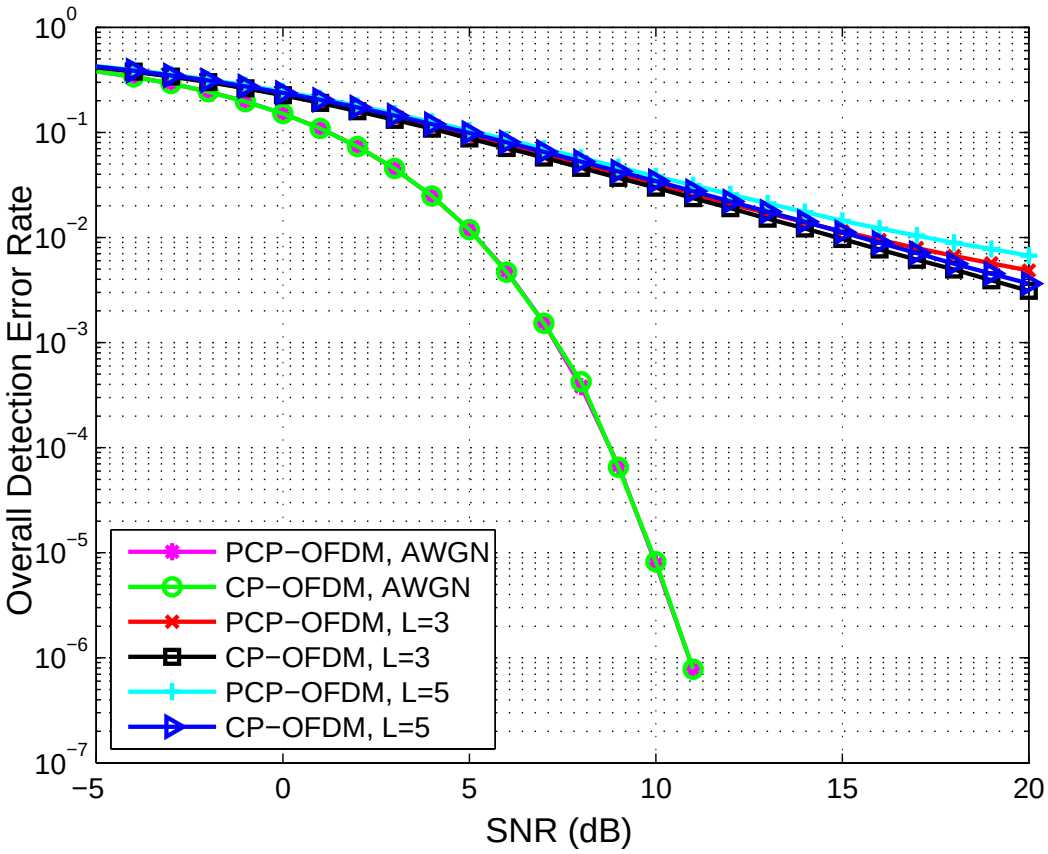

Figure 7.7: Overall detection error rate under three different channels.

Chapter 8

Conclusions and Future Work

This final chapter summarizes our contributions and points out several topics for future study.

8.1 Conclusions

In wireless communications, the notion of physical layer security exploiting the security mechanisms of physical level, is a new promising paradigm for secure wireless networks. Although physical layer security has the potential of significantly enhancing the security level of wireless systems by exploring unique features of wireless medium, it is fair to acknowledge that the effectiveness and robustness of existing physical layer security approaches are challenged under severe channel conditions in practice. In this dissertation, we have mainly investigated the physical layer authentication to enhance the security performance of wireless systems.

In Chapter 2, security challenges of wireless communications have been illustrated first, and then addressed based on a comprehensive literature survey of existing wireless security techniques. Moreover, the system modeling of conventional OFDM has been introduced, and the security vulnerabilities of wireless OFDM systems have been discussed as well.

In Chapter 3, we have proposed a robust physical layer authentication scheme for wireless communications based on a hypothesis testing of the inherent properties of CIR in a time-varying multipath environment. The variation between two consecutive CIRs from a transmit-

ter of interest was monitored at the receiver in order to distinguish between different transmitters for authentication purpose. To improve the authentication performance, we developed a new test statistic based on the difference between noise-mitigated CIRs in order to minimize the impact of noise and interference from the wireless environment. To achieve this goal, a SNR-dependent threshold was utilized to eliminate the excessive noise in the estimated CIRs prior to conducting the authentication process. An adaptive threshold for authentication decision has also been achieved based on the developed test statistic. The theoretical FAR and PD have been analyzed to evaluate the robustness of the proposed authentication scheme. Additionally, an OFDM system were employed to validate the proposed scheme and the related theoretical analysis.

In Chapter 4, an enhanced CIR-based physical layer authentication scheme has been proposed to address the issue of unreliable spoofing detection caused by fast channel variation. Specifically, channel prediction technique has been employed to predict future CIRs that were further exploited in the authentication analysis. Moreover, multiple CIR differences were observed by the receiver in a long range based on the channel predictor in order to increase the robustness of decision procedures. In order to find optimal value of the threshold in decision rule, an optimization problem has been defined based on minimizing the total error rate under false alarm constraints. Finally, the performance of the proposed scheme have been validated by using Monte-Carlo method.

Another channel-based physical layer authentication enhancement scheme has been proposed in Chapter 5. Particularly, the characteristics of channel amplitude and multipath time delay spread were integrated in order to enhance the authentication performance. A two dimensional quantization method has been developed to preprocess the channel variations. More specifically, two one-bit quantizers were used to quantize the temporal channel variations in the dimensions of channel amplitude and path delay, respectively. By exploiting the one-bit quantizers, the proposed authentication scheme has been formulated as a simply hypothesis testing problem. For performance analysis, FAR and PD have been defined based on the developed test statistic, and their closed-form expressions have been derived as well. In order to evaluate the performance of the proposed scheme, Monte-Carlo method has been utilized and the results were compared with that of the closed-form derivations. Additionally, the optimal parameters

that satisfying our optimization problem were found by using exhaustive search method in the simulations.

In Chapter 6, motivated by the advantages of cooperative transmissions, a novel physical layer authentication scheme has been proposed by exploiting the advantages of AF cooperative relaying. The essence of the proposed scheme was to select the best relay among multiple AF relays, such that legitimate transmitter would experience better channel conditions than a spoofer. Towards this goal, two best relay selection schemes have been developed based on the notion of maximizing the SNR ratios of the legitimate link to the spoofing link at the destination and relays, respectively. For performance analysis, we defined our performance metrics based on the outage of effective SNR ratios and the probability of spoofing detection. The closed-form expressions of the outage probabilities for proposed relay selection schemes have been derived. The performance of the proposed authentication scheme were compared with that of a DT scheme. According to numerical results, the proposed scheme outperformed the benchmark method in terms of the outage and spoofing detection.

In Chapter 7, a new continuous physical layer authentication technique with time-varying transmission parameters has been investigated to enhance the security of wireless OFDM system. A PCP sequence, which introduced an additional signaling link to carry the time-varying transmission parameters, has been employed in each OFDM symbol for physical layer authentication. The new PCP sequences were generated with the same time and frequency domain characteristics as data-carrying OFDM signals to reduce the interception probability. With the proper recovery of system parameters and interference cancellation, only legitimate users can successfully decode the PCP sequence and obtain necessary parameters to decode OFDM data. In addition, a cross layer design approach, which leveraged the dependency among PCP configurations, authentication performance and transmitting performance, has been developed to continuously generate optimal PCPs according to dynamic communication conditions. Numerical simulations have shown the improvement in the system performance in terms of system robustness, security and stealth.

8.2 Future Work

There are several topics related to the presented research worthwhile for further study. Some of them are listed as follows:

- On the topic of CIR-based physical layer authentication in wireless communications, we investigated the inherent properties of CIR to achieve robust authentication performance. However, other physical layer attributes can be also explored and combined with CIR characteristics to enhance the authentication performance.

- In the proposed relay selection strategy for cooperative wireless communications, the best relay has been chosen among a collection of trusted relays. However, malicious nodes may impersonate authenticated relays in order to get access to the transmitted information and forward false messages to the destination. Considering a practical scenario without the assumption of a complete trust between relay nodes, cooperative jamming or cryptographic techniques can be exploited in relay selection to prevent malicious threats.

- Regarding to the enhancement of secure transmissions based on wireless OFDM systems, we proposed a continuous physical layer authentication technique to prevent passive eavesdroppers. Other security threats can also bring severe issues to the legitimate transmissions over wireless OFDM networks, thereby our work can be extended to a general scenario by exploiting the physical layer information to secure against several attacks.

Bibliography

[1] A. E. Earle, *Wireless Security Handbook*, Auerbach Publications, 2005.

[2] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66-74, Apr. 2011.

[3] Z. Li, W. Xu, R. Miller and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proc. ACM WiSe*, Sept. 2006, pp. 33-42.

[4] D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proc. ACM Workshop Wireless Security*, 2006, pp. 43-52.

[5] Y. Chen, W. Trappe and R. Martin, "Detecting and localizing wireless spoofing attacks," in *Proc. IEEE Sensor, Mesh and Ad Hoc Commun. and Networks*, Jun. 2007, pp. 193-202.

[6] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, "Fingerprints in the ether: using the physical layer for wireless authentication," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2007, pp. 4646-4651.

[7] P. L. Yu, J. S. Baras and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forens. Security*, vol. 3, no. 1, pp. 38-51, Mar. 2008.

[8] L. Xiao, L. J. Greenstern, N. B. Mandayam and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5948-5956, Dec. 2009.

[9] F. He, H. Man, D. Kivanc and B. McNair, "EPSON: enhanced physical security in OFDM networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1-5.

[10] J. K. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *Proc. IEEE Int. Conf. Commun. syst. and networks*, Mar. 2010, pp. 1-9.

[11] P. Baracca, N. Laurenti and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564-2573, Jul. 2012.

[12] D. Shan, K. Zeng, W. Xiang, P. Richardson and Y. Dong, "PHY-CRAM: physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas in Commun.*, vol. 31, no. 9, pp. 1817-1827, Sept. 2013.

[13] A. Candore, O. Kocabas and F. Koushanfar, "Robust stable radiometric fingerprinting for wireless devices," in *IEEE Int. Workshop Hardware-Oriented Security and Trust*, Jul. 2009, pp. 43-49.

[14] W. E. Cobb, E. D. Laspe, R. O. Baldwin, M. A. Temple and Y. C. Kim, "Intrinsic Physical-Layer Authentication of Integrated Circuit," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 1, pp. 14-24, Feb. 2012.

[15] H. Li, X. Wang and Y. Zou, "Exploiting transmitter I/Q imbalance for estimating the number of active users," in *Proc. IEEE Global Commun. Conf.*, Dec. 2013, pp. 3318-3322.

[16] W. Hou, X. Wang, J.-Y. Chouinard and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658-1667, May 2014.

[17] M. M. Ur Rahman, A. Yasmeen and J. Gross, "PHY layer authentication via drifting oscillators," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 716-721.

[18] M. C. Vanderveen, A.-J. van der Veen and A. Paulraj, "Estimation of multipath parameters in wireless communications," *IEEE Trans. Signal Processing*, vol. 46, no. 3, pp. 682-290, Mar. 1998.

[19] A. Mishra, M. Shin and W. A. Arbaugh, "Your 802.11 network has no clothes," *IEEE Commun. Magazine*, pp. 44-51, 2002.

[20] D. Prabakar, M. Marikkannan and S. Karthik, "Various security threats and issues in wireless networks: a survey," *Int. J. Adv. Research Comput. Eng. and Technol.*, vol. 1, no. 10, pp. 296-299, Dec. 2012.

[21] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[22] A. E. Earle, *Wireless Security Handbook*, Auerbach Publications, 2005.

[23] H. Altunbasak, S. Krasser, H. L. Owen, J. Grimminger, H.-P. Huth and J. Sokol, "Securing layer 2 in local area networks," in *Proc. Int. Conf. Networking*, Apr. 2005, pp. 699-706.

[24] E. Cole, J. Fossen, S. Northcutt and H. Pomeranz, *SANS Security Essentials with CISSP CBK*, SANS Press, 2003.

[25] K. Zeng, K. Govindan and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56-62, Oct. 2010.

[26] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications (2nd Edn.)*, Springer, 2007.

[27] B. Schneier, "Cryptographic design vulnerabilities," *IEEE Comput.*, vol. 31, no. 9, pp. 29-33, Sept. 1998.

[28] Y. Sun, W. Trappe and K. J. R. Liu, *Network-Aware Security for Group Communications*, Springer, 2007.

[29] R. Housley and W. Arbaugh, "Security problems in 802.11-based networks," *Commun. Of the ACM*, vol. 46, no. 5, pp. 31-34, 2003.

[30] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 40-47, Feb. 2012.

[31] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. Journal*, vol. 28, 1949.

[32] W. C. Jakes Jr., *Microwave Mobile Communications*. Wiley, 1974.

[33] Y. Liu, S. C. Draper and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 5, pp. 1484-1497, Oct. 2012.

[34] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 1520-1524.

[35] F. He, W. Wang and H. Man, "REAM: rake receiver enhanced authentication method," in *Proc. IEEE Military Commun. Conf.*, Oct. 2010, pp. 2205-2210.

[36] V. Brik, S. Banerjee, M. Gruteser and S. Oh, "Wireless device identification with radiometric signatures," In *Proc. ACM Int. Conf. Mobile Computing and Networking*, Sept. 2008, pp. 116-127.

[37] W. E. Cobb, E. W. Garcia, M. A. Temple, R. O. Baldwin and Y. C. Kim, "Physical layer identification of embedded devices using RF-DNA fingerprinting," in *Proc. IEEE Military Commun. Conf.*, Oct. 2010, pp. 2168-2173.

[38] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," *Canadian Journal Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27-33, 2007.

[39] W. C. Suski II, M. A. Temple, M. J. Mendenhall and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in *Proc. IEEE Global Commun. Conf.*, Nov. 2008, pp. 1-5.

[40] V. Lakafosis, "RF fingerprinting physical objects for anticounterfeiting applications," *IEEE Trans. Microw. Theory Tech.*, vol. 59, no. 2, pp. 504-514, Feb. 2011.

[41] J. G. Proakis, *Digital Communications*, 4th edn., New York: McGraw-Hill, 2001.

[42] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Sept. 2005, pp. 2152-2155.

[43] Z. Li, W. Trappe and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. Conf. Inform. Sci. Syst.*, Mar. 2007, pp. 905-910.

[44] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inform. Theory*, Jun. 2007, pp. 2466-2470.

[45] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: the MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.

[46] S. Shafiee, N. Liu and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: the 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033-4039, Sept. 2009.

[47] A. Khisti, G. Wornell, A. Wiesel and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int Symp. Inform. Theory*, Jun. 2007, pp. 2471-2475.

[48] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inform. Theory*, Jul. 2008, pp. 524-528.

[49] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: the MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[50] T. Liu and S. Shamai, "A note on the secrecy capacity of the multipleantenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2547-2553, Jun. 2009.

[51] P. L. Yu and B. M. Sadler, "MIMO authentication via deliberate fingerprinting at the physical layer," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 606-615, Sept. 2011.

[52] N. Goergen, W. S. Lin, K. J. R. Liu and T. C. Clancy, "Authenticating MIMO transmissions using channel-like fingerprinting," in *Proc. IEEE Global Commun. Conf.*, Dec. 2010, pp. 1-6.

[53] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, "MIMO-assisted channel-based authentication in wireless networks," in *Proc. IEEE Conf. Inf. Sci. and Syst.*, Mar. 2008, pp. 642-646.

[54] X. Li and J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Commun.*, vol. 2, no. 3, pp. 24-32, May 2007.

[55] H. Wen and G. Gong, "A cross-layer approach to enhance the security of wireless networks based on MIMO," in *Proc. IEEE Conf. Inf. Sci. and Syst.*, Mar. 2009, pp. 935-939.

[56] H. Wen, G. Gong and P.-H. Ho, "MIMO cross-layer secure communication architecture based on STBC," in *Proc. IEEE Global Commun. Conf.*, Dec. 2010, pp. 1-5.

[57] J. Garg, P. Mehta and K. Gupta, "A review on cooperative communication protocols in wireless world," *Int. Journal Wireless & Mobile Networks*, vol. 5, No. 2, Apr. 2013, pp. 107-126.

[58] A. Bletsas, A. Lippnian and D. P. Reed, "A simple distributed method for relay selection in cooperative diversity wireless networks, based on reciprocity and channel measurements," in *Proc. IEEE Vehicular Technology Conference (VTC Spring)*, Jun. 2005, pp. 1484-1488.

[59] A. Bletsas, A. Khisti, D. P. Reed and A. Lippman,, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, pp. 659-672, Mar. 2006.

[60] E. C. van der Meulen, "Transmission of information in a T-terminal discrete memoryless channel," Ph.D. dissertation, Univ. California, Berkeley, CA, Jun. 1968.

[61] E. C. van der Meulen. *Three-Terminal Communication Channels. Advances in Applied Probability*, 1971.

[62] T. M. Cover and A. A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inform. Theory*, vol. 25, no. 5, pp. 572-584, Sept. 1979.

[63] K. J. R. Liu, A. K. Sadek, W. Su and A. Kwasinski. *Relay Channels and Protocols. In Cooperative Communication and Networking*, Cambridge University Press, 2009.

[64] M. Dohler and Y. Li. *Cooperative Communications: Hardware, Channel and PHY*. John Wiley and Sons, 2010.

[65] Q. Li, R. Q. Hu, Q. Yi and G. Wu, "Cooperative wireless communications for wireless networks: techniques and applications in LTE-advanced systems," *IEEE Wireless Commun.*, vol. 19, no. 2, pp. 22-29, Apr. 2012.

[66] C. Chen, B. Zheng, X. Zhao and Z. Yan, "A novel weighted cooperative routing algorithm based on distributed relay selection," in *Proc. IEEE Int. Symp. Wireless Pervasive Computing*, Feb. 2007, pp. 5-7.

[67] S. Abdulhadi, M. Jaseemuddin and A. Anpalagan, "A survey of distributed relay selection schemes in cooperative wireless ad hoc networks," *Wireless Pers. Commun.*, vol. 63, no. 4, pp. 917-935, Apr. 2012.

[68] P. Liu, Z. Tao, Z. Lin, E. Erkip and S. Panwar, "Cooperative wireless communications: a cross-layer approach", *IEEE Wireless Commun.*, vol. 13, no. 4, pp. 84-92, Aug. 2006.

[69] W. Chen, L. Dai, K. B. Letaief and Z. Cao, "A unified cross-layer framework for resource allocation in cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 8, pp. 3000-3012, Aug. 2008.

[70] Y. Chen, Y. Yang and W. Yi, "A cross layer strategy for cooperative diversity in wireless sensor networks," *Journal of Electronics (China)*, vol. 29, no. 1-2, pp. 33-38, Mar. 2012.

[71] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Secure wireless communication via cooperation," In *Proc. IEEE Conf. Commun., Control, and Computing*, Sept. 2008, pp. 1132-1138.

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

[73] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

[74] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inform. Theory*, vol. 57, no. 1, pp. 137-155, Jan. 2011.

[75] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1-5.

[76] G. Zheng, L.-C. Choo and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Processing*, vol. 59, no. 3, pp. 1317-1322, Mar. 2011.

[77] I. Krikidis, J. S. Thompson, P. M. Grant and S. McLaughlin, "Power allocation for cooperative-based jamming in wireless networks with secrecy constraints," in *Proc. IEEE Workshops Global Commun. Conf.*, Dec. 2010, pp. 1177-1181.

[78] L. Tang, X. Gong, J. Wu and J. Zhang, "Secure wireless communication via cooperative relaying and jamming," in *Proc. IEEE Workshops Global Commun. Conf.*, Dec. 2011, pp. 849-853.

[79] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communication," *IEEE Trans. Inf. Forens. Security*, vol. 2, no. 2, pp. 198-212, Jun. 2007.

[80] IEEE Standard, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Network-Specific Requirement - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," Jun. 2007.

[81] IEEE Standard, "IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput," Oct. 2009.

[82] IEEE Standard, "The Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," Jun. 2004.

[83] 3GPP LTE Encyclopedia, "An Introduction to LTE," Dec. 2010.

[84] H. Holma and A. Toskala, *LTE for UMTS OFDMA and SC-FDMA Based Radio Access*, Wiley, Ed., 2009.

[85] Y. Li and G. L. Stuber, Eds., *Orthogonal Frequency Division Multiplexing for Wireless Communications*. New York, NY: Springer-Verlag, 2006.

[86] R.W. Chang, "Synthesis of band-limited orthogonal signals for multichannel data transmissions," *Bell Syst. Tech. Journal*, vol. 45, pp. 1775-1796, Dec. 1966.

[87] S. B. Weinstein and P. M. Ebert, "Data transmission by frequency division multiplexing using the discrete Fourier transform," *IEEE Trans. Commun.*, vol. 19, no. 10, pp. 628-634, Oct. 1971.

[88] T. C. Clancy, "Efficient OFDM denial: pilot jamming and pilot nulling", in *Proc. IEEE Int. Conf. Commun.*, Jun. 2011.

[89] C. Patel, G. Stuber and T. Pratt, "Analysis of OFDM/MC-CDMA under imperfect channel estimation and jamming," in *Proc. IEEE Wireless Commun. and Networking Conf.*, Mar. 2004, pp. 954-958.

[90] M. J. L. Pan, T. C. Clancy and R. W. McGwier, "Jamming attacks against OFDM timing synchronization and signal acquisition," in *Proc. IEEE Military Commun. Conf.*, Oct. 2012, pp. 1-7.

[91] T. Cui and C. Tellambura, "Blind receiver design for OFDM systems over doubly selective channels," *IEEE Trans. Wireless Commun.*, vol. 55, no. 5, pp. 906-917, May 2007.

[92] H. Li, Y. Bar-Ness, A. Abdi, O. S. Somekh and W. Su, "OFDM modulation classification and parameters extraction," in *Proc. IEEE Int. Conf. Cognitive Radio Oriented Wireless Networks and Commun.*, 2006, pp. 1-6.

[93] M. Khan, M. Asim, V. Jeoti and R. Manzoor, "On secure OFDM system: chaos based constellation scrambling," In *Proc. IEEE Int. Conf. Intelligent and Advanced Systems*, Nov. 2007, pp. 484-488.

[94] A. Chorti, "Masked-OFDM: a physical layer encryption for future OFDM applications," in *Proc. IEEE Workshops Global Commun. Conf.* , Dec. 2010, pp. 1254-1258.

[95] D. Reilly and G. Kanter, "Noise-enhanced encryption for physical layer security in an OFDM radio," In *Proc. IEEE radio and wireless symposisum*, Jan. 2009, pp. 344-347.

[96] U. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1350-1356, Jul. 2000.

[97] L. Xiao, L. J. Greenstein, N. B. Mandayam and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. on Wireless Commun.*, vol. 7, no. 7, pp. 2571-2579, Jul. 2008.

[98] N. Patwari, and S. K. Kasera, "Temporal link signature measurements for location distinction," *IEEE Trans. on Mobile Computing*, vol. 10, no. 3, pp. 449-462, Mar. 2011.

[99] S. Rosati, G. E. Corazza and A. V. Coralli, "OFDM channel estimation with optimal threshold-based selection of CIR samples," in *Proc. IEEE Global Telecommunication Conference (GLOBECOM)*, Nov. 30-Dec. 4 2009, pp. 1-7.

[100] F.-X. Socheleau, A. A.-El-Bey and S. Houcke, "Non data-aided SNR estimation of OFDM signals," in *IEEE Communication Letters*, vol. 12, no. 11, pp. 813-815, Nov. 2008.

[101] A. Mood, A. G. Franklin and C. B. Duane, *Introduction to the Theory of Statistics (Third Edition)*. McGraw-Hill, 1974.

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

[103] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the physical layer for enhanced security," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 63-70, Oct. 2010.

[104] F. J. Liu, X. Wang and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. IEEE Military Communications Conference (MILCOM)*, Nov. 2011, pp. 538-542.

[105] F. J. Liu, X. Wang and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE International Conference on Communications (ICC)*, pp. 4724-4728, Jun. 2013.

[106] M. K. Ozdemir and H. Arslan, "Channel estimation for wireless OFDM systems," *Commun. Surveys Tuts.*, vol. 9, no. 2, pp. 18-48, Second Quarter 2007.

[107] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd Edition, Prentice-Hall, 2002.

[108] M. K. Simon, *Probability Distributions Involving Gaussian Random Variables: A Handbook for Engineers and Scientists*. Springer, 2002.

[109] M. Shin, J. Ma, A. Mishra and W. A. Arbaugh, "Wireless network security and interworking," *Proc. IEEE*, vol. 94, pp. 455-466, Feb. 2006.

[110] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[111] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, 1978.

[112] G. J. Simmons, "Authentication theory/coding theory," in *Proc. CRYPTO84 on Advances in Cryptology*, NewYork: Springer-Verlag, 1985, pp. 411-431.

[113] L. Lai, H. Gamal, and H. Poor, "Authentication over noisy channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 906-916, Feb. 2009.

[114] A. Duel-Hallen, "Fading channel prediction for mobile radio adaptive transmission systems," *Proc. IEEE*, vol. 95, no. 12, pp. 2299-2313, Dec. 2007.

[115] S. Haykin, *Neural Networks and Learning Machines (Third Edition)*. Prentice Hall, 2008, ch. 3.

[116] A. Papulis, *Probability, Random Variables, and Stochastic Processes (Third Edition)*. McGraw-Hill, 1991.

[117] V.-H. Pham, X. Wang and J. Nadeau, "Long term cluster-based channel envelope and phase prediction for dynamic link adaptation," *IEEE Commun. Letters*, vol. 15, no. 7, pp. 713-715, Jul. 2011.

[118] J. Li, A. P. Petropulu and H. V. Poor, "Cooperative transmission for relay networks based on second-order statistics of channel state information," *IEEE Trans. on Signal Processing*, vol. 59, no. 3, pp. 1280-1291, Mar. 2011.

[119] J. Li, A. P. Petropulu and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. on Signal Processing*, vol. 59, no. 10, pp. 4985-4997, Oct. 2011.

[120] Z. Ding, K. K. Leung, D. L. Goeckel and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.* vol. 30, no. 2, pp. 359-368, Feb. 2012.

[121] J. Chen, R. Zhang, L. Song, Z. Han and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forens. and Security*, vol. 7, no. 1, pp. 310-320, Feb. 2012.

[122] H.-M. Wang, Q. Yin and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. on Signal Processing*, vol. 60, no. 7, pp. 3532-3545, Jul. 2012.

[123] J. Kim, A. Ikhlef and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *Journal of Communications and Networks*, vol. 14, no. 4, pp. 364-373, Aug. 2012.

[124] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus and A. Yener, "Cooperative security at the physical layer: a summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16-28, Sept. 2013.

[125] Y.-W. P. Hong, P.-C. Lan and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 29-40, Sept. 2013.

[126] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[127] I. Krikidis, J. Thompson, S. McLaughlin and N. Goertz, "Amplify-and-forward with partial relay selection," *IEEE Commun. Letter*, vol. 12, no. 4, pp. 235-237, Apr. 2008.

[128] J. N. Laneman, D. N. C. Tse and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062-3080, Dec. 2004.

[129] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Alan Jeffrey and Daniel Zwillinger (eds.), Seventh Edition, Academic Press, 2007.

[130] Y. Sheng, K. Tan, G. Chen, D. Kotz and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *Proc. IEEE INFOCOM 2008*, Apr. 2008, pp. 1768-1776.

[131] M. Bogdanoski, P. Latkoski, A. Risteski and B. Popovski, "IEEE 802.16 security issues: a survey," in *Proc. IEEE TELFOR 2008*, Nov. 2008, pp. 199-202.

[132] H. Yang, F. Ricciato, S. Lu and L. Zhang, "Securing a wireless world," *Proc. IEEE*, vol. 94, no. 2, pp. 442-454, Feb. 2006.

[133] X. Wang, Y. Wu and H.-C. Wu, "A new adaptive OFDM system with precoded cyclic prefix for cognitive radio," in *Proc. IEEE ICC*, May 2008, pp. 3642-3646.

[134] X. Wang, P. Ho and Y. Wu, "Robust channel estimation and ISI cancellation for OFDM systems with suppressed features," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 5, pp. 963-972, May 2005.

[135] X. Wang, F. J. Liu, D. Fan, H. Tang and P. C. Mason, "Continuous physical layer authentication using a novel adaptive OFDM system," in *Proc. IEEE International Conference on Communications (ICC)*, Jun. 2011, pp. 1-5.

[136] X. Wang, H. Li and H. Lin, "A new adaptive OFDM system with precoded cyclic prefix for dynamic cognitive radio communications," *IEEE J. Sel. Areas in Commun.*, vol. 29, no. 2, pp. 431-442, Feb. 2011.

[137] B. Muquet, Z. Wang, G. B. Giannakis, M. D. Courville and P. Duhamel, "Cyclic prefixing or zero padding for wireless multicarrier transmissions," in *IEEE Trans. Commun.*, vol. 50, no. 12, pp. 2136-2148, Dec. 2002.

Appendix A

Derivation of the Probability $P(S = k)$

We assume that a random variable S is a sum of two random variables S_T and S_Z, i.e., $S = S_T + S_Z$. S_T and S_Z are independent to each other and their values are determined from two intervals, that is, $0 \leq S_T \leq L$ and $0 \leq S_Z \leq L-1$, respectively. Therefore, we can easily obtain that $0 \leq S \leq 2L-1$. In this Appendix, we derive the probability of S equal to a fixed value k, where k is a non-negative integer between 0 and $2L-1$.

First of all, we derive the probabilities $P(S_T = i)$ and $P(S_Z = j)$ where i and j are two non-negative integers with $0 \leq i \leq L$ and $0 \leq j \leq L-1$. Based on the definitions of S_T and S_Z in equations (5.11) and (5.12), the probabilities $P(S_T = i)$ and $P(S_Z = j)$ can be derived by

$$P(S_T = i) = \binom{L}{i} (P_T)^i (1-P_T)^{L-i}, \tag{A.1}$$

and

$$P(S_Z = j) = \binom{L-1}{j} (P_Z)^j (1-P_Z)^{L-1-j}, \tag{A.2}$$

where P_T is the probability of the output of quantizer $Q_T[\cdot]$ equal to one, and P_Z is the probability of the output of quantizer $Q_Z[\cdot]$ equal to one.

Since the value of S is the sum of S_T and S_Z and $0 \leq k \leq 2L-1$, two cases are considered to derive the probability $P(S = k)$. Particularly, if $0 \leq k \leq L-1$, the probability $P(S = k)$ can

be expressed by

$$
\begin{aligned}
P(S = k) &= P(S_T = 0, S_Z = k) + P(S_T = 1, S_Z = k-1) \\
&\quad + \cdots + P(S_T = k, S_Z = 0) \\
&= P(S_T = 0)P(S_Z = k) + P(S_T = 1)P(S_Z = k-1) \\
&\quad + \cdots + P(S_T = k)P(S_Z = 0) \\
&= \binom{L}{0}(1-P_T)^L\binom{L-1}{k}(P_Z)^k(1-P_Z)^{L-1-k} \\
&\quad + \binom{L}{1}P_T(1-P_T)^{L-1}\binom{L-1}{k-1}(P_Z)^{k-1}(1-P_Z)^{L-k} \\
&\quad + \cdots + \binom{L}{k}(P_T)^k(1-P_T)^{L-k}\binom{L-1}{0}(1-P_Z)^{L-1} \\
&= \sum_{v=0}^{k}\binom{L}{v}(P_T)^v(1-P_T)^{L-v} \times \binom{L-1}{k-v}(P_Z)^{k-v}(1-P_Z)^{L-1-k+v},
\end{aligned} \tag{A.3}
$$

If $L \le k \le 2L-1$, the probability $P(S = k)$ can be derived by

$$
\begin{aligned}
P(S = k) &= P(S_T = k-L+1, S_Z = L-1) \\
&\quad + P(S_T = k-L+2, S_Z = L-2) \\
&\quad + \cdots + P(S_T = L, S_Z = k-L) \\
&= P(S_T = k-L+1)P(S_Z = L-1) \\
&\quad + P(S_T = k-L+2)P(S_Z = L-2) \\
&\quad + \cdots + P(S_T = L)P(S_Z = k-L) \\
&= \binom{L}{k-L+1}(P_T)^{k-L+1}(1-P_T)^{2L-k-1}\binom{L-1}{L-1}(P_Z)^{L-1} \\
&\quad + \binom{L}{k-L+2}(P_T)^{k-L+2}(1-P_T)^{2L-k-2} \times \binom{L-1}{L-2}(P_Z)^{L-2}(1-P_Z) \\
&\quad + \cdots + \binom{L}{L}(P_T)^L\binom{L-1}{k-L}(P_Z)^{k-L}(1-P_Z)^{2L-k-1} \\
&= \sum_{v=k-L}^{L-1}\binom{L}{k-v}(P_T)^{k-v}(1-P_T)^{L-k+v} \times \binom{L-1}{v}(P_Z)^v(1-P_Z)^{L-1-v}.
\end{aligned} \tag{A.4}
$$

Appendix B

Derivation of CDF of W_i

In this part, we derive the CDF of the random variable W_i defined in (6.21). The CDF of this random variable can be expressed as

$$\begin{aligned} P(W_i \leq w) &= P\Big(\frac{P_R|h_{R_iB}|^2 + (P_E\sigma^2_{ER_i} + \sigma^2_n)}{P_R|h_{R_iB}|^2 + (P_A\sigma^2_{AR_i} + \sigma^2_n)} \leq w\Big) \\ &= P\Big(P_R|h_{R_iB}|^2(1-w) \leq w(P_A\sigma^2_{AR_i} + \sigma^2_n) - (P_E\sigma^2_{ER_i} + \sigma^2_n)\Big). \end{aligned} \tag{B.1}$$

Depending on whether $P_A\sigma^2_{A,R_i}$ is smaller than or equal to $P_E\sigma^2_{E,R_i}$ or if it is greater than $P_E\sigma^2_{E,R_i}$, two different cases are possible. For the case that $P_A\sigma^2_{A,R_i} > P_E\sigma^2_{E,R_i}$, by considering the different possibilities, the CDF of W_i can be easily shown to be as follows

$$P(W_i \leq w) = \begin{cases} 1 & w \geq 1 \\ 1 - e^{\frac{w(P_A\sigma^2_{AR_i}+\sigma^2_n)-(P_E\sigma^2_{ER_i}+\sigma^2_n)}{-(1-w)P^2_R\sigma^2_{R_iB}}} & \frac{P_E\sigma^2_{ER_i}+\sigma^2_n}{P_A\sigma^2_{AR_i}+\sigma^2_n} < w < 1 \\ 0 & 0 \leq w \leq \frac{P_E\sigma^2_{ER_i}+\sigma^2_n}{P_A\sigma^2_{AR_i}+\sigma^2_n}. \end{cases} \tag{B.2}$$

Moreover, under the condition that $P_A\sigma^2_{A,R_i} \leq P_E\sigma^2_{E,R_i}$, CDF of W_i is equal to

$$P(W_i \leq w) = \begin{cases} 1 & w \geq \frac{P_E\sigma^2_{ER_i}+\sigma^2_n}{P_A\sigma^2_{AR_i}+\sigma^2_n} \\ e^{\frac{w(P_A\sigma^2_{AR_i}+\sigma^2_n)-(P_E\sigma^2_{ER_i}+\sigma^2_n)}{-(1-w)P^2_R\sigma^2_{R_i}B}} & 1 < w < \frac{P_E\sigma^2_{ER_i}+\sigma^2_n}{P_A\sigma^2_{AR_i}+\sigma^2_n} \\ 0 & 0 \leq w \leq 1. \end{cases} \tag{B.3}$$

Appendix C

Derivation of Integral $F(t)$

We define a definite integral function $F(t)$ as

$$F(t) = \int_0^u \frac{1}{(t+p_1)^2} e^{\frac{-p_2}{t}} dt, \tag{C.1}$$

where $u > 0$, $p_1 > 0$ and $p_2 > 0$.

Using the change of variable $s = \frac{1}{t}$, we can derive that

$$\begin{aligned} F(t) &= \int_{\frac{1}{u}}^{\infty} \frac{1}{(\frac{1}{s}+p_1)^2} e^{-p_2 s} \frac{ds}{s^2} \\ &= \int_{\frac{1}{u}}^{\infty} \frac{1}{(1+p_1 s)^2} e^{-p_2 s} ds, \end{aligned} \tag{C.2}$$

and using the change of variable $g = 1 + p_1 s$, we can further derive that based on [129, eq.(3.351.4)],

$$\begin{aligned} F(t) &= \frac{1}{p_1} e^{\frac{p_2}{p_1}} \int_{1+\frac{p_1}{u}}^{\infty} \frac{1}{g^2} e^{-\frac{p_2}{p_1} g} dg \\ &= \frac{1}{p_1} e^{\frac{p_2}{p_1}} \left(\frac{p_2}{p_1} \mathrm{Ei}\Big(-\frac{p_2}{p_1}(1+\frac{p_1}{u}) \Big) + \frac{e^{-\frac{p_2}{p_1}(1+\frac{p_1}{u})}}{1+\frac{p_1}{u}} \right). \end{aligned} \tag{C.3}$$

Curriculum Vitae

Name:	Jiazi Liu
Post-Secondary Education and Degrees:	Jilin University Changchun, Jilin, P. R. China 2003 - 2007 B.E.Sc Jilin University Changchun, Jilin, P. R. China 2007 - 2009 M.E.Sc The University of Western Ontario London, Ontario, Canada 2010 - 2015 Ph.D.
Related Work Experience:	Teaching Assistant The University of Western Ontario 2010 - 2013 Research Assistant The University of Western Ontario 2010 - 2015

Publications:

[1] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," submitted to *IEEE Wireless Commun.*.

[2] J. Liu and X. Wang, "Physical layer authentication enhancement using amplify-and-forward cooperative relays," submitted to *EURASIP J. Wirel. Commun. Netw.*.

[3] J. Liu, A. Refaey, X. Wang and H. Tang, "Reliability enhancement for CIR-based physical layer authentication," *Security and Communication Networks*, vol. 8, no. 4, pp. 661-671, Mar. 2015.

[4] F. J. Liu, X. Wang and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE International Conference on Communications (ICC)*, Jun. 2013, pp. 4724-4728.

[5] F. J. Liu, X. Wang and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. IEEE Military Communications Conference (MILCOM)*, Nov. 2011, pp. 538-542.

[6] X. Wang, F. J. Liu, D. Fan, H. Tang and P. C. Mason, "Continuous physical layer authentication using a novel adaptive OFDM system," in *Proc. IEEE International Conference on Communications (ICC)*, Jun. 2011, pp. 1-5.