11-23-2015 12:00 AM

# Wireless Device Authentication Techniques Using Physical-Layer Device Fingerprint

Peng Hao
*The University of Western Ontario*

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

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

# WIRELESS DEVICE AUTHENTICATION TECHNIQUES USING PHYSICAL-LAYER DEVICE FINGERPRINT

(Thesis format: Monograph)

by

Peng Hao

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

# Abstract

Due to the open nature of the radio signal propagation medium, wireless communication is inherently more vulnerable to various attacks than wired communication. Consequently, communication security is always one of the critical concerns in wireless networks. Given that the sophisticated adversaries may cover up their malicious behaviors through impersonation of legitimate devices, reliable wireless authentication is becoming indispensable to prevent such impersonation-based attacks through verification of the claimed identities of wireless devices.

Conventional wireless authentication is achieved above the physical layer using upper-layer identities and key-based cryptography. As a result, user authenticity can even be validated for the malicious attackers using compromised security key. Recently, many studies have proven that wireless devices can be authenticated by exploiting unique physical-layer characteristics. Compared to the key-based approach, the possession of such physical-layer characteristics is directly associated with the transceiver's unique radio-frequency hardware and corresponding communication environment, which are extremely difficult to forge in practice. However, the reliability of physical-layer authentication is not always high enough. Due to the popularity of cooperative communications, effective implementation of physical-layer authentication in wireless relay systems is urgently needed. On the other hand, the integration with existing upper-layer authentication protocols still has many challenges, e.g., end-to-end authentication. This dissertation is motivated to develop novel physical-layer authentication techniques in addressing the aforementioned challenges.

In achieving enhanced wireless authentication, we first specifically identify the technique challenges in authenticating cooperative amplify-and-forward (AF) relay. Since AF relay only works at the physical layer, all of the existing upper-layer authentication protocols are ineffective in identifying AF relay nodes. To solve this problem, a novel device fingerprint of AF relay consisting of wireless channel gains and in-phase and quadrature imbalances (IQI) is proposed. Using this device fingerprint, satisfactory authentication accuracy is achieved when the signal-to-noise ratio is high enough. Besides, the optimal AF relay identification system is studied to maximize the performance of identifying multiple AF relays in the low signal-to-noise regime and small IQI. The optimal signals for quadrature amplitude modulation and phase shift keying modulations are derived to defend against the repeated access attempts made by some attackers

with specific IQIs.

Exploring effective authentication enhancement technique is another key objective of this dissertation. Due to the fast variation of channel-based fingerprints as well as the limited range of device-specific fingerprints, the performance of physical-layer authentication is not always reliable. In light of this, the physical-layer authentication is enhanced in two aspects. On the one hand, the device fingerprinting can be strengthened by considering multiple characteristics. The proper characteristics selection strategy, measurement method and optimal weighted combination of the selected characteristics are investigated. On the other hand, the accuracy of fingerprint estimation and differentiation can be improved by exploiting diversity techniques. To be specific, cooperative diversity in the form of involving multiple collaborative receivers is used in differentiating both frequency-dependent and frequency-independent device fingerprints. As a typical combining method of the space diversity techniques, the maximal-ratio combining is also applied in the receiver side to combat the channel degeneration effect and increase the fingerprint-to-noise ratio.

Given the inherent weaknesses of the widely utilized upper-layer authentication protocols, it is straightforward to consider physical-layer authentication as an effective complement to reinforce existing authentication schemes. To this end, a cross-layer authentication is designed to seamlessly integrate the physical-layer authentication with existing infrastructures and protocols. The specific problems such as physical-layer key generation as well as the end-to-end authentication in networks are investigated. In addition, the authentication complexity reduction is also studied. Through prediction, pre-sharing and reusing the physical-layer information, the authentication processing time can be significantly shortened.

**Keywords:** Wireless communications, physical-layer authentication, device identification, device fingerprinting, diversity, amplify-and-forward relaying, cross-layer authentication.

*To my parents.*

# Acknowledgments

Pursuing doctoral degree in The University of Western Ontario is a memorable experience for me. Many people supported and helped me during my four years study.

First of all, I would like to express my gratitude to my supervisor, Dr. Xianbin Wang, for his precious guidance and constant supervision as well as giving helpful advise in my graduate career. Without Dr. Wang's inspiration and help, I am not able to complete this dissertation.

I would like to thank Dr. Ben Rubin for chairing my thesis defence exam. I also would like to thank the examiners Dr. Helen Tang, Dr. Evgueni Bordatchev, Dr. Anestis Dounavis and Dr. Vijay Parsa for reviewing and improving my dissertation.

I also would like to especially thank my friend Dr. Aydin Behnad, for his patient and selfless advise to my research projects. It is enjoyable to work and discuss the research problems with him. I would like to thank my "Big Friend", Mr. Mohamed Abu Sharkh, who supported me in many aspects during my living in Canada. I really appreciate every conversation that relieves my stress and every suggestion from this trustable friend. Also, my deep thanks to all other colleagues and friends I met in Canada. It is my great pleasure to make friends or/and work with them.

Last but most importantly, I own my heartfelt gratitude to my dearest parents. Although they are thousands of miles away from me during the days I studied in Canada, I can always get the strongest support from them! There are no words sufficient enough to express my full gratitude to my parents.

# Contents

# List of Figures

# List of Tables

# List of Abbreviations

| | |
|---|---|
| **5G** | 5th Generation Mobile Networks or Wireless Systems |
| **A/D** | Analog-to-Digital |
| **AF** | Amplify-and-Forward |
| **AFE** | Analog Front-End |
| **AP** | Access Point |
| **AWGN** | Additive White Gaussian Noise |
| **BS** | Base Station |
| **CBC-MAC** | Cipher Block Chaining Message Authentication Code |
| **CFO** | Carrier Frequency Offset |
| **CIR** | Channel Impulse Response |
| **CSI** | Channel State Information |
| **CSMA/CA** | Carrier Sense Multiplex Access with Collision Avoidance |
| **D/A** | Digital-to-Analog |
| **DF** | Decode-and-Forward |
| **DOA** | Direction of Arrival |
| **FA** | False Alarm |

| | |
|---|---|
| **FD** | Frequency-Dependent |
| **FI** | Frequency-Independent |
| **GLRT** | Generalized Likelihood Ratio Test |
| **GLRT-CLM** | Generalized Likelihood Ratio Test for Classic Linear Model |
| **i.i.d.** | Independent and Identically Distributed |
| **IP** | Internet Protocol |
| **I/Q** | In-phase and Quadrature-phase |
| **IQI** | In-phase and Quadrature-phase Imbalance |
| **LO** | Local Oscillator |
| **LPF** | Low-Pass Filter |
| **LRT** | Likelihood Ratio Test |
| **LS** | Least Square |
| **MAC** | Medium Access Control |
| **MD** | Miss Detection |
| **mmWave** | Millimeter Wave |
| **MRC** | Maximal-Ratio Combining |
| **OFDM** | Orthogonal Frequency-Division Multiplexing |
| **OSI** | Open System Interconnection |
| **PDF** | Probability Density Function |
| **PER** | Packet Error Rate |
| **PHY** | Physical-Layer |

**PSK** Phase Shift Keying

**QAM** Quadrature Amplitude Modulation

**QPSK** Quadrature Phase Shift Keying

**RF** Radio Frequency

**RSSI** Received Signal Strength Indicator

**RTT** Round-Trip Time

**SINR** Signal-to-Interference-plus-Noise Ratio

**SNR** Signal-to-Noise Ratio

# Chapter 1

# Introduction

## 1.1 Research Motivation

Although the shared nature of radio propagations enables convenient "anywhere" wireless access, it simultaneously introduces many security vulnerabilities to wireless systems. Compared to wired communication systems, the broadcast signals in wireless networks are accessible to both legitimate and illegitimate devices that are currently sharing the wireless medium. This feature becomes the root of security threats in wireless communications and it can be exploited for unauthorized access and even malicious attacks. Since the direct attacks are easy to detect, the sophisticated attacker usually covers its vicious behaviors through impersonating a legitimate entity. To clearly reveal this kind of attack scenario, Alice, Bob and Eve are introduced according to the terminologies of communication security [1]. As shown in Fig.1.1, Alice and Bob denote the intended wireless transmitter and receiver, respectively. Eve is the unauthorized attacker. Eve's objective is try to impersonate Alice and deceive Bob into bellieving that Bob is currently communicating with the legitimate Alice rather than Eve. Once the deceit is successful, the communication between Bob and Eve will be leaked and exposed to various malicious attacks.

In practice, authentication technique is used to protect the wireless systems from this kind of impersonation-based attacks. The concept of authentication is defined as [2]

*"Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system."* — The Special Publication 800 series.

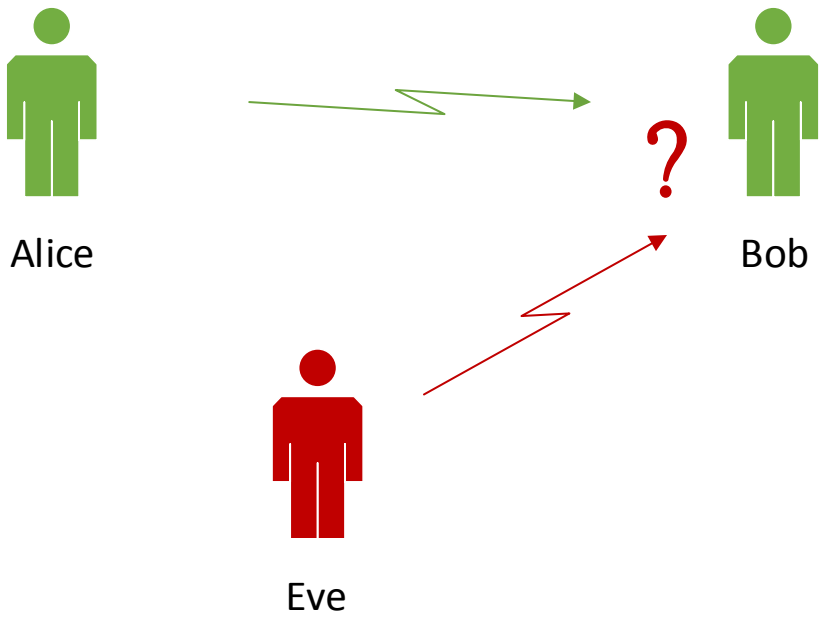


Figure 1.1: "Alice-Bob-Eve" attacking scenario.

In wireless systems, the objective of authentication is to verify the authenticity of the identities claimed by wireless devices. In the scenario of "Alice-Bob-Eve", authentication technique can be used to detect the presence of Eve. If the presence of an attacker is confirmed, the receiver is able to do some other actions for defending against Eve's illegitimate access. Therefore, wireless authentication is the primary task in protecting wireless communications.

Traditionally, authentication processing is accomplished above the physical layer through checking the upper-layer identities of devices and using key-based cryptography. However, due to the upper-layer identity is not directly associated with the stable hardware components of devices, the sophisticated attacker can easily change its digital address to a legitimate one for the sake of being identified as a legitimate device. Regarding the method of using key-based cryptography, it inherently suffers from many problems in key management, high computational cost of encryption algorithms and intolerable communication delay in wireless systems [3]. In light of this, the physical-layer authentication technique is emerging as a promising complement to the upper-layer methods.

Different from upper-layer security schemes, physical-layer authentication utilizes some unique physical-layer characteristics related to wireless transceivers to identify the signal trans-

mitter. These characteristics are used as the device fingerprint of wireless transmitters. Contrary to upper-layer identity and key that can be possessed by any devices, the physical-layer device fingerprint is directly associated with the unique hardware of wireless devices and communication channel, which is extremely difficult to mimic. These characteristics can be typically classified into two types, which are the wireless link attribute and radio-frequency analog front-end (RF-AFE) imperfection [4]. Specifically, the wireless channel reflects the unique communication environment between the intended transmitter and receiver. The RF-AFE imperfection is a distinguishable hardware feature generated from the imperfect device fabrication. These physical-layer characteristics, which represent the identity of the communicating transmitter, can automatically distort all transmitted signals. Also, the channel and RF-AFE imperfection estimation and compensation techniques are equipped in most present receivers so that the receiver can directly use these ready-made estimates for authentication without posing high hardware implementation cost or communication throughput reduction.

Although physical-layer authentication is drawing more research attention, many challenging issues remain for future works. We briefly summarize four main issues as follows.

First, the performance of current physical-layer authentication methods should be enhanced. At present, many authentication schemes using various physical-layer characteristics, such as channel state information (CSI) [5], received signal strength indicator (RSSI) [6], carrier frequency offset (CFO) [7] and in-phase and quadrature-phase (I/Q) imbalance [8], have been proposed. However, all these characteristics are not perfect device fingerprints. Regarding the channel-based characteristics (e.g., CSI and RSSI), the most challenging issue is the timely monitoring and updating of the wireless channel states. This authentication scheme relies on checking the similarity of two continuous channel related attributes. In practice, the performance is usually unsatisfactory in mobile and open outdoor scenarios. In mobile cases, the channel states vary dramatically, resulting in high false alarm rates. In outdoor cases, as a result of lacking multipath effect, the fingerprints cannot be clearly differentiated. The RF-AFE imperfection-based device fingerprint usually has the problem of limited range. Since the hardware imperfections are usually small values in practice, the accurate differentiation of such delicate differences becomes the key point of obtaining high authentication performance. In light of this, the physical-layer authentication enhancement techniques including better fin-

gerprinting techniques and characteristic differentiation techniques are in high demand.

Second, the fast emerging 5th generation (5G) related techniques, such as millimeter wave (mmWave) transmission, massive deployed small cells and vast heterogeneous devices, will potentially engender urgent technical problems in current physical-layer authentication schemes. For example, the authentication handover may become very frequently when mobile users are transferring between the shrunken cells. Therefore, it is also important to survey the impacts of the new physical-layer related techniques on the performance of authentication in 5G. Then, researchers can further consider corresponding solutions to mitigate the negative impacts.

Third, effective physical-layer authentication solutions are urgently demanded in some special scenarios, especially in wireless amplify-and-forward (AF) cooperative relaying systems. Specifically, AF relay nodes, also known as physical reflectors, only working in the physical-layer. Due to this working feature, all of the existing well-defined upper-layer involved authentication protocols cannot authenticate AF relays. Although the identification technique for another commonly used decode-and-forward relaying strategy has been investigated in [9], to the best knowledge of the author, there is no comprehensive work for the special case of AF relaying. Consequently, the applicable physical-layer fingerprinting techniques for the AF relay system is worth studying.

Finally, the integration of physical-layer authentication techniques with existing upper-layer authentication protocols and standardized wireless infrastructure is another significant obstacle of applying this authentication technique into practice. Physical-layer authentication is expected to work as an important complement to the existing upper-layer security schemes and achieve better security performance. Therefore, it is valuable to study comprehensive cross-layer technique which can effectively integrate physical-layer method with existing upper-layer methods without causing any conflicts.

## 1.2 Dissertation Contributions

The main contributions of this dissertation are summarized as follows.

- A comprehensive literature survey of current wireless authentication techniques is presented. Specifically, we survey traditional and physical-layer authentication methods and

identify their weakness and strength, which points out the necessity of using physical-layer authentication as a security enhancement. The main problems of current physical-layer authentication are discussed, which includes low reliability, effective and conflict-free integration with existing upper-layer security protocols and standard infrastructures, and the new impacts due to the upcoming 5G communication related techniques.

- A novel wireless relay identification specifically for AF systems is proposed. Relay identification is a useful technique to secure wireless cooperative systems. However, the identification of AF relay nodes is more challenging since AF relay only works in the physical layer, implying that all existing upper-layer identification protocols cannot handle this special case. A comprehensive AF relay identification is proposed through checking in-phase and quadrature imbalance (IQI) and wireless channel features. Satisfactory identification accuracy is achieved in the case of multiple AF relays.

- An enhanced device fingerprinting technique is proposed. Given the fact that the authentication performance using only one physical-layer characteristics is not always reliable, we propose choosing multiple proper characteristics according to the real communication environment to generate more robust and applicable device fingerprints. Particularly, RSSI and PER are first considered together to create enhanced device fingerprints. Then, a general multi-characteristics-based fingerprinting method is investigated. Meanwhile, the optimal weights are derived for combining the multiple characteristics. Using our enhanced fingerprinting technique, the attacker detection probability can be significantly increased compared to using only one characteristic.

- To improve the capability of differentiating the delicate difference between selected fingerprints, enhanced device fingerprint observation and estimation methods are proposed by exploiting diversity techniques. Precisely, the collaboration of multiple receivers (i.e., multiuser diversity) is considered to process the both frequency-dependent and frequency-independent IQI based device fingerprints and obtain higher detection probability than using one receiver. Additionally, maximal-ratio combining in a multiple antennas enabled receiver (i.e., space diversity) is considered in improving the accuracy of fingerprint estimation.

- A seamless integration of the physical-layer and key-based upper-layer authentication scheme is proposed. Given that physical-layer authentication is an important complement to existing key-based security schemes, the seamless integration technique is highly demanded. A cross-layer authentication design using a physical-layer key generation is proposed to achieve this goal. Furthermore, the authentication handover complexity can be significantly reduced by using our physical-layer key generation, which is especially valuable to the upcoming 5G communications.

## 1.3 Dissertation Organization

The remainder of this dissertation is organized as follows.

In Chapter 2, the literature survey regarding the fundamentals of traditional and physical-layer authentication techniques is discussed. The common attack types in wireless systems are reviewed. The current challenging issues and potential forthcoming problems in the wireless authentication research area are identified.

In Chapter 3 and 4, we address the problem of identifying AF relay solely in physical layer. Chapter 3 studies AF relay differentiation. According to the physical-layer working principle of AF relay nodes, the joint Rx/Tx IQI and wireless channel factors are used to generate a novel fingerprint to distinguish two AF relays nodes. The statistics of this fingerprint are analyzed and exploited in a hypothesis testing to verify the claimed identity of the current communicating AF relay node.

Chapter 4 aims at investigating the optimal design for AF relay identification. Given that RF-AFE imperfection estimation and compensation are basics for improving reception quality in most of receivers, we propose directly making use of these LS estimation results for fingerprinting AF relay nodes. The effective identification algorithm is designed to distinguish the malicious AF relay from multiple legitimate relays. The optimal signals are derived for quadrature amplitude modulation (QAM) and phase shift keying (PSK) modulations for the sake of maximizing the capability of identifying and tracking the malicious relays with specific steady-state imperfection values. More robust suboptimal solutions are also proposed whose identification performance is sufficiently close to the optimal designs.

Chapters 5 and 6 focus on enhancing the current physical-layer authentication performance. Chapter 5 investigates the combination of multiple physical-layer characteristics to generate enhanced wireless device fingerprints. An 802.11 wireless WiFi device authentication is first proposed using two specific attributes, which are RSSI and PER. Then, a more general scheme using a weighted combination of multiple RF-AFE imperfections is studied. The optimal weights for the best detection performance are also discussed in this chapter.

Diversity techniques including multiuser and space diversities are exploited as another effective method to improve the reliability of physical-layer authentication in Chapter 6. Through involving in multiple receivers, two collaborative authentication schemes (distributed scheme and centralized scheme) are proposed. On the other hand, the maximal-ratio combining technique is considered in a receiver equipping with multiple antennas to improve the estimation accuracy of the device fingerprints.

Chapter 7 focuses on the cross-layer authentication system design. Given the advantages of using physical-layer technique, the effective integration method of combining multi-layer methods are discussed. A novel physical-layer key using physical-layer attributes is proposed as an example to achieve this seamless integration. Furthermore, the complexity reduction of the authentication procedure is investigated through using our physical-layer key.

In Chapter 8, the conclusions and future works are presented.

# Chapter 2

# Background and Literature Review

Wireless transmission makes "anytime" and "anywhere" communication a reality. However, it also induces more vulnerabilities in wireless systems, as the electromagnetic waves propagated in an open transmission medium can be easily heard by unintended adversaries. Thus, the authentication technique becomes a necessity to detect wireless adversaries. In this chapter, the traditional and physical-layer authentication schemes are surveyed in terms of working fundamentals, related works and current technically challenging issues. The requirements of the cross-layer authentication system are also discussed in details. The motivation of this chapter is to familiarize the readers with the wireless authentication-related issues and lay the foundation for the rest of the dissertation.

## 2.1 Traditional Wireless Authentication Techniques

In conventional wireless systems, the security issues of authentication, confidentiality and integrity are handled above the physical layer by mainly relying on upper-layer identity verification and key-based cryptography.

Regarding the upper-layer identity, the most commonly employed identity for authentication purpose is the media access control (MAC) address. For example, IEEE 802.15.4 protocol based wireless systems can define a device's digital address in the MAC sublayer, which is laid over the physical layer. In an IEEE 802.15.4 network, the MAC address of devices can be inserted in the MAC header of the message packet in the packet encapsulating procedure.

Since MAC address is network-wide unique, the intended packet receiver can verify the MAC address of the transmitter to prevent unauthorized access.

However, this kind of authentication scheme is vulnerable to identity-based attacks. Here, we introduce two easily launched and harmful identity-based attacks, the spoofing attack [6] and the Sybil attack [10]. The spoofing attacker can mimic the identity of another device. For instance, when a spoofing attacker changes its MAC identity to an authorized one, this attacker has a high chance of bypassing the MAC address verification mechanism. In identity-based Sybil attacks, an attacker can create multiple faked identities and present as multiple devices. As a result of a successful Sybil attack, the routing performance can be significantly degraded since the deceived entity thinks multiple nodes rather than one node are utilized to create an optimal routing. Above all, identity-based attacks are based on changing the upper-layer identity. Since upper-layer identity, typically a string of numbers, can be easily revised, this kind of attack can be conveniently launched again and again but hard to completely eradicate by upper-layer identity verification schemes.

Key-based cryptography is another widely used upper-layer security technique. Fig.2.1 shows the basic working principle of encryption in protecting wireless communication security. Alice first uses key $K$ to encrypt message $M_1$ into codeword $C$. Then, $C$ is decrypted by Bob to generate $M_2$. Ideally, it is expected that $M_1 = M_2$ if Bob knows $K$. Eve cannot decrypt the $C$ without the knowledge of $K$. The authenticity of Alice can be verified at Bob by checking the decryption results. For example, if Bob can obtain some secret information only shared between Alice and Bob from the decryption, the current transmitter could be identified as Alice. Generally, there are two basic encryption types, the symmetric key and asymmetric key.

Symmetric key algorithm is a class of algorithms that uses the same key for both the encryption of plaintext and the decryption of ciphertext. In this algorithm, the key must be secretly shared among the authorized entities. Once the key is leaked, the communication security cannot be guaranteed. Regarding asymmetric key algorithm, the term “asymmetric” means the use of different keys to perform the encryption and decryption as contrasted with “symmetric” cryptography, which relies on the same key to perform both. Precisely, asymmetric key cryptography requires two separate keys, one is private and the other one is public. The private key is used to decrypt ciphertext or to create a digital signature and it is kept in Alice, whereas

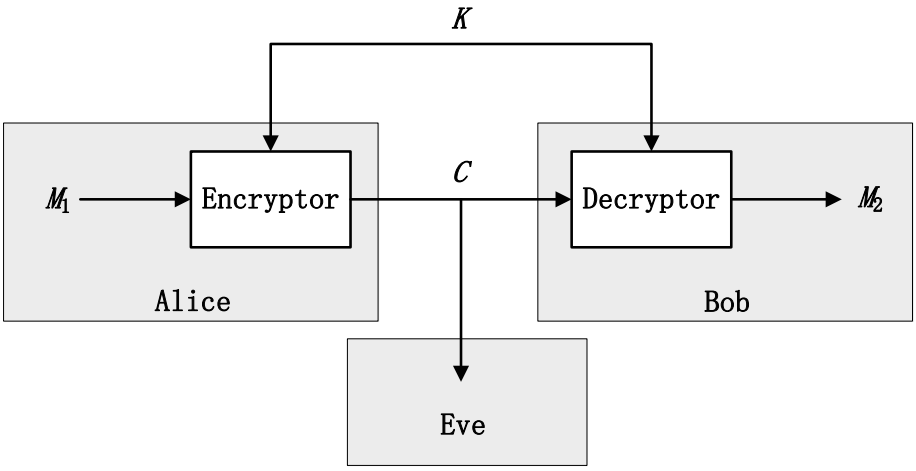


Figure 2.1: Block digram of encryption-based security.

the public key is used to encrypt plaintext or to verify a digital signature and it is available for anyone. In the context of authentication, it is assumed that Alice writes a message for Bob and signs it by encrypting the message using her private key. In order to verify that the message was originally sent from Alice, Bob decrypts it using the public key. On the premise that only Alice owns the private key, the decrypted readable message means that it is Alice who wrote this message.

Although cryptography is an effective method to defend against identity-based attacks, its application in wireless systems still has many limitations. Five main limitations are summarized as follows.

- Secure and timely symmetric key sharing in highly dynamic and large-scale networks comprised of a large number of mobile and heterogeneous devices is becoming a challenging task. More importantly, key management in such complex networks may require multiple hops transmission and involve many entities, as a result of which secure key exchange is hard to guarantee.

- Asymmetric key algorithms usually have a high computational cost. The effectiveness of cryptographic scheme is based upon the computational infeasibility of cracking the encryption algorithm within a short time duration, as a result of which it is termed as computational security. In fact, the actual wireless nodes are normally featured as small-power devices and severely constrained in computation and storage capability for eco-

nomic reasons. Therefore, the utilization of high complexity encryption algorithms in such wireless devices can result in long latency, which is intolerable for delay-sensitive communications.

- Upper-layer cryptography-based authentication is not suitable for all wireless device authentication cases. In practice, there are some wireless devices, such as AF relay nodes, only work in the physical layer. In this case, the complex cryptography is ineffective.

- Some new vulnerabilities may be introduced into the implementation of cryptographic systems. For example, the improper reuse of some random parameters or forgetting to destroy plaintext could be exploited by attackers to break the whole system [11].

- The premise that it is computationally infeasible to break the digital key is still mathematically unproven [3]. With the rapid growth of the processing power of attackers, the time spent on cracking a digital security key could be shortened remarkably. Once the digital key is obtained by an attacker, the cryptographic system is broken.

Based on the above discussion, it is clear that both upper-layer identity verification and cryptography-based authentication schemes have severe problems when applied in wireless systems. The root of these problems is that the upper-layer information is not directly associated with the devices so that it can be easily modified. Given the fact that any user, including the attacker, who possesses the digital address or key can be identified as legitimate, the detection of this attacker is extremely difficult. Therefore, it is valuable to explore stable and unique physical-layer characteristics to generate device fingerprint and investigate corresponding physical-layer authentication techniques.

## 2.2 Physical-Layer Authentication Techniques

In this section, the physical-layer authentication techniques are reviewed in terms of RF fingerprinting types, authentication model, related works and the related challenging issues.

Physical-layer security technique was pioneered by Shannon in 1948 [12]. Shannon proposed the basic principle of information-theoretic security, and discussed perfect secrecy in a

noiseless model using the concept of mutual information as

$$I(M;C) = 0 \tag{2.1}$$

where $M$ and $C$ denote the original message and codeword, respectively. Equation (2.1) implies that an eavesdropper cannot obtain any information about $M$ even if it has the knowledge of $C$. Thus, the best strategy to recover the original message $M$ is to guess its value randomly. Subsequently, the wiretap channel model was introduced and exploited by Wyner in [13]. Wyner showed that when a wiretapper's (i.e., eavesdropper's) channel is a degraded version of the main channel (Alice-Bob channel), Alice and Bob can exchange perfectly secure messages at a non-zero rate in the presence of the wiretapper.

However, the information-theoretic security mainly concentrates on securing the confidentiality of wireless communications through preventing passive eavesdropping/wiretapping. In practice, potential attackers may not always keep "silent" (i.e., passive eavesdropping), but also can actively launch malicious attacks on the legitimate devices located within their coverage at any time. Sophisticated adversaries can even impersonate another legitimate device (e.g., Alice) to disguise its identity. As a result, the adversary can freely eavesdrop the data transmission between Alice and Bob without being detected. Even worse, the adversary can directly communicate with Bob to corrupt the communication performance of Bob since Bob is beguiled into thinking he is currently communicating with Alice.

Physical-layer authentication is emerging to fight against active impersonation attackers. In 1984, Simmons considered the active eavesdropper and studied the authentication theory under noiseless channel [14]. The case of authentication over noisy channel is investigated in [15]. Furthermore, hypothesis testing model is considered in authentication theory by Maurer in [16]. Thanks to Maurer's work, hypothesis testing became a common approach in the authentication technique to effectively differentiate legitimate and illegitimate transceivers. Based on the aforementioned theoretic fundamentals, many physical-layer authentication schemes are proposed by exploiting the physical-layer characteristics as device fingerprint. Same as the biological fingerprint of human beings, the basic idea of physical-layer device fingerprinting is using some transmission-associated physical-layer attributes to uniquely represent the wire-

less transmitter's identity. Given that such attributes play the important role of fingerprinting wireless devices, a comprehensive review of their categories is given in the next subsection.

### 2.2.1 Device Fingerprinting Types

As early as the 1960s, the U.S. military applied specific emitter identification (SEI), a device-specific fingerprinting technique, to detect enemy radars [17]. After that, extensive research efforts were made to explore more applicable physical-layer characteristics for identifying wireless transceivers. In view of the significance of device fingerprinting, it is necessary to review the device fingerprinting types.

In light of our purpose is distinguishing the wireless devices, the eligible characteristics should reflect the differences between different devices. From the practice perspective, the characteristics selected as the device fingerprints should have the following features: 1) *unique*, 2) *accessible* and 3) *unforgeable*.

The requirement of unique is to guarantee that the selected physical-layer characteristics are distinguishable from device to device. This requirement can be further classified as locally unique and globally unique. To be specific, the locally unique mainly ensures the fingerprint is unique within the scope of a network. Globally unique is stronger than locally unique, as its name implies, which means that the device fingerprint is distinguishable in any network comprised of a larger number of heterogeneous devices.

The accessible feature means that the eligible device fingerprint can be extracted at a low expense by the entity that needs to perform the authentication. For instance, the radio-frequency component related characteristics are good choices as these characteristics can automatically tag their effects to the transmitted signals. These distorted signals can be thereby treated as the carrier of the transmitter's fingerprint. In this case, the receiver is able to conveniently extract the information of unique RF related characteristics through analyzing the received signals. In fact, most of the current receivers are equipped with the function to estimate and compensate the RF impairment from the signal, which can potentially reduce the authentication implementation cost.

The unforgeable feature concentrates on the safety of the used device fingerprint. Ideally,

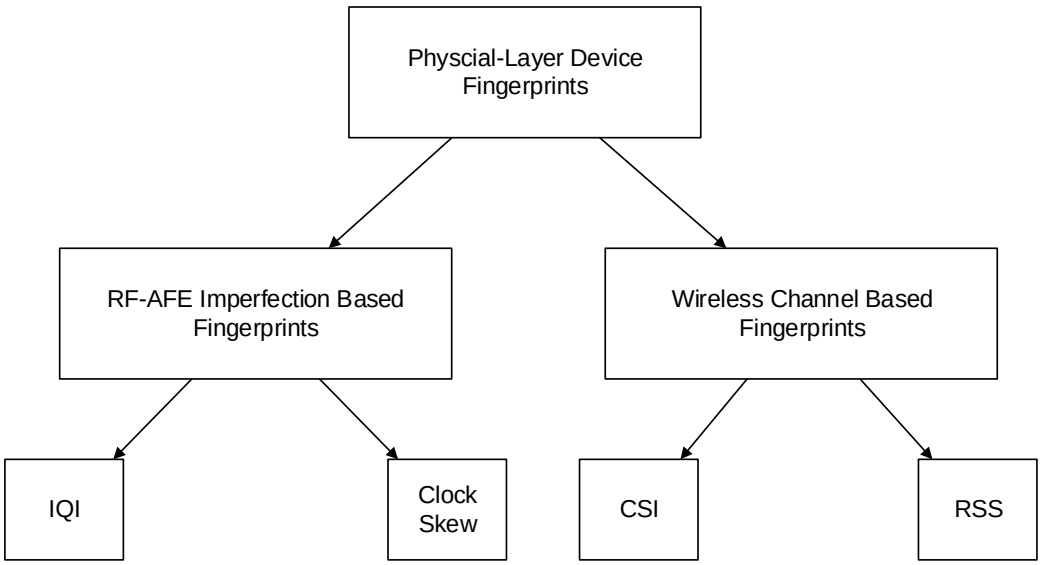


Figure 2.2: Classifications of physical-layer device fingerprints and some examples.

it is expected that the used device fingerprint cannot be forged at all. Similar to computational security, the 100% safety of using a device fingerprint is extremely hard to guarantee in practice. The feasible requirement seeks to make sure the adversary cannot perfectly mimic the device fingerprint and the procedure of mimicking should cause a significantly high cost. For example, the time consumed on imitating a similar enough fingerprint is much longer than the time of an authentication session.

Based on present physical-layer authentication researches, many transmission related characteristics qualify for fingerprinting wireless devices. Typically, these characteristics can be classified into two categories [4, 18]: wireless channel based fingerprint and RF-AFE imperfection based fingerprint. Fig.2.2 shows the classification and some typical examples. In the following, we describe both fingerprinting techniques and discuss their problems.

***Wireless Channel-Based Fingerprint***

The wireless transmission link can offer some unique physical layer attributes between a pair of directly communicating transmitter and receiver. Given that the geographic position of a device is unique, the transmitted signal will be affected by the unique environmental factors corresponding to the transmitter. In practice, such factors include path loss, multi-path and shadowing during wireless propagation. By assuming the wireless channel status experienced

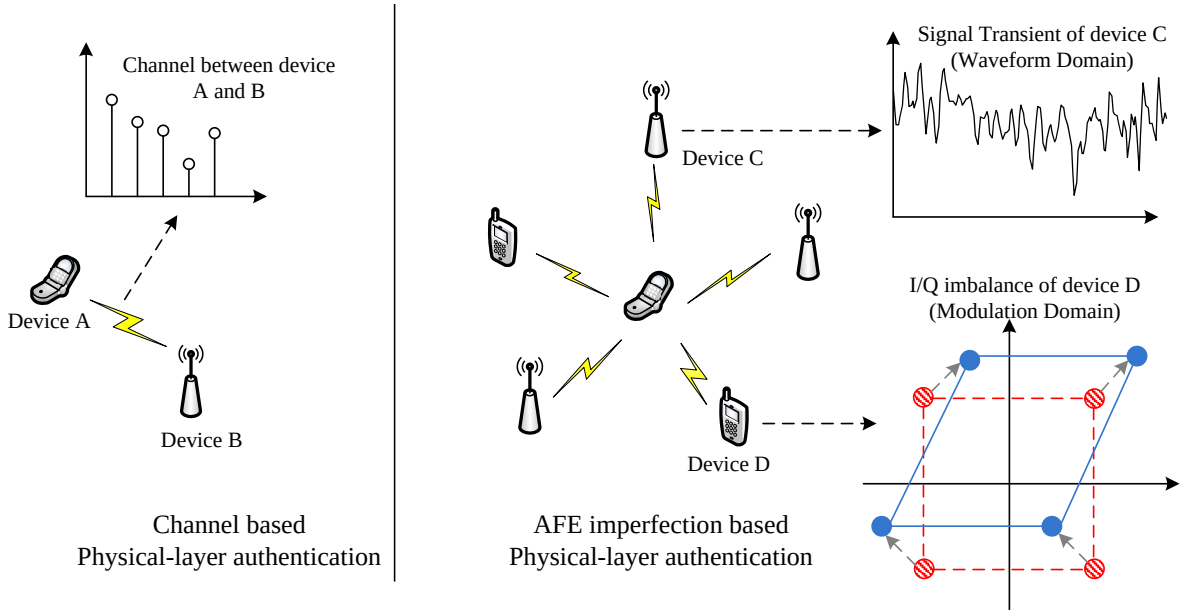


Figure 2.3: Comparison of existing channel based and RF-AFE imperfection based physical-layer authentication techniques.

by the transmitted signals cannot be controlled by any devices, the wireless channel related information is robust for uniquely identifying the transceiver pair (transmitter-receiver). Two typical examples of the wireless channel based fingerprint are channel state information (CSI) and received signal strength (RSS).

In wireless communications, CSI refers to the channel properties of a communication link. This information describes how a signal propagates from the transmitter to the receiver and represents the combined effect of, for example, scattering, fading and power decay with distance. In practice, the spatial diversity and temporal property randomizes the radio channel between a transmitter and a receiver, which are deployed in two locations. Furthermore, in a rich multi-path indoor environment, the adversary-receiver channel states have been proved to be significantly different from the legitimate transmitter-receiver channel states if this adversary is locating in a wavelength away from the legitimate transmitter [19].

RSS is a common metric that can be conveniently read by the receiver from the received packets. It is a sensitive reflection of the transmission power, the distance between transmitter and receiver and current communication environment. In the “Alice-Bob-Eve” scenario, the failure to exactly mimic Alice’s transmission power will give raise to a different RSS readings at Bob. Even if the transmission power of Eve is the same as that of Alice, the observed RSS

at Bob is always different. It is because the transmitted signals are inevitably further distorted by complex communication environment factors, which are out of Eve's control. Since RSS is an important metric for evaluating the receiving sensitivity of antenna and signal quality, RSS information is available in most of the current communication platforms. Therefore, it is easy to make use of RSS readings for implementing authentication systems. Some works are taking the advantages of using RSS to detect the malicious attackers such as proposed in [6, 20].

Although the randomness and fast variation features of the channel make the channel-based fingerprint unforgeable, this also results in many impractical limitations. In this fingerprinting approach, the receiver has to continuously estimate channel related attributes and compare them with the previous estimates before these attributes become temporally and spatially uncorrelated. If the difference between the compared estimates is larger than a reasonable value, the current transmitter will be claimed as an attacker. Therefore, delays in the monitoring and estimating of attributes will result in severe authentication errors, for instance, legitimate devices will be detected as attackers by mistake. Unfortunately, the updating of attributes can be interrupted in most sleep mode enabled networks such as IEEE 802.15.4 networks. As a result, the first authentication cannot be performed since there is no previous fingerprint for comparison. It thereby has to rely on extra techniques, such as encryption, to solve this problem [21]. We call this the first-time authentication problem. In practice, timely updating of the channel states becomes a challenge in highly dynamic environments (e.g., vehicle-to-vehicle communications), environments without rich multipath (e.g., open outdoor communications) and sleep mode enabled networks (e.g., IEEE 802.15.4 networks). Consequently, these factors limit the development of wireless channel-based authentication in practical applications.

***RF-AFE Imperfection-Based Fingerprints***

RF-AFE imperfection-based fingerprint, also known as device-specific fingerprint, refers to the non-idealities from the analog components in the RF chain. As shown in Fig.2.4, the conventional RF chain mainly consists of analog-to-digital (A/D) and digital-to-analog (D/A) converters, power amplifier, mixer, local oscillator and low-pass filter. Generally at the transmitter side, the modulated digital signal is converted to an analog signal. Then, frequency lower than a certain cutoff is filtered out. After that, the signal is up-converted to a high frequency and amplified before being emitted to the wireless channel. At the receiver side, the

opposite processes are performed to recover the signals in the digital domain. Unfortunately, due to imperfect circuit manufacturing, the fabricated analog components are not ideal. To reduce the manufacturing costs, the manufacturer usually produces circuit components according to a criterion called tolerance/accuracy. This criterion indicates the maximal error ranges of the corresponding property values. In practice, the circuit components within the tolerance can meet most of the performance requirements. For example, a $2\times10^3$ ohm resistor with 5% tolerance means a dynamic error as high as 100 ohm.

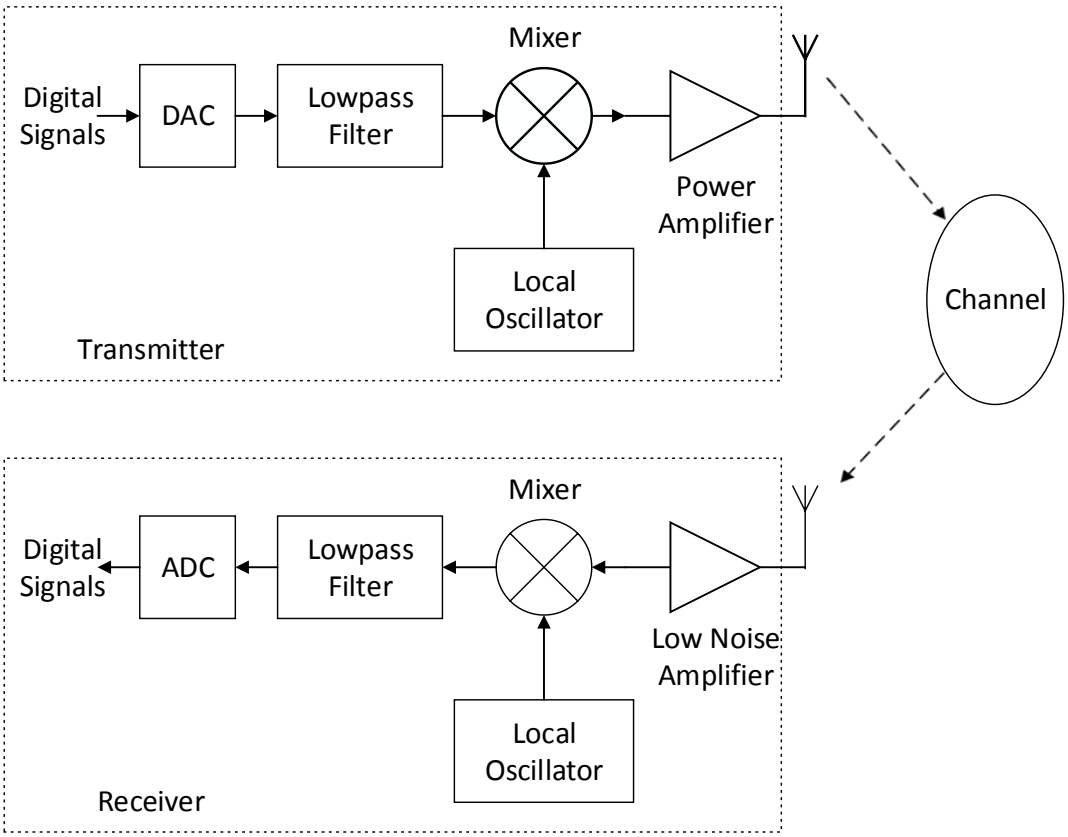


Figure 2.4: RF front-end block diagram for transmitter and receiver.

Given that fabrication variations are not completely predictable and controllable [22], such RF-AFE imperfections generated in fabrications are distinct in different devices. Furthermore, the experimental results in [23] show that the RF-AFE imperfections of the devices with the same product model are still distinguishable. Another important feature of RF-AFE imperfection is that the imperfection information can be automatically tagged in any transmitted signal.

This can reduce the additional cost of generating fingerprints and make the fingerprints accessible at the receiver. Further, this imperfection is hard to mimic since the hardware-level changes, especially in well-fabricated devices, are excessively difficult. Thus, many RF-AFE imperfections are exploited for physical-layer authentication. The in-phase and quadrature imbalance (IQI) and clock skew are presented as two typical examples in the following.

IQI mainly refers to amplitude and phase mismatches between in-phase (I) and quadrature (Q) branches in a transceiver's signal processing [22]. Ideally, the analog components in both I and Q branches would have exactly the same performance characteristics, but this rarely happens in practice. The impairment of the local oscillator (LO) will cause frequency-independent (FI) IQI, which implies unequal gains as well as a not exact 90° phase shift between the I and Q (I/Q) branches. The impacts of amplitude mismatch and phase-shift mismatch on 4-QAM constellations in the I and Q plane are illustrated in Fig. 2.5 and Fig. 2.6, respectively. As one of the typical I/Q signal processing architecture based implementations, the direct conversion (also called the zero intermediate frequency) transceiver inherently suffers more from IQI [24]. In practice, the presence of IQI is especially pronounced in most of the orthogonal frequency division multiplexing (OFDM) based wireless communication systems. In addition, it is also acknowledged that IQI may become more severe and device-specific in multiple antennas scenarios and millimeter wave transmission [67]. Consequently, IQI can be a good choice of fingerprint to identify wireless transceivers, such as reported in [25, 26, 27].

The basis of clock skew fingerprinting is that achieving exact synchronization of two clocks built in two different wireless devices is impossible. In fact, the most important part of clocks is the crystal oscillator, which is able to create an electrical signal with specific frequency. Although the frequency of the created signals is accurate enough to meet most of the application requirements, the minor error still exists due to the imperfect fabrication factor. Besides, another important factor is that the crystal oscillator will unavoidably age, which degenerates the frequency accuracy of the generated signal. For example, if a crystal oscillator has an accuracy of 20 ppm (parts-per-million, $10^{-6}$), which is typical for customer electronics, and the expected carrier frequency is 5GHz, a frequency offset up to 100KHz may exist. Due to the individual difference, the clock skew is unique in different wireless transceivers and can be used as a device fingerprint. For example in [28], the clock skew is used in detecting the presence

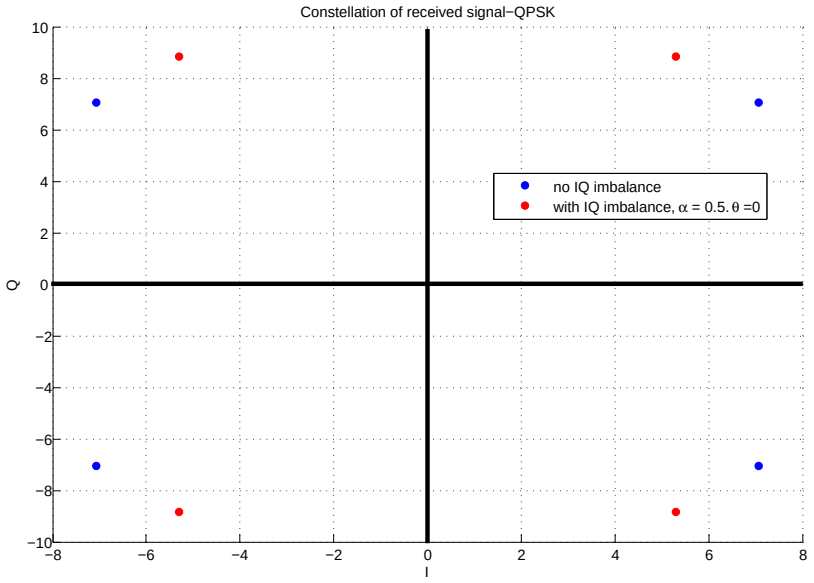


Figure 2.5: 4QAM constellation with amplitude imbalance.

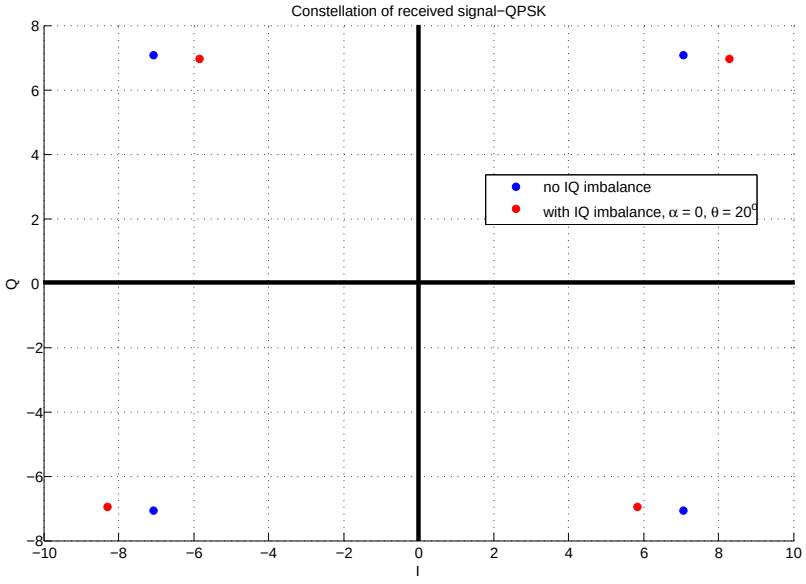


Figure 2.6: 4QAM constellation with phase imbalance.

of unauthorized access point devices. Similar to IQI, the clock offset is an inherent property that already exists in wireless devices, thereby requiring no additional equipment to produce it. However, the defect is that its measurement is generally based on the reports of a time stamp,

which is easy to intercept and mimic. Furthermore, the clock offset is not as stable as IQI in the mobile scenario due to the Doppler effect.

It is worth noting that there is another manmade hardware fingerprint which is called physical unclonable function (PUF). PUF is a physical entity embodied in a physical structure. It works based on the unique device signatures that can be generated by specially designed complex integrated circuit (IC) [29, 30]. Take delay PUF for an instance, the physical signature of wireless devices can be yielded from the random variations in the delays of the specific part of circuits (e.g., wires and transistors). This means that if the same input is given to different PUFs, the corresponding delays of the outputs are different. Therefore, the PUF can implement the challenge-response authentication, where the challenge refers to the input of the PUF and the response is the corresponding output. The main disadvantage of using PUF is the high cost, as it always requires additional IC to produce the unclonable characteristic. Furthermore, these ICs have to be different from device to device for insuring their uniqueness.

In summary, the RF-AFE imperfection shows great advantages in providing stable and vast characteristics for device authentication compared with the wireless channel based fingerprinting method. Moreover, the RF-AFE imperfection is directly associated with the authentication target (i.e., wireless transmitter), rather than the communication environment. Thus, RF-AFE imperfection based device fingerprinting is more simply and effective. However, the main problem of this fingerprinting technique is that the distinction of the selected hardware-level imperfection between different devices is usually small. In practice, its observation and estimation would be further corrupted by noise and interference. All of these factors can degenerate the device differentiation accuracy.

### 2.2.2 Physical-Layer Authentications Related Techniques

It is fact that the physical layer is able to provide sufficient characteristics for authentication purpose. The corresponding characteristic processing technique is another key point that could significantly influence the authentication performance. This subsection focuses on introducing the authentication related techniques.

***Authentication Model***

As above-mentioned, physical-layer fingerprints can be classified into wireless channel-based and RF-AFE imperfection-based types. Correspondingly, two basic authentication models for the two fingerprinting types are shown in Fig.2.7 .

Fig. 2.7(a) considers the case of using RF-AFE imperfection-based fingerprint. In this case, the signal $S$ is tagged with the unique and unclonable hardware-level characteristic of Alice to create the authentication message $AM$. Bob should check the authentication tag from the received $AM$ to verify the identity of the sender. It is worth mentioning that this fingerprint tagging usually can be accomplished without sacrificing data throughput. This is because the signal is inevitably and automatically distorted by RF-AFE imperfection, and we are interested in using the distortion information rather than the data contents for device authentication. As a contrary example, the authentication using watermarking [31, 32] generally requires additional bits to carry the authentication tag instead of carrying data, thereby the data throughput is penalized.

In Fig. 2.7(b), the transmitted signals are randomly affected by the communication environment rather than by Alice, and become unique as a result. These randomized channel-related attributes in the transmitted signals are assumed to be known only by the authorized Alice and Bob. Consequently, Bob can verify the sender's identity by checking these attributes.

***Hypothesis Testing***

In the authentication procedure, one major concern is deciding whether the current transmitter is legitimate Alice or illegitimate Eve. Herein, the hypothesis testing technique is introduced to model this decision step.

Hypothesis testing in the authentication theory is first proposed by Maurer in [16]. After this work, the binary hypothesis testing became a well-accepted model to determine the true identity of signal transmitter. Binary hypothesis testing has two hypotheses, the null hypothesis $\mathcal{H}_0$ and the alternative hypothesis $\mathcal{H}_1$. This can be mathematically represented as

$$\begin{cases} \mathcal{H}_0: & f \text{ belongs to Alice} \\ \mathcal{H}_1: & f \text{ belongs to Eve} \end{cases}, \tag{2.2}$$

where $\mathcal{H}_0$ denotes that the current examined fingerprint $f$ belongs to Alice, while $\mathcal{H}_1$ means $f$

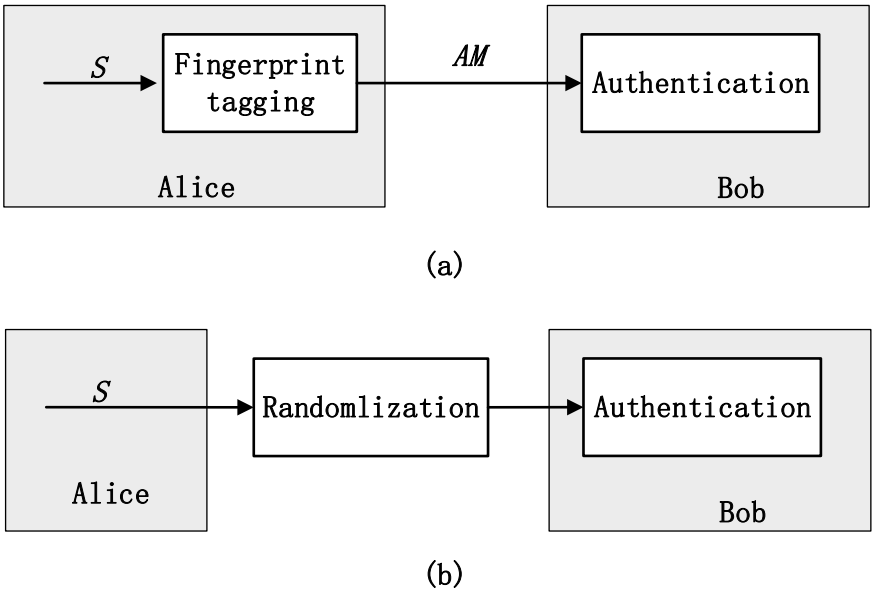


Figure 2.7: Physical-layer authentication models using (a) RF-AFE imperfection-based and (b) wireless channel-based fingerprinting techniques.

is the fingerprint of Eve, implying an illegitimate attacker is detected.

However, it is possible to make incorrect decisions when judging the origin of device fingerprints. Wrong decisions may produce two types of errors, type I error and type II error. A type I error is also termed as a false alarm, and it refers to the incorrect rejection of a true null hypothesis. In authentication scenario, it means claiming Eve as the transmitter when Alice is the actual transmitter. A type II error is the failure to reject an alternative hypothesis which is also called a miss detection. In authentication, the accuracy of hypothesis testing results is very important. For example, once the miss detection error is made, the attacker can consequently obtain the authorized access to the network, which can likely result in severe information leakage and data throughput decrease.

***Neyman-Pearson Lemma***

Neyman-Pearson lemma can be generally used to decide $\mathcal{H}_0$ and $\mathcal{H}_1$ in the hypothesis testing. Neyman-Pearson lemma can be given as [33, eq. 3.3]:

*To maximize $P_D$ for a given $P_{FA} = \alpha$, decide $\mathcal{H}_1$ if*

$$L(x) = \frac{p(x;\mathcal{H}_1)}{p(x;\mathcal{H}_0)} > T, \tag{2.3}$$

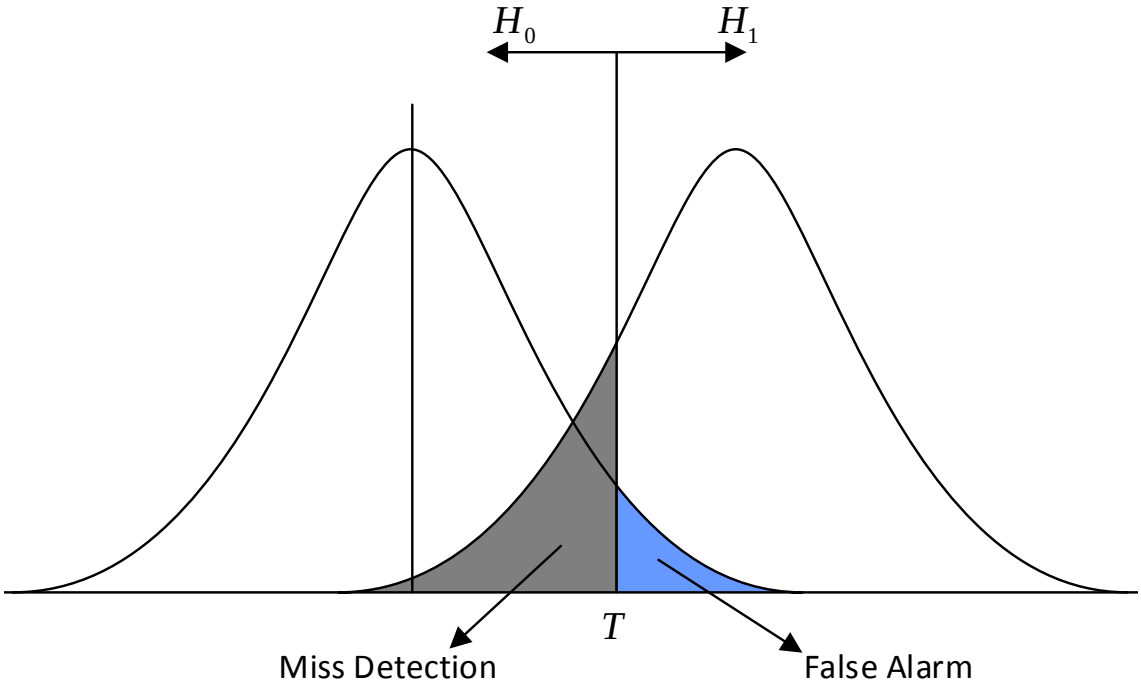


Figure 2.8: Decision regions by adjusting threshold in a binary hypothesis testing.

*where the threshold $T$ can be calculated from*

$$P_{FA} = \int_{\{x:L(x)>T\}} p(x;\mathcal{H}_0)dx = \alpha. \tag{2.4}$$

Here, $P_{FA}$ is the false alarm probability, and $P_D$ denotes the detection probability. In (2.3), the function $L(x)$ is termed as the likelihood ratio since it indicates for each value of $x$ the likelihood of $\mathcal{H}_1$ divided by the likelihood of $\mathcal{H}_0$. In Fig.2.8, the hypothesis testing with the decision regions and threshold described in Neyman-Pearson lemma is illustrated as an example.

It is noteworthy that this Neyman-Pearson lemma-based test is called likelihood ratio test (LRT). In engineering practice, LRT is a widely used tool for deciding the true hypothesis. LRT is very useful in wireless authentication since $\mathcal{H}_1$ is a dangerous case which means the existence of an attacker in the current communication system. Therefore, the feature of maximizing the detection probability can meet the requirement of improving the capability of detecting the potential attackers.

### 2.2.3 Related Works

Thanks to the contributions of many research pioneers, the physical-layer authentication technique experienced a period of rapid development.

Starting with the wiretap channel model proposed by Wyner, researchers started to consider security techniques to protect wireless communications from malicious wiretapping in the physical layer. In the preliminary stage of physical-layer security investigation, the researchers concentrated on the theoretical analysis of passive wiretapping. In [14, 34], the authors discussed the presence of active eavesdroppers which gives rise to the demand of physical-layer authentication. Some authentication methods using additional bits to carry authentication tag were proposed. In [31], the embedded watermark based authentication system is analyzed and designed. The author of [35] proposed a stealthy physical-layer authentication tagging method that also occupies some payload to carry the authentication tags. Motivated by the working principles of encryption, some studies have tried to design light-weight and stealthy coding in the physical layer for authentication. For example, a continuous physical-layer authentication technique using time-varying transmission parameters was investigated based on a novel adaptive OFDM system [36], where the novel adaptive OFDM system was proposed in [37]. In this authentication scheme, a precoded cyclic prefix (PCP) is used to replace general cyclic prefix to enhance the authentication accuracy. It is assumed that only legitimate users can successfully decode the PCP sequence in order to obtain necessary parameters for decoding the OFDM data.

In recent years, many researchers have proposed physical-layer authentication schemes through exploiting the unique transmission characteristics (i.e., wireless channel-based fingerprints and RF-AFE imperfection-based fingerprints). Based on Maurer's work about authentication theory and hypothesis testing, the wireless channel states can be used to model the legitimate and illegitimate transmitters in a binary hypothesis testing. To be specific, in Xiao's studies [19, 38, 39], channel multipath related physical-layer authentication systems were designed for a static scenario, a mobile terminal scenario and the frequency-selective Rayleigh channel case, respectively. In [40], Liu studied both the channel amplitude and the multi-path delay dimensions of channel impulse response (CIR) to mitigate the negative impacts of the

noise and channel estimation errors. In [41], three CIR-based authentication schemes are proposed to enhance the authentication reliability. As another important channel related attribute, RSS is also widely studied in many researches to detect, localize and identify wireless transmitters [6, 20, 42]. In [20], the RSS is used to distinguish identity-based attackers in wireless sensor networks. Further, in [6], both detection and localization techniques of identity-based attacker are considered. The author in [42] applied RSS readings in authentication and localization in wireless local area networks.

To overcome the aforementioned impractical problems of using channel based fingerprinting, many research efforts have been made in exploiting more available RF-AFE imperfection based fingerprinting. In [43] and [7], wireless authentication using constant and time-varying CFO is proposed, respectively. The author of [4] considered imperfect input/output characteristics of the digital-to-analog converter and the power amplifier as device fingerprints. The IQI is also widely investigated in [44, 45, 26, 8, 27]. To be specific, the IQI in terms of I/Q origin offset, amplitude imbalance and phase imbalance is reported as device-specific characteristics in [44, 45]. In [26], the amount of active wireless users in a network is counted by checking the IQI feature. In [27], the multiple collaborative receivers are used to detect both frequency-dependent and independent IQIs. The author of [8] proposed using joint receiving and transmitting IQI to identify amplify-and-forward relay nodes.

## 2.3 Problems and Challenging Issues in Current Wireless Authentication

In this section, the problems as well as challenging issues in current physical-layer authentication schemes and corresponding cross-layer authentication implementations are presented. Also, the feasible methods for solving these challenges are briefly introduced. The detailed solutions will be presented in the following chapters of this dissertation.

### 2.3.1 Implementation Limitations in Cooperative Wireless Systems

Wireless relaying is commonly utilized in communication networks to increase the communication coverage, system throughput as well as prolong the battery life. However, as a drawback of this approach, involving relay nodes can potentially introduces new security threats and challenges to the wireless systems. A sophisticated malicious relay can be selected for signal forwarding with a higher chance through impersonating an authorized relay and pretending to be the best one compared with other relays [9]. Once this impersonation succeeds, the communications between the deceived entities are exposed to various attacks launched by malicious relay, e.g., ghost-and-leech attack [52] or denial of service attack [9, 53]. As summarized in [54], a malicious relay node can send source node the faked helper ready-to-send control packet to block the source-destination link establishment via the legitimate relays. In general, malicious relay nodes can initiate cooperative relay and then avoid it or use on-off behavior in transmission to slow down the communications. Even worse, the deceived terminals can even be viciously de-authorized and de-associated from the network [55]. Therefore, the relay identification process is emerging to become an inevitable part of the cooperative relaying systems to detect the unauthorized access attempts made by malicious relays. Especially, relay authentication is highly demanded in the scenarios where multiple trusted relays are required to cooperate in order to provide physical-layer security, e.g., to prevent the eavesdroppers from overhearing [56, 57].

Based on the strategies of relaying, the two typical relay protocols are amplify-and-forward (AF) and decode-and-forward (DF). In AF relay protocol, the amplified version of received signal is retransmitted whereas in the DF relay protocol, the received signal is first decoded and the estimated signal is then forwarded toward the destination. Although a cross-layer DF relay identification has been investigated in [9], AF relay identification is a more challenging issue mainly because the AF relay only works in physical-layer without applying any content modifications on the forwarded signals. This implies that all existing upper-layer identification methods are not applicable to the AF relaying case. In light of this, it is necessary to go down to the physical layer and explore some device-specific characteristics for fingerprinting AF relays.

### 2.3.2 Low Reliability Problem of Physical-Layer Authentication

Although the effectiveness of identifying wireless devices in the physical layer has been proved, its performance sometimes suffers from low reliability problem. As discussed above, both wireless channel-based fingerprinting and RF-AFE imperfection-based fingerprinting have their own shortcomings. Due to the dramatic variation of channel, the corresponding channel based fingerprint is featured as time-varying. This feature requires very frequent fingerprint estimation and comparison in practice. Failure to do so will significantly increase the unwelcome false alarm probability. The limited ranges of RF-AFE imperfection may result in two similar device-specific fingerprints, which are hard to differentiate. Even worse, with the consideration of noise corruption at the receiving procedure, the accurate fingerprint detection and differentiation will become extremely challenging. For these reasons, physical-layer authentication performance is not always reliable.

Two aspects can be considered to enhance physical-layer authentication performance. First, the device fingerprinting technique can be improved using multiple physical-layer characteristics. The basic idea is to involve multiple different characteristics in fingerprint generation in order to mitigate the inherent shortcomings of using only one characteristic. The choice of physical-layer characteristics for authentication depends upon the specific application scenarios. For instance, the stable RF-AFE imperfections are proper choices in mobile communications; the wireless channel based characteristics can work well in indoor static scenarios. In practice, researchers can even consider the combination of both channel-based and RF-AFE imperfection based characteristics since it is an extremely low possibility that an attacker can occasionally experience the same communication channel and own the nearly identical RF-AFE imperfections at the same time. Besides, the way of implementing the combination can be optimized to achieve the best authentication performance. For example, different weights can be set for each selected attributes according to their reliability; the authenticity decision can be made either separately or integrally based on the multiple selected characteristics. Second, the fingerprint estimation and detection methods can be enhanced. As an example, receiver diversity is an effective means to combat wireless fading, and raise channel capacity through increasing the signal-to-noise-ratio (SNR). Given that the estimated characteristic can

be treated as a desired signal, we believe the desired signal detection can be improved through using diversity technique. In a cooperative system, the source usually covers multiple relays for optimal relay selection, which facilitates the collaborative authentication strategy. For instance, many relays may receive the authentication signal from the same source due to the broadcast nature of the wireless medium. Thus, multiple relays making use of cooperative observations can authenticate the transmitter together to achieve improved authenticity decision accuracy.

### 2.3.3 Challenges in Cross-Layer Authentication Implementation

It is well acknowledged that physical-layer authentication is complementary to the traditional upper-layer authentication schemes. Therefore, the effective cross-layer authentication design with the goal of enlarging the application scope and improving authentication performance is emerging as an urgent research topic in recent years.

According to the open systems interconnection (OSI) model [46], the 7 layers (from bottom to top) are the physical layer, data link layer, network layer, transport layer, session layer, presentation layer and application layer. Each layer has its own functionality and corresponding security vulnerabilities. For instance, in the data link layer (also known as the MAC layer), the multiple devices can be managed to access a shared transmission medium using channel access control mechanisms such as carrier sense multiple access with collision avoidance (CSMA/CA). In each device, the network interface controller with a MAC address is usually built in. MAC address can be used for authentication when granting or denying access to the devices. However, MAC address spoofing and theft are usual attacks in this layer. In the network layer, the Internet Protocol (IP) address is a numerical label assigned to each device of a global network. Similarly, attackers can focus on spoofing and hijacking the IP address to crack the routing. Since these addresses are also digital bits, they are usually encrypted together with the transmitted data in the payload of each layer in the cryptographic security mechanisms. Generally, multiple authentication techniques in different layers are used at the same time, including MAC layer authentication [47], network layer authentication [48] and transport layer authentication [49]. For example, the cipher block chaining message authentication code (CBC-MAC), which is a common message authentication code, is applied in the

MAC layer in IEEE 802.15.4 enabled networks [50].

Given the fact that most of the current networks rely on the upper-layer cryptography for authentication, the first problem of the cross-layer authentication design is the seamless integration of physical-layer and upper-layer authentication schemes. The point of this cross-layer system implementation is that the physical-layer technique should be utilized by the existing upper-layer method to enhance the authentication performance rather than evoking conflicts.

Another potential obstacle of the practical integration development is the end-to-end authentication extension. In large-scale wireless networks, the authentication and key exchange are often required between two devices that are not directly linked. But most of the current physical-layer authentications are confined to device-to-device authentication as they rely on the characteristics obtained from the directly received signals. Consequently, this method is hard to be used in network-wide end-to-end authentication.

Finally, the increasing implementation complexity is also an important problem of cross-layer authentication, especially in the 5G communication era. It is predictable that three timely challenges will correspondingly emerge.

***Compatibility***

In 5G, the devices need to be equipped with multiple radio access technologies (RTAs). A specific example is that the 5G-enabled devices ought to be backward compatible to support legacy 3G and 4G devices. Moreover, some functions of layers may be redefined, for example, the handoffs may no longer exist in layer 3 anymore [51]. Hence, correctly determining the authenticity of various devices operating in diverse upper-layer protocols will be more difficult. Hence, it is worth finding more ubiquitous physical-layer characteristics and process them to become suitable for different upper-layers' authentication processing.

***Cellular link establishment in mmWave communications***

To authenticate a user, the link should be established first between the user and base station (BS) or access point (AP). Currently, security-oriented beamforming, a directional technique, is widely used in wireless devices to enlarge transmit/receive gain in a certain direction. Since the highly direction-sensitive beams are hard to align in mmWave communications [51], it can be foreseen that the authentication handover for a mobile user equipped with the beamforming technique may not be completed due to the unsuccessful link acquisition. Another feature of 5G

is the adoption of millimeter level wave transmission to increase communication throughput. However, the mmWave cellular link establishment will be confronted with alignment difficulty.

***Authentication handover latency***

In 5G, the mobile users will be frequently moving from different base stations or access points covered cells, which results in frequent authentication handover processes. Traditionally, the authentication handover is based on specially designed cryptographic keys and multiple handshakes. In practice, the authentication handover has to involve multiple entities including users, APs, BSs and servers. The communications between those entities with complicated encryption algorithm are usually time-consuming. Therefore, the latency caused by a large number of handover processes will become an inevitable problem in 5G.

In brief, these new compatibility, mmWave link acquisition and latency problems of authentication handover primarily result from the gradual increase in complexity of the communication conditions in 5G. Therefore, the physical-layer authentication technique is also expected to overcome these challenging issues, such as through simplifying the authentication procedure.

## 2.4 Summary

In this chapter, the traditional wireless authentication techniques, in terms of upper-layer identity verification and key-based cryptography, are first reviewed. The limitations of these two typically used methods are discussed. Specifically, the former one is vulnerable to identity-based attacks such as address spoofing, while the later one has many key management related problems and suffers from the computational cost of the key algorithm. It is important to note that one special AF relay scenario is pointed out since the upper-layer authentication methods cannot handle this case. A comprehensive survey of the present physical-layer authentication is then presented in the order of reviewing the device fingerprints, related techniques and state-of-the-art works. Finally, the problems and challenging issues of the present physical-layer authentication are discussed. Specifically, the inherent low reliability problem caused by either the fast variation of channel or the limited range of device-specific characteristics is revealed. The urgent challenging issues in cross-layer authentication implementation are also presented. Consequently, the physical-layer AF relay identification, effective reliability

enhancement techniques and cross-layer design, which are the main concerns of the rest of this dissertation, are critical for the development of physical-layer authentication.

# Chapter 3

# Physical-Layer AF Relay Differentiation Technique

In this chapter, we start from the working principle of AF relay and consequently propose a novel AF relay fingerprint through analyzing the relayed signals at the destination node side for differentiating AF relay nodes. This differentiation technique is applied into the authentication application and show accepted authentication accuracy in our study.

## 3.1 Introduction

As discussed in Chapter 2, the differentiation of AF relay nodes is a special issue as all existing upper-layer approaches are ineffective. Therefore, physical-layer method is necessary in authenticating AF relay in order to protect the security of cooperative wireless communications. Besides security aspect, the applications of relay differentiation can also be extended to wireless device localization and tracing [58, 59].

To distinguish AF relays in physical-layer, the primary point is finding appropriate physical-layer characteristics for fingerprinting AF relays. According to the AF relay's working principles, the received signals of AF relay should be down-converted from passband to baseband, amplified at the baseband, and then up-converted to passband for re-transmission. This is mainly because AF relays, specifically half-duplex relays, must buffer the received signals before emitting them through RF front-end for the purpose of synchronization [60, 61]. Since

the buffering operation can only be efficiently accomplished in digital domain and the high frequency passband signal is hard to digitally process, the signal down conversion becomes essential to the buffering operation [62]. Due to the down and up conversion operations at the RF components of AF relay, the relayed signals inevitably suffer from more several RF distortions than the signals transmitted by the regular transmitters. Consequently, RF-AFE imperfections are suitable for fingerprinting AF relay nodes.

In-phase and quadrature imbalance (IQI) is one of the most typical RF-AFE imperfections at AF relay nodes. The IQI can result in different deformations to constellation diagram in I/Q modulation systems. The impacts of IQI to the signal modulation performance of AF relaying system are widely analyzed in details in [63, 64, 65, 66]. In the perspective of authentication, IQI also has been studied for fingerprinting wireless devices by many authors [44, 45, 26, 8]. In [44, 45], the I/Q gain and phase-shift imbalances are reported as applicable features for device identification. Besides, the former one further experimentally validates the identification performance in the scenario of multiple 802.11n multiple-input multiple-output transmitters. In [26], the IQI distinctions of different devices is used to count the number of devices in a network, and it has shown satisfactory performance when the IQI is high enough.

In practice, the received signal at destination is affected by the device-specific IQI of AF relay as well as the unique channel gain between the relay and destination. Therefore, it is valuable to extract these unique effects through analyzing the received signal to identify AF relay nodes. In this chapter, a novel physical-layer relay differentiation scheme is proposed for authenticating the wireless AF relay nodes. We first study the unique joint Rx/Tx IQI nature of AF-based relay nodes and derive the AF relay fingerprint at destination node using IQI and channel related parameters. A two-parameter hypothesis testing is then adopted to differentiate the relay nodes based on this fingerprint. In order to maximize the capability of detecting minor difference between the IQI device fingerprints, the generalized likelihood ratio test (GLRT) for classical linear model is adopted to the hypothesis decision algorithm. Finally, the performance of the proposed authentication scheme are validated by numerical simulations. It is shown that by using the GLRT for classical linear model, our scheme outperforms a previous work, introduced in [26], in deciding true hypothesis.

The remainder of this chapter is organized as follows. Section 3.2 introduces the system

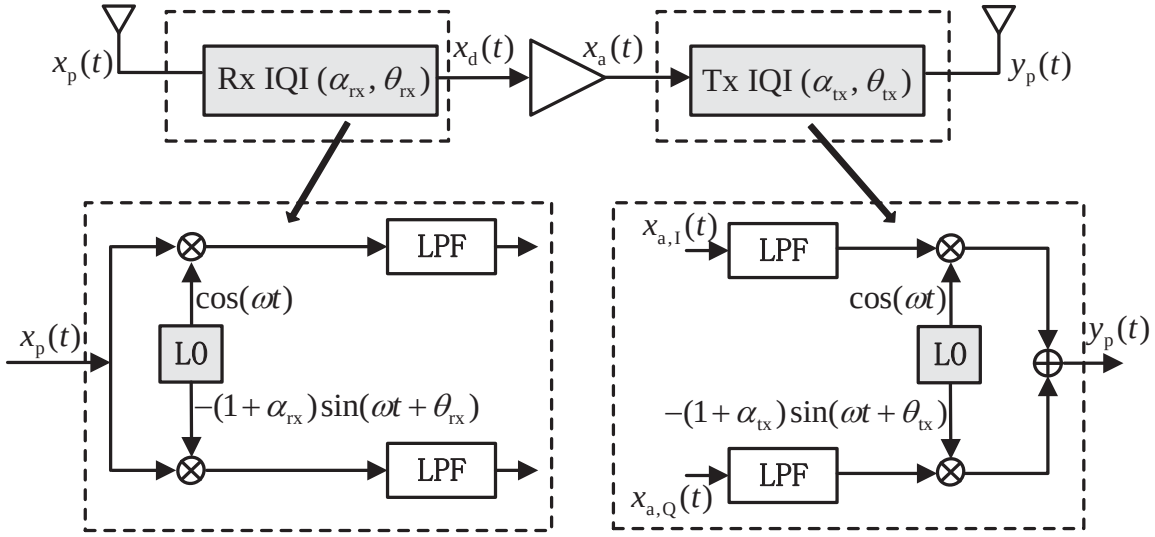


Figure 3.1: Rx/Tx IQI model of AF relay.

model with IQI in AF relay. In Section 3.3, the IQI and channel gain-based device fingerprint of AF relay is analyzed and validated. Also, a two-parameter hypothesis testing model for relay differentiation is presented. In Section 3.4, the authentication method is proposed. Section 3.5 presents the numerical assessment results. Finally, this chapter is concluded in Section 3.6.

*Notations*: $(\cdot)^*$ and $(\cdot)^T$ denote complex conjugate and transpose operators, respectively. Bold lowercase letters denote vectors. For vector $\mathbf{a}$, the $n$th element is denoted by $a_{[n]}$. $\Re\{x\}$ and $\Im\{x\}$ denote the real and imaginary part of $x$, respectively.

## 3.2 System Model

A dual-hop AF relay system consisting of one source node (S), one destination node (D), and multiple relay nodes (R) is considered. The downlink communication S→R→D is considered here and it is assumed that D is outside of the communication coverage of S, i.e., there is no S→D direct link. Further, each node works with single antenna and the relays are half-duplex working in two phases. In the first phase, S transmits signals to a selected R. In the second phase, the selected R amplifies the received signal and retransmits it to D. Also, it is supposed that there are malicious relays existing among the multiple relay nodes claiming as legitimate ones. Hence, it is required for D to be able to authenticate R by analyzing the received signals.

As shown in Fig.3.1 and similar to [61], one AF relay is modeled as one receive component with Rx IQI, one amplifier with gain $a$, and one transmit component with Tx IQI. Also, the asymmetrical IQI model [63] is used, in which the in-phase (I) branch is assumed ideal, while the quadrature-phase (Q) branch is modeled with IQI. In this system model, we only consider the IQI of R. Further, the frequency-independent IQI caused by the LO of relay nodes is considered in our analysis as it plays the more dominant role than the frequency-dependent IQI in practice [68].

In the front-end of the receiving component, the time domain passband input $x_{\mathrm{p}}$ is down-converted by an imperfect local-oscillator (LO) and distorted by frequency-independent IQI, where the representation of $x_{\mathrm{p}}(t)$ can be given by

$$x_{\mathrm{p}}(t) = x_{\mathrm{I}}(t)\cos(\omega t) - x_{\mathrm{Q}}(t)\sin(\omega t) = \Re\{x(t)e^{j\omega t}\}, \tag{3.1}$$

where $x(t)$ is the equivalent baseband with $x_{\mathrm{I}}(t)$ and $x_{\mathrm{Q}}(t)$ denote the I and Q component of $x(t)$. In this model, the signal of Q branch is affected by receiving gain imbalance $\alpha_{\mathrm{rx}}$ and phase shift imbalance $\theta_{\mathrm{rx}}$ as $-x_{\mathrm{p}}(t)(1+\alpha_{\mathrm{rx}})\sin(\omega t+\theta_{\mathrm{rx}})$. Substituting for (3.1), omitting the $2\omega t$ items (filtered by the following low-pass filter), and after multiplying by 2 for mathematical simplicity, the baseband signals representation of I and Q branches are given by

$$x_{d,\mathrm{I}}(t) = x_{\mathrm{I}}(t), \tag{3.2a}$$

$$x_{d,\mathrm{Q}}(t) = (1+\alpha_{\mathrm{rx}})x_{\mathrm{Q}}(t)\cos\theta_{\mathrm{rx}} - (1+\alpha_{\mathrm{rx}})x_{\mathrm{I}}(t)\sin\theta_{\mathrm{rx}}. \tag{3.2b}$$

Accordingly, the output of the receiving component $x_{\mathrm{d}}(t)$ is given by

$$\begin{aligned} x_{\mathrm{d}}(t) &= x_{d,\mathrm{I}}(t) + jx_{d,\mathrm{Q}}(t) \\ &= \mu_{\mathrm{rx}}x(t) + \nu_{\mathrm{rx}}x^{*}(t) \end{aligned} \tag{3.3}$$

where $\mu_{rx}$ and $\nu_{rx}$ are defined as

$$\mu_{rx} = \frac{1}{2}[1 + (1 + \alpha_{rx})e^{-j\theta_{rx}}], \tag{3.4}$$

$$\nu_{rx} = \frac{1}{2}[1 - (1 + \alpha_{rx})e^{j\theta_{rx}}] = 1 - \mu_{rx}^{*}. \tag{3.5}$$

In the amplifier, $x_d(t)$ is multiplied by the amplification gain $a$ to generate

$$x_a(t) = ax_d(t) = x_{a,I}(t) + jx_{a,Q}(t), \tag{3.6}$$

where $x_{a,I}(t)$ and $x_{a,Q}(t)$ denote its I and Q components, respectively. An IQI-free amplifier with known fixed amplitude gain $a$ is assumed. After that, in the transmitter component, the signals are up-converted by an imperfect LO with the gain imbalance $\alpha_{tx}$ and phase shift imbalance $\theta_{tx}$. Hence, the passband signal $y_p(t)$ is forwarded towards the destination, and it can be represented as

$$\begin{aligned} y_p(t) &= ax_{a,I}(t)\cos(\omega t) - ax_{a,Q}(t)(1 + \alpha_{tx})\sin(\omega t + \theta_{tx}) \\ &= \Re\{y(t)e^{j\omega t}\}. \end{aligned} \tag{3.7}$$

Herein, $y(t)$ denotes the baseband equivalent signals and is expressed as

$$\begin{aligned} y(t) &= -ax_{a,Q}(t)(1 + \alpha_{tx})\sin\theta_{tx} + ax_{a,I}(t) + jax_{a,Q}(t)(1 + \alpha_{tx})\cos\theta_{tx} \\ &= \frac{a}{2}[(1 + (1 + \alpha_{tx})e^{j\theta_{tx}})(x_{a,I}(t) + jx_{a,Q}(t)) + (1 - (1 + \alpha_{tx})e^{j\theta_{tx}})(x_{a,I}(t) - jx_{a,Q}(t))] \\ &= a\mu_{tx}x_a(t) + a\nu_{tx}x_a^{*}(t), \end{aligned} \tag{3.8}$$

where

$$\mu_{tx} = \frac{1}{2}[1 + (1 + \alpha_{tx})e^{j\theta_{tx}}], \tag{3.9}$$

$$\nu_{tx} = \frac{1}{2}[1 - (1 + \alpha_{tx})e^{j\theta_{tx}}] = 1 - \mu_{tx}. \tag{3.10}$$

It is noteworthy that the baseband domain is considered in rest of this chapter for analysis simplicity. Using (3.3) and (3.8), and after rearrangements, we get

$$y(t) = ax(t)(\mu_{\text{tx}}\mu_{\text{rx}} + \nu_{\text{tx}}\nu_{\text{rx}}^*) + ax^*(t)(\mu_{\text{tx}}\nu_{\text{rx}} + \nu_{\text{tx}}\mu_{\text{rx}}^*). \tag{3.11}$$

Then, the signal $y(t)$ passes through the R→D wireless channel towards the destination. Since the key concern of this study is to investigate the authentication technique and its enhancement, the wireless channel is simplified as additive white Gaussian noise flat fading and it is assumed that the channel is perfectly estimated. Accordingly, the discrete expression of the received signal at destination is given by

$$y_{[n]} = a\big[x_{[n]}(\mu_{\text{tx}}\mu_{\text{rx}} + \nu_{\text{tx}}\nu_{\text{rx}}^*) + x_{[n]}^*(\mu_{\text{tx}}\nu_{\text{rx}} + \nu_{\text{tx}}\mu_{\text{rx}}^*)\big]h_{[n]} + w_{[n]}, \tag{3.12}$$

where $h_{[n]}$ denotes the channel gain; while $\{w_{[n]}\} \sim \mathcal{CN}(0, \sigma_0^2)$ denote the independent and identically distributed (i.i.d.) samples of the complex additive white Gaussian noise.

## 3.3 Two-Parameter Hypothesis Testing

In this section, the received signal $y_{[n]}$ is analyzed to derive the joint Rx/Tx IQI dependent device fingerprint of relay node. Then, this fingerprint is used to model a two-parameter hypothesis testing for further AF relay differentiation.

As shown in (3.11), the IQI contributes to both the desired signal $x$ and the image signal component $x^*$. In order to reveal the different relays' unique IQI impact on signals, the 4-QAM constellation pattern with the presence of Rx/Tx IQI is shown in Fig.3.2.

The constellation patterns in Fig.3.2 (a), (b), (c) and (d) are generated from four different relays with different IQI quantities. The ideal symbols are $\{e^{-j\frac{3}{4}\pi}, e^{j\frac{3}{4}\pi}, e^{-j\frac{1}{4}\pi}, e^{j\frac{1}{4}\pi}\}$. As shown in this figure, the IQI in relays leads to the deformation of constellation pattern compared to the ideal IQI-free case. Moreover, it is shown that this deformation is unique for every individual relay due to their different IQI parameters. In addition, as a hardware-level feature, IQI is stable once the device is fabricated. Consequently, the device-specific IQI is eligible to be used as device fingerprint of AF relay node.

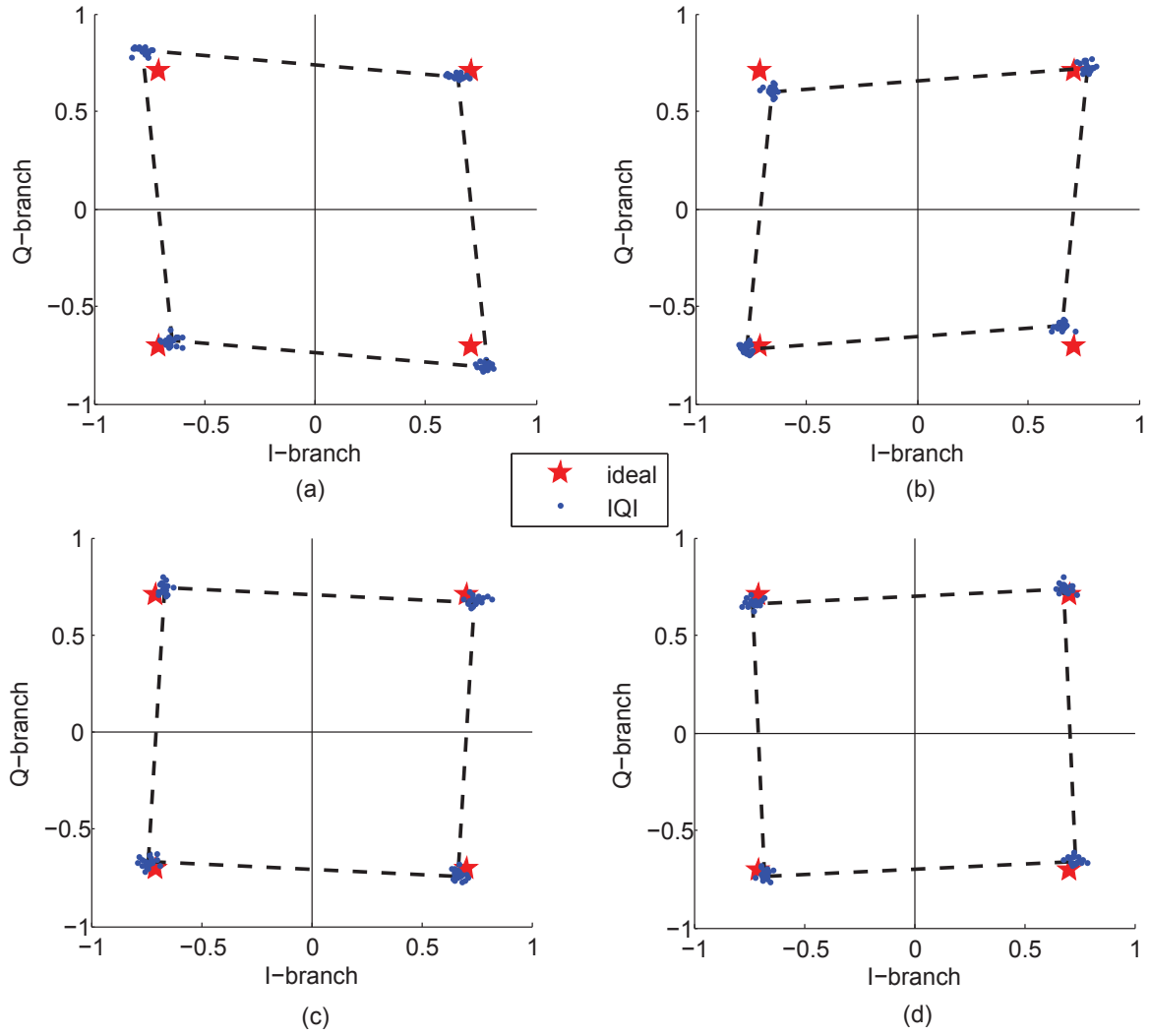


Figure 3.2: IQI distorted 4-QAM constellation patterns of 4 AF relays with $a = 1$ and (a) $(\alpha_{rx}, \theta_{rx}, \alpha_{tx}, \theta_{tx}) = (0.03, 5^o, 0.03, 5^o)$; (b) $(\alpha_{rx}, \theta_{rx}, \alpha_{tx}, \theta_{tx}) = (-0.03, -5^o, -0.03, -5^o)$; (c) $(\alpha_{rx}, \theta_{rx}, \alpha_{tx}, \theta_{tx}) = (0.05, 3^o, -0.05, -3^o)$; (d) $(\alpha_{rx}, \theta_{rx}, \alpha_{tx}, \theta_{tx}) = (0.04, -3^o, -0.05, 2^o)$.

Since the unique IQI quantity rather than the content of signal is used for authentication, we are able to use the known training signals $x_{[n]}$ to generate device fingerprint. Substituting for $\mu_{rx}$, $\nu_{rx}$, $\mu_{tx}$, and $\nu_{rx}$ from (3.4), (3.5), (3.9), and (3.10) into (3.12), and subtracting $ah_{[n]}x_{[n]}$ from both sides, the eq.(3.13) can be derived. Assuming that the current measurement at destination consists of $N$ observations, the fingerprint can be obtained as

$$\mathbf{f} = \mathbf{m} + \mathbf{w}_m + j(\mathbf{k} + \mathbf{w}_k) \tag{3.14}$$

$$
\begin{aligned}
f_{[n]} &= y_{[n]} - a h_{[n]} x_{[n]} \\
&= \underbrace{2a[(\Im\{x_{[n]}\} - 2\Im\{x_{[n]}\mu_{\mathrm{rx}}\})(\Re\{h_{[n]}\}\Im\{\mu_{\mathrm{tx}}\} + \Im\{h_{[n]}\}\Re\{\mu_{\mathrm{tx}}\}) + \Im\{h_{[n]}\}\Im\{x_{[n]}\mu_{\mathrm{rx}}\}]}_{m} + \underbrace{\Re\{w_{[n]}\}}_{w_m} \\
&+ j\underbrace{2a[(\Im\{x_{[n]}\} - 2\Im\{x_{[n]}\mu_{\mathrm{rx}}\})(\Im\{h_{[n]}\}\Im\{\mu_{\mathrm{tx}}\} - \Re\{h_{[n]}\}\Re\{\mu_{\mathrm{tx}}\}) - \Re\{h_{[n]}\}\Im\{x_{[n]}\mu_{\mathrm{rx}}\}]}_{k} + j\underbrace{\Im\{w_{[n]}\}}_{w_k}
\end{aligned}
\tag{3.13}
$$

---

where the $N \times 1$ vector $\mathbf{f}$ denotes $N$ estimated fingerprints based on the corresponding observations.

In order to verify if the cooperating relay is legitimate, we compare its fingerprint with the validated fingerprints in the database using hypothesis testing. In practice, once one relay passes the verification procedure through the upper layers and joins the network, this relay is added to the validated relay set. The destination node obtains its IQI parameters and stores them in the database. $\mathbf{f}_0 = \mathbf{m}_0 + j\mathbf{k}_0$ is defined as one validated device fingerprint calculated by destination node. Therefore, when an $\mathbf{f}$ is estimated as given by (3.14), it is compared with $\mathbf{f_0}$ as

$$
\begin{aligned}
\mathbf{f} - \mathbf{f}_0 &= \Delta\mathbf{m} + \mathbf{w}_m + j(\Delta\mathbf{k} + \mathbf{w}_k) \\
&= \mathbf{c} + j\mathbf{d},
\end{aligned}
\tag{3.15}
$$

where $\Delta\mathbf{m} = \mathbf{m} - \mathbf{m}_0$, $\Delta\mathbf{k} = \mathbf{k} - \mathbf{k}_0$, $\mathbf{c} = \Re\{\mathbf{f}\} - \Re\{\mathbf{f}_0\}$, $\mathbf{d} = \Im\{\mathbf{f}\} - \Im\{\mathbf{f}_0\}$.

The binary hypothesis testing is used to decide whether the two compared fingerprints, $\mathbf{f}$ and $\mathbf{f}_0$, are from the same relay or not. $\mathcal{H}_0$ denotes the hypothesis that $\mathbf{f}$ and $\mathbf{f}_0$ belong to the same relay. In this case, $\Delta m_{[i]} = 0$ and $\Delta k_{[i]} = 0$. While the alternative hypothesis $\mathcal{H}_1$ is defined as $\mathbf{f}$ and $\mathbf{f}_0$ belong to two different relay nodes which implies that at least one of $\Delta m_{[i]}$ and $\Delta k_{[i]}$ is not zero. Hence, the two parameters ($\Delta m_{[i]}$ and $\Delta k_{[i]}$) can be used to model the hypothesis testing as

$$\begin{cases} \mathcal{H}_0: & \Delta m_{[i]} = \Delta k_{[i]} = 0 \\ \mathcal{H}_1: & \Delta m_{[i]}^2 + \Delta k_{[i]}^2 \neq 0 \end{cases}. \tag{3.16}$$

Under hypothesis assumptions $\mathcal{H}_0$ and $\mathcal{H}_1$ , $\{c_{[i]}\}$ and $\{d_{[i]}\}$ are two sets of Gaussian random variables. In this case, $c_{[i]}, d_{[i]} \sim N(0, \sigma^2)$ under $\mathcal{H}_0$, where $\sigma^2 = \frac{\sigma_0^2}{2}$; while $c_{[i]} \sim N(\Delta m_{[i]}, \sigma^2)$ and $d_{[i]} \sim N(\Delta k_{[i]}, \sigma^2)$ under $\mathcal{H}_1$. Consequently, the device fingerprint can be separated into two parameters and used in a two-parameter hypothesis testing.

## 3.4 AF Relay Authentication Method

In this section, differentiation method is explored to accurately decide the true hypothesis ($\mathcal{H}_0$ or $\mathcal{H}_1$). Consider that making wrong decision is possible, the false alarm (FA) and miss detection (MD) as two error types are defined according to the terminologies in detection theory. In our case, the errors cannot be completely prevented mainly because our estimated fingerprints are inevitably corrupted by noises. Therefore, it is a crucial challenge to make the accurate hypothesis decision with the presence of noises.

For presentation simplicity, three probabilities are first defined: $P_{\text{FA}}$, the probability of FA; $P_{\text{MD}}$, the probability of MD; $P_{\text{D}}$, the probability of correctly detecting $\mathcal{H}_1$. In engineering practice, a required acceptable $P_{\text{FA}}$ is usually set as the threshold in advance, and then the hypothesis testing is performed according to this threshold. Therefore, the objective can be modeled as maximizing the capability of finding the minor difference between among IQI fingerprints. If the difference exceeds the $P_{\text{FA}}$ determined threshold, $\mathcal{H}_1$ is claimed; otherwise, $\mathcal{H}_0$ is decided.

To achieve this objective, the likelihood ratio test (LRT) is used to deal with the hypothesis decision problem. According to the Neyman-Pearson lemma [33], LRT is able to maximize $P_{\text{D}}$ within a required $P_{\text{FA}}$. In order to apply LRT, three $2N \times 1$ vectors are composed as

$$\mathbf{a} = [c_{[1]} \;\; d_{[1]} \;\; c_{[2]} \;\; d_{[2]} \cdots \;\; c_{[N]} \;\; d_{[N]}]^T$$

$$\mathbf{b} = [\Delta m_{[1]} \;\; \Delta k_{[1]} \;\; \Delta m_{[2]} \;\; \Delta k_{[2]} \cdots \Delta m_{[N]} \;\; \Delta k_{[N]}]^T$$

$$\mathbf{w} = [w_{m[1]} \;\; w_{k[1]} \;\; w_{m[2]} \;\; w_{k[2]} \cdots w_{m[N]} \;\; w_{k[N]}]^T.$$

Accordingly, we can obtain

$$\mathbf{a} = \mathbf{b} + \mathbf{w}. \tag{3.17}$$

In this case, the hypothesis testing model is equivalent to

$$\begin{cases} \mathcal{H}_0 : \;\; \mathbf{b} = 0 \\ \mathcal{H}_1 : \;\; \mathbf{b} \neq 0 \end{cases}. \tag{3.18}$$

Since $\mathbf{w}$ consists of i.i.d. zero mean Gaussian random variables, the likelihood function of $\mathbf{a}$ can be given by

$$p(\mathbf{a}; \mathbf{b}) = \frac{1}{(2\pi\sigma^2)^N} \exp\left[-\frac{(\mathbf{a}-\mathbf{b})^T(\mathbf{a}-\mathbf{b})}{2\sigma^2}\right]. \tag{3.19}$$

The LRT can be performed to decide $\mathcal{H}_1$ as

$$G(\mathbf{a}; \mathbf{b}) = \frac{p(\mathbf{a}; \mathbf{b}_{\mathcal{H}_1})}{p(\mathbf{a}; \mathbf{b}_{\mathcal{H}_0})} > T, \tag{3.20}$$

where $\mathbf{b}_{\mathcal{H}_0}$ and $\mathbf{b}_{\mathcal{H}_1}$ denote the corresponding $\mathbf{b}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. $T$ is the threshold corresponding to the maximum tolerable false alarm probability, $P_{\text{FA}}$.

Since vector $\mathbf{b}$ is unavailable to the destination node, the LRT cannot be performed. The GLRT for classical linear model (GLRTL) is adopted to deal with this problem. In GLRTL, the maximum likelihood estimation (MLE) of $\mathbf{b}$ is utilized to perform (3.20) as

$$G(\mathbf{a}; \hat{\mathbf{b}}) = \frac{p(\mathbf{a}; \hat{\mathbf{b}}_{\mathcal{H}_1})}{p(\mathbf{a}; \hat{\mathbf{b}}_{\mathcal{H}_0})} > T, \tag{3.21}$$

where $\hat{\mathbf{b}}_{\mathcal{H}_0}$ and $\hat{\mathbf{b}}_{\mathcal{H}_1}$ denote the MLE of $\mathbf{b}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively.

Under $\mathcal{H}_1$, the only constraint for $\mathbf{b}$ is to exclude the set satisfying $\mathbf{b} = 0$. Therefore, $\hat{\mathbf{b}}$

(unconstrained MLE of $\mathbf{b}$) can be derived by solving two partial derivative equations as

$$\frac{\partial \ln p(\mathbf{a};\hat{\mathbf{b}})}{\partial \hat{b}_{[i]}} = 0, \tag{3.22a}$$

$$\frac{\partial \ln p(\mathbf{a};\hat{\mathbf{b}})}{\partial \hat{b}^2_{[i]}} < 0. \tag{3.22b}$$

In this case, the result of second order partial derivative in (3.22b) is $-\frac{1}{\sigma^2}$, which is always less than zero. While (3.22a) equivalents to $\hat{\mathbf{b}} = \mathbf{a}$. In light of that the probability of a random variable to be a certain value is zero, it can be safely concluded that $\hat{\mathbf{b}}_{\mathcal{H}_1} = \mathbf{a}$. While under $\mathcal{H}_0$, it is clear that $\hat{\mathbf{b}}_{\mathcal{H}_0} = 0$.

After taking the logarithm of both sides of (3.21), and substituting $\hat{\mathbf{b}}_{\mathcal{H}_0}$, $\hat{\mathbf{b}}_{\mathcal{H}_1}$ and (3.19), we can obtain

$$\begin{aligned} &2\ln G(\mathbf{a};\hat{\mathbf{b}}) \\ &= -\frac{[(\mathbf{a}-\hat{\mathbf{b}}_{\mathcal{H}_1})^T(\mathbf{a}-\hat{\mathbf{b}}_{\mathcal{H}_1}) - (\mathbf{a}-\hat{\mathbf{b}}_{\mathcal{H}_0})^T(\mathbf{a}-\hat{\mathbf{b}}_{\mathcal{H}_0})]}{\sigma^2} \\ &= \frac{\hat{\mathbf{b}}^T_{\mathcal{H}_1}\hat{\mathbf{b}}_{\mathcal{H}_1}}{\sigma^2} = \frac{\mathbf{a}^T\mathbf{a}}{\sigma^2} \\ &> 2\ln T = T'. \end{aligned} \tag{3.23}$$

The distribution of $\frac{\mathbf{a}}{\sigma}$ can be given by

$$\frac{\mathbf{a}}{\sigma} \sim \begin{cases} N(0,\mathbf{i}), & \text{under } \mathcal{H}_0 \\ N(\frac{\mathbf{b}_{\mathcal{H}_1}}{\sigma},\mathbf{i}), & \text{under } \mathcal{H}_1 \end{cases}, \tag{3.24}$$

where $\mathbf{i}$ denotes the vector satisfying $i_{[n]} = 1$. Given that the sum of squares of normal random variables follows different chi-squared distributions, the distributions of $A$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ can be respectively given as

$$A = \frac{\mathbf{a}^T\mathbf{a}}{\sigma^2} \sim \begin{cases} \chi^2_{2N}, & \text{under } \mathcal{H}_0 \\ \chi^2_{2N}(\rho), & \text{under } \mathcal{H}_1 \end{cases}, \tag{3.25}$$

where $\chi^2_{2N}$ is the central chi-squared distribution with $2N$ degrees of freedom; while $\chi^2_{2N}(\rho)$ denotes the non-central chi-squared distribution with $2N$ degrees of freedom and non-centrality parameter $\rho$. In this case, the non-centrality parameter is defined as

$$\rho = \frac{\mathbf{b}^T_{\mathcal{H}_1}\mathbf{b}_{\mathcal{H}_1}}{\sigma^2}.$$

Accordingly, the probability density function (PDF) of $A$ under $\mathcal{H}_0$ can be given by

$$p_{\mathcal{H}_0(A)} = \frac{A^{N-1}e^{-\frac{1}{2}A}}{2^N\Gamma(N)}, \tag{3.26}$$

where $\Gamma(x) = \int_0^\infty u^{x-1}e^{-u}du$ is the Gamma function. Additionally, the PDF of $A$ under $\mathcal{H}_1$ is given by

$$p_{\mathcal{H}_1(A)} = \frac{1}{2}(\frac{A}{\rho})^{\frac{N-1}{2}}e^{-\frac{1}{2}(A+\rho)}I_{N-1}(\sqrt{A\rho}), \tag{3.27}$$

where $I_{N-1}(\cdot)$ is the modified Bessel function of the first kind with order $N-1$.

Hence, the false alarm rate is calculated as

$$\begin{aligned} P_{\text{FA}} &= P\{A > T'|\mathcal{H}_0\} \\ &= \int_{T'}^{+\infty} p_{\mathcal{H}_0(A)}dA = Q_{\chi^2_N}(T'), \end{aligned} \tag{3.28}$$

where $Q_{\chi^2_{2N}}(\cdot)$ is the right-tail probability for $\chi^2_{2N}$ random process.

Given the fact that $2N$ is an even number and according to [69, eq. 26.4.5], the $Q_{\chi^2_{2N}}(T')$ can be expressed as

$$Q_{\chi^2_{2N}}(T') = e^{-\frac{T'}{2}}\sum_{i=0}^{N-1}\left(\frac{T'}{2}\right)^i\frac{1}{i!}. \tag{3.29}$$

In practice, $T'$ is obtained by inverting (3.29) according to the required $P_{\text{FA}}$ as $T' = Q^{-1}_{\chi^2_{2N}}(P_{\text{FA}})$. Eventually, $P_{\text{D}}$ can be analytically computed as

$$P_{\text{D}} = \int_{T'}^{+\infty} p_{\mathcal{H}_1(A)}dA. \tag{3.30}$$

The probability of MD can be calculated as

$$P_{\mathrm{MD}} = 1 - P_{\mathrm{D}}. \tag{3.31}$$

Now we are able to decide whether or not the identity of current relay is the same with the compared validated one.

## 3.5 Simulation Results

In this section, the performance of the proposed IQI based AF relay authentication scheme is evaluated in orthogonal frequency-division multiplexing (OFDM) communication system. An OFDM system is considered with 4-QAM modulation, 32 sub-carriers, and cyclic prefix with a length of 6. Also, the amplifier gain is $a = 1$. The simulation results are based on $10^5$ independent realizations of the system.

The analytical $P_{\mathrm{D}}$ in (3.30) is compared with the simulation results in Fig.3.3. In this comparison, we set the current AF relay with IQI parameter as $(\alpha_{\mathrm{rx}}, \theta_{\mathrm{rx}}, \alpha_{\mathrm{tx}}, \theta_{\mathrm{tx}}) = (0.05, 2^{\mathrm{o}}, 0.05, 2^{\mathrm{o}})$. While, the validated relay's IQI is $(-0.04, -5^{\mathrm{o}}, -0.04, -5^{\mathrm{o}})$. It can be seen that the simulation results can perfectly match the expected analytical results. The corresponding threshold $T'$ declines with the growth of $P_{\mathrm{FA}}$ as expected. In addition, it can be seen that the detection probability remains above 98% under SNR=15 dB, while significantly decreases when SNR becomes 13 dB. The drop is caused by the unstable channel factor in the fingerprint.

The performance of authentication scheme in detecting the illegitimate relay among several legitimate relays is evaluated in Fig.3.4. Here, four validated relays are set with IQI parameters $(-0.05, 2^{\mathrm{o}}, -0.05, 2^{\mathrm{o}})$, $(0.04, -2^{\mathrm{o}}, 0.04, -2^{\mathrm{o}})$, $(0.03, 3^{\mathrm{o}}, -0.02, -3^{\mathrm{o}})$ and $(-0.01, -5^{\mathrm{o}}, -0.01, -5^{\mathrm{o}})$. Besides, one illegitimate relay is assumed to have IQI $(0.04, -4^{\mathrm{o}}, -0.05, 3^{\mathrm{o}})$. Fig.3.4 shows $P_{\mathrm{D}}$ in terms of $P_{\mathrm{FA}}$ for this simulation setup. As expected, the capability of detecting $\mathcal{H}_1$ is increasing with the required false alarm rate varying from 0.01 to 0.1, and the higher signal-to-noise ratio (SNR) at destination results in the higher detection probability. For instance, it is observed that the overall $P_{\mathrm{D}}$ is higher than 98.3% and 99.932% when the SNR is 22 dB and 24 dB, respectively.

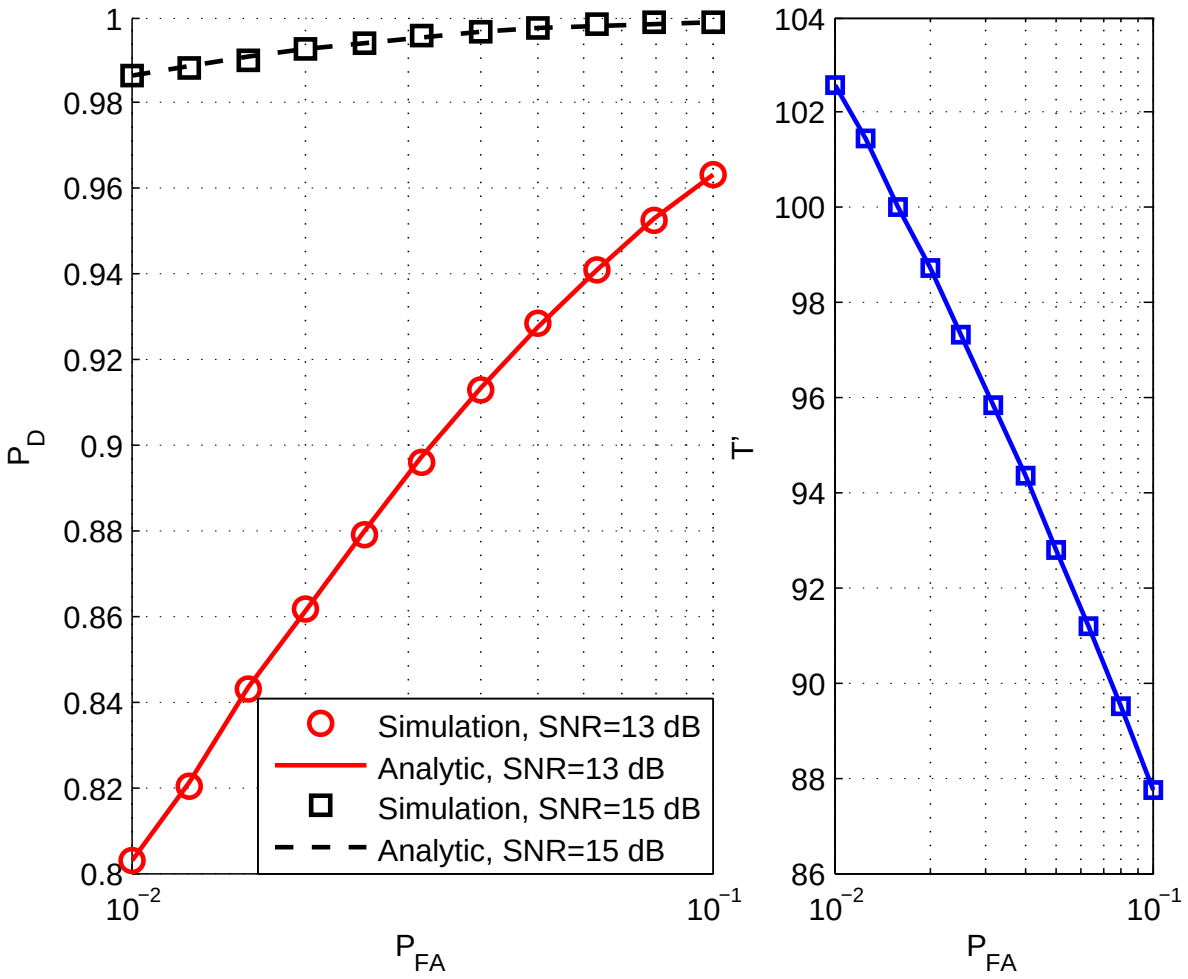


Figure 3.3: Simulation vs. Analytical results of $P_{\mathrm{D}}$, and the corresponding threshold.

In Fig.3.5, the performance of our Rx/Tx IQI GLRTL hypothesis decision algorithm is compared with the previous introduced Tx IQI hypothesis testing based work in [26] which can be referred to as distance test (DT) method. In DT, one Tx IQI based parameter is estimated as device fingerprint, and it follows complex Gaussian distribution which can be treated as equivalent to $\mathbf{f}$ given by (3.14). Then, this parameter is averaged to decrease the variance. After that, the distance between the averaged parameter $\hat{\mu}_k$ and the validated parameter is calculated. Finally, the hypothesis testing is carried out by comparing this distance with a $P_{\mathrm{FA}}$ dependent threshold.

In this simulation, $\mathbf{f}$ is processed using DT, and then its $P_{\mathrm{D}}$ is compared with our GLRTL approach to evaluate their hypothesis decision accuracy. The same simulation setups as used

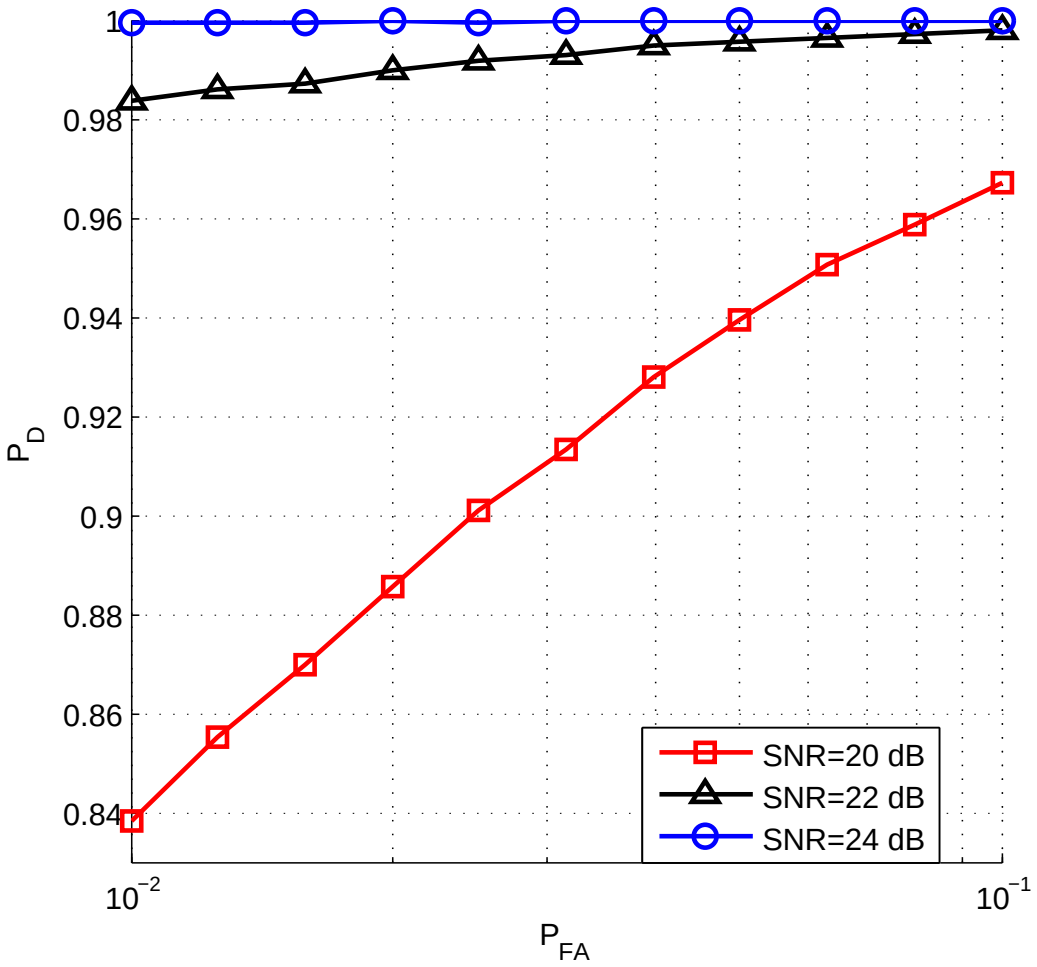


Figure 3.4: $P_{\mathrm{D}}$ vs. $P_{\mathrm{FA}}$ under 4 validated AF relay nodes and 1 illegitimate AF relay node.

for Fig.3.4 are employed. Fig.3.5 shows the results for both approaches. It can be seen that our proposed authentication scheme reveals significant enhancement in terms of the detection capability compare to the DT method. Therefore, our GLRTL is more effective than DT and it can be used to further improve the work in [26]. Additionally, it is noticed that DT method requires relatively large IQI quantities (amplitude and phase imbalances are up to 0.3 and $15^{\mathrm{o}}$ in [26]) to achieve the satisfying hypothesis decision performance. While, it is shown that our authentication can differentiate AF relays even with delicate IQI distinctions.

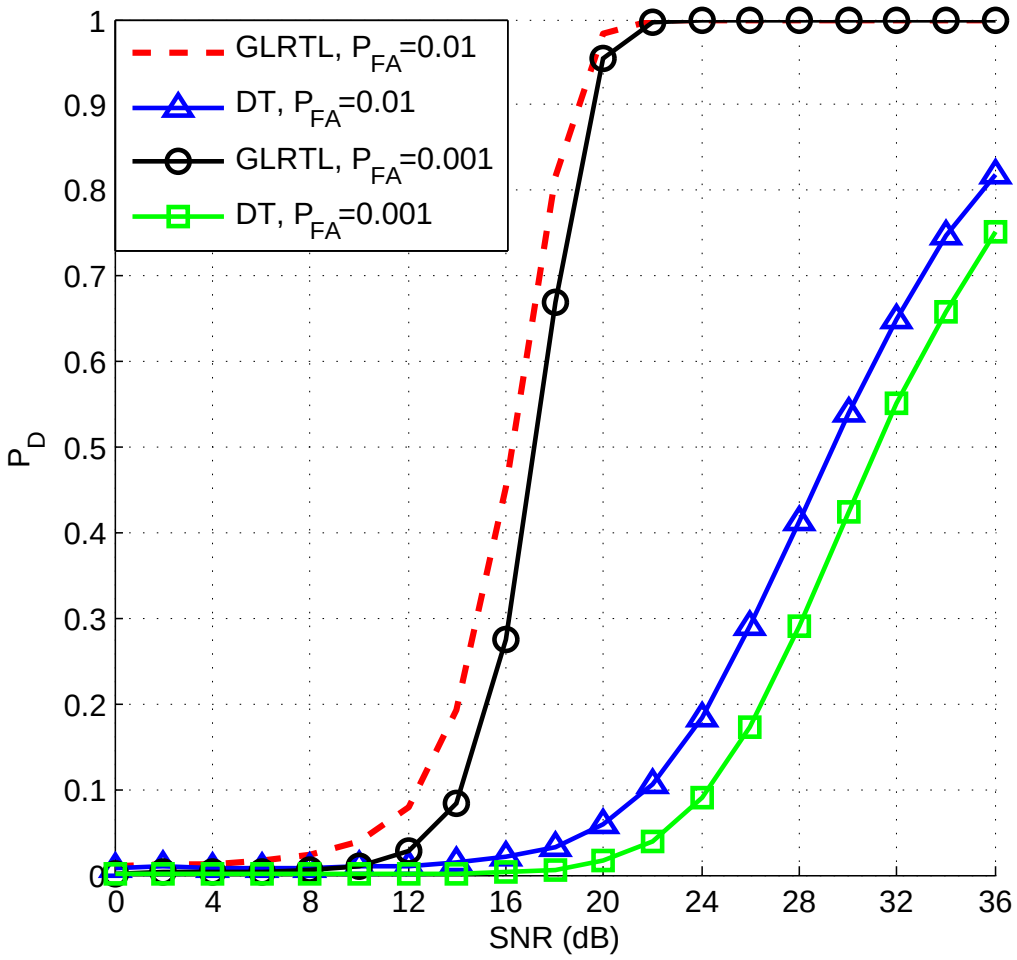


Figure 3.5: Performance comparison between GLRTL and DT.

## 3.6 Summary

In this chapter, a novel relay authentication scheme is proposed through exploiting Rx/Tx IQI in AF relay and the unique channel gains between relay and destination nodes. To be precise, the IQI-based device fingerprints were derived by analyzing the distorted signals at destination node. A two-parameter hypothesis testing model is then developed to determine whether the current AF relay is the same with the compared legitimate AF relay. To achieve satisfying performance in deciding the true hypothesis, a GLRTL based authentication method is proposed. The performance assessment results validated our derived formulas, and showed high authentication accuracy both in $\mathcal{H}_0$ and $\mathcal{H}_1$. In addition, our GLRTL method showed significant improvement in differentiating delicate IQI differences compared to another existing DT

method. Due to the proposed AF relay authentication system essentially depends upon a binary hypothesis testing, only one AF relay is considered in the authentication procedure. However, the malicious relay can use Sybil attack to claim multiple faked identities. Further, the practical wireless cooperative system usually consists of multiple relay nodes. Therefore, more advance AF relay identification with the consideration of the presence of multiple relays is still needed. Partial works of this chapter can be found in my published research paper [8].

# Chapter 4

# Optimal Wireless AF Relay Identification System

In Chapter 3, two AF relay nodes can be differentiated by examining the IQI and wireless channel related attributes. However, the practical cooperative relaying systems usually comprise more than one selectable relay nodes. Further, due to the time-varying channel factor is involved in the fingerprint generation, the reliability of differentiation performance is deteriorated if channel is fast varying. To address these shortcomings, the optimal AF relay identification system is investigated in this chapter.

## 4.1 Introduction

It has been proved that the AF relay can only be differentiated in physical-layer. Recall Chapter 3, a new device fingerprint comprised of IQI and channel gain is generated at the destination node for the AF relay authentication. However, since the wireless channels are time-varying, the performance of this method is degraded especially in the low SNR regime with small IQI. To improve the authentication performance, more stable device fingerprinting is demanded.

As studied in [70], wireless devices inevitably suffer from RF-AFE imperfections due to the imperfect hardware fabrications. Since RF-AFE imperfection is unique and distinct from device to device, it can be used to identify wireless transmitters in physical layer [18, 4]. As shown in [23], the RF-AFE imperfections of devices of the same product model are still distin-

guishable. These results demonstrate that, with more powerful device fingerprinting technique, the AF relay can be uniquely identified from multiple AF relay nodes even the RF-AFE imperfections are minor.

In this chapter, an optimal AF relay identification technique using IQI, a typical RF imperfection, is investigated. Given that IQI estimation and compensation are basics in most receivers for improving reception performance, a novel relay identification is proposed, which directly makes use of the ready-made IQI estimates at the receiver side. There are two direct advantages of using this approach. On the one hand, its implementation can become practical and simple since it can be widely utilized in most existing wireless devices and the extra IQI and channel-based fingerprint generation is no longer needed. On the other hand, the reliability performance can be improved as the channel variation effect is removed from fingerprint. In summary, the main contributions of this chapter are as follows.

- A new AF relay IQI fingerprinting method is proposed which directly uses the commonly available least square (LS) estimation of joint Rx/Tx IQI of an AF relay at the receiver (destination). Compared to the previous work of the authors in [26], this new method is more stable and no extra fingerprint generation is needed.

- The dynamic ranges of the joint Rx/Tx IQI fingerprint and the signal-to-IQI-distortion ratio are derived for the realistic ranges of the amplitude and phase shift imbalances. These ranges give insight into identifying the main technical strengths and limitations of the IQI-based AF relay identification. These results can be generally used in other AF relay IQI-related studies as well.

- An effective IQI-based AF relay identification protocol is introduced to identify a relay among a group of relays with minor IQIs. Since the small IQI measurements are corrupted by noise in practice, differentiating the relays becomes a challenging problem. Hence, a GLRT-based hypothesis testing is first used to maximize the detection probability for a given false alarm rate in differentiating two relays. Then, an identification algorithm using this differentiation method is designed. Numerical results demonstrate that the introduced algorithm outperforms the authors' previous method [26] and another possible identification method based on the work in [8] in terms of distinguishing

delicate IQI-fingerprint differences with a higher correct identification rate.

- Optimal training signals for quadrature amplitude modulation (QAM) and phase-shift keying (PSK) modulations are designed aiming at maximizing the capability of detecting an AF relay with specific IQI values. Furthermore, more robust suboptimal solutions are proposed whose identification performances are sufficiently close to the optimal designs.

The remainder of this chapter is organized as follows. Section 4.2 introduces the system model with joint Rx/Tx IQI of AF relays. In Section 4.3, the joint Rx/Tx IQI-based fingerprint of AF relay is analyzed. The relay differentiation method by verifying IQI fingerprint is presented in Section 4.4. In Section 4.5, the relay identification algorithm for multiple relays scenario is given. In Section 4.6, the optimal and suboptimal signal designs are presented. Section 4.7 presents the numerical results and discussions. Finally, this chapter is concluded in Section 4.8.

*Notations*: $(\cdot)^*$, $\mathbb{E}[\cdot]$, $|\cdot|$ and $(\cdot)^T$ $(\cdot)^H$ denote conjugate, expectation, absolute value, transpose and conjugate transpose operations, respectively. Bold lowercase and uppercase letter denotes vector and matrix, respectively. For vector $\mathbf{a}$, we use $a_k$ to denote its $k$th element. $\mathbf{I}$ denotes unit matrix. det($\mathbf{A}$) denotes the determinant of matrix $\mathbf{A}$. $\Re\{x\}$ and $\Im\{x\}$ denote real part and imaginary part of $x$, respectively.

## 4.2 System Model

In this section, the overall AF relay identification system model using the LS estimation of IQI is presented.

In an AF relay, all signal processing is accomplished in the physical layer. To be specific, the in-band received signal is down-converted, amplified, up-converted and finally forwarded towards the destination node [60, 61][1]. An AF relay can thereby be modeled as the cascade of a receiving component, an amplification factor and a transmission component [61, 63, 64, 71], as shown in Fig.3.1.

[1] In AF relay, the received passband signals should be first down-converted in order to be buffered in baseband. Then, the buffered signals are up-converted for transmission.

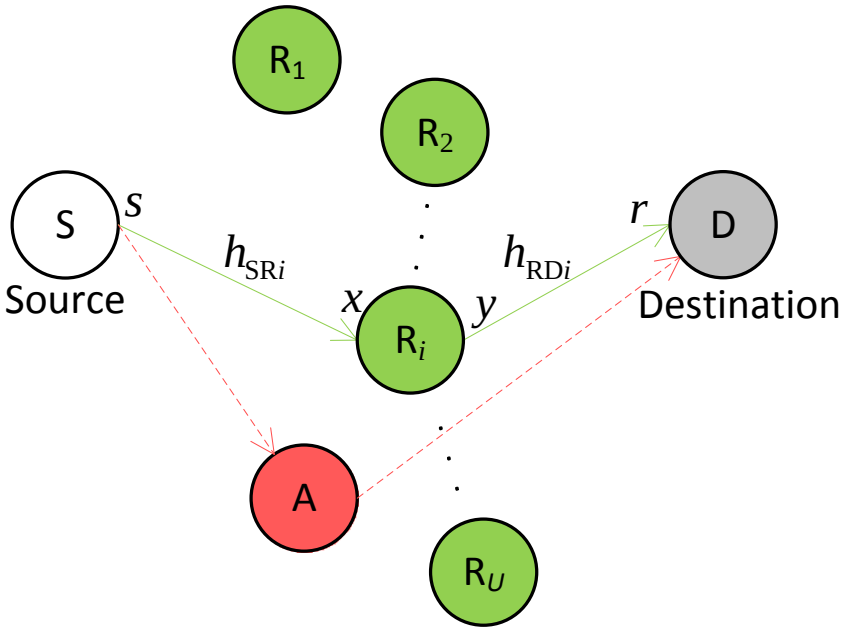


Figure 4.1: Wireless AF relay system with the presence of impersonation attacker.

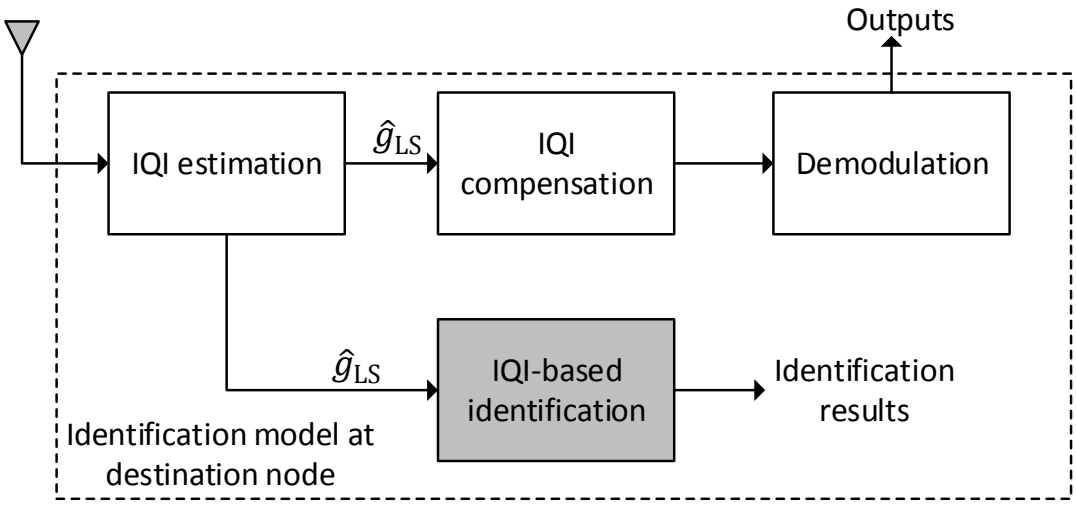


Figure 4.2: Block digram of identification implementation at destination.

Based on the results in (3.11), we are able to rewrite $y(t)$ in terms of the input signal $x(t)$ as

$$y(t) = g_1 x(t) + g_2 x^*(t), \tag{4.1}$$

where $g_1 \triangleq a(\mu_{\text{tx}}\mu_{\text{rx}} + \nu_{\text{tx}}\nu_{\text{rx}}^*)$ and $g_2 \triangleq a(\mu_{\text{tx}}\nu_{\text{rx}} + \nu_{\text{tx}}\mu_{\text{rx}}^*)$ are joint Rx/Tx IQI parameters. For simplicity, all of the following analyses are done in the baseband domain.

As shown in Fig.4.1, we consider a dual-hop AF relay system consisting of one source node (S), one destination node (D), and $U$ legitimate AF relay nodes $\text{R}_i$, $i = 1, 2, \ldots, U$, as well as an illegitimate AF relay attacker (A). All source, relays and destination nodes are single antenna and operate in half-duplex mode. This means that the signal transmission is performed in two phases. In the first phase, S transmits signal towards the relays. In the second phase, a selected relay retransmits the amplified signal towards D. D is assumed to be far apart from S so that there is no direct link between them. It is further assumed that the S–$\text{R}_i$ and $\text{R}_i$–D channels experience independent slow fading so that the channel fading gains $h_{\text{SR}}$ and $h_{\text{RD}}$ are independent and fixed during every sample observation [35]. Also, it is assumed that D has the knowledge of channel information. The complex zero-mean additive white Gaussian noises $n_{\text{SR}}$ and $n_{\text{RD}}$ with variances $\sigma_{\text{SR}}^2$ and $\sigma_{\text{RD}}^2$ are considered for the two phases, respectively. As shown in Fig.4.2, the received signals at the destination are sampled and processed for IQI estimation, compensation and relay identification. Similar to [63], it is assumed that S and D are IQI-free and focus on the IQI caused by the AF relays.

The IQI estimation is usually carried out using training signals so that the same training signals are used in our identification system. In the first phase, $N$ training signals are transmitted from S to the selected relay $\text{R}_i$. At $\text{R}_i$, the $k$th received signal can be represented as

$$x_{i,k} = s_k h_{\text{SR}i} + n_{\text{SR}i,k}, \tag{4.2}$$

where $s_k$ is the $k$-th transmitted signal and has the transmission power $P = \mathbb{E}[s_k^* s_k]$, $k = 1, 2, \cdots, N$. For simplicity in representation, the subscript $i$ is omitted in the following.

In the second phase, using (4.1) and (4.2), the received Rx/Tx IQI distorted signals at D

can be represented as

$$r_k = g_1 h_{\mathrm{SR}} h_{\mathrm{RD}} s_k + g_2 h_{\mathrm{SR}}^* h_{\mathrm{RD}} s_k^* + n_k, \tag{4.3}$$

where $n_k = g_1 h_{\mathrm{RD}} n_{\mathrm{SR}k} + g_2 h_{\mathrm{RD}k} n_{\mathrm{SR}k}^* + n_{\mathrm{RD}k}$ and its variance is given by $\sigma^2 = \sigma_{\mathrm{RD}}^2 + \sigma_{\mathrm{SR}}^2(|g_1|^2 + |g_2|^2)|h_{\mathrm{RD}}|^2$.

As illustrated in Fig.4.2, the LS estimator, as a typical IQI estimator[26][68][72], is employed at the destination to estimate the IQI of relay and feed the estimates to the following compensation and identification processes. After some manipulations, the matrix representation of (4.3) can be given as

$$\mathbf{r} = \mathbf{H}_s \mathbf{g} + \mathbf{n}, \tag{4.4}$$

where

$$\mathbf{H}_s = \left[ h_{\mathrm{SR}} h_{\mathrm{RD}} \mathbf{s} \;\mid\; h_{\mathrm{SR}}^* h_{\mathrm{RD}} \mathbf{s}^* \right]_{N \times 2}, \tag{4.5}$$

$$\mathbf{g} = \begin{bmatrix} g_1 & g_2 \end{bmatrix}^T. \tag{4.6}$$

Using the LS estimator of [72, eq. 15], the corresponding LS estimation of the IQI parameter vector $\mathbf{g}$ can be written as

$$\begin{aligned} \hat{\mathbf{g}}_{\mathrm{LS}} &= (\mathbf{H}_s^H \mathbf{H}_s)^{-1} \mathbf{H}_s^H \mathbf{r} \\ &= \mathbf{g} + (\mathbf{H}_s^H \mathbf{H}_s)^{-1} \mathbf{H}_s^H \mathbf{n}, \end{aligned} \tag{4.7}$$

where for the second equality we have substituted for $\mathbf{r}$ from (4.4) into the derivations. In the analyses, this estimated IQI parameter vector $\hat{\mathbf{g}}_{\mathrm{LS}}$ is used as the device fingerprint for identifying the current AF relay.

## 4.3 AF Relay IQI-based Device Fingerprinting Analysis

Since the IQI parameter plays an important role of device fingerprint in our identification system, this section focuses on analyzing its features and impacts to our system.

### 4.3.1 Analysis for the received IQI distorted signals

From (4.3), it can be seen that the received signal is comprised of three components, the desired signal (i.e., $s$), the image signal (i.e., $s^*$) and the inevitable noises.

Under an ideal IQI-free condition implying $\alpha_{\text{tx}} = \alpha_{\text{rx}} = 0$ and $\theta_{\text{tx}} = \theta_{\text{rx}} = 0^o$, $g_1 = a$ and $g_2 = 0$ can be consequently obtained. It can be observed from (4.3) that, in fact, the IQI parameter $g_2$ contributes to the presence of image signal component in the received signal.

Based on (4.3), the received signal-to-interference-plus-noise ratio (SINR) can be computed as

$$\begin{aligned}\gamma_1 &= \frac{|g_1 h_{\text{SR}} h_{\text{RD}}|^2 P}{|g_2 h_{\text{SR}} h_{\text{RD}}|^2 P + \sigma_{\text{RD}}^2 + (|g_1|^2 + |g_2|^2)\sigma_{\text{SR}}^2 |h_{\text{RD}}|^2} \\ &= \frac{|g_1|^2 \gamma_{\text{SR}} \gamma_{\text{RD}}}{|g_2|^2 \gamma_{\text{SR}} \gamma_{\text{RD}} + \frac{|g_1|^2 + |g_2|^2}{P} \gamma_{\text{RD}} + \frac{1}{P\sigma_{\text{SR}}^2}},\end{aligned} \tag{4.8}$$

where $\gamma_{\text{SR}} = \frac{|h_{\text{SR}}|^2}{\sigma_{\text{SR}}^2}$ and $\gamma_{\text{RD}} = \frac{|h_{\text{RD}}|^2}{\sigma_{\text{RD}}^2}$.

### 4.3.2 Analysis for the IQI parameters

Since this study is based on differentiating IQI parameters $g_1$ and $g_2$, it is important to analyze their ranges and relative relation. We first apply Euler's formula to derive the complex expression of IQI parameters in terms of the Rx/Tx amplitude and phase-shift imbalances, which can be given by (4.9)(4.10).

Without loss of generality, the ranges of amplitude and phase-shift imbalances are assumed as $|\theta_{\text{tx}}| \leqslant \theta_{m1}, |\theta_{\text{rx}}| \leqslant \theta_{m2}, |\alpha_{\text{tx}}| \leqslant \alpha_{m1}, |\alpha_{\text{rx}}| \leqslant \alpha_{m2}$. Accordingly, the ranges of $\Re\{g_1\}$, $\Im\{g_1\}$, $\Re\{g_2\}$ and $\Im\{g_2\}$ can be determined as

$$
\begin{aligned}
g_1 =& a\bigg(\frac{1}{4}(1+(1+\alpha_{\text{tx}})e^{j\theta_{\text{tx}}})(1+(1+\alpha_{\text{rx}})e^{-j\theta_{\text{rx}}}) + \frac{1}{4}(1-(1+\alpha_{\text{tx}})e^{j\theta_{\text{tx}}})(1-(1+\alpha_{\text{rx}})e^{-j\theta_{\text{rx}}})\bigg) \\
=& \frac{a}{2}(1+(1+\alpha_{\text{tx}})(1+\alpha_{\text{rx}})\cos(\theta_{\text{tx}}-\theta_{\text{rx}})) + j\frac{a}{2}(1+\alpha_{\text{tx}})(1+\alpha_{\text{rx}})\sin(\theta_{\text{tx}}-\theta_{\text{rx}}),
\end{aligned} \tag{4.9}
$$

$$
\begin{aligned}
g_2 =& a\bigg(\frac{1}{4}(1+(1+\alpha_{\text{tx}})e^{j\theta_{\text{tx}}})(1-(1+\alpha_{\text{rx}})e^{j\theta_{\text{rx}}}) + \frac{1}{4}(1-(1+\alpha_{\text{tx}})e^{j\theta_{\text{tx}}})(1+(1+\alpha_{\text{rx}})e^{j\theta_{\text{rx}}})\bigg) \\
=& \frac{a}{2}(1-(1+\alpha_{\text{tx}})(1+\alpha_{\text{rx}})\cos(\theta_{\text{tx}}+\theta_{\text{rx}})) - j\frac{a}{2}(1+\alpha_{\text{tx}})(1+\alpha_{\text{rx}})\sin(\theta_{\text{tx}}+\theta_{\text{rx}}).
\end{aligned} \tag{4.10}
$$

Table 4.1: Ranges of $\Re\{g_1\}$, $\Im\{g_1\}$, $\Re\{g_2\}$ and $\Im\{g_2\}$.

| IQI Parameters | $\Re\{g_1\}$ | $\Im\{g_1\}$ | $\Re\{g_2\}$ | $\Im\{g_2\}$ |
|---|---|---|---|---|
| $\theta_{m1}=\theta_{m2}=10^o$, $\alpha_{m1}=\alpha_{m2}=0.2$ | [0.801, 1.22] | [-0.246, 0.246] | [-0.22, 0.199] | [-0.246, 0.246] |
| $\theta_{m1}=\theta_{m2}=5^o$, $\alpha_{m1}=\alpha_{m2}=0.05$ | [0.924, 1.051] | [-0.189, 0.189] | [-0.051, 0.076] | [-0.189, 0.189] |

$$
\begin{aligned}
\frac{a}{2}+\frac{a}{2}\alpha_{min}\cos\theta_{max} \leqslant& \Re\{g_1\} \leqslant \frac{a}{2}+\frac{a}{2}\alpha_{max} \\
-\frac{a}{2}\alpha_{max}\sin\theta_{max} \leqslant& \Im\{g_1\} \leqslant \frac{a}{2}\alpha_{max}\sin\theta_{max} \\
\frac{a}{2}-\frac{a}{2}\alpha_{max} \leqslant& \Re\{g_2\} \leqslant \frac{a}{2}-\frac{a}{2}\alpha_{min}\cos\theta_{max} \\
-\frac{a}{2}\alpha_{max}\sin\theta_{max} \leqslant& \Im\{g_2\} \leqslant \frac{a}{2}\alpha_{max}\sin\theta_{max},
\end{aligned} \tag{4.11}
$$

where $\alpha_{min}=(1-\alpha_{m1})(1-\alpha_{m2})$, $\alpha_{max}=(1+\alpha_{m1})(1+\alpha_{m2})$ and $\theta_{max}=\theta_{m1}+\theta_{m2}$. Referring to the IQI settings in [72][73], a relatively large IQI case ($\theta_{m1}=\theta_{m2}=10^o, \alpha_{m1}=\alpha_{m2}=0.2$) and a small IQI case ($\theta_{m1}=\theta_{m2}=5^o, \alpha_{m1}=\alpha_{m2}=0.05$) are considered as two examples. The ranges of IQI parameters are calculated as shown in TABLE 4.1. It can be seen that the IQI parameter range is an extremely small interval in practice.

To reveal the relative amount of $g_1$ and $g_2$, we here referring to the definition of signal-to-IQI-distortion ratio as used in [70] and calculate this ratio for our AF relay system as given in (4.12). From the representation of (4.12), it is found that the ideal IQI-free condition, i.e.,

$$\gamma_2 = \frac{|g_1|^2}{|g_2|^2} = \frac{1 + (1+\alpha_{\text{tx}})^2(1+\alpha_{\text{rx}})^2 + 2(1+\alpha_{\text{tx}})(1+\alpha_{\text{rx}})\cos(\theta_{\text{tx}} - \theta_{\text{rx}})}{1 + (1+\alpha_{\text{tx}})^2(1+\alpha_{\text{rx}})^2 - 2(1+\alpha_{\text{tx}})(1+\alpha_{\text{rx}})\cos(\theta_{\text{tx}} + \theta_{\text{rx}})}. \tag{4.12}$$

$\theta_{m1} = \theta_{m2} = 0, \alpha_{m1} = \alpha_{m2} = 0$, can result in a zero denominator and a real positive numerator. In this case, the value of $\gamma_2$ is positive infinity. We further derive the range of $\gamma_2$, which is given by

$$\gamma_2 \in \left[1 + \frac{4}{\frac{\max(A_{max}, B_{max})}{\cos\theta_{m1}\cos\theta_{m2}} + 2\tan\theta_{m1}\tan\theta_{m2} - 2}, \infty\right), \tag{4.13}$$

where $A_{max} = (1+\alpha_{m1})(1+\alpha_{m2}) + \frac{1}{(1+\alpha_{m1})(1+\alpha_{m2})}$, $B_{max} = (1-\alpha_{m1})(1-\alpha_{m2}) + \frac{1}{(1-\alpha_{m1})(1-\alpha_{m2})}$.

The proof of equation (4.13) is presented as follows. The derivations for the minimum value of $\gamma_2$ can be summarized as an optimization problem, which is given by

$$\arg\min_{\alpha,\theta_{\text{tx}},\theta_{\text{rx}}} \left(\frac{1 + \alpha^2 + 2\alpha\cos(\theta_{\text{tx}} - \theta_{\text{rx}})}{1 + \alpha^2 - 2\alpha\cos(\theta_{\text{tx}} + \theta_{\text{rx}})}\right), \tag{4.14a}$$

$$\text{s.t.} \quad \alpha = (1+\alpha_{\text{tx}})(1+\alpha_{\text{rx}}),$$

$$|\theta_{\text{tx}}| \leqslant \theta_{m1}, |\theta_{\text{rx}}| \leqslant \theta_{m2},$$

$$|\alpha_{\text{tx}}| \leqslant \alpha_{m1}, |\alpha_{\text{rx}}| \leqslant \alpha_{m2}. \tag{4.14b}$$

Using the constraints (4.14b), the range of $\alpha$ can be determined as

$$(1-\alpha_{m1})(1-\alpha_{m2}) \leqslant \alpha \leqslant (1+\alpha_{m1})(1+\alpha_{m2}). \tag{4.15}$$

After using addition and subtraction theorems of sine function, (4.14a) can be simplified as

$$1 + \frac{4\alpha\cos\theta_{\text{tx}}\cos\theta_{\text{rx}}}{1 + \alpha^2 - 2\alpha(\cos\theta_{\text{tx}}\cos\theta_{\text{rx}} - \sin\theta_{\text{tx}}\sin\theta_{\text{rx}})}$$
$$= 1 + \frac{4}{(\alpha + \frac{1}{\alpha})(\cos\theta_{\text{tx}}\cos\theta_{\text{rx}})^{-1} + 2\tan\theta_{\text{tx}}\tan\theta_{\text{rx}} - 2}. \tag{4.16}$$

It is noteworthy that both numerator and denominator are divided by $\alpha \cos\theta_{\text{tx}} \cos\theta_{\text{rx}}$ in the derivation of (4.16). However, it is reasonable in our case as the amplitude mismatch and phase mismatch are usually small enough to ensure $\alpha > 0$ and $\cos\theta_{\text{tx}} \cos\theta_{\text{rx}} > 0$ in real applications.

According to the inequality of arithmetic and geometric means [74], we can obtain

$$2 = 2\sqrt{\alpha \cdot \frac{1}{\alpha}} \leqslant \alpha + \frac{1}{\alpha} \leqslant \max(A_{max}, B_{max}), \tag{4.17}$$

where $A_{max} = (1+\alpha_{m1})(1+\alpha_{m2}) + \frac{1}{(1+\alpha_{m1})(1+\alpha_{m2})}$, $B_{max} = (1-\alpha_{m1})(1-\alpha_{m2}) + \frac{1}{(1-\alpha_{m1})(1-\alpha_{m2})}$. It is notable that the monotonicity of $\alpha + \frac{1}{\alpha}$ in (4.17) is considered to find its upper bound.

Further, we can also refer to the monotonicity of cosine and tangent, and get

$$\cos\theta_{m1} \cos\theta_{m2} \leqslant \cos\theta_{\text{tx}} \cos\theta_{\text{rx}} \leqslant 1, \tag{4.18}$$

$$-\tan\theta_{m1} \tan\theta_{m2} \leqslant \tan\theta_{\text{tx}} \tan\theta_{\text{rx}} \leqslant \tan\theta_{m1} \tan\theta_{m2}. \tag{4.19}$$

Based on (4.17)-(4.19), the lower bound of (4.16) can be figured out as

$$\begin{aligned} &1 + \frac{4}{(\alpha + \frac{1}{\alpha})(\cos\theta_{\text{tx}} \cos\theta_{\text{rx}})^{-1} + 2\tan\theta_{\text{tx}} \tan\theta_{\text{rx}} - 2} \\ &\geqslant 1 + \frac{4}{\frac{\max(A_{max}, B_{max})}{\cos\theta_{m1} \cos\theta_{m2}} + 2\tan\theta_{m1} \tan\theta_{m2} - 2}. \end{aligned} \tag{4.20}$$

Finally, the range of $\gamma_2$ can be obtained as shown in (4.13).

The infinity in (4.13) denotes the IQI-free case. We also substitute for the aforementioned large and small IQIs in (4.13) and compute its range in dB as $10\log_{10}(\gamma_2) \in [11.142 \text{ dB}, \infty)$ and $[14.854 \text{ dB}, \infty)$, respectively.

Based on the above analysis, the challenges of using IQI parameters in our relay identification can be summarized as follows. First, although the actual AF relay device fingerprints (i.e., $g_1$ and $g_2$) are stable, their values usually locate in a small interval especially under the small IQI condition. Second, the useful information afforded from IQI parameters for identifi-

cation is limited. Equation (4.11) shows that the image parts of $g_1$ and $g_2$ have exactly the same range interval, which implies the two parts may provide very similar information. Besides, the range analysis of $\gamma_2$ reveals that $g_2$ is extremely less than $g_1$, which makes $g_2$ hard to detect and differentiate. Finally, the accurate estimation and detection of such a small IQI parameters with presence of noises is also a challenge. It is noteworthy that the IQI analysis results of this section can be not only benefit to our identification system design but also be useful in other AF relay IQI estimation and compensation system designs.

## 4.4 Generalized Likelihood Ratio Test (GLRT) Based AF Relay Differentiation

In this section, GLRT is applied to differentiate AF relays based on the estimated IQI parameters.

In order to decide whether the estimated IQI parameters belong to a validated AF relay or not, the offset between $\hat{\mathbf{g}}_{\text{LS}}$ and another pre-validated device fingerprint ($\mathbf{g}_v$) is first computed as

$$\begin{aligned}\mathbf{g}_{\text{off}} &= \hat{\mathbf{g}}_{\text{LS}} - \mathbf{g}_v \\ &= \Delta\mathbf{g} + (\mathbf{H}_s^H\mathbf{H}_s)^{-1}\mathbf{H}_s^H\mathbf{n},\end{aligned} \tag{4.21}$$

where $\Delta\mathbf{g} = \mathbf{g} - \mathbf{g}_v$. In practical use, the validated fingerprints can be obtained and pre-stored when the corresponding legitimate relays are associated and authenticated in the networks. A binary hypothesis testing can be modeled based on offset as

$$\begin{cases} \mathcal{H}_0: & \Delta\mathbf{g} = \mathbf{0} \\ \mathcal{H}_1: & \Delta\mathbf{g} \neq \mathbf{0} \end{cases} \tag{4.22}$$

where hypothesis $\mathcal{H}_0$ represents the fingerprint of current relay is exactly the same with the pre-validated relay's fingerprint, which produces $\Delta\mathbf{g} = \mathbf{0}$; while hypothesis $\mathcal{H}_1$ represents the two compared device fingerprints belong two different relays. Based on this hypothesis testing,

the key point of relay identification is detecting $\Delta\mathbf{g}$ with the presence of correlated complex random variable $(\mathbf{H}_s^H\mathbf{H}_s)^{-1}\mathbf{H}_s^H\mathbf{n}$. The likelihood ratio test (LRT) is used to detect $\Delta\mathbf{g}$. Since the likelihood of $\mathbf{g}_{\text{off}}$ is required in LRT, the mean and covariance of $\mathbf{g}_{\text{off}}$ are derived as

$$\mathbb{E}[\mathbf{g}_{\text{off}}] = \mathbb{E}[\Delta\mathbf{g}] + (\mathbf{H}_s^H\mathbf{H}_s)^{-1}\mathbf{H}_s^H\mathbb{E}[\mathbf{n}] = \Delta\mathbf{g}, \tag{4.23a}$$

$$\begin{aligned}
&\mathbb{E}[(\mathbf{g}_{\text{off}} - \Delta\mathbf{g})(\mathbf{g}_{\text{off}} - \Delta\mathbf{g})^H] \\
=&(\mathbf{H}_s^H\mathbf{H}_s)^{-1}\mathbf{H}_s^H\mathbb{E}[\mathbf{n}\mathbf{n}^H]\mathbf{H}_s(\mathbf{H}_s^H\mathbf{H}_s)^{-1} \\
=&\sigma^2(\mathbf{H}_s^H\mathbf{H}_s)^{-1}\mathbf{H}_s^H\mathbf{I}\mathbf{H}_s(\mathbf{H}_s^H\mathbf{H}_s)^{-1} \\
=&\sigma^2(\mathbf{H}_s^H\mathbf{H}_s)^{-1}.
\end{aligned} \tag{4.23b}$$

According to (4.23a) (4.23b) and thanks to the property that any linear combination of Gaussian random variables is still Gaussian distributed, it can be obtained that $\mathbf{g}_{\text{off}}$ is complex normal distributed as $\mathbf{g}_{\text{off}} \sim CN(\Delta\mathbf{g}, \Sigma)$ in our case, where $\Sigma$ is a $2 \times 2$ positive definite Hermitian matrix [75] and defined as

$$\begin{aligned}
\Sigma &= \sigma^2(\mathbf{H}_s^H\mathbf{H}_s)^{-1} \\
&= \frac{\sigma^2}{|h_{\text{SR}}h_{\text{RD}}|^4(\sum_{i=1}^{N}\sum_{j=1}^{N}|s_i|^2|s_j|^2 - |\sum_{i=1}^{N}s_i|^2)} \\
&\times \begin{bmatrix} R_1 & R_2 \\ R_3 & R_4 \end{bmatrix},
\end{aligned} \tag{4.24}$$

where

$$R_1 = |h_{\text{SR}}h_{\text{RD}}|^2\sum_{i=1}^{N}|s_i|^2, \tag{4.25a}$$

$$R_2 = -(h_{\text{SR}}^*)^2|h_{\text{RD}}|^2\sum_{i=1}^{N}s_i^{*2}, \tag{4.25b}$$

$$R_3 = R_2^*, \tag{4.25c}$$

$$R_4 = R_1. \tag{4.25d}$$

It is notable that $\mathbf{g}_{\text{off}}$ is zero mean complex normal distributed under $\mathcal{H}_0$; while it becomes

non-zero mean under $\mathcal{H}_1$. Therefore, the likelihood function of $\mathbf{g}_{\text{off}}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ can be, respectively, given by [76]

$$p(\mathbf{g}_{\text{off}}|\mathcal{H}_0) = \frac{1}{\pi^2|\det(\Sigma)|} e^{-\mathbf{g}_{\text{off}}^H \Sigma^{-1} \mathbf{g}_{\text{off}}}, \tag{4.26}$$

$$p(\mathbf{g}_{\text{off}}|\mathcal{H}_1) = \frac{1}{\pi^2|\det(\Sigma)|} e^{-(\mathbf{g}_{\text{off}}-\Delta\mathbf{g})^H \Sigma^{-1} (\mathbf{g}_{\text{off}}-\Delta\mathbf{g})}. \tag{4.27}$$

Using (4.26) and (4.27), LRT can be performed to decide $\mathcal{H}_1$ if [33]

$$L(\mathbf{g}_{\text{off}}) = \frac{p(\mathbf{g}_{\text{off}}|\mathcal{H}_1)}{p(\mathbf{g}_{\text{off}}|\mathcal{H}_0)} > \eta, \tag{4.28}$$

where $\eta$ is a real positive number.

Given that the vector $\Delta\mathbf{g}$ may be unknown at destination, this LRT cannot outcome processable results for further differentiation in this case. To improve the practicability of our system, we consider this more challenging case and apply GLRT to overcome this problem. In GLRT, the maximum likelihood estimation (MLE) of $\Delta\mathbf{g}$ is used to replace the unknown vector in (4.28). The MLE of $\Delta\mathbf{g}$ is defined as

$$\begin{aligned} \Delta\hat{\mathbf{g}}_{\text{MLE}} &= \underset{\Delta\mathbf{g}}{\text{argmax}}\ p(\mathbf{g}_{\text{off}}|\Delta\mathbf{g}) \\ &= \underset{\Delta\mathbf{g}}{\text{argmax}} \frac{e^{-(\mathbf{g}_{\text{off}}-\Delta\mathbf{g})^H \Sigma^{-1} (\mathbf{g}_{\text{off}}-\Delta\mathbf{g})}}{\pi^2|\det(\Sigma)|}. \end{aligned} \tag{4.29}$$

Using (4.21) and (4.24), we can obtain

$$\begin{aligned} &-(\mathbf{g}_{\text{off}} - \Delta\mathbf{g})^H \Sigma^{-1} (\mathbf{g}_{\text{off}} - \Delta\mathbf{g}) \\ &= -\frac{1}{\sigma^2} \sum_{i=1}^{N} n_i^2 \leqslant 0. \end{aligned} \tag{4.30}$$

Given that $e^x$ is a monotone increasing function, the range of $e^{-\frac{1}{\sigma^2}\sum_{i=1}^{N} n_i^2}$ can be determined as $(0, 1]$. The likelihood can be maximized when $-\frac{1}{\sigma^2}\sum_{i=1}^{N} n_i^2 = 0$, which is equivalent to

$\Delta\mathbf{g} = \mathbf{g}_{\text{off}}$. Consequently, $\Delta\hat{\mathbf{g}}_{\text{MLE}} = \mathbf{g}_{\text{off}}$. So that the logarithmic GLRT can be performed as

$$\begin{aligned} & G(\mathbf{g}_{\text{off}}) \\ &= \ln\left(\frac{p(\mathbf{g}_{\text{off}}|\Delta\hat{\mathbf{g}}_{\text{MLE}}, \mathcal{H}_1)}{p(\mathbf{g}_{\text{off}}|\mathcal{H}_0)}\right) \\ &= \ln\left(\frac{(\pi^2 \det(\Sigma))^{-1} e^{-(\mathbf{g}_{\text{off}}-\Delta\hat{\mathbf{g}}_{\text{MLE}})^H \Sigma^{-1}(\mathbf{g}_{\text{off}}-\Delta\hat{\mathbf{g}}_{\text{MLE}})}}{(\pi^2 \det(\Sigma))^{-1} e^{-\mathbf{g}_{\text{off}}^H \Sigma^{-1}\mathbf{g}_{\text{off}}}}\right) \\ &= \mathbf{g}_{\text{off}}^H \Sigma^{-1}\mathbf{g}_{\text{off}} > T. \end{aligned} \tag{4.31}$$

The result of GLRT shows that if the metric $A = \mathbf{g}_{\text{off}}^H \Sigma^{-1}\mathbf{g}_{\text{off}}$ is larger than the threshold $T$, the hypothesis $\mathcal{H}_1$ is claimed; otherwise, $\mathcal{H}_0$ is determined.

In the next step, the value of $T$ should be carefully determined. In engineering practice, the threshold is usually pre-determined according to a desired false alarm probability. Hence, it is necessary to obtain the probability density functions (PDF) of $A$ and compute $T$ by solving the following equation

$$\int_T^\infty p(A|\mathcal{H}_0)dA = P_{\text{FA}}, \tag{4.32}$$

where $p(A|\mathcal{H}_0)$ denotes the PDF of $A$ under $\mathcal{H}_0$. We can derive the PDF of $A$ under hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ as

$$p(A|\mathcal{H}_0) = Ae^{-A}, A > 0 \tag{4.33}$$

$$p(A|\mathcal{H}_1) = \sqrt{\frac{2A}{\beta}}\, e^{-\frac{2A+\beta}{2}} I_1(\sqrt{2\beta A}), A > 0 \tag{4.34}$$

where $I_1(\cdot)$ is the modified Bessel function of the first kind with order 1 and it is defined as

$$I_1(x) = \sum_{k=0}^{\infty} \frac{(\frac{1}{2}x)^{2k+1}}{k!\Gamma(k+2)}, \tag{4.35}$$

where $\Gamma(\cdot)$ is gamma function. The parameter $\beta$ in (4.34) is defined as

$$\beta = 2(\lambda_1|b_1|^2 + \lambda_2|b_2|^2), \tag{4.36}$$

where $\lambda_1$ and $\lambda_2$ are the eigenvalues of $\Sigma^{-1}$; $b_1$ and $b_2$ are the elements of vector $\mathbf{b}$ which is given by

$$\mathbf{b} = \mathbf{Q}\Delta\mathbf{g}, \tag{4.37}$$

where $\mathbf{Q}$ is $2 \times 2$ matrix whose $i$th column is the eigenvector of $\Sigma^{-1}$ corresponding to the eigenvalue $\lambda_i$, and $\mathbf{Q}\mathbf{Q}^H = \mathbf{I}$.

In the following, we derive the PDFs of $A$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ which are given in (4.33) and (4.34). It can be observed that $A$ is dependent on a correlated complex normally distributed vector $\mathbf{g}_{\text{off}}$. Since $\Sigma^{-1}$ is positive definite Hermitian matrix, all eigenvalues of $\Sigma^{-1}$ are real positive. The eigendecomposition of matrix $\Sigma^{-1}$ can be performed as

$$\Sigma^{-1} = \mathbf{Q}^H\mathbf{\Lambda}\mathbf{Q} \tag{4.38}$$

where $\mathbf{\Lambda} = \text{diag}(\lambda_1, \lambda_2)$ with its elements $\lambda_i > 0, i = 1, 2$ denoting the $i$th eigenvalue of $\Sigma^{-1}$; $\mathbf{Q}$ is $2 \times 2$ matrix whose $i$th column is the eigenvector of $\Sigma^{-1}$ corresponding to $\lambda_i$. Substituting for (4.38) in metric $A$, we can obtain

$$\begin{aligned} A &= \mathbf{g}_{\text{off}}^H\Sigma^{-1}\mathbf{g}_{\text{off}} \\ &= \mathbf{g}_{\text{off}}^H\mathbf{Q}^H\mathbf{\Lambda}\mathbf{Q}\mathbf{g}_{\text{off}} \\ &= \mathbf{d}^H\mathbf{\Lambda}\mathbf{d} \\ &= \lambda_1|d_1|^2 + \lambda_2|d_2|^2 \end{aligned} \tag{4.39}$$

where $\mathbf{d} = \mathbf{Q}\mathbf{g}_{\text{off}} = [d_1, d_2]^T$ and $d_1, d_2$ are two independent random variables since $\text{cov}(d_1, d_2) = \text{cov}(d_2, d_1) = 0$ as shown in (4.40). Given (4.21)(4.24)(4.37) and orthogonal matrix $\mathbf{Q}$, the co-

variance matrix of $\mathbf{d}$ can be computed as

$$\begin{aligned}
\text{cov}(\mathbf{d}) =& \mathbb{E}[(\mathbf{d}-\mathbf{b})(\mathbf{d}-\mathbf{b})^H] \\
=& \mathbf{Q}(\mathbf{H}_s^H\mathbf{H}_s)^{-1}\mathbf{H}_s^H\mathbb{E}[\mathbf{n}\mathbf{n}^H]\mathbf{H}_s(\mathbf{H}_s^H\mathbf{H}_s)^{-1}\mathbf{Q}^H \\
=& \sigma^2\mathbf{Q}(\mathbf{H}_s^H\mathbf{H}_s)^{-1}(\mathbf{H}_s^H\mathbf{H}_s)(\mathbf{H}_s^H\mathbf{H}_s)^{-1}\mathbf{Q}^H \\
=& \mathbf{Q}\Sigma\mathbf{Q}^H \\
=& \mathbf{Q}\mathbf{Q}^H\mathbf{\Lambda}^{-1}\mathbf{Q}\mathbf{Q}^H \\
=& \text{diag}\left(\frac{1}{\lambda_1},\frac{1}{\lambda_2}\right) \\
=& \begin{bmatrix} \text{cov}(d_1) & \text{cov}(d_1,d_2) \\ \text{cov}(d_2,d_1) & \text{cov}(d_2) \end{bmatrix}.
\end{aligned} \tag{4.40}$$

Therefore, it can be obtained that $d_1 \sim CN(b_1, \frac{1}{\lambda_1}), d_2 \sim CN(b_2, \frac{1}{\lambda_2})$, where $b_i$ is defined in (4.37). Since $b_i = 0$ under $\mathcal{H}_0$ and $b_i \neq 0$ under $\mathcal{H}_1$, $A$ follows scaled central/non-central chi-squared distributions under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. Therefore, the normalized $K = 2A$ can be expressed based on (4.39) as

$$K = k_1^2 + k_2^2 + k_3^2 + k_4^2 \tag{4.41}$$

where

$$\begin{aligned}
k_1 =& \sqrt{2\lambda_1}\Re\{d_1\} \sim \begin{cases} \mathcal{H}_0: & N(0,1) \\ \mathcal{H}_1: & N(\sqrt{2\lambda_1}\Re\{b_1\},1) \end{cases} \\
k_2 =& \sqrt{2\lambda_1}\Im\{d_1\} \sim \begin{cases} \mathcal{H}_0: & N(0,1) \\ \mathcal{H}_1: & N(\sqrt{2\lambda_1}\Im\{b_1\},1) \end{cases} \\
k_3 =& \sqrt{2\lambda_2}\Re\{d_2\} \sim \begin{cases} \mathcal{H}_0: & N(0,1) \\ \mathcal{H}_1: & N(\sqrt{2\lambda_2}\Re\{b_2\},1) \end{cases} \\
k_4 =& \sqrt{2\lambda_2}\Im\{d_2\} \sim \begin{cases} \mathcal{H}_0: & N(0,1) \\ \mathcal{H}_1: & N(\sqrt{2\lambda_2}\Im\{b_2\},1) \end{cases}.
\end{aligned} \tag{4.42}$$

In the case, the PDF of $K$ under $\mathcal{H}_0$ can be given as a central chi-squared PDF with 4 degrees of freedom as [69]

$$p_K(K|\mathcal{H}_0) = \frac{1}{4} K e^{-\frac{K}{2}}, K > 0. \tag{4.43}$$

While under $\mathcal{H}_1$, $K$ follows the standard non-central chi-squared distribution with 4 degrees of freedom and non-centrality $\beta_1$ and its PDF can be given as

$$p_K(K|\mathcal{H}_1) = \frac{1}{2} \sqrt{\frac{K}{\beta_1}} e^{-\frac{K+\beta_1}{2}} I_1(\sqrt{K\beta_1}), K > 0 \tag{4.44}$$

where the non-centrality is defined as

$$\begin{aligned} \beta_1 = &(\sqrt{2\lambda_1}\Re\{b_1\})^2 + (\sqrt{2\lambda_1}\Im\{b_1\})^2 \\ &+(\sqrt{2\lambda_2}\Re\{b_2\})^2 + (\sqrt{2\lambda_2}\Im\{b_2\})^2. \end{aligned} \tag{4.45}$$

It can be seen that $\beta_1$ equals to $\beta$ in (4.36).

The PDF of $A$ can be derived according to the PDF of $K$. In this case, $p_A(x) = 2p_K(2x)$ since $A = \frac{1}{2}K$. In light of this, the PDF of $A$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ can be obtained by first replacing $K$ with $2A$ in (4.43) and (4.44) and then multiply the two PDFs by 2, which produces (4.33) and (4.34), respectively.

Substituting (4.33) into (4.32), we are able to give the representation of $P_{\text{FA}}$ as

$$P_{\text{FA}} = Q_{A|\mathcal{H}_0}(T) = (T+1)e^{-T}, \tag{4.46}$$

where $Q_{A|\mathcal{H}_0}(\cdot)$ denotes the rights tail probability of $A$ under $\mathcal{H}_0$. Accordingly, the threshold $T$ can be calculated by inversing this function as

$$T = Q^{-1}_{A|\mathcal{H}_0}(P_{\text{FA}}). \tag{4.47}$$

Using (4.47) and (4.34), the detection probability can be calculated as

$$\begin{aligned} P_{\mathrm{D}} &= P_{rob}(A > T|\mathcal{H}_1) \\ &= \int_{Q^{-1}_{A|\mathcal{H}_0}(P_{\mathrm{FA}})}^{\infty} \sqrt{\frac{2A}{\beta}}\, e^{-\frac{2A+\beta}{2}} I_1(\sqrt{2\beta A})dA \\ &= Q_2(\sqrt{\beta}, \sqrt{2Q^{-1}_{A|\mathcal{H}_0}(P_{\mathrm{FA}})}), \end{aligned} \tag{4.48}$$

where $Q_\nu(a, b)$ represents the generalized Marcum Q-function with real order $\nu$ and positive $a, b$.[77, pp.219-223].

As a result, relay differentiation can be completed by checking whether or not the current AF relay has the same IQI device fingerprint with the compared one.

## 4.5 AF Relay Identification Algorithm

In practice, there can be more than one relay in a cooperative communication system and therefore the relay identification process should be capable of identifying one relay among a group of relays. Here, we present an identification algorithm based on the proposed GLRT-based differentiation technique to handle this multi-relay scenario.

For presentation convenience, the AF relay $R_{\mathrm{AF}}$ is considered as our identification target. This identification algorithm is required to decide whether the identity of $R_{\mathrm{AF}}$ is matched with any of the $U_1$ pre-identified relays or not. If not, an alarm should be given to report $R_{\mathrm{AF}}$ as a new AF relay. The detailed identification algorithm is given in Algorithm 1.

After performing this algorithm, the identity of the target relay $R_{\mathrm{AF}}$ can be determined. If $R_{\mathrm{AF}}$ is a new one, the variable *alarm* will be 1, and an alarm will be given; otherwise, $R_{\mathrm{AF}}$'s identity can be obtained in variable $ID$.

## 4.6 Optimal Signal Design for Enhancing Device Identification Performance

In real attacking scenario, the attackers are usually some fixed devices. They can launch impersonation attacks again and again by spoofing the upper-layer identities, e.g., media access

**Algorithm 1** AF relay identification algorithm

!t

$\Phi \leftarrow \{id_1, id_2, \cdots, id_{U_1}\}$ *%$U_1$ pre-recorded identities*
$ID \leftarrow \hat{\mathbf{g}}_{\mathrm{LS}}$ *%$R_{AF}$'s identity*
$l \leftarrow 0$
$idx \leftarrow \{0\}$ *%$U_1$ zeros*
**for** $i \leftarrow 1$ to $U_1$ **do**
    **if** $ID \neq id_i$ **then** *%use GLRT-based differentiation*
                *%to compare ID and $id_i$*
        $l \leftarrow l + 1$
        $idx_l \leftarrow i$
    **end if**
**end for**
**if** $l = 0$ **then**
    $alarm \leftarrow 1$  *%give an alarm*
**else if** $l = 1$ **then**
    $alarm \leftarrow 0$
    $ID \leftarrow idx_1$
**else** *%find the minimum Euclidean distance between l relays and return the corresponding index*
    $alarm \leftarrow 0$
    $idx_{\min} \leftarrow min(|A_l - T|)$
    $ID \leftarrow idx_{\min}$
**end if**

control address spoofing [78]. Since the attacker can easily mimic another legitimate identity by changing upper-layer information once it is detected and any devices who possess the legitimate upper-layer identity including attackers will be trusted again, this kind of attacks are hard to be eradicated by upper-layer identity based identification method. Given the fact that IQI is an inherently stable hardware imperfection, the fixed IQIs of device can be directly targeted once this device is detected as an attacker. This feature can be exploited to enhance the capability of detecting some specific attackers in our study.

It is assumed that one AF relay attacker has been detected by our IQI-based identification and thereby its IQI parameter has been recorded. Since our objective is to prevent future impersonation attacks from this attacker, we here focus on maximizing the detection probability $P_{\mathrm{D}}$ as shown in (4.48).

The three arguments of $P_{\mathrm{D}}$ are positive $\sqrt{\beta}$, $\sqrt{2Q^{-1}_{A|\mathcal{H}_0}(P_{\mathrm{FA}})}$ and the real order 2. It can been known that arguments $\sqrt{2Q^{-1}_{A|\mathcal{H}_0}(P_{\mathrm{FA}})}$ and 2 are fixed constants. Due to the results of monotonicity investigation of the generalized Marcum Q-function in [79], our derived detection probability is a strictly increasing function with respect to $\sqrt{\beta}$. Since the transmitted signals $\mathbf{s}$ are the only controllable variables, the key point of maximizing $P_{\mathrm{D}}$ is to find the maximal value of $\beta$ through adjusting $\mathbf{s}$.

According to (4.24) (4.36) (4.37) and let $\mathbf{\Lambda} = \mathrm{diag}(\lambda_1, \lambda_2)$, $\beta$ can be rewritten as

$$\begin{aligned}\beta &= 2\mathbf{b}^H\mathbf{\Lambda}\mathbf{b} \\ &= 2\Delta\mathbf{g}^H\Sigma^{-1}\Delta\mathbf{g} \\ &= \frac{2}{\sigma^2}\Delta\mathbf{g}^H\mathbf{H}_s^H\mathbf{H}_s\Delta\mathbf{g}.\end{aligned} \tag{4.49}$$

For analysis convenience, $\mathbf{H}_s$ is decomposed as

$$\mathbf{H}_s = \mathbf{S}\mathbf{H}, \tag{4.50}$$

where

$$\mathbf{S} = [\mathbf{s} \mid \mathbf{s}^*]_{N\times 2}, \tag{4.51}$$

$$\mathbf{H} = \mathrm{diag}(h_1, h_2). \tag{4.52}$$

Herein, $h_1 = h_{\mathrm{SR}} h_{\mathrm{RD}}$ and $h_2 = h_{\mathrm{SR}}^* h_{\mathrm{RD}}$. Substituting (4.50) into (4.49), we can obtain

$$\begin{aligned} J &= \frac{1}{2}\sigma^2\beta \\ &= \Delta\mathbf{g}^H\mathbf{H}^H\mathbf{S}^H\mathbf{S}\mathbf{H}\Delta\mathbf{g} \\ &= h_1^*\Delta g_1^* h_1 \Delta g_1 \mathbf{s}^H\mathbf{s} + h_1\Delta g_1 h_2^*\Delta g_2^*\mathbf{s}^T\mathbf{s} \\ &+ h_1^*\Delta g_1^* h_2\Delta g_2\mathbf{s}^H\mathbf{s}^* + h_2^*\Delta g_2^* h_2\Delta g_2\mathbf{s}^T\mathbf{s}^* \\ &= (|h_1\Delta g_1|^2 + |h_2\Delta g_2|^2)\sum_{i=1}^{N}|s_i|^2 \\ &+ 2\Re\{h_2^*\Delta g_2^* h_1\Delta g_1\sum_{i=1}^{N} s_i^2\}. \end{aligned} \tag{4.53}$$

In this case, maximizing $\beta$ is equivalent to maximizing $J$. Given that the value of $s$ is subject to specific constellation pattens, the square quadrature amplitude modulation (QAM) and circle phase-shift keying (PSK) as two basic modulation schemes are respectively considered to derive the optimal $s$ leading to the maximal $J$.

### 4.6.1 Square QAM Modulation Case

In QAM modulation, the signal is represented as $s_i = a_i + jb_i$. Let $l = |h_1\Delta g_1|^2 + |h_2\Delta g_2|^2$, $c = \Re\{h_2^*\Delta g_2^* h_1\Delta g_1\}$ and $d = \Im\{h_2^*\Delta g_2^* h_1\Delta g_1\}$, then $J$ can be expressed as

$$\begin{aligned} J &= \sum_{i=1}^{N} J_i \\ &= (l+2c)\sum_{i=1}^{N} a_i^2 + (l-2c)\sum_{i=1}^{N} b_i^2 - 4d\sum_{i=1}^{N} a_i b_i, \end{aligned} \tag{4.54}$$

where $J_i$ is defined as

$$J_i = (l+2c)a_i^2 + (l-2c)b_i^2 - 4da_i b_i. \tag{4.55}$$

Thanks to that $s_i$ are independent, we are able to separately design $s_i$ to maximize $J_i$, and $J$

will be maximized as a result. The rules of optimal signal design under square QAM modulations are summarized as Proposition 1.

**Proposition 1** *If $d < 0$, the optimal $s_i$ is the signal locates in the angles of the constellation square in the first and third quadrants of I/Q coordinate plane.*

*If $d > 0$, the optimal $s_i$ is the signal that locates in the angles of the constellation square in the second and fourth quadrants of I/Q coordinate plane.*

*If $d = 0$, the optimal $s_i$ is the signal that locates in any angles of the constellation square of the I/Q coordinate plane.*

The proof of Proposition 1 is given as follows. According to (4.55), $J_i$ can be expressed as a summation of two quadratic components, which is given by

$$J_i = \underbrace{(l+2c)(a_i - \frac{2d}{l+2c}b_i)^2}_{\zeta_i} + \underbrace{\frac{l^2-4c^2-4d^2}{l+2c}b_i^2}_{\kappa_i}. \tag{4.56}$$

Setting $h_1\Delta g_1 = c_1 + jd_1$ and $h_2\Delta g_2 = c_2 + jd_2$ to analyze the coefficients of quadratic components $\zeta_i$ and $\kappa_i$. The $l$, $c$ and $d$ can be expressed as

$$l = c_1^2 + c_2^2 + d_1^2 + d_2^2, \tag{4.57a}$$

$$c = c_1c_2 + d_1d_2, \tag{4.57b}$$

$$d = d_1c_2 - d_2c_1. \tag{4.57c}$$

Accordingly, the representation of coefficient $l + 2c$ can be given by

$$l + 2c = (c_1 + c_2)^2 + (d_1 + d_2)^2 > 0 \tag{4.58}$$

and the second coefficient is

$$\frac{l^2-4c^2-4d^2}{l+2c} = \frac{(c_1^2+d_1^2-c_2^2-d_2^2)^2}{(c_1+c_2)^2+(d_1+d_2)^2} \geqslant 0. \tag{4.59}$$

Equations (4.58) and (4.59) show that the coefficients of both $\zeta_i$ and $\kappa_i$ are positive. Therefore, the maximum value of $J_i$ can be achieved only if the the maximum values of $(a_i - \frac{2d}{l+2c}b_i)^2$

and $b_i^2$ can be simultaneously achieved. Given that $l + 2c > 0$, it can be seen that the values of $(a_i - \frac{2d}{l+2c}b_i)^2$ and $b_i^2$ depend upon the sign of $d$ and the maximum modulus of $a_i$, $b_i$.

Without loss of generality, it is assumed that the maximum values of $|a_i|$ and $|b_i|$ are $a_{max} > 0$ and $b_{max} > 0$, respectively, under the current QAM modulation. For the square constellation case, $a_{max} = b_{max}$.

If $d = 0$, (4.56) reduces to

$$J_i = (l + 2c)a_i^2 + \frac{l^2 - 4c^2 - 4d^2}{l + 2c}b_i^2. \tag{4.60}$$

In this case, $J_i$ can be maximized when $|a_i| = a_{max}$ and $|b_i| = b_{max}$, which implies the four angles of the constellation square.

If $d < 0$, it results in $-\frac{2d}{l+2c} > 0$. Thus, the quadratic components $(a_i - \frac{2d}{l+2c}b_i)^2$ and $b_i^2$ can be maximized when $a_i = a_{max}, b_i = b_{max}$ or $a_i = -a_{max}, b_i = -b_{max}$, which corresponds to the square angles in the first and third quadrants.

If $d > 0$, then $-\frac{2d}{l+2c} < 0$. In this case, $a_i$ and $b_i$ are required to have opposite signs and satisfy $a_i = a_{max}, b_i = -b_{max}$ or $a_i = -a_{max}, b_i = b_{max}$, which corresponds to the square angles in the second and fourth quadrants.

***Practical Implementation Discussion***: Although the optimal design can maximize the attacker detection ability, it may induce a potential risk in practical implementation. To be specific, the value of optimal signal has only two options when $d > 0$ or $d < 0$. This may occasionally result in a singular matrix $\mathbf{H}_s^H\mathbf{H}_s$, and make this matrix's inverting process suffer from low accuracy problem, e.g., the calculation of covariance matrix $\Sigma$.

To avoid this theoretically possible risk, a simply suboptimal signal design is proposed as an alternative. Instead of applying Proposition 1 to all signals, we can intentionally design a small portion of the signals using the following rules.

If $d > 0$ or $d < 0$, the suboptimal signals are the two points locating in the same quadrant with the optimal signal and being closest to the optimal signal. It is notable that this suboptimal is not suitable for 4-QAM since 4-QAM only has one point in every quadrant.

### 4.6.2 Circle PSK Modulation Case

In $M$-PSK modulation, the constellation diagram is a circle and the signal can be generally represented as $s_i = A_s e^{j\theta_i}$, where $A_s$ denotes the constant signal amplitude and $\theta_i$ denotes the phase-shift. Similarly, an optimal signal design under the PSK modulation is proposed as Proposition 2.

**Proposition 2** *The optimal $s_i$ is the signal that can satisfy $\theta_i = \frac{-\phi}{2}$ or $\theta_i = \frac{-\phi}{2} + \pi$, where*

$$\begin{aligned}\phi &= \angle(h_2^* \Delta g_2^* h_1 \Delta g_1) \\ &= \arctan\left(\frac{\Im\{h_2^* \Delta g_2^* h_1 \Delta g_1\}}{\Re\{h_2^* \Delta g_2^* h_1 \Delta g_1\}}\right) \in (-\pi, \pi].\end{aligned} \tag{4.61}$$

The proof of Proposition 2 is given as follows. Recall eq.(4.53), it can be obtained that the first item $(|h_1 \Delta g_1|^2 + |h_2 \Delta g_2|^2) \sum_{i=1}^{N} |s_i|^2$ is fixed and not controllable. Hence, the maximization of $J$ depends upon whether the second item $2R = 2\Re\{h_2^* \Delta g_2^* h_1 \Delta g_1 \sum_{i=1}^{N} s_i^2\}$ can be maximized by adjusting $s_i$.

For analysis convenience, we apply Euler's formula and set

$$h_2^* \Delta g_2^* h_1 \Delta g_1 = G e^{j\phi}, \tag{4.62}$$

where $\phi$ is defined as

$$\phi = \arctan\left(\frac{\Im\{h_2^* \Delta g_2^* h_1 \Delta g_1\}}{\Re\{h_2^* \Delta g_2^* h_1 \Delta g_1\}}\right) \in (-\pi, \pi].$$

According to (4.62) and $s_i = A_s e^{j\theta_i}$, we can obtain

$$\begin{aligned}R =& \Re\{G e^{j\phi} \sum_{i=1}^{N} A_s^2 e^{j2\theta_i}\} \\ =& A_s^2 G \sum_{i=1}^{N} \cos(2\theta_i + \phi).\end{aligned} \tag{4.63}$$

Since $\theta_i$ is independent, $\theta_i$ can be separately adjusted to maximize every $R_i$, where $R_i$ is defined as

$$R_i = A_s^2 G \cos(2\theta_i + \phi). \tag{4.64}$$

As a result, $R$ will be maximized because $R = \sum_{i=1}^{N} R_i$.

Considering the $(-\pi, \pi]$ range limit of $\theta_i$ and $\phi$, it can be concluded that $R_i$ can achieve its maximum value when $\theta_i = \frac{-\phi}{2}$ or $\theta_i = \frac{-\phi}{2} + \pi$.

***Practical Implementation Discussion***: Since $\phi$ can be any degree whereas the values of $\theta_i$ are subject to the number of points used in the PSK constellation diagram, the engineers may have to consider the specific constellation and choose the $M$-PSK symbol with the closest angle to $\theta_i$.

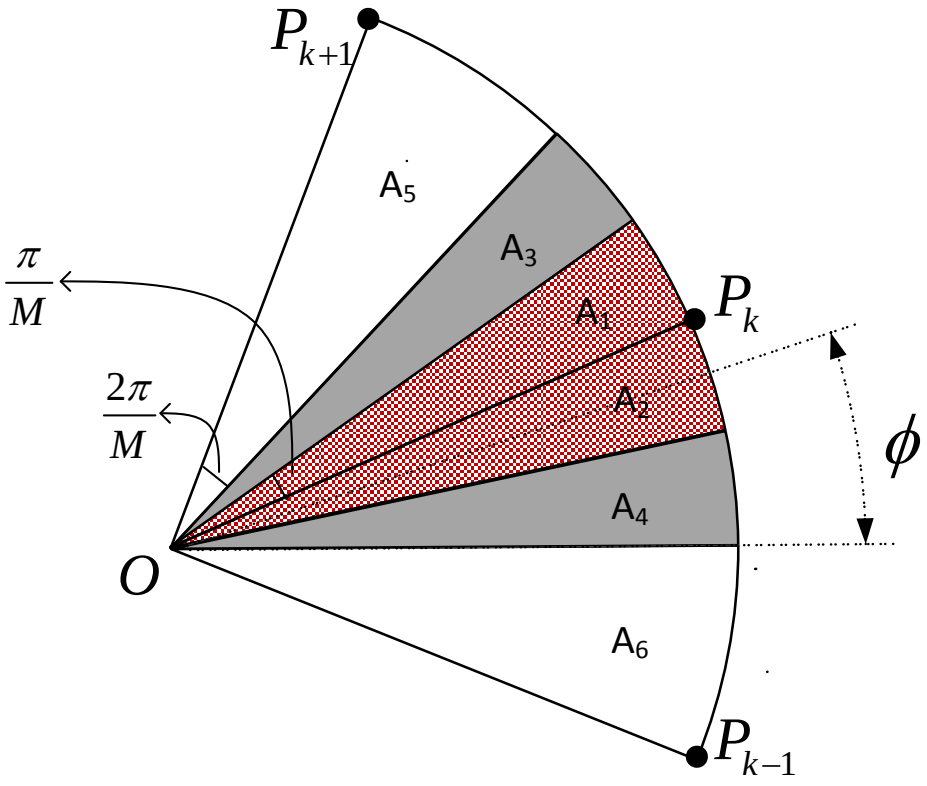


Figure 4.3: The suboptimal signal design for PSK modulation case.

As with the QAM case, there is also a possibility of having a singular matrix, $\mathbf{H}_s^H\mathbf{H}_s$. A suboptimal design is also proposed to solve this problem. As shown in Fig.4.3, $P_k$ denotes the point corresponding to the square of the $k$th PSK constellation point ($P_k$), i.e., $P_k = s_{P_k}^2 = A_s^2 e^{j2\theta_k}$. It is notable that $P_k$ can correspond to multiple $s_{P_k}$ since their squares may be overlapped, for example, $(A_s e^{j\theta_k})^2 = (A_s e^{j(\theta_k+\pi)})^2$. As shown in this figure, the phase shift between two neighboring points (e.g., $P_k$ and $P_{k-1}$) is $\frac{4\pi}{M}$. The phase shifts of $A_1$, $A_2$, $A_3$, and $A_4$ are $\frac{\pi}{M}$, while the phase shifts of $A_5$ and $A_6$ are $\frac{2\pi}{M}$. It is assumed that $-\phi$ is closer to $P_k$ than $P_{k-1}$ and $P_{k+1}$, which means that it falls in the red or gray sectors. We here take two signals ($s_i$, $s_{i+1}$) combination into account to approach the desired phase $-\phi$. The rules of our suboptimal approach is described as follows.

1. If $-\phi$ falls in $A_1$ or $A_2$, we set $s_i = s_{P_{k+n}}, s_{i+1} = s_{P_{k-n}}, n = 0, 1, 2\cdots$.

2. If $-\phi$ falls in $A_3$, we set $s_i = s_{P_{k+n}}, s_{i+1} = s_{P_{k+1-n}}$.

3. If $-\phi$ falls in $A_4$, we set $s_i = s_{P_{k+n}}, s_{i+1} = s_{P_{k-1-n}}$.

In practical implementation, we can first consider Proposition 2 for designing signals and then flexibly replace a portion of these signals by applying this suboptimal approach according to the application requirement. For example, if the total number of $s$ is odd $O_1$, Proposition 2 can be applied to the first $O_2$ signals, where $O_2$ is odd and $O_2 < O_1$. Then, the remaining $O_1 - O_2$ signals can be designed using the suboptimal method.

## 4.7 Evaluation Results

In this section, numerical results are presented to validate our derived equations and evaluate our proposed IQI-based AF relay identification system.

### 4.7.1 Numerical Results for IQI Device Fingerprint

The ranges of IQI device fingerprint and $\gamma_2$, which are discussed in Section III, are first simulated. Fig.4.4 shows the values of $\Re\{\mathbf{g}_1\}, \Im\{\mathbf{g}_1\}, \Re\{\mathbf{g}_2\}$ and $\Im\{\mathbf{g}_2\}$ vs. $\alpha$, where $\alpha = (1 + \alpha_{\text{rx}})(1 + \alpha_{\text{tx}})$. The Rx/Tx IQIs are set as $\theta_{\text{rx}} = 5^o$, $\theta_{\text{tx}} = 10^o$, $\alpha = 0.64 - 1.44$ and

$a = 1$. It can be seen that $\Re\{\mathbf{g}_1\}$ is much larger than the other three parameters, which reflects the practical effects of small IQI values on eq. (4.9) (4.10). Besides, as predicted that the varying ranges of $\Im\{\mathbf{g}_1\}$ and $\Im\{\mathbf{g}_2\}$ are close and small leading to a more challenging differentiation. In addition, the four simulated parameters also validate our analytical results derived in (4.11) whose ranges are [0.8188, 1.2173], [0.0279, 0.0628], [-0.1955, 0.1909] and [-0.1863, -0.0828], respectively.

Fig.4.5 reveals the log-scale $\gamma_2$ defined as $10\log_{10}\gamma_2$. As expected, the maximal values of three simulated $10\log_{10}\gamma_2$ appear at $\alpha = 1$, implying the case of no amplitude imbalances given the simulation setups. We also consider $\alpha_{m1} = \alpha_{m2} = 0.2$ corresponding to $\alpha = 0.64 - 1.44$ and apply (4.13) to calculate the minimal values of $10\log_{10}\gamma_2$. The calculated results are 11.9032 dB, 12.5637 dB and 12.8595 dB in the order of red, blue and black curves, which can well match the simulated values.

The two above simulations validate our analysis of IQI fingerprint in Section III. It is believed that this result can not only improve our identification system but also be useful in many other IQI relevant works. For example, engineers can design more targeted IQI estimation and compensation systems with a full consideration of our results of IQI ranges. Also, our results about the achievable $\gamma_2$ can be used as a practical criteria to make the IQI reduction goal and evaluate the performance of IQI compensation system.

### 4.7.2 Evaluation Results for Proposed AF Relay Identification Technique

In this subsection, the performance of proposed IQI-based AF relay differentiation, identification algorithm, optimal and suboptimal signal design are evaluated. Furthermore, our identification technique is compared with another two latest IQI-based identification techniques. In the following simulations, the Rayleigh fading channel, amplification gain $a = 1$, 16-QAM and 16-PSK modulations are used. To evaluate the identification performance with challenging condition of minor IQIs, the amplitude imbalance and phase-shift imbalance in our simulations are intentionally set within $-0.05 - 0.05$ and $-5^o - 5^o$ compared to some relatively large IQIs cases, such as a typical example in [26], the IQIs are $-0.3 - 0.3$ and $-15^o - 15^o$. The results are based on $10^5$ independent realizations of our system.

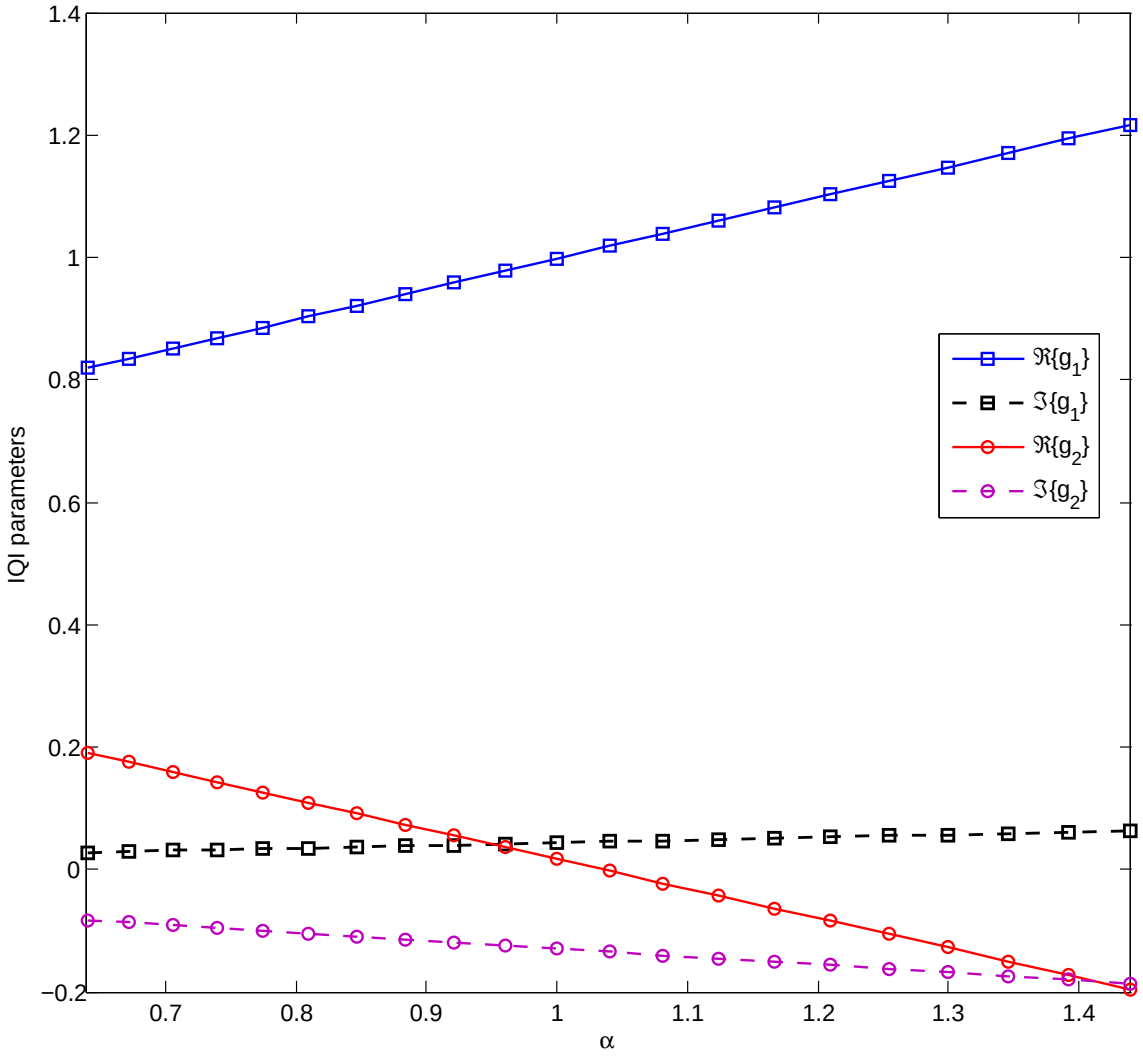


Figure 4.4: IQI parameters vs. $\alpha$ under $\theta_{\text{rx}} = 5^o, \theta_{\text{tx}} = 10^o$.

In Fig.4.6, the analytical $P_{\text{D}}$ as derived in (4.48) is compared with the simulation results. It shows that the analytical $P_{\text{D}}$ of both QAM and PSK cases can sufficiently approach the simulated $P_{\text{D}}$. As expected, a higher SNR results in higher $P_{\text{D}}$ mainly because the IQI estimates are more accurate and thereby improves the following differentiation performance. The threshold $T$ decreases with $P_{\text{FA}}$ varying from $10^{-3}$ to 1 since $T$, as shown in (4.47), is produced by $Q^{-1}_{A|\mathcal{H}_0}$ which is a monotonically decreasing function. The detection performances between QAM and PSK are compared in Fig.4.7. It is observed that with the increase of SNR and $P_{FA}$, the $P_D$ is also keeping increasing. The $P_D$ of all cases can almost achieve 100% when SNR approaching

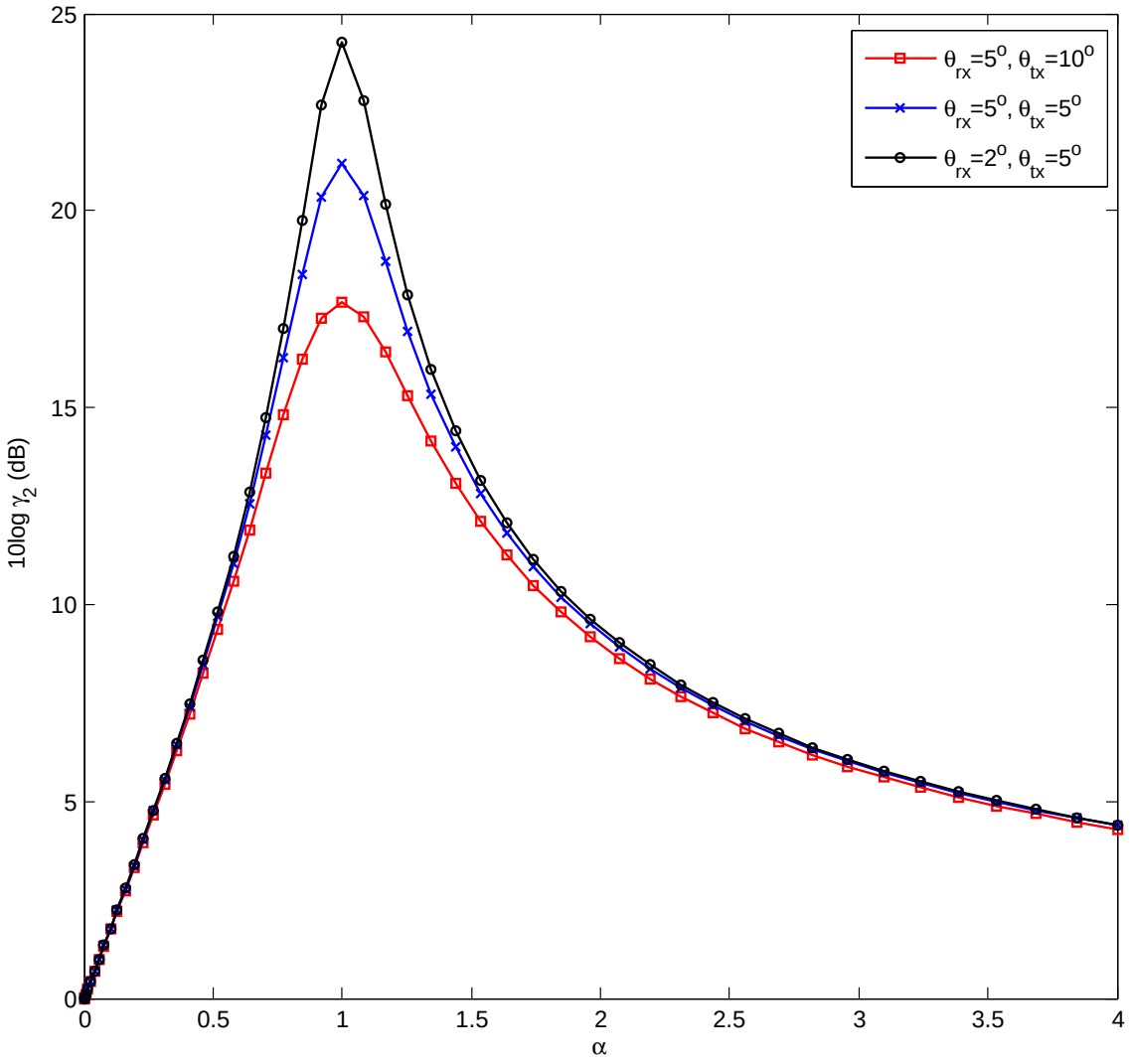


Figure 4.5: The range of $\gamma_2$ vs. $\alpha$ under different $\theta_{\text{rx}}$ and $\theta_{\text{tx}}$.

25 dB. In addition, it is also observed that the detection performance of QAM is always better than PSK under the same simulation setup, which is mainly due to that QAM is more robust to IQI than PSK.

We assess the enhancements of using the proposed optimal signal (i.e., Proposition 1 and 2) and suboptimal designs in terms of $P_{\text{D}}$ as shown in Fig.4.8. To clearly reveal the enhancements, more severe conditions are intentionally considered. To be specific, closer IQIs between current relay and the validated relay, lower SNR=15 dB and a small number $N = 14$ are used. Besides, due to the impractical problems in implementing optimal methods as discussed in Section VI,

the theoretically achievable $P_{\mathrm{D}}$ of optimal methods is used as upper bound and it is analytically computed using (4.48) with a maximized $\beta$. The results show that our suboptimal solution can be implemented at the expense of only a detection probability loss of averagely 2.59% and 1.68% in QAM and PSK, respectively, compared to the optimal method. On the other hand, this suboptimal method also shows an average 34.54% and 23.43% higher $P_{\mathrm{D}}$ than the methods without using any optimal designs. Therefore, it can be concluded that the suboptimal solution is able to significantly improve the capability of detecting some specific attackers in severe conditions and can be implemented more practically than the optimal solution with minor optimality sacrifice.

To evaluate the identification performance, we consider multiple relays consisting of four legitimate ones and one impersonation attacker and simulate this case using the identification algorithm as proposed in Section V. The IQIs of these five relays are randomly chosen from the aforementioned ranges $-0.05-0.05$ and $-5^{o}-5^{o}$. It is assumed that one relay, either legitimate or illegitimate, will be randomly selected from these five relays each time. Compared to only determining $\mathcal{H}_0$ or $\mathcal{H}_1$, the task of this evaluation is more challenging since it is further required to give the correct identity of the current relay from the four legitimate candidates or give an alarm if an illegitimate relay with small and similar IQIs is selected. To show the advantages of our proposed identification method, another two latest IQI-based device identification methods are simulated and compared as shown in Fig.4.9. For presentation simplicity, we call the methods in [8] and [26] as VF and DT since they are using Varying Fingerprint and Distance Testing, respectively. The correct identification rate (CIR) is defined as the total number of correct identity claims plus correct alarms divided by the total number of simulation iterations. It is shown that our method is superior to VF and DT in terms of the CIR in all simulated cases. The significant enhancement is gained because our fingerprint is more reliable than VF and our identification technique is more accurate in small IQI case than DT. Another important advantage is that our identification can achieve better performance and using less signals. It can be seen that the CIR of our method with $N = 32$ is even higher than VF with $N = 512$. Therefore, the number of training signals required in our method is much shorter.

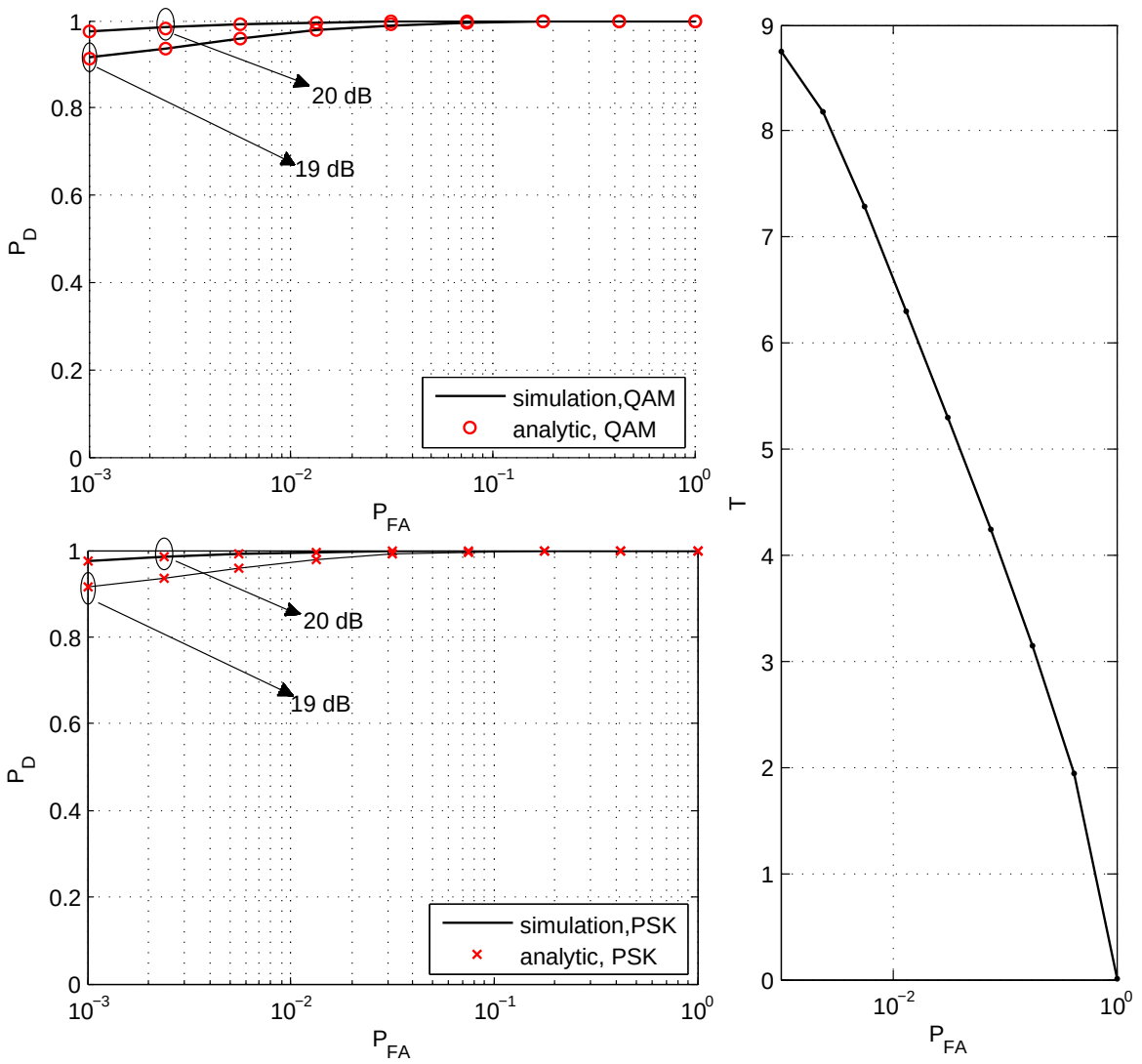


Figure 4.6: Analytical and simulated $P_{\mathrm{D}}$ vs. $P_{\mathrm{FA}}$ and corresponding $T$. The current AF relay has $(\alpha_{\mathrm{rx}}, \theta_{\mathrm{rx}}, \alpha_{\mathrm{tx}}, \theta_{\mathrm{tx}}) = (-0.03, 5^{\mathrm{o}}, 0.05, 4^{\mathrm{o}})$, the validated AF relay owns $(\alpha_{\mathrm{rx}}, \theta_{\mathrm{rx}}, \alpha_{\mathrm{tx}}, \theta_{\mathrm{tx}}) = (0.02, 5^{\mathrm{o}}, -0.05, -4^{\mathrm{o}})$ and $N = 14$.

## 4.8 Summary

In this chapter, the AF relay device identification using IQI is investigated. Since the IQI estimation and compensation are necessary techniques in most wireless receivers, we proposed to directly use the LS estimated IQI parameters as device fingerprint and further give a comprehensive analysis of this fingerprint in terms of several ranges and its challenges to our identification system. It is worth noting that this general analysis is not only benefit to improving our identification but also can be referred when designing most other LS estimator

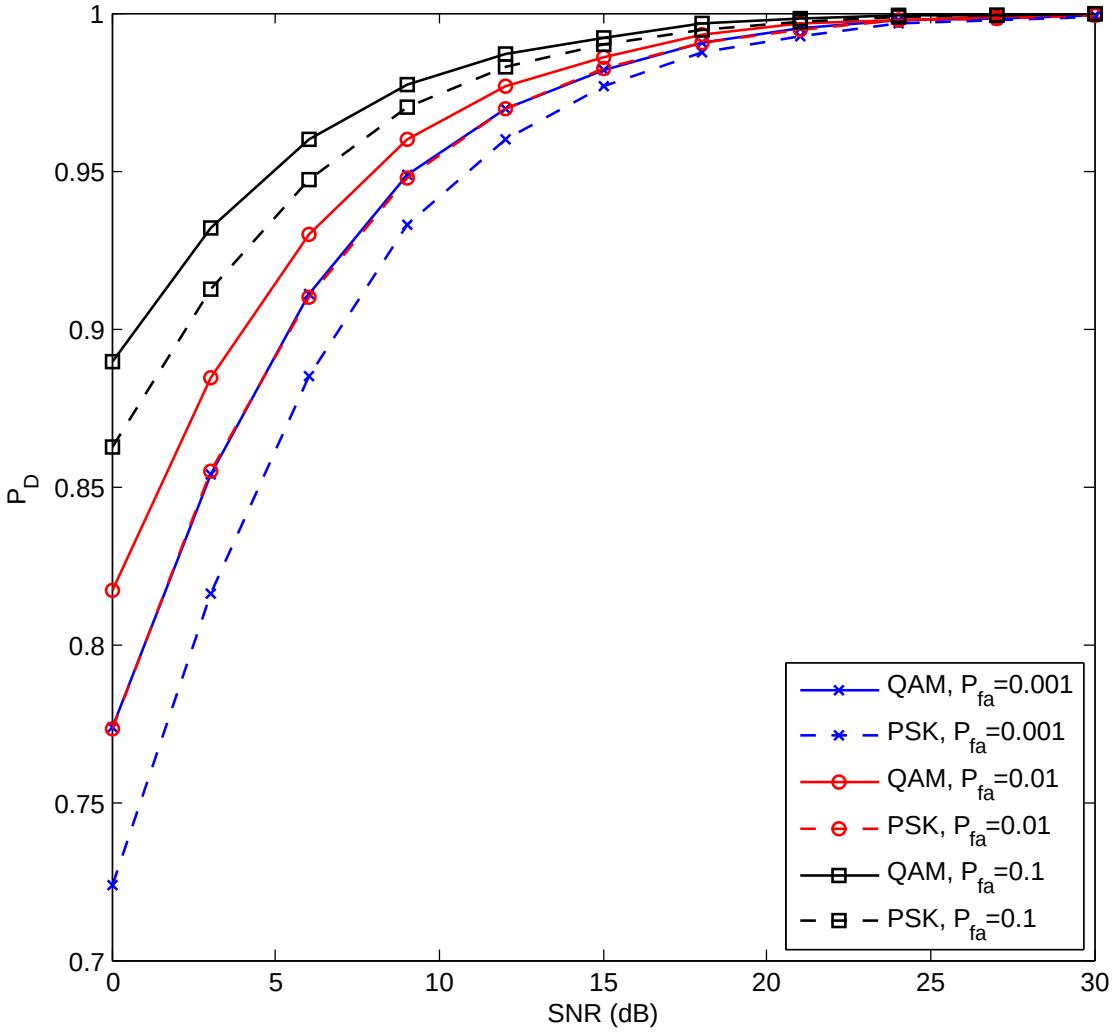


Figure 4.7: $P_D$ vs SNR under different $P_{FA}$ settings.

based IQI wireless systems. AF relay differentiation is accomplished using this IQI fingerprint and derived detection probability and threshold. The optimal signal designs for QAM and PSK modulations are further proposed for the sake of maximizing the capability of detecting some specific attackers. To overcome the potential impractical problems of our optimal design, two suboptimal solutions are proposed which can achieve sufficient close performance of the optimal ones. Besides, a high accuracy identification algorithm is also proposed based on our differentiation method. The simulation results show that our identification method outperforms another two IQI-based device identification methods in terms of the correct identification rate and the number of required signals. To be specific, our identification is able to achieve higher

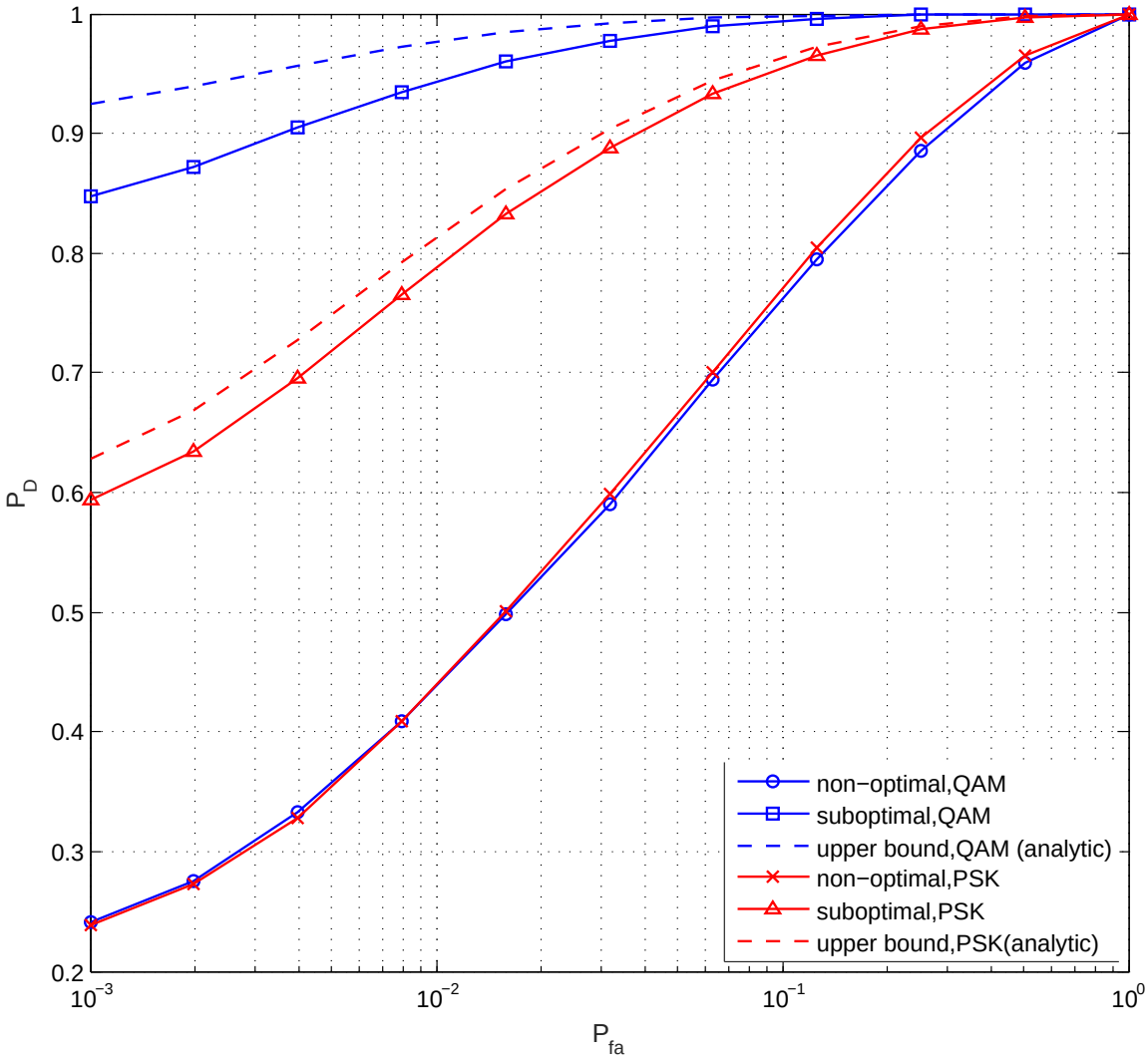


Figure 4.8: Detection probabilities comparison between suboptimal and non-optimal signal design and the corresponding upper bounds. The current AF relay has $(\alpha_{\text{rx}}, \theta_{\text{rx}}, \alpha_{\text{tx}}, \theta_{\text{tx}}) = (-0.03, 3^{\text{o}}, 0.03, 3^{\text{o}})$, the validated AF relay owns $(\alpha_{\text{rx}}, \theta_{\text{rx}}, \alpha_{\text{tx}}, \theta_{\text{tx}}) = (0.02, 5^{\text{o}}, -0.05, -4^{\text{o}})$, SNR=16 dB, $N = 14$.

correct identification rate with significantly lesser signal amount.

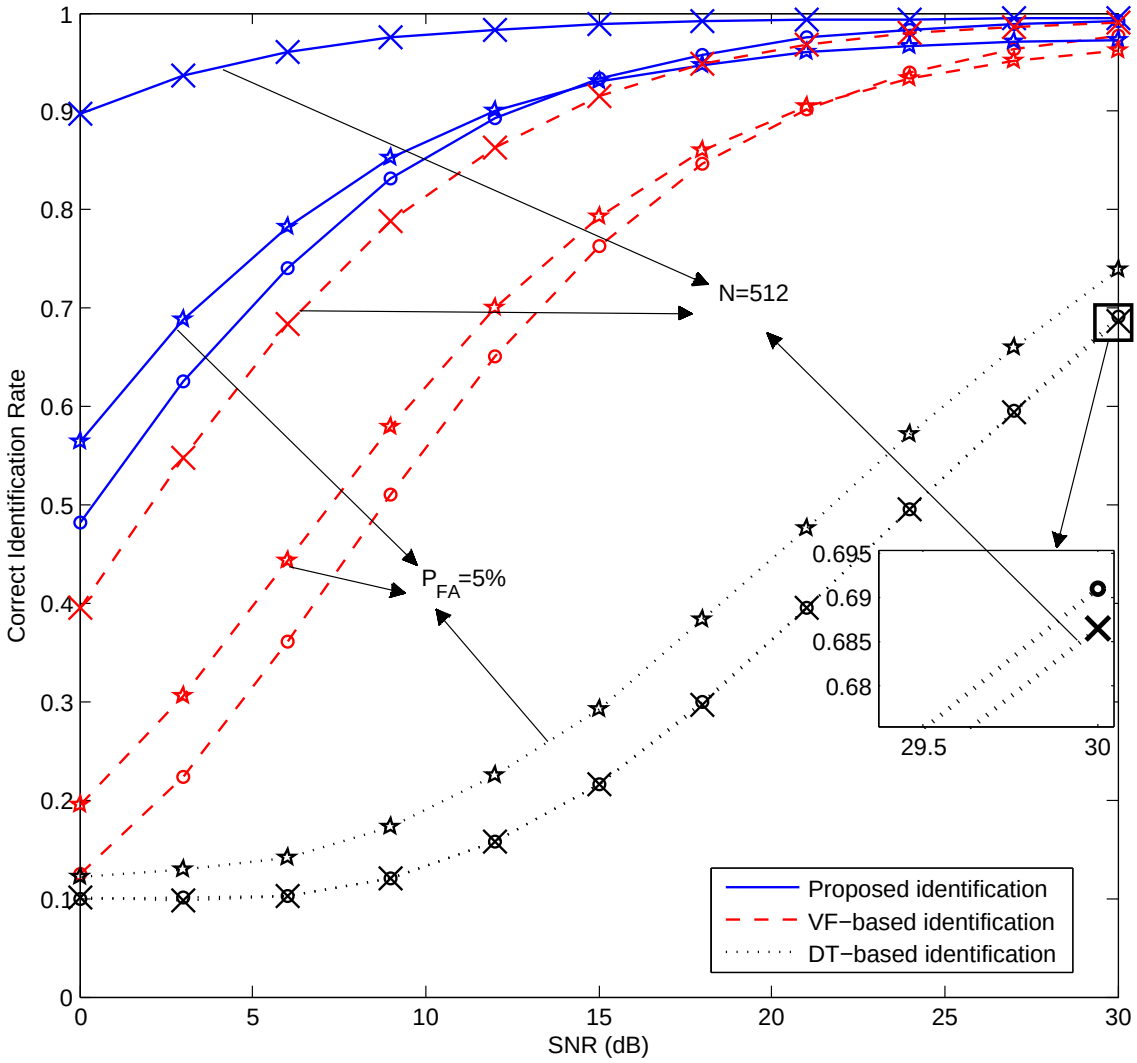


Figure 4.9: Identification performance comparisons between proposed methods and VF, DT based methods. The cross marker denotes $N = 512, P_{\text{FA}} = 1\%$, star marker denotes $N = 32, P_{\text{FA}} = 5\%$, circle marker denotes $N = 32, P_{\text{FA}} = 1\%$.

# Chapter 5

# Enhanced Device Fingerprinting using Multiple Physical-Layer Characteristics

Device fingerprinting directly affects the authentication performance so that its enhancement technique is emerging as one of the useful paradigm for improving physical-layer authentication. This chapter emphasizes on the device fingerprinting enhancement techniques using multiple physical-layer characteristics.

## 5.1 Introduction

Wireless communications devices can be authenticated by verifying their inherent physical-layer characteristics. Specifically, such techniques exploit the specific characteristics of wireless link between the transmitter and receiver or radio-frequency (RF) front-end imperfections of transmitters as device fingerprints [18]. Since these characteristics can automatically distort transmitted signals, which introduce device-dependent impacts to the received signals, the identities of transmitters can be validated by the receiver.

Many authentication schemes are proposed by exploitation of the properties of communication links to detect spoofing transmitters, most of which are typically based on single physical-layer variable/attribute. In [19, 80, 81], physical-layer authentication schemes based on consecutive channel frequency responses (CFRs) are investigated. The channel impulse response (CIR) is analyzed to identify the transmitter in [82]. A continuous physical-layer authentica-

tion based on an adaptive orthogonal frequency division multiplexing (OFDM) is proposed in [36]. In [83], an authentication scheme based on RSSI is investigated. However, this technique requires the cooperation of additional reference nodes as the RSSI values from two transmitters can be close even if they are located in different positions.

As a matter of fact, technical challenges still exist in applying the current single-variable authentication techniques. On one hand, the selected physical-layer attributes are not always accessible in particular platforms. In order to obtain the information of expected physical-layer attributes, additional hardware level changes may be required, which significantly reduces the application potential of authentication schemes. On the other hand, it is noteworthy that due to the interference, noise and time variation inherited to wireless communications, physical-layer attributes used for authentication typically fluctuates in a dynamic range, which further leads to the low reliability of single-variable authentication. Therefore, it is valuable to consider more robust device fingerprint consisted of more than one unique physical-layer characteristics. This is chapter focuses on such device fingerprinting enhancement technique using multiple physical-layer characteristics. A received signal strength indicator (RSSI) and packet error rate (PER) dependent device fingerprint is first investigated to specifically authenticate IEEE 802.11 WiFi devices. Then, a more general multi-dimensional device fingerprinting scheme is studied.

To be specific, an easily implementable authentication technique is presented to improve the spoofing detection performance by using the PER and RSSI. Both of them are readily available in most of IEEE 802.11 platforms. RSSI can be obtained by simply converting the specific received power reading at the IEEE 802.11 platform. On the other hand, PER is a statistical quantity which can be obtained by analyzing the received packets. There are many remarkable advantages by employing the two attributes together. Firstly, our proposed scheme can be simply realized at the receiver without requiring additional equipments which raises its application potential. Secondly, the fingerprinting reliability is enhanced as it is nearly impossible for the adversary to simultaneously emulate two environment as well as user-dependent attributes.

Since the channel-based authentication suffers from poor signal quality and channel variation in mobile and outdoor scenarios [4], the stable RF front-end imperfections have been considered in some authentication researches. In [27] and [43], the authors propose to differen-

tiate different transceivers based on in-phase/quadrature (I/Q) imbalance and carrier frequency offset. However, completely relying on only one characteristic is not always reliable since the selected characteristic may not have enough dynamic range for accurate differentiation. To mitigate this problem, it is straightforward to consider more than one characteristics in order to verify the claimed device identity in multiple aspects. In [23], several radiometric signatures including frequency error, I/Q offset, magnitude error and phase error are reviewed. In [4], the imperfect input/output characteristics of digital-to-analog converter and power amplifier are studied for identifying wireless users. However, it is critical to investigate the effective utilization of multiple device-specific characteristics for optimizing the authentication performance. We are thereby motivated to provide a general approach of utilizing multiple device-specific characteristics to enhance the performance of wireless device authentication. To be more specific, a weighted combination of a number of $N$ characteristics is considered and the likelihood ratio test is applied to process this combined device fingerprint. The optimal weight of each selected characteristic is also determined for maximizing the detection probability.

The rest of this chapter is organized as follows. In Section 5.2, the RSSI and PER based authentication is presented in terms of authentication model, hypothesis decision rule, experimental setup as well as the simulation results. Section 5.3 concentrates on introducing the general authentication method using multiple device-specific characteristics. To be specific, the observation model of multi-characteristics at the receiver is first presented. Then, the authentication method and corresponding optimal weights are described. The numerical results are also given to validate the proposed authentication system. Finally, this chapter is concluded in Section 5.4.

## 5.2 An Enhanced Device Fingerprinting using PER and RSSI

### 5.2.1 Authentication Model

To elaborate the attack challenges that can be addressed by this authentication model, Alice, Bob and Eve are introduced as three different entities according to the conventional terminologies in communication security related studies. Herein, Alice, Bob and Eve are three individual

wireless nodes to construct a communication system. More specifically, the legitimate transmitter (Alice) is able to send packets to the intended receiver (Bob), while the adversary (Eve) attempts to impersonate Alice to communicate with Bob. In order to spoof Bob, Eve tries her best to impersonate Alice by mimicking the one of Alice's attributes which can be used in the common single-variable-based authentication technique.

Herein, it is assumed that this communication system is utilizing the RSSI-based authentication technique to identify transmitters. The RSSI from one wireless node is defined as [84]

$$P_{(d)}[dBm] = P_{(d_0)}[dBm] - 10\alpha \log_{10}(\frac{d}{d_0}) + S, \tag{5.1}$$

where $d$ is the distance between the wireless node and receiver, $P_{(d_0)}$ represents the transmission power of a reference node at the reference distance $d_0$, $\alpha$ is path loss exponent, and $S$ is the zero-mean Gaussian noise. Therefore, Eve is able to manipulate its transmission power and position to make her RSSI pattern close to Alice's. Consequently, Eve can stand a good chance of being undetected. Therefore, it is significant to consider the second attribute, such as PER in this study, to enhance Bob's capability in detecting illegitimate transmitters. The PER is defined as

$$PER = \frac{N_{RXErrors}}{N_{RXCorrect} + N_{RXErrors}}, \tag{5.2}$$

where $N_{RXErrors}$ is the number of received error packets and $N_{RXCorrect}$ is the number of received correct packets.

In fact, PER and RSSI are reflections of the current communication quality, and show natural randomicity. However, they are only partly related to each other as the PER and RSSI are determined by different factors according to (5.1) and (5.2), and also related to some uncontrollable channel-based factors such as the effect of multi-path. Additionally, they are not acquired at the same time scale, which also reduces their correlation. In this case, the adversary is not able to simply mimic PER and RSSI separately, as the procedure of mimicking one attribute also leads to some unexpected variations of the other one. Hence, it is nearly impossible to

imitate two highly random transmission attributes at the same time in order to spoof Bob.

In our proposed scheme, Bob is capable of differentiating either the received packets from Alice or Eve. In particular, when the packets from Alice arriving at Bob, they are first analyzed to obtain the unique valid PER and RSSI pattern profiles. Then the valid PER and RSSI profiles are recorded by Bob for further comparisons. Herein, it is assumed that PER and RSSI are interfered by different white Gaussian noises to properly reflect the impacts of interferences to the communication system. Indeed, the determination of a Gaussian probability density function (PDF) requires the accurate estimate of corresponding mean and variance. Therefore, in order to obtain the valid PER and RSSI pattern profiles from Alice, the mean values ($\mathbf{A}$) and variances ($\sigma^{\mathbf{2}}$) of PER and RSSI are estimated at Bob by analyzing the packets transmitted by Alice. Particularly, it is defined that $\mathbf{A} = [A_0 \quad A_1]^T$, where $A_0$ and $A_1$ respectively represent the mean values of PER and RSSI from Alice; while $\sigma^{\mathbf{2}} = [\sigma_0^2 \quad \sigma_1^2]^T$, where $\sigma_0^2$ and $\sigma_1^2$ respectively represent the variances of PER and RSSI from Alice. In our scheme, $\mathbf{A}$ and $\sigma^{\mathbf{2}}$ are recorded by Bob as the valid profiles of transmission attributes. After that, Bob constantly samples $N$ PER and RSSI profiles from the received packets. In addition, $\mathbf{A'} = [A'_0 \quad A'_1]^T$ is defined to represent the mean values of PER and RSSI from the current sampled $N$ packets and $\sigma'^{\mathbf{2}} = [\sigma'^2_0 \quad \sigma'^2_1]^T$ is defined to represent the variances of PER and RSSI from the current sampled $N$ packets. Bob can compare this new attributes profiles with the recorded ones to see whether they can match up. To be specific, if the current sampled $N$ packets are transmitted by Eve, the $\mathbf{A}$ and $\mathbf{A'}$ cannot be exactly the same, which produces $\mathbf{\Delta A} = \mathbf{A} - \mathbf{A'} = [\Delta A_0 \quad \Delta A_1]^T$. $\mathbf{\Delta A}$, reflecting the discrepancy of Alice and Eve in terms of PER and RSSI, is used to detect the illegitimate transmitter.

### 5.2.2 Hypothesis Testing and Decision Rule

The binary hypothesis testing model has been commonly used in various single-variable based authentications. Given that this study simultaneously utilizes two distinct attributes, the conventional single-variable hypothesis testing model is extended to two-variable format. The two variables are defined to specifically represent PER and RSSI in this new two-variable hypothesis testing model. The two-variable mean-shifted hypothesis testing model can be defined as

follows:

$$\begin{cases} \mathcal{H}_0: & \mathbf{X} = \mathbf{W} \\ \mathcal{H}_1: & \mathbf{X} = \Delta\mathbf{A} + \mathbf{W}' \end{cases}, \tag{5.3}$$

where $\mathcal{H}_0$ represents the received packets are from legitimate Alice; $\mathcal{H}_1$ means the received packets are transmitted by illegitimate Eve; $\mathbf{X} = \hat{\mathbf{X}} - \mathbf{A} = \begin{bmatrix} x_{[0][0]} & \cdots & x_{[0][N-1]} \\ x_{[1][0]} & \cdots & x_{[1][N-1]} \end{bmatrix}$, where $\hat{\mathbf{X}} = \begin{bmatrix} \hat{x}_{[0][0]} & \cdots & \hat{x}_{[0][N-1]} \\ \hat{x}_{[1][0]} & \cdots & \hat{x}_{[1][N-1]} \end{bmatrix}$ represents the samples, the first and second row of $\mathbf{X}$ represent the $N$ mean-shifted samplings of PER and RSSI, respectively; $\mathbf{W} = \begin{bmatrix} w_{[0][0]} & \cdots & w_{[0][N-1]} \\ w_{[1][0]} & \cdots & w_{[1][N-1]} \end{bmatrix}$ and $\mathbf{W}' = \begin{bmatrix} w'_{[0][0]} & \cdots & w'_{[0][N-1]} \\ w'_{[1][0]} & \cdots & w'_{[1][N-1]} \end{bmatrix}$ are two white Gaussian noises with zero mean values and variances $\sigma^2$ and $\sigma'^2$, respectively.

In this hypothesis testing model, the offset $\Delta\mathbf{A} = \mathbf{0}$ in $\mathcal{H}_0$, while $\Delta\mathbf{A} \neq \mathbf{0}$ under $\mathcal{H}_1$ as the attributes profiles from Alice and Eve are not the same. However, in practice the authentication attributes are inevitably affected by noises and in turn they are fluctuating in a certain range, which leads to the received attributes profiles cannot exactly match up the valid attributes profiles even the received packets are actually come from the legitimate transmitter. Generally, a threshold is introduced to solve this problem when using hypothesis testing. Precisely, if $|\Delta\mathbf{A}|$ is less than a pre-determined threshold, $\mathcal{H}_0$ is accepted; otherwise, $\mathcal{H}_1$ is decided.

The generalized likelihood ratio test (GLRT) is employed to fulfill the authentication. To be specific, under $\mathcal{H}_0$, the joint PDF for PER or RSSI can be defined as

$$p_m(\mathbf{X}; \mathcal{H}_0) = \frac{\exp\left[-\frac{1}{2\sigma_m^2}\sum_{i=0}^{N-1} x_{[m][i]}^2\right]}{(2\pi\sigma_m^2)^{\frac{N}{2}}}, \tag{5.4}$$

where $m = 0$ or 1 indicates the PER or RSSI. Similarly, under $\mathcal{H}_1$, the joint PDF for the $m$th

variable is

$$p_m(\mathbf{X};\mathbf{\Theta}_1,\mathcal{H}_1)=\frac{\exp\left[-\frac{1}{2\sigma'^2_m}\sum_{i=0}^{N-1}(x_{[m][i]}-\Delta A_m)^2\right]}{(2\pi\sigma'^2_m)^{\frac{N}{2}}}, \tag{5.5}$$

where $\mathbf{\Theta_1}=\begin{bmatrix}\Delta A_m & \sigma'^2_m\end{bmatrix}$ under $\mathcal{H}_1$.

Generally, $\mathcal{H}_1$ can be decided if

$$L_{m(x)}=\frac{p_m(\mathbf{X};\hat{\mathbf{\Theta}}_1,\mathcal{H}_1)}{p_m(\mathbf{X};\mathcal{H}_0)}>\gamma, \tag{5.6}$$

where $\gamma$ is a threshold and its value is able to influence whether to accept $\mathcal{H}_0$ or accept $\mathcal{H}_1$. $\hat{\mathbf{\Theta}}_1=\begin{bmatrix}\Delta\hat{A}_m & \hat{\sigma}'^2_m\end{bmatrix}$ is the estimation of $\mathbf{\Theta_1}$. In practice, after sampling $N$ packets the receiver is able to calculate the mean and variance of PER/RSSI. $\hat{\sigma}'^2_m$ is set to equal to this variance. Regarding the $\Delta\hat{A}_m$, it can be obtained by subtracting $\mathbf{A}$ from this mean.

The decision rule based on hypothesis testing is provided to accomplish the two-variable authentication. At first, each variable (PER and RSSI) separately identifies the transmitter based on the hypothesis testing in deciding whether to claim the transmitter as legitimate or not. Subsequently, the decisions are combined for consideration in determining the final assessment. The decision procedure can be summarized for each variable as follows.

According to (5.4), (5.5), and (5.6), the specific GLRT for the PER or RSSI can be executed as

$$\frac{\frac{1}{(2\pi\hat{\sigma}'^2_m)^{\frac{N}{2}}}\exp\left[-\frac{1}{2\hat{\sigma}'^2_m}\sum_{i=0}^{N-1}(x_{[m][i]}-\Delta\hat{A}_m)^2\right]}{\frac{1}{(2\pi\hat{\sigma}^2_m)^{\frac{N}{2}}}\exp\left[-\frac{1}{2\hat{\sigma}^2_m}\sum_{i=0}^{N-1}x^2_{[m][i]}\right]}>\gamma, \tag{5.7}$$

where $m$ =0 or 1 represents PER or RSSI. Substituting $\hat{\sigma}^2_m=\frac{1}{N}\sum_{i=0}^{N-1}x^2_{[m][i]}$ and $\hat{\sigma}'^2_m=\frac{1}{N}\sum_{i=0}^{N-1}(x_{[m][i]}-\Delta\hat{A}_m)^2$ and taking the logarithms to produce

$$\Delta\hat{A}^2_m>\hat{\sigma}'^2_m(\gamma^{\frac{2}{N}}-1). \tag{5.8}$$

As a result, the threshold can be set as

$$T_{[m]} = \hat{\sigma'}_m \sqrt{|\gamma^{\frac{2}{N}} - 1|}, \tag{5.9}$$

where $T_{[m]}, m = 0, 1$ is the threshold for PER or RSSI. Specifically, the authentication of each variable is executed by comparing $|\Delta\hat{A}_m|$ with $T_{[m]}$. If $|\Delta\hat{A}_m| < T_{[m]}$, this variable (PER or RSSI) claims Alice as the legitimate transmitter; otherwise, this variable claims Eve.

Thus, the false alarm probability $P_{fa[m]}, m = 0, 1$ for PER or RSSI can be calculated based on the corresponding threshold $T_{[m]}$ as

$$\begin{aligned} P_{fa[m]} &= P(|\Delta\hat{A}_m| > T_{[m]}; \mathcal{H}_0) \\ &= P(\Delta\hat{A}_m > T_{[m]}; \mathcal{H}_0) + P(\Delta\hat{A}_m < -T_{[m]}; \mathcal{H}_0). \end{aligned} \tag{5.10}$$

Given that $\Delta\hat{A}_m \sim \mathcal{N}(0, \sigma_m^2/N)$ under $\mathcal{H}_0$, the equation (5.10) can be simply expressed by the $Q$-function to produce

$$P_{fa[m]} = 2\,Q\left(\frac{T_{[m]}\sqrt{N}}{\hat{\sigma}_m}\right), \tag{5.11}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$. Therefore, the threshold $T_{[m]}$ can be determined from $P_{fa[m]}$ by

$$T_{[m]} = \frac{\hat{\sigma}_m}{\sqrt{N}} Q^{-1}\left(\frac{P_{fa[m]}}{2}\right), \tag{5.12}$$

where $Q^{-1}(x)$ is the inverse of $Q$-function. Furthermore, (5.12) implies that the threshold $T_{[m]}$ can be artificially adjusted by changing the value of $P_{fa[m]}$ when $\hat{\sigma}_m$ and $N$ is pre-determined. Considering that $\Delta\hat{A}_m \sim \mathcal{N}(\Delta A_m, \sigma'^2_m/N)$ under $\mathcal{H}_1$, the probability of detection $P_{d[m]}, m = 0, 1$

for PER or RSSI is

$$\begin{aligned} P_{d[m]} &= P(|\Delta\hat{A}_m| > T_{[m]}; \mathcal{H}_1) \\ &= Q\left(\frac{T_{[m]} - \Delta\hat{A}_m}{\sqrt{\hat{\sigma'}_m^2/N}}\right) + Q\left(\frac{T_{[m]} + \Delta\hat{A}_m}{\sqrt{\hat{\sigma'}_m^2/N}}\right) \\ &= Q\left(\frac{\hat{\sigma}_m}{\hat{\sigma'}_m} Q^{-1}\left(\frac{P_{fa[m]}}{2}\right) - \sqrt{\frac{N\Delta\hat{A}_m^2}{\hat{\sigma'}_m^2}}\right) \\ &+ Q\left(\frac{\hat{\sigma}_m}{\hat{\sigma'}_m} Q^{-1}\left(\frac{P_{fa[m]}}{2}\right) + \sqrt{\frac{N\Delta\hat{A}_m^2}{\hat{\sigma'}_m^2}}\right). \end{aligned} \tag{5.13}$$

Consequently, the corresponding probability of miss detection $P_{m[m]}, m = 0, 1$ under $\mathcal{H}_1$ can be written as

$$P_{m[m]} = 1 - P_{d[m]}. \tag{5.14}$$

Presently, the hypothesis testing theory is completed for each variable.

In the decision rule, the final decision is based on the majority variables' decision. Given that the two variables may claim different transmitters, the final decision rule should take this case into consideration. Precisely, if one variable claims Alice while the other one claims Eve, we consider that the received packets are actually transmitted by Eve. In this way, the performance in detecting spoofing attacks can be enhanced since it is extremely hard to deceive Bob in terms of both PER and RSSI. The probability of detection $P_d$ can be expressed as

$$P_d = P_{d[0]}P_{d[1]} + (1 - P_{d[0]})P_{d[1]} + P_{d[0]}(1 - P_{d[1]}), \tag{5.15}$$

where $P_{d[0]}$ and $P_{d[1]}$ are probability of detection of PER and RSSI, respectively.

### 5.2.3 Experiment and Simulation Results

#### Experiment

Fig. 5.1 shows the IEEE 802.11g experimental setup. Three wireless nodes are located

spatially in different positions in Room 338 of Thompson Engineering Building of the University of Western Ontario to set up the "Alice-Bob-Eve" communication system. All of the three wireless devices are the same product model. In this communication system, Bob serves as a receiver; while Alice and Eve serve as legitimate and illegitimate transmitters, respectively. Additionally, a network analyzer is connected to Bob to expediently display the real-time statistical results of the PER and RSSI. In this simple network, the distance ($D_1$) between Alice and Bob is 6 meters, and data rate is 18 Mbit/s. In addition, the sample interval for Bob is 1 second and the number of measured samples is 839.

To identify different transmitters, the first step is to measure the valid attributes profiles of Alice, and store these attributes' profiles in Bob. For the RSSI, the attribute profiles (mean and variance) are calculated based on the samples at Bob. For the PER, we first calculate the PER during every sample interval to get 839 statistics. After that, the mean and variance can be computed based on these statistics.

In order to thoroughly test the performance of our scheme in its ability in detecting an attacker, the device settings of Eve are set as identical as possible with Alice which enables Eve to better imitate the PER and RSSI of Alice. Precisely, the TX power of Eve is set to be the same with Alice. Eve is close to the position of Alice, and the distance ($D_2$) between Eve and Bob is set to be 6 meters as well. After that, the similar experiment is done to obtain 836 samples and calculated the invalid PER and RSSI profiles from Eve.

**Simulation**

Three basic aspects are mainly concerned in assessing the proposed authentication performances: the probability of detection $P_d$, the probability of false alarm $P_{fa}$ and the sample number $N$. Among them, $P_d$ implies the capability of detecting the adversary; $P_{fa}$ is a criterion to evaluate the authentication in aspect of making an incorrect final decision; $N$ is directly related to the processing time and accuracy of authentication. It is noteworthy that all of the data used in the simulations are derived from the experiment mentioned above.

In Fig. 5.2, the simulation curves perfectly match the expected theoretical curves in the proposed decision rule, which validates our derivations.

In Fig. 5.3, in order to show the enhancement of our proposed authentication scheme, the $P_d$ of PER, RSSI and two different decision rules are compared. Specifically, rule #1 is the

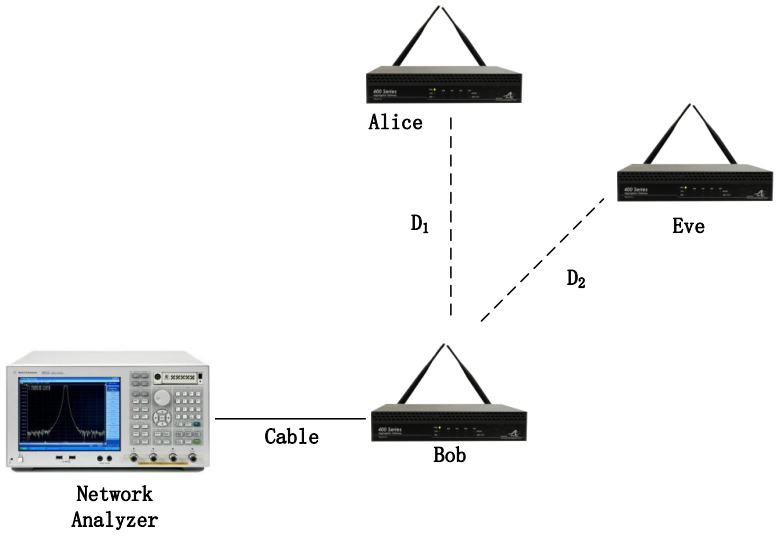


Figure 5.1: The experimental setup using IEEE 802.11g Atheros platform.

decision rule as mentioned in the previous section. It claims Eve when the two variables claim different transmitters; while rule #2 considers the received packets are from Alice in this case. To simplify the analysis, the $P_{fa}$ of PER and the $P_{fa}$ of RSSI are set to be the same, linearly ranging from 0.01 to 0.3. As shown in the figure, with the increasing of $P_{fa}$, all of the curves show the expected ascendant trend, which implies a higher tolerance of the false alarm will bring a better performance in detecting attacks. Additionally, it is clear that the $P_d$ of rule #1 is extremely higher than the $P_d$ of single-variable. However, rule #2 does not show an acceptable performance in detecting attacks since its effective miss detection is higher.

$N$ is another factor that significantly impacts the authentication performance. Generally, on one hand, a large number of samplings will positively improve the accuracy of the authentication results. On the other hand, excessive samplings will result in the procedure of processing data to be time-consuming which will significantly reduce its utility value. In Fig. 5.4, the curves of the proposed decision rule #1 for $P_d$ vs $P_{fa}$ with $N = 50, 100, 150$ are provided separately. Hence, the appropriate $N$ should be selected carefully by considering the tradeoffs.

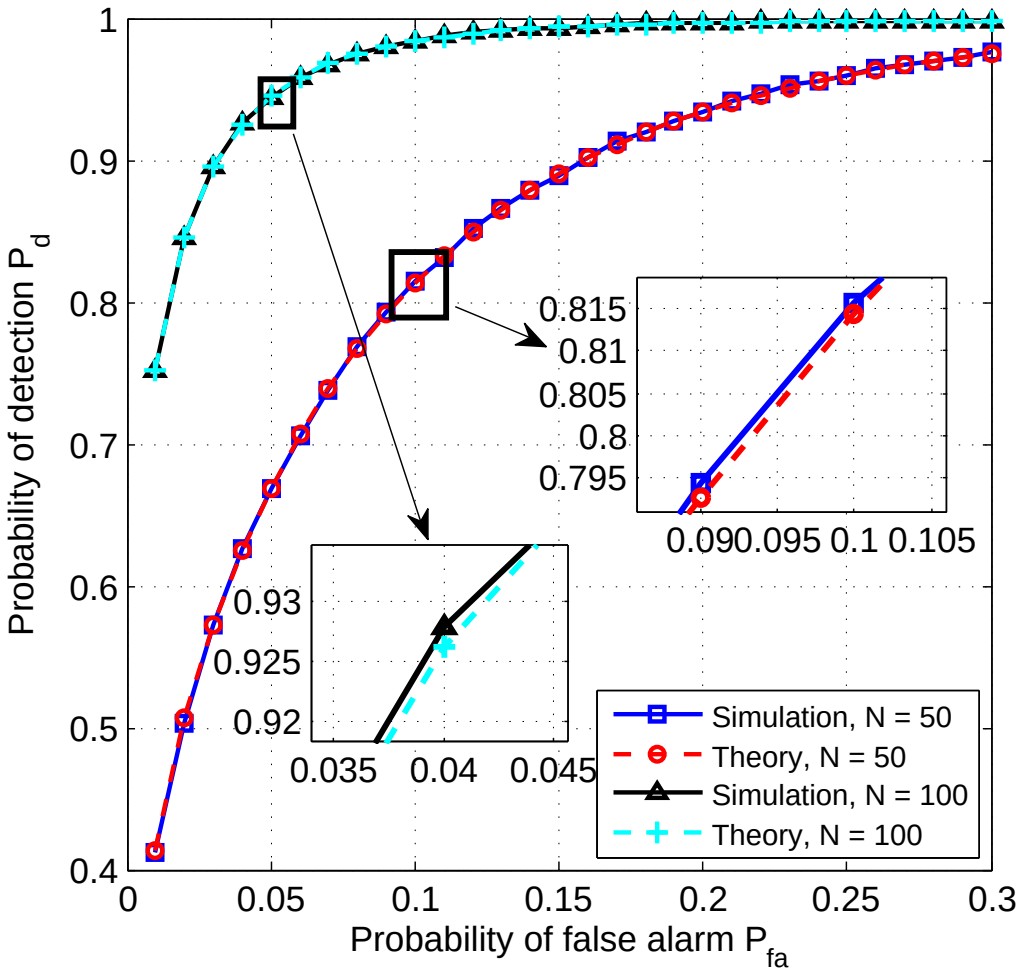


Figure 5.2: Simulation results vs. theoretical results under $N = 50$ and 100, respectively.

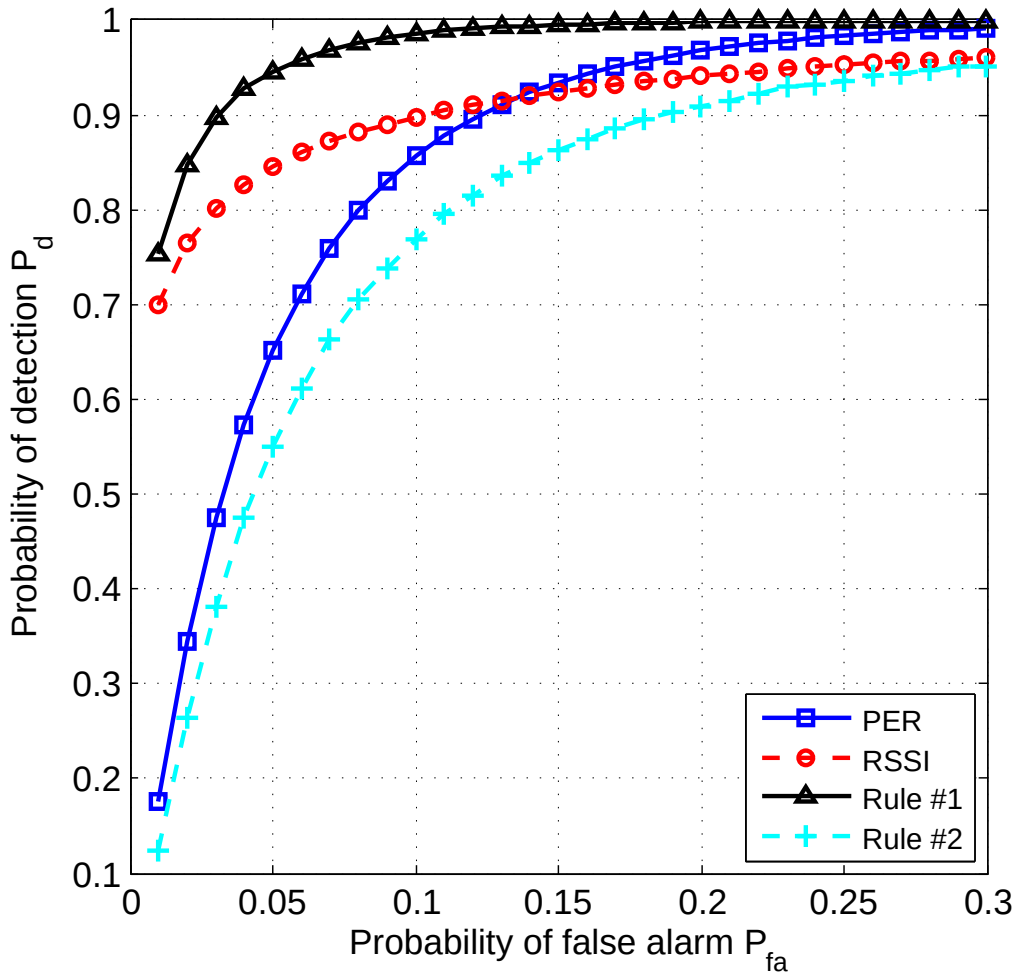


Figure 5.3: Probability of detection vs. probability of false alarm under $N = 100$.

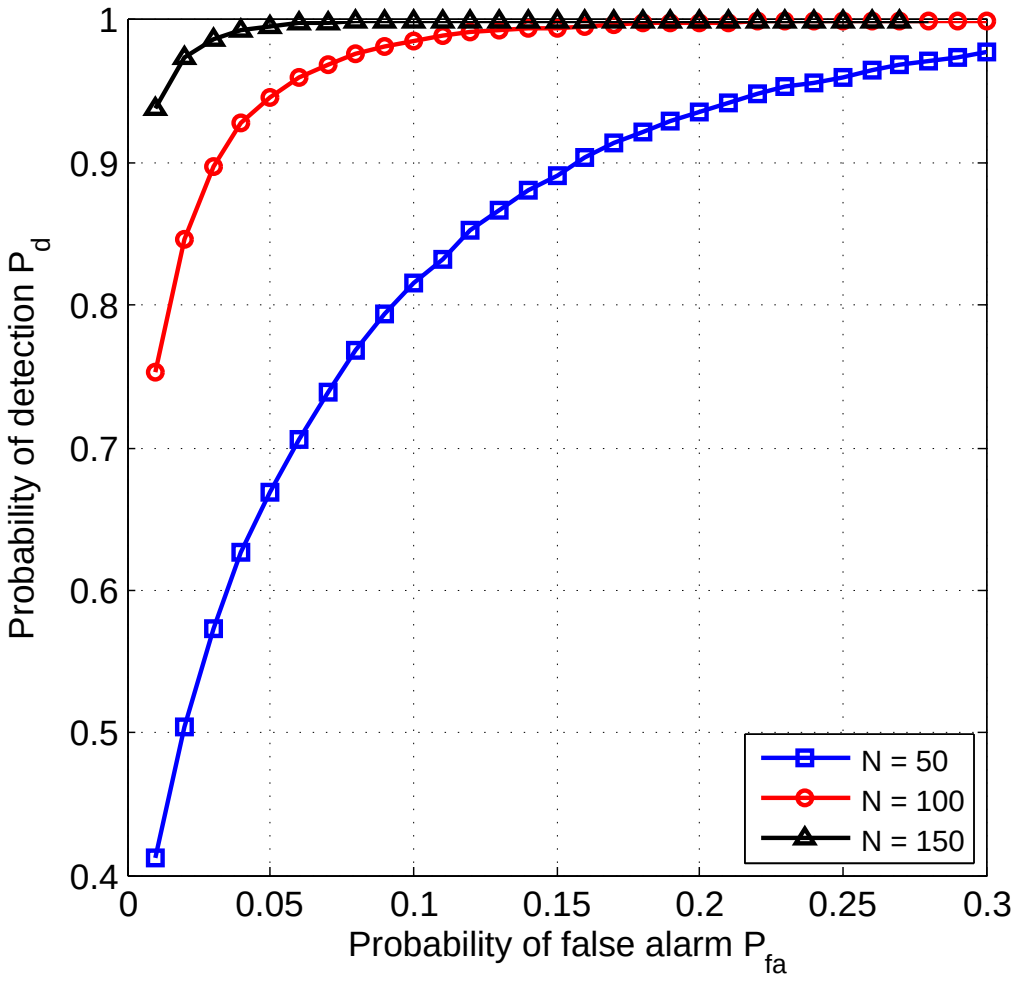


Figure 5.4: Probability of detection using different number of samplings.

## 5.3 A General Device Fingerprinting using Multiple Weighted Device-Specific Characteristics

In this section, a general authentication method using multiple device-specific characteristics is presented. The contents of this section is partially based on [85].

*Notations*: Bold uppercase and lowercase letters denote matrix and vector, respectively. For matrix $\mathbf{A}$, we use $\mathbf{a}_n$ to denote its $n$th row and $a_{ij}$ to denote its element of the $i$th row and $j$th column.

### 5.3.1 Weighted Multi-Characteristics Device Authentication

The model of multiple device-specific characteristics is first presented. Similar to [86], in which two channel-based attributes are modeled, we here assume $N$ device-specific characteristics (i.e., time-invariant RF front-end imperfections) and each characteristic has $M$ observations at the receiver. The corresponding $N \times M$ matrix representation of observed characteristics can be defined as

$$\begin{aligned}\mathbf{Y} &= \mathbf{X}_r + \mathbf{W} \\ &= \begin{bmatrix} x_{r_1} & x_{r_1} & \cdots & x_{r_1} \\ x_{r_2} & x_{r_2} & \cdots & x_{r_2} \\ \vdots & & \ddots & \vdots \\ x_{r_N} & x_{r_N} & \cdots & x_{r_N} \end{bmatrix} + \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1M} \\ w_{21} & w_{22} & \cdots & w_{2M} \\ \vdots & & \ddots & \vdots \\ w_{N1} & w_{N2} & \cdots & w_{NM} \end{bmatrix},\end{aligned} \tag{5.16}$$

where $\mathbf{X}_r$ and $\mathbf{W}$ denote the actual values of time-invariant characteristics and additive white Gaussian noises (AWGN) with known variances. In this case, the $n$th row of $\mathbf{Y}$ denote a number of $M$ noisy estimates of the $n$th attribute, which follows the distribution as $\mathbf{y}_n \sim N(x_{r_n}, \sigma_n^2)$.

After obtaining $\mathbf{Y}$, the receiver is able to compare it with the validated characteristics $\mathbf{X}_v$ to produce the offset as

$$\Delta\mathbf{X} = \mathbf{X}_r - \mathbf{X}_v + \mathbf{W}, \tag{5.17}$$
$$= \begin{bmatrix} x_1 & x_1 & \cdots & x_1 \\ x_2 & x_2 & \cdots & x_2 \\ \vdots & & \ddots & \vdots \\ x_N & x_N & \cdots & x_N \end{bmatrix} + \mathbf{W},$$

where

$$\mathbf{X}_v = \begin{bmatrix} x_{v_1} & x_{v_1} & \cdots & x_{v_1} \\ x_{v_2} & x_{v_2} & \cdots & x_{v_2} \\ \vdots & & \ddots & \vdots \\ x_{v_N} & x_{v_N} & \cdots & x_{v_N} \end{bmatrix} \tag{5.18}$$

Different weights are assigned to each characteristic and use the hypothesis testing based detection theory to identify different wireless devices.

The mean of the $n$th attribute offset in (5.17) can be calculated as $m_n = \frac{1}{M}\sum_{i=1}^{M}\Delta x_{ni}$. Then, $m_n$ is divided by $\frac{\sigma_n}{\sqrt{M}}$ producing

$$A_n = \frac{\sqrt{M}m_n}{\sigma_n} \sim N(\frac{x_n\sqrt{M}}{\sigma_n}, 1). \tag{5.19}$$

The weighted sum of the $N$ selected attributes in (5.19) can be expressed as

$$S = \sum_{i=1}^{N} w_i A_i \sim N(\sqrt{M}\sum_{i=1}^{N}\frac{w_i x_i}{\sigma_i}, \sum_{i=1}^{N} w_i^2). \tag{5.20}$$

The weights $w_i$ are assumed to be adjustable real constants satisfying $w_i x_i > 0$.

As a result, a binary hypothesis testing can be utilized to analyze $S$ as

$$\begin{cases} \mathcal{H}_0: & x_i = 0 \\ \mathcal{H}_1: & x_i \neq 0 \end{cases}, \tag{5.21}$$

where the hypothesis $\mathcal{H}_0$ denotes that the current device has the same characteristics with the validated device so that $x_i = 0$; otherwise, $\mathcal{H}_1$ is decided to claim a different transmitter.

A logarithm of likelihood ratio test (LRT) can be performed to decide the hypothesis $\mathcal{H}_1$ if the ratio is larger than a threshold $r$, which can be expressed as

$$\begin{aligned} &\ln\left(\frac{p_{\mathcal{H}_1}(S)}{p_{\mathcal{H}_0}(S)}\right) > r \\ &\ln\left(\frac{(\sqrt{2\pi\sum_{i=1}^{N} w_i^2})^{-1}\exp[\frac{-(S-\sqrt{M}B)^2}{2\sum_{i=1}^{N} w_i^2}]}{(\sqrt{2\pi\sum_{i=1}^{N} w_i^2})^{-1}\exp[\frac{-S^2}{2\sum_{i=1}^{N} w_i^2}]}\right) > r \\ &S > \frac{r\sum_{i=1}^{N} w_i^2}{\sqrt{M}B} + \frac{\sqrt{M}B}{2} = T, \end{aligned} \tag{5.22}$$

where $p_{\mathcal{H}_0}(S)$ and $p_{\mathcal{H}_1}(S)$ denote the likelihood functions of $S$ under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. $B = \sum_{i=1}^{N} \frac{w_i x_i}{\sigma_i}$, and $T$ is the threshold for determining whether $S$ belongs to $\mathcal{H}_0$ or $\mathcal{H}_1$. It is noteworthy that the value of $T$ is not available due to that $x_i$ is usually unknown in practice. To overcome this problem, a given false alarm probability is set as usually employed in engineering practice, and this probability is used to calculate the corresponding threshold $T$. In this case, the false alarm rate can be computed as

$$\begin{aligned} P_{\text{FA}} &= P\{S > T|\mathcal{H}_0\} \\ &= \int_{T}^{+\infty} p_{\mathcal{H}_0(S)} dS \\ &= Q\left(\frac{T}{\sqrt{\sum_{i=1}^{N} w_i^2}}\right), \end{aligned} \tag{5.23}$$

where $Q(\cdot)$ is the Q-function and it is defined as

$$Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}u^2} du.$$

By solving (6.48), the threshold $T$ can be obtained as

$$T = \sqrt{\sum_{i=1}^{N} w_i^2} Q^{-1}\left(P_{\mathrm{FA}}\right) > 0, \tag{5.24}$$

where $Q^{-1}(\cdot)$ is the inverse of Q-function. Accordingly, the detection probability can be computed using this $T$ as

$$\begin{aligned} P_{\mathrm{D}} &= P\{S > T|\mathcal{H}_1\} \\ &= \int_T^{+\infty} p_{\mathcal{H}_1(S)} dS \\ &= Q\left(Q^{-1}\left(P_{\mathrm{FA}}\right) - \frac{\sqrt{M}\sum_{i=1}^{N} \frac{w_i x_i}{\sigma_i}}{\sqrt{\sum_{i=1}^{N} w_i^2}}\right). \end{aligned} \tag{5.25}$$

### 5.3.2 Optimal Weights Derivation for Maximizing Detection Probability

This section focuses on the weights design since it is apparent that the weights can directly affect the detection performance as revealed in eq.(5.25).

(5.25) is analyzed to derive the optimal weights to maximize the detection probability. Given that Q-function is monotonically decreasing and $Q^{-1}(P_{\mathrm{FA}})$ is a constant under the given $P_{\mathrm{FA}}$, it is concluded that maximizing $P_{\mathrm{D}}$ is equivalent to finding the maximum value of

$$f(w) = \frac{\sqrt{M}\sum_{i=1}^{N} \frac{w_i x_i}{\sigma_i}}{\sqrt{\sum_{i=1}^{N} w_i^2}}.$$

To achieve this goal, we first find the $w$ values that make the partial derivative of $f(w)$ equal to zero. Then, these values are compared with the boundary values of $w$ to finally find the correct

$w$. Therefore, the partial derivative of $f(w)$ with respect to $w$ is

$$\frac{\partial f(w)}{\partial w_k} = \frac{\sqrt{M}}{\sum_{i=1}^{N} w_i^2}\left(\frac{x_k}{\sigma_k}\sqrt{\sum_{i=1}^{N} w_i^2} - \frac{B w_k}{\sqrt{\sum_{i=1}^{N} w_i^2}}\right) = 0. \tag{5.26}$$

After some arrangements, the results can be obtained as

$$\frac{x_k}{\sigma_k w_k} = \frac{B}{\sum_{i=1}^{N} w_i^2} = C, \tag{5.27}$$

where $C$ is a constant. Based on (5.27), $f(w)$ can be rewritten as

$$f(w) = \sqrt{M \sum_{i=1}^{N} \frac{x_i^2}{\sigma_i^2}}. \tag{5.28}$$

Then, the boundary condition for $f(w)$ can be examined as

$$\lim_{w_k \to \infty} f(w) = \lim_{w_k \to \infty} \frac{\sqrt{M}\sum_{i=1}^{N} \frac{w_i x_i}{\sigma_i}}{\sqrt{\sum_{i=1}^{N} w_i^2}} = \frac{\sqrt{M} x_k}{\sigma_k}. \tag{5.29}$$

The comparison of (5.28) and (5.29) is shown as

$$\begin{aligned} \sqrt{M}\sqrt{\sum_{i=1}^{N} \frac{x_i^2}{\sigma_i^2}} &= \sqrt{M}\sqrt{\frac{x_k^2}{\sigma_k^2} + \sum_{i=1, i\neq k}^{N} \frac{x_i^2}{\sigma_i^2}} \\ &\geq \sqrt{M}\sqrt{\frac{x_k^2}{\sigma_k^2}}. \end{aligned} \tag{5.30}$$

Therefore, the optimal weights can be expressed as

$$w_k = \frac{x_k}{\sigma_k C}. \tag{5.31}$$

Substituting for $w$ from (5.31) in (5.25), the maximal detection probability can be expressed as

$$P_{\mathrm{D}_{MAX}} = Q\left(Q^{-1}(P_{\mathrm{FA}}) - \sqrt{M \cdot SNR}\right), \tag{5.32}$$

where $SNR = \sum_{i=1}^{N} \frac{x_i^2}{\sigma_i^2}$ denotes the summation of signal to noise ratio of each characteristic, where the signals here denote the actual characteristic offsets. However, since the $x_i$ are usually unknown in practice, it is hard to obtain the optimal weights as derived in (5.31).

### 5.3.3 Simulation Results

Three MATLAB simulations are performed to evaluate the performance of our wireless device authentication system. We mainly focus on the values of $P_{\mathrm{D}}$ in different evaluation conditions based on the required $P_{\mathrm{FA}}$.

The derived threshold and detection probability in equation (5.25) are verified. The setups of this simulation are as follows. $N = 3$, the weights are $[2, -2, 2]$. The $N$ estimates of characteristics are represented in a randomly generated vector $[21, 49.5, 72]$ (i.e., any column of $\mathbf{X}_r$) and the validated characteristics are set to be $[20.6, 50, 71.6]$, which implies the delicate actual characteristic offsets are within 2%. The simulation results vs. analytic results of (5.25) and the corresponding threshold of (5.24) are shown in Fig.5.5. It can be seen that the simulation and analytic results can match as expected, which validates the correctness of our derivations. Also, the threshold keeps decreasing with the increase of $P_{\mathrm{FA}}$.

We also evaluate the authentication performance under different values of $N = 1, 3, 5$. In this particular simulation, we set the estimated characteristics and validated characteristics are $[21, 49.5, 72, 50, 60]$ and $[20.6, 50, 71.6, 49.7, 59.7]$, respectively. It is noteworthy that the first $N$ elements can be chosen from these two vectors, where $N$ is set to be $1, 3, 5$. The rest simulation setups are the same with the previous one. The comparison results are shown in Fig.5.6. It can be seen that the detection probabilities of using more than one characteristics (i.e., the red and blue curves) are significantly improved comparing with using single characteristic (i.e., black curve). The $P_{\mathrm{D}}$ of both $N = 3$ and $N = 5$ remain above 90% in this simulation, and continue to rise to almost 100% simultaneously when $P_{\mathrm{FA}}$ reaches 1.58%. Therefore, it can be

predicted that the $P_{\mathrm{D}}$ may not be remarkably increased by solely considering larger $N$ in this case.

In the third simulation, the system with optimal weights is evaluated. The same simulation setups as described in the first simulation are utilized. Regarding the weights, we set the optimal weights as derived in (5.31), which is $w_{\mathrm{opt}\,k} = \frac{x_k}{\sigma_k}, k = 1, 2, \cdots, N$. While, we utilize another set of equal weights as $w_{\mathrm{equ}\,k} = \frac{\sum_{k=1}^{N} |w_{\mathrm{opt}\,k}|}{N}$ and compare its authentication performance with the optimal weights as shown in Fig.5.7. In this figure, it can be observed that the $P_{\mathrm{D}}$ of optimal weights maintains higher than the equal weights with the $P_{\mathrm{FA}}$ varying from $10^{-3}$ to $10^{-1}$. It is noteworthy that different weight settings, e.g., all weights are 1, may lead to different simulation results. However, the optimal must be always higher than any other weight settings. In addition, this optimal weights are difficult to obtain in practice as aforementioned. In fact, the designers can adjust the weight of different characteristic according to the practical application requirements.

## 5.4 Summary

This chapter has two main parts. In the first part, an enhanced device fingerprinting technique using PER and RSSI is proposed. The two-variable authentication method is proven to be practical, as the variables of PER and RSSI are easily accessible at the receiver during the communication processing. More precisely, by comparing the differences between Alice and Eve in terms of PER and RSSI, each variable could draw a conclusion of whether the received packets are from a legitimate transmitter or not. Consequently, the accuracy of the final decision is significantly enhanced by considering PER and RSSI together. The effectiveness of the proposed two-variable authentication is validated by simulation results. All data used in the simulation are derived from IEEE 802.11g Atheros platform. Moreover, the authentication results show a higher capability in detecting the spoofing attacks than the single-variable based authentication schemes. As a matter of fact, the proposed scheme is not only applicable to IEEE 802.11 but also can be employed in many other wireless communication scenarios.

In the second part, the device authentication enhancement technique using multiple characteristics is studied. Through simultaneously considering more than one device-specific charac-

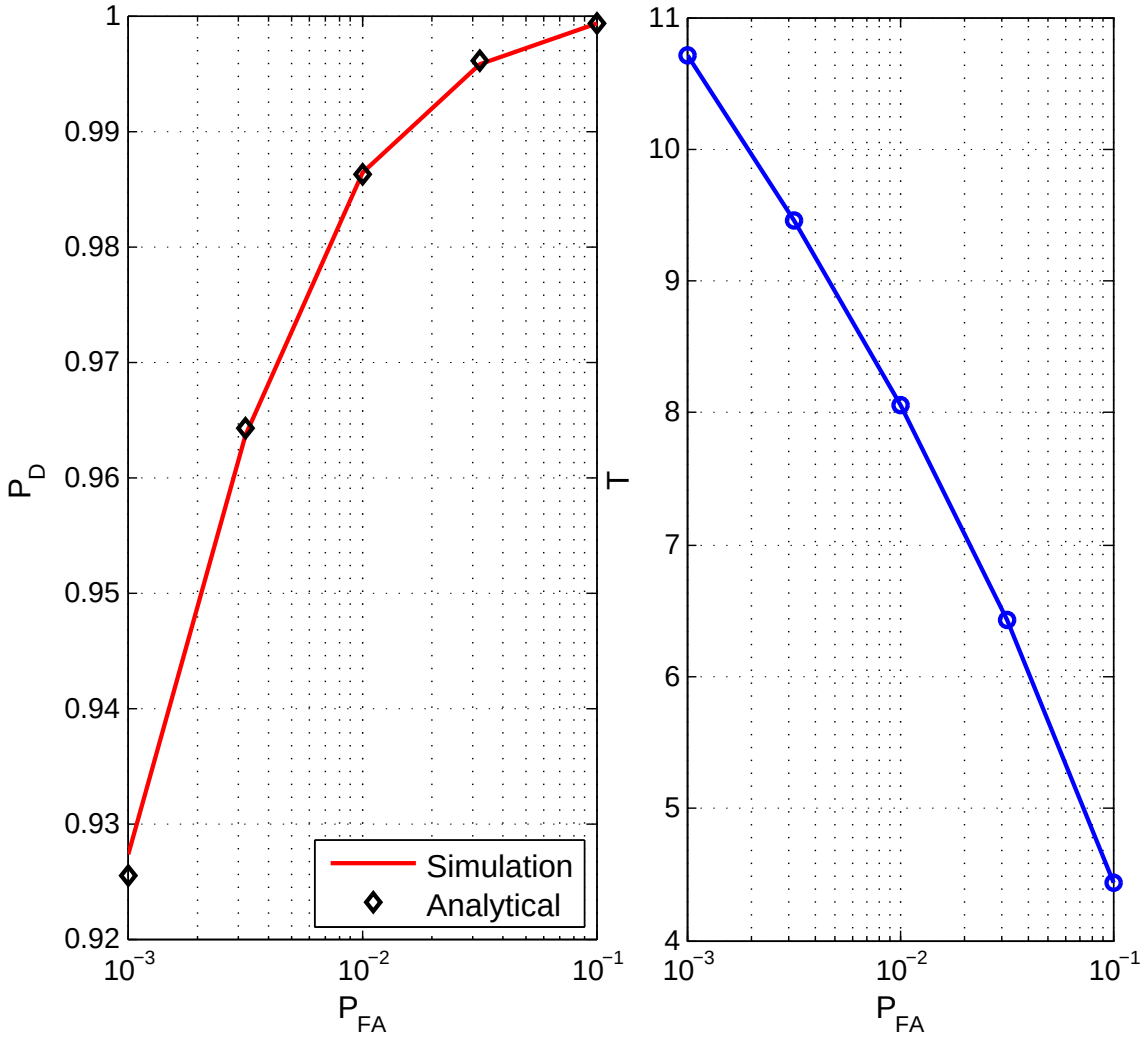


Figure 5.5: Simulation vs. analytic results of $P_{\mathrm{D}}$, and the corresponding threshold.

teristics, a device fingerprint is generated by computing the weighted combination of multiple device dependent characteristics. The LRT is applied to process the new device fingerprint in assisting the wireless device authentication. In addition, the optimal weights are derived for maximizing the detection probability. The numerical results of our authentication system can validate the theoretical derivations and show expected enhancement in terms of the improved detection probability.

The works of this chapter can be partially found in my published papers [85, 86]

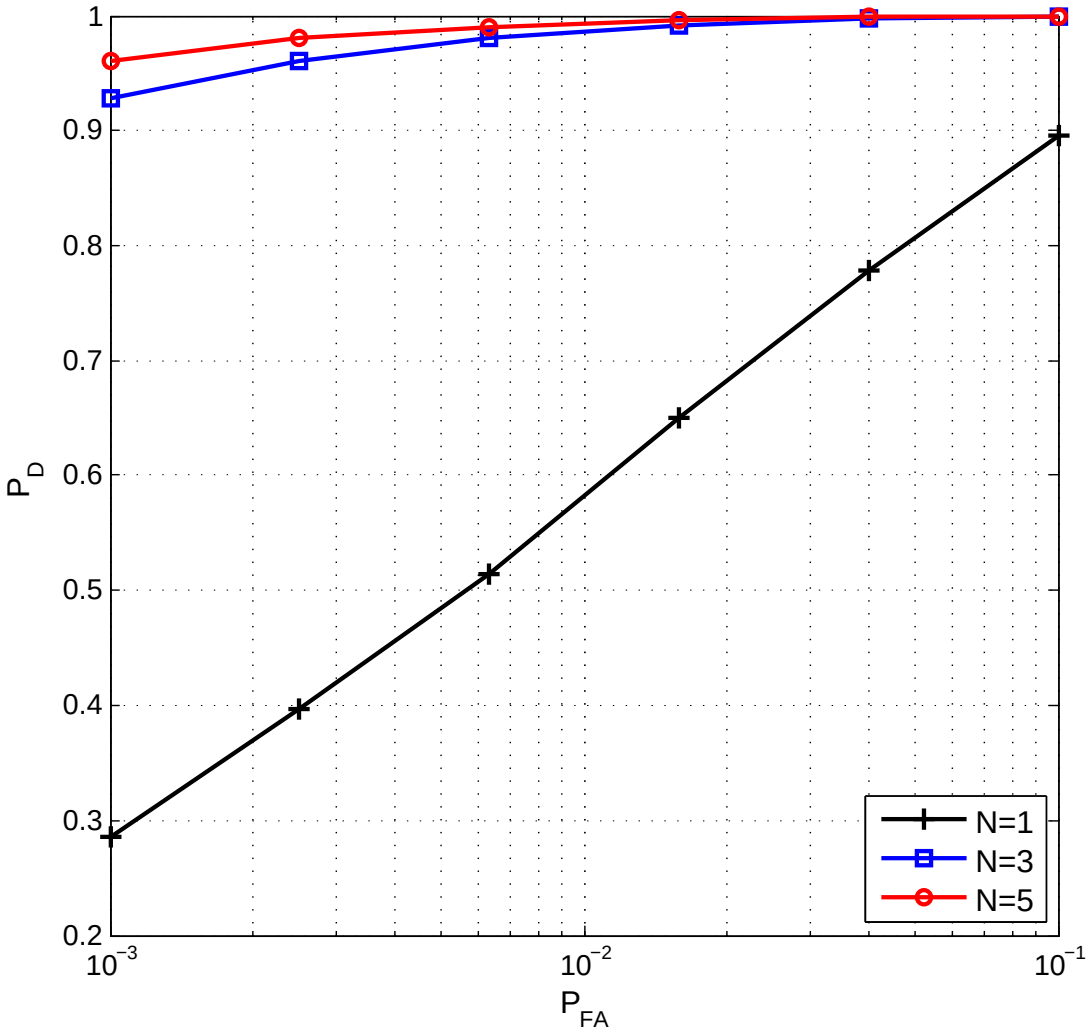


Figure 5.6: Authentication performance with different number of characteristics.

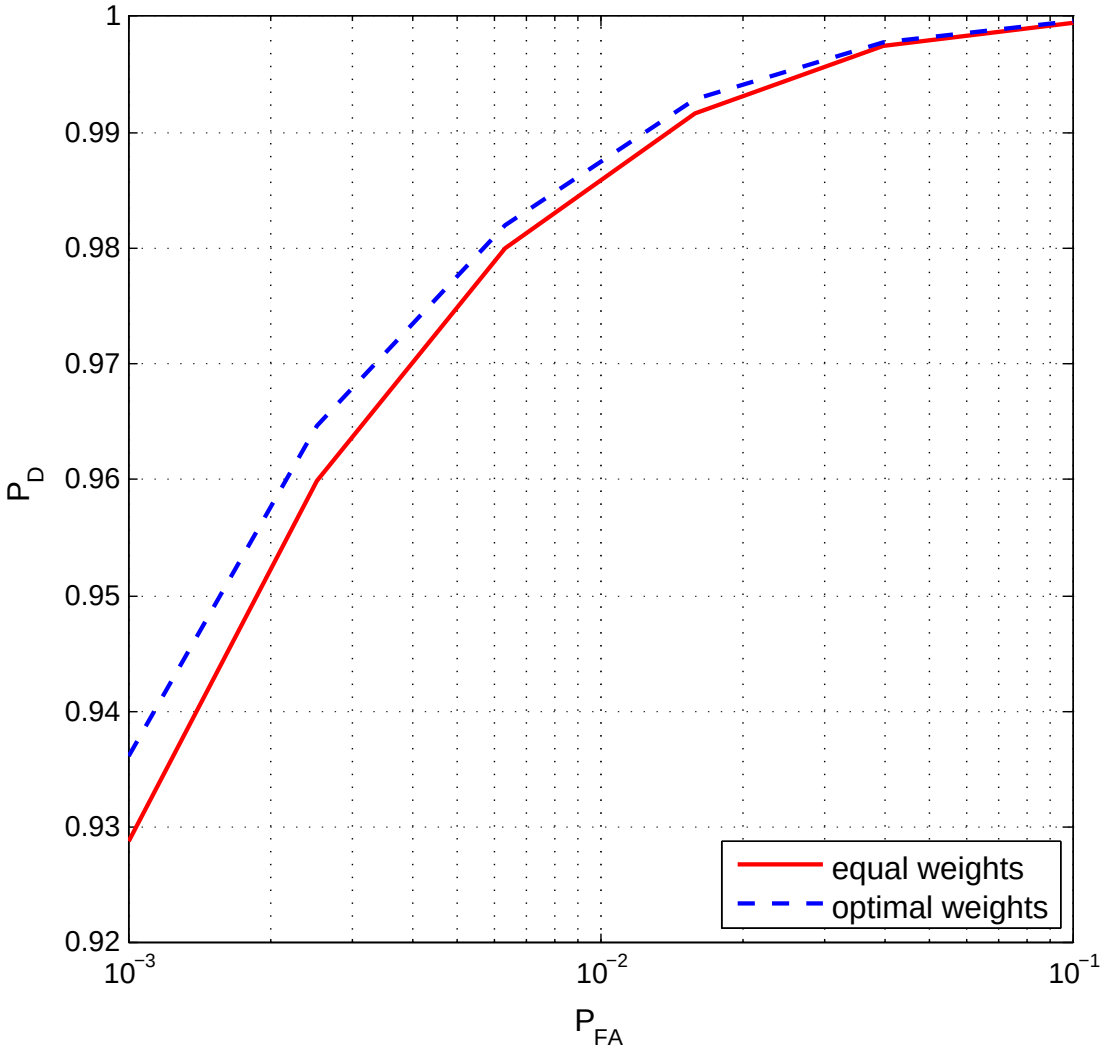


Figure 5.7: Authentication performance comparison of $P_D$ with equal weights and optimal weights.

# Chapter 6

# Physical-Layer Authentication Enhancement by Exploiting Diversity Techniques

The enhanced multi-characteristic based device fingerprinting technique is investigated in last chapter as one effective method to mitigate the authentication performance limitations. While following the device fingerprint generation, the step of fingerprint differentiation is straightforwardly becoming another key point for improving the reliability performance of physical-layer authentication. This chapter introduces diversity techniques to mitigate the negative factors in fingerprint differentiation procedure.

## 6.1 Introduction

In practice, the RF-AFE imperfection distinction between different devices is usually a small quantity, which means the fingerprint offset is small. Also, the fading and noise from wireless transmission can further degenerate the detection of such small offset. This can dramatically decrease the fingerprint-to-noise-ratio (FNR) and thereby lower performances of fingerprint differentiation. Therefore, the low FNR problem is actually the main factor that limits the performance of physical-layer authentication using RF-AFE imperfection-based device fingerprints.

Diversity technique can be used to solve the low FNR problem. Traditionally, the objective of using diversity technique is increasing the transmission reliability in the form of achieving larger diversity gain. In current wireless systems, the diversity techniques such as antenna diversity and cooperative diversity are widely adopted. For instances, today's WiFi devices are generally equipped with multiple antennas so that the multi-antenna diversity has significant potential in authenticating this kind of devices. The cooperative diversity related techniques can be conveniently applied to most communication networks since a network normally consists of more than one wireless devices. Motivated by the considerable advantages of using diversity technique, antenna and cooperative diversity techniques are applied in physical-layer authentication in this chapter.

Antenna diversity, also known as space diversity, is an effective means to combat wireless fading, and raise channel capacity through increasing the signal-to-noise-ratio (SNR). In the perspective of device fingerprint, the estimated fingerprint, which consists of physical-layer characteristics, can be treated as equivalent to the desired signal. Thus, it is straightforward that this diversity technique can also be used to improve the device fingerprint estimation accuracy and alleviate the low FNR problem as a benefit. Antenna diversity usually employs different combining methods as a post processing to recover the desired signals. Typically, there are four combining methods, the selection combining, threshold combining, maximal-ratio combining (MRC) and equal-gain combining. For example, using MRC, the obtained fingerprint of every antenna is multiplied by a specially designed weight. In doing so, the FNR can be maximized at the combiner outputs.

In a wireless network, the source node usually covers multiple receivers. It is worth mentioning that the multiple receivers here can either play the role of relay in cooperative system or general receivers in the case of conventional transmitter-receiver pairs. Let us take the cooperative relaying system as an example to illustrate the potential benefit of using cooperative diversity in physical-layer authentication performance improvement. In a cooperative system, multiple relays can receive different signal versions. However, the RF-AFE imperfections contained in these received signals are the same since these signals are emitted by the same transmitter. This feature facilitates the covered relays in performing authentication using various collaborative strategies. Besides, the selected optimal relay usually is experiencing the best

communication link so that it is more likely having the highest FNR, which is of high value in solving low FNR problem as well.

This chapter is divided into two parts in order to discuss the device-specific fingerprint-based physical-layer authentication enhancement using two different diversity techniques.

In the first part, the collaboration of multiple wireless receivers is proposed to authenticate the direct-conversion architecture-based wireless devices. The basic idea is to fully take advantage of the more powerful processing capability of multiple receivers than only using one receiver in order to achieve more accurate device-specific fingerprints differentiation performance. Regarding the fingerprint selection, both frequency-dependent (FD) IQI [87] and frequency-independent (FI) [88] IQI are considered. This is because that as one of the typical I/Q signal processing architecture based implementations, direct conversion transceiver inherently suffers more from IQI [89, 90]. The IQI feature of direct-conversion transceivers has been well studied such as in [91, 92, 93, 94]. In practice, the presence of IQI draws wide attention in most of the orthogonal frequency division multiplexing (OFDM) based wireless communication systems. This is because the direct conversion architecture is widely used in OFDM systems to achieve low-cost, low-power and small size, which simultaneously aggravates I/Q mismatches. Given the massive utilization of direct-conversion and OFDM techniques in current wireless transceivers, IQIs are suitable for authenticating such general transceivers. Precisely, the IQI of a direct-conversion architecture-based transmitter is first estimated by intended receiver as well as other trusted receivers locating within the effective transmitter's communication coverage. Although the processing power of separate wireless node may be limited, the multiple nodes can gain stronger processing capacity. The distributed and centralized methods are thereby designed to improve the data process in the authentication procedure.

In the second part, the antenna diversity at the receiver side is considered to increase FNR. Different from using multiple receivers, the antennas normally do not equip with separate processor. Thereby, multiple antennas usually do not benefit the wireless system with significantly increased processing capacity but the combining diversity. In this authentication scheme, the maximal ratio combining (MRC) technique, a typical combining diversity, is considered as an example to recover the desired device fingerprint. The simulation results show higher detection probability by using our method.

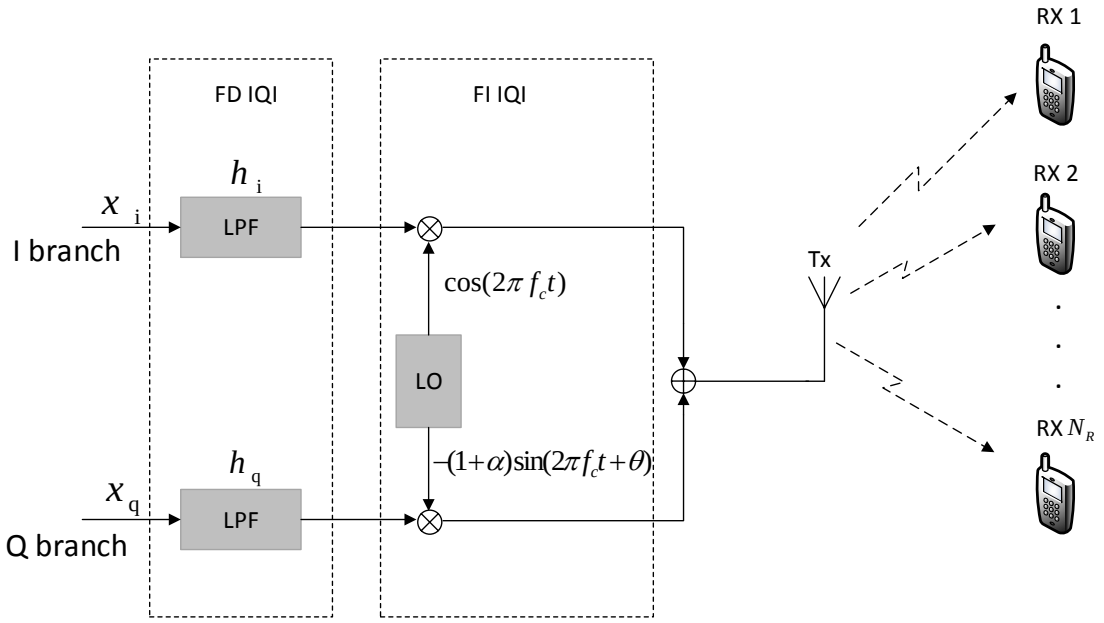


Figure 6.1: System model with FD and FI Tx IQI.

## 6.2 Enhanced Physical-Layer Authentication through Collaboration of Multiple Receivers

### 6.2.1 System Model

As shown in Fig.6.1, a direct conversion architecture-based OFDM system with FD and FI Tx IQI is considered. One input OFDM signal first passes through a general direct conversion architecture transmitter, and it is affected by FD and FI IQI in this procedure. Then the distorted signal arrives at a number of $N_R$ receivers through wireless transmission. Finally, the received signal at each receiver is processed for collaborative authentication. In this system model, Tx is the current transmitter, while Rx1 is the intended receiver and the other $N_R - 1$ Rxs are collaborative receivers. A single transmitter single receiver scenario is considered in the aforementioned propagation procedure. Then, this model is extended to multi-receiver collaborative authentication.

Herein, $x(t) = x_{\mathrm{i}}(t) + jx_{\mathrm{q}}(t)$ represents one baseband OFDM signal, where $x_{\mathrm{i}}(t)$ and $x_{\mathrm{q}}(t)$ denote the input signal for I and Q branches, respectively. The impulse responses of LPFs of I and Q branches are respectively given by $h_{\mathrm{i}}(t)$ and $h_{\mathrm{q}}(t)$. Therefore, the signal after experiencing

FD IQI impact can be expressed as

$$x_{\mathrm{LPF}}(t) = x_{\mathrm{i}}(t) \otimes h_{\mathrm{i}}(t) + j x_{\mathrm{q}}(t) \otimes h_{\mathrm{q}}(t), \tag{6.1}$$

where $\otimes$ denotes convolution. In addition, LO introduces gain mismatch $\alpha$ and phase mismatch $\theta$ to $x_{\mathrm{LPF}f}(t)$ when $x_{\mathrm{LPF}}(t)$ passing through it. The output signal of LO is given by

$$\begin{aligned} x_{\mathrm{LO}}(t) = {} & \Re\{x_{\mathrm{LPF}}(t)\} \cos(2\pi f_c t) \\ & - \Im\{x_{\mathrm{LPF}}(t)\}(1+\alpha) \sin(2\pi f_c t + \theta), \end{aligned} \tag{6.2}$$

where $\Re\{\cdot\}$ and $\Im\{\cdot\}$ respectively denote real and imaginary parts of a complex variable.

Based on (6.1) and (6.2), the equivalent discrete baseband expression of $x_{\mathrm{LO}}$ can be written as

$$\begin{aligned} x_{\mathrm{LO}}[n] = \frac{1}{2} & ((h_{\mathrm{i}}[n] + (\mu - 1) h_{\mathrm{q}}[n]) \otimes x[n] \\ & + (h_{\mathrm{i}}[n] - (\mu - 1) h_{\mathrm{q}}[n]) \otimes x^*[n]), \end{aligned} \tag{6.3}$$

where $(\cdot)^*$ denotes complex conjugate; $\mu \triangleq 1 + (1+\alpha)e^{j\theta}$ is a complex parameter representing the FI IQI. Similar to [22], the sampled analog quantities (e.g. $h_{\mathrm{i}}$) can be represented as vectors of the length $N$ to satisfy the $N$-point circular convolution in the discrete models. If the length is not enough, it is expanded to $N$ with padding zeros.

To further simplify the mathematical expression, a vector $\epsilon$ is defined to satisfy $h_{\mathrm{q}}[n] = \epsilon[n] h_{\mathrm{i}}[n]$. Substituting $\epsilon[n]$, the expression of (6.3) can be simplified as

$$x_{\mathrm{LO}}[n] = \gamma[n] h_{\mathrm{i}}[n] \otimes x[n] + (1 - \gamma[n]) h_{\mathrm{i}}[n] \otimes x^*[n], \tag{6.4}$$

where $\gamma[n] \triangleq \frac{1}{2}[1 + \epsilon[n](\mu - 1)]$ denotes the FD and FI IQI parameter. If I and Q branches are perfectly balanced that indicating $\alpha = 0$, $\theta = 0$ and $\epsilon = [1, 1, \cdots, 1]$, the IQI parameter $\gamma$ will reduce to $[1, 1, \cdots, 1]$.

Then, the distorted signal is transmitted to receivers through wireless propagation. The

received signal $y$ can be modeled as

$$y[n] = x_{\mathrm{LO}}[n] \otimes h_{\mathrm{c}}[n] + w[n], \tag{6.5}$$

where $h_{\mathrm{c}}[n]$ is channel impulse response; $\{w[n]\}$ are modeled as independent and identical distributed complex additive white Gaussian noises with zero mean and covariance $\sigma_w^2$, which implies $w[n] \sim \mathcal{CN}(0, \sigma_w^2)$.

After receiving signal, the receiver analyzes the received $y[n]$ and estimates the IQI for authentication. Since this study focuses on exploiting the estimates based authentication algorithms, and IQI estimation techniques have been investigated in depth in many researches such as [95] and [96], a perfect channel estimation is assumed to simplify the IQI estimation procedure. Also, we consider the training signal and assume receivers have the knowledge of $x[n]$. This assumption does not weaken our authentication scheme as our scheme is independent of the content of transmitted signal, but depends on the IQI impact on the transmitted signal. In other words, this scheme still works even when attackers know the content of transmitted signals. In addition, it is supposed that the receiver IQI-free for simplicity. It is noteworthy that different IQIs of multiple receivers can be further considered in the future work to study the authentication performance difference under different receiving IQIs.

Substituting (6.4) into (6.5) and taking the $N$-point discrete Fourier transform of both sides for (6.5), and after some rearrangements, we obtain

$$\begin{aligned} \mathcal{F}_{[n]}(\gamma h_{\mathrm{i}}) = & \frac{Y[n] - H_{\mathrm{i}}[n]\mathcal{F}_{[n]}(x^*)H_{\mathrm{c}}[n]}{(X[n] - \mathcal{F}_{[n]}(x^*))H_{\mathrm{c}}[n]} \\ & - \frac{W[n]}{(X[n] - \mathcal{F}_{[n]}(x^*))H_{\mathrm{c}}[n]}, \end{aligned} \tag{6.6}$$

where $\mathcal{F}(\cdot)$ denotes discrete Fourier transform, and $\mathcal{F}_{[n]}(\cdot)$ represents the $n$th element of $\mathcal{F}(\cdot)$. Also, $\mathcal{F}_{[n]}(x^*)$ is given by

$$\mathcal{F}_{[n]}(x^*) = \begin{cases} X_1^*, & n = 1 \\ X_{N+2-n}^*, & n = 2, 3, \cdots, N \end{cases}. \tag{6.7}$$

In addition, $Y$, $H_{\mathrm{i}}$, $X$, $\mathcal{F}(x^*)$, $H_{\mathrm{c}}$ and $W$ denote the discrete Fourier transform of corresponding $y$, $h_{\mathrm{i}}$, $x$, $x^*$, $h_{\mathrm{c}}$ and $w$, respectively.

Then the $N$-point inverse discrete Fourier transformation of (6.6) is conducted to recover $\gamma h_{\mathrm{i}}$, and the result can be expressed as

$$\bar{\beta} = \beta + \bar{w}, \tag{6.8}$$

where $\bar{\beta}[n] = \mathcal{F}^{-1}_{[n]}\left(\frac{Y - H_{\mathrm{i}}\mathcal{F}(x^*)H_{\mathrm{c}}}{(X - \mathcal{F}(x^*))H_{\mathrm{c}}}\right)$ is estimated value of Tx IQI at receiver, $\beta[n] = \gamma[n]h_{\mathrm{i}}[n]$ represents its actual value, and $\bar{w}[n] = \mathcal{F}^{-1}_{[n]}\left(\frac{W}{(X - \mathcal{F}(x^*))H_{\mathrm{c}}}\right)$ is random Gaussian variable. Here, $\mathcal{F}^{-1}(\cdot)$ represents the inverse discrete Fourier transform. For further analysis, the vector expressions of $\bar{\beta}, \beta$ and $\bar{w}$ are given by

$$\begin{aligned}
\bar{\beta} &= [\bar{\beta}[1], \bar{\beta}[2], \cdots, \bar{\beta}[N_1], \cdots, \bar{\beta}[N]] \\
\beta &= [\beta[1], \beta[2], \cdots, \beta[N_1], 0, 0, \cdots, 0] \\
\bar{w} &= [\bar{w}[1], \bar{w}[2], \cdots, \bar{w}[N_1], \cdots, \bar{w}[N]]
\end{aligned}$$

Given that only the first $N_1$ elements in $\beta$ are not zeros as well as $\Re\{\beta[n]\} = \frac{1}{2}[1 + \epsilon[n](1 + \alpha)\cos\theta]h_{\mathrm{i}}[n]$ does not lose any information of IQI, only the real parts of the first $N_1$ elements of $\bar{\beta}$ are taken into consideration in the following, which produces a vector as

$$B = [\Re\{\bar{\beta}[1]\}, \Re\{\bar{\beta}[2]\}, \cdots, \Re\{\bar{\beta}[N_1]\}]. \tag{6.9}$$

In this case, $B[k](k = 1, 2, \cdots, N_1)$ follows Gaussian distribution, which is expressed as $B[k] \sim \mathcal{N}(\mu[k], \sigma^2)$. Here, $\mu[k] = \Re\{\beta[k]\}$ and $\sigma^2 = \frac{1}{2N}\sum_{n=1}^{N} C^2[n]\sigma_w^2$ where $C[n] = \mathcal{F}^{-1}_{[n]}\left(\frac{1}{(X - \mathcal{F}(x^*))H_{\mathrm{c}}}\right)$. The coefficient $N$ in $\sigma^2$ is introduced by the inverse discrete Fourier transformation.

In the following, the analysis is extended with considering the scenario of multiple receivers. Considering the estimates of $N_R$ receivers are affected by different $h_{\mathrm{c}}$ and $w$, the estimated IQIs at $N_R$ receivers are distinct. Based on this, the offsets at the $l$th receiver can be obtained by computing the subtractions as

$$\Delta B_l[k] = B_l[k] - B'[k], \tag{6.10}$$

where $B_l$ represents the estimated $B$ at the $l$th receiver, and $B'$ is the $B$ of one validated transmitter. Every receiver has stored the same $B'$. Now a $N_R \times N_1$ offset matrix $\Delta\mathbf{B}$ can be defined by setting each row of it as $\Delta B_l$, which is given by

$$\Delta\mathbf{B} = \begin{bmatrix} \Delta B_{11} & \cdots & \Delta B_{1N_1} \\ \Delta B_{21} & \cdots & \Delta B_{2N_1} \\ \vdots & \ddots & \vdots \\ \Delta B_{N_R1} & \cdots & \Delta B_{N_RN_1} \end{bmatrix}. \tag{6.11}$$

In (6.11), $\Delta B_{lk}$ indicates the $k$th element in $\Delta B_l$. Based on the aforementioned results, $\{\Delta B_{lk}\}$ are Gaussian random variables with distribution $\mathcal{N}(\mu_k, \sigma_l^2)$, where $\mu_k = \mu[k] - B'[k]$ and $\sigma_l^2$ denotes $\sigma^2$ of the $l$th receiver. It is apparent that $\mu_k$ is only related to the offsets between the actual IQI of current transmitter and the stored IQI of the validated transmitter. As a result, the binary hypothesis testing can be modeled as

$$\begin{cases} \mathcal{H}_0: & \mu_k = 0 \\ \mathcal{H}_1: & \mu_k \neq 0 \end{cases}. \tag{6.12}$$

If the current transmitter is the validated one, their device fingerprints should be exactly the same, therefore it is $\mathcal{H}_0$ and $\mu_k = 0$. Otherwise, the current transmitter is an attacker, their fingerprints must be different. In this case, $\mathcal{H}_1$ is claimed.

### 6.2.2 Collaborative Authentication using Distributed and Centralized Methods

In this subsection, the authentication methods are introduced to decide whether $\mathcal{H}_0$ or $\mathcal{H}_1$ is correct by analyzing $\Delta\mathbf{B}$. The challenge of this procedure is that $\mu_k$ is corrupted by the zero-mean Gaussian noise, and thereby it is not directly available at the receiver in practice. This situation will dramatically degenerate the authentication performance. To achieve satisfactory authentication accuracy, two multi-receiver collaborative authentication methods are proposed. It is noteworthy that our authentication scheme still works with only one receiver (Rx1) by

setting $N_R = 1$.

***Distributed Method***

In this authentication method, all $N_R$ receivers first separately makes a decision about whether or not the current transmitter is the validated one based on their own estimated Tx IQI information. After that, the intended receiver, Rx1, can make the final decision by combining all of $N_R$ decisions.

$\Delta B_{lk}$ is first normalized by dividing $\sigma_l$ to acquire $A_{lk} = \frac{\Delta B_{lk}}{\sigma_l} \sim \mathcal{N}(\frac{\mu_k}{\sigma_l}, 1)$. Then the offset matrix in this method becomes

$$\mathbf{A} = \begin{bmatrix} A_{11} & \cdots & A_{1N_1} \\ A_{21} & \cdots & A_{2N_1} \\ \vdots & \ddots & \vdots \\ A_{N_R1} & \cdots & A_{N_RN_1} \end{bmatrix}. \tag{6.13}$$

At the $l$-th receiver, the data are processed as

$$S_l = \sum_{k=1}^{N_1} A_{lk}^2. \tag{6.14}$$

Under $\mathcal{H}_0$, $S_l$ follows central chi-squared distribution with $N_1$ degrees of freedom, which can be represented as $S_l \sim \chi^2_{N_1}$. While under $\mathcal{H}_1$, $S_l$ follows non-central chi-squared distribution with $N_1$ degrees of freedom and non-centrality parameter $\lambda = \sum_{k=1}^{N_1} (\frac{\mu_k}{\sigma_l})^2$, which can be denoted as $S_l \sim \chi^2_{N_1}(\lambda)$.

At the $l$th receiver, the authentication procedure is performed by comparing the metric $S_l$ with a false alarm rate dependent threshold $T_l$. To be specific, if $S_l$ is less than $T_l$, $\mathcal{H}_0$ is decided; otherwise, $\mathcal{H}_1$ is claimed. Under $\mathcal{H}_0$, the probability density function (PDF) of $S_l$ is given by

$$p_{\mathcal{H}_0(S_l)} = \frac{S_l^{\frac{N_1-2}{2}} e^{-\frac{1}{2}S_l}}{2^{\frac{N_1}{2}}\Gamma(\frac{N_1}{2})}, \tag{6.15}$$

where $\Gamma(x) = \int_0^\infty u^{x-1}e^{-u}du$ is the Gamma function. The PDF of $S_l$ under $\mathcal{H}_1$ is given by

$$p_{\mathcal{H}_1(S_l)} = \frac{1}{2}\left(\frac{S_l}{\lambda}\right)^{\frac{N_1-2}{4}} e^{-\frac{1}{2}(S_l+\lambda)} I_{\frac{N_1-2}{2}}(\sqrt{\lambda S_l}), \tag{6.16}$$

where $I_r(\cdot)$ is the modified Bessel function of the first kind and order $r$. It has the series representation defined as

$$I_r(x) = \sum_{i=0}^{\infty} \frac{\left(\frac{x}{2}\right)^{2i+r}}{i!\Gamma(r+i+1)}. \tag{6.17}$$

Based on (6.14) and (6.15), the false alarm rate of the $l$th receiver, can be computed by

$$\begin{aligned} P_{\mathrm{FA}_l} &= P\{S_l > T_l|\mathcal{H}_0\} \\ &= \int_{T_l}^{+\infty} p_{\mathcal{H}_0(S_l)} dS_l = Q_{\chi^2_{N_1}}(T_l), \end{aligned} \tag{6.18}$$

where $Q_{\chi^2_{N_1}}(\cdot)$ is right-tail probability for a $\chi^2_{N_1}$ random variable, and it has different mathematical expression depending on the parity of $N_1$. For an odd $N_1$, it has the expression as

$$Q_{\chi^2_{N_1}}(T_l) = \begin{cases} 2Q(\sqrt{T_l}) & N_1 = 1 \\ 2Q(\sqrt{T_l}) + \frac{e^{-\frac{T_l}{2}}}{\sqrt{\pi}} \sum\limits_{i=1}^{\frac{N_1-1}{2}} \frac{(i-1)!(2T_l)^{i-\frac{1}{2}}}{(2i-1)!} & N_1 \geqslant 3 \end{cases} \tag{6.19}$$

and for an even $N_1$, it is given by

$$Q_{\chi^2_{N_1}}(T_l) = e^{-\frac{T_l}{2}} \sum_{i=0}^{\frac{N_1}{2}-1} \frac{T_l^i}{2^i i!}. \tag{6.20}$$

In (6.19), $Q(\cdot)$ denotes the Q-function, which is defined as

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}u^2} du. \tag{6.21}$$

In practical implementation, $T$ can be determined by inverting (6.18) to achieve a specified

false alarm rate as

$$T_l = Q^{-1}_{\chi^2_{N_1}}(P_{\mathrm{FA}_l}). \tag{6.22}$$

Using the threshold $T_l$, the $l$th receiver is able to make its own decision about either to claim $\mathcal{H}_0$ or $\mathcal{H}_1$. Also, the detection rate of the $l$th receiver can be calculated as

$$P_{\mathrm{D}_l} = P\{S_l > T_l|\mathcal{H}_1\} = \int_{T_l}^{+\infty} p_{\mathcal{H}_1(S_l)} dS_l. \tag{6.23}$$

Then, Rx1 should combine all of these decisions and make the final decision. To enhance the detection capability, a stringent decision rule is chosen in this distributed method. To be precise, Rx1 considers the current Tx is legitimate only under the condition of no collaborative receiver claims $\mathcal{H}_1$. Accordingly, the final effective false alarm rate becomes

$$P_{\mathrm{EFA}} = 1 - \prod_{l=1}^{N_R}(1 - P_{\mathrm{FA}_l}). \tag{6.24}$$

Similarly, the final effective detection rate can be calculated by

$$P_{\mathrm{ED}} = 1 - \prod_{l=1}^{N_R}(1 - P_{\mathrm{D}_l}). \tag{6.25}$$

***Centralized Method***

Besides the distributed method, another centralized data processing authentication method is proposed. In this centralized method, Rx1 first collects the estimated IQIs from other $N_R - 1$ receivers to obtain $\Delta\mathbf{B}$, then authenticates the current transmitter based on $\Delta\mathbf{B}$. In brief, all data processing and decision are made by Rx1 instead of a total number of $N_R$ receivers.

After obtaining $\Delta\mathbf{B}$, Rx1 processes data as

$$S_l = \frac{1}{N_1}\sum_{k=1}^{N_1} \Delta B_{lk}. \tag{6.26}$$

Under $\mathcal{H}_0$, $S_l \sim \mathcal{N}(0, \sigma^2_{S_l})$ with PDF $p_{\mathcal{H}_0(S_l)}$; while under $\mathcal{H}_1$, $S_l \sim \mathcal{N}(A, \sigma^2_{S_l})$ with PDF $p_{\mathcal{H}_1(S_l)}$. Here, $A = \frac{1}{N_1}\sum_{k=1}^{N_1}\mu_k$ is a constant, and $\sigma^2_{S_l} = \frac{\sigma^2_l}{N_1}$.

To maximize the detection rate under $\mathcal{H}_1$, Neyman-Pearson test is performed as

$$\frac{\prod_{l=1}^{N_R} p_{\mathcal{H}_1(S_l)}}{\prod_{l=1}^{N_R} p_{\mathcal{H}_0(S_l)}} > T, \tag{6.27}$$

which produces

$$\begin{aligned} \frac{1}{N_R}\sum_{l=1}^{N_R}\frac{S_l}{\sigma_{S_l}^2} &> \frac{\ln T}{N_R A} + \frac{A}{2N_R}\sum_{l=1}^{N_R}\frac{1}{\sigma_{S_l}^2} = T'_+ > 0, A > 0 \\ \frac{1}{N_R}\sum_{l=1}^{N_R}\frac{S_l}{\sigma_{S_l}^2} &< \frac{\ln T}{N_R A} + \frac{A}{2N_R}\sum_{l=1}^{N_R}\frac{1}{\sigma_{S_l}^2} = T'_- < 0, A < 0. \end{aligned} \tag{6.28}$$

Since $T'_+ = -T'_-$, (6.28) can be simplified as

$$|D| > T'_+, \tag{6.29}$$

where $D = \frac{1}{N_R}\sum_{l=1}^{N_R}\frac{S_l}{\sigma_{S_l}^2}$. In this case, $D \sim \mathcal{N}(0, \frac{1}{N_R^2}\sum_{l=1}^{N_R}\frac{1}{\sigma_{S_l}^2})$ with PDF $p_{\mathcal{H}_0(D)}$ under $\mathcal{H}_0$; while $D \sim \mathcal{N}(\frac{A}{N_R}\sum_{l=1}^{N_R}\frac{1}{\sigma_{S_l}^2}, \frac{1}{N_R^2}\sum_{l=1}^{N_R}\frac{1}{\sigma_{S_l}^2})$ with PDF $p_{\mathcal{H}_1(D)}$ under $\mathcal{H}_1$. As a result, the authentication procedure becomes a comparison between the metric $|D|$ and threshold $T'_+$. More specifically, if $|D| > T'_+$ is satisfied, $\mathcal{H}_1$ will be decided; otherwise, $\mathcal{H}_0$ will be decided. Based on this decision rule, the false alarm rate can be computed by

$$\begin{aligned} P_{\text{FA}} &= P\{|D| > T'_+ | \mathcal{H}_0\} \\ &= \int_{T'_+}^{+\infty} p_{\mathcal{H}_0(D)} dD + \int_{-\infty}^{T'_-} p_{\mathcal{H}_0(D)} dD \\ &= 2Q\left(\frac{N_R T'_+}{\sqrt{\sum_{l=1}^{N_R}\frac{1}{\sigma_{S_l}^2}}}\right) \end{aligned} \tag{6.30}$$

Based on (6.30), threshold $T'_+$ can be determined according to a specified $P_{\text{FA}}$ as

$$T'_+ = \frac{1}{N_R}\sqrt{\sum_{l=1}^{N_R}\frac{1}{\sigma_{S_l}^2}}\, Q^{-1}\left(\frac{P_{\text{FA}}}{2}\right), \tag{6.31}$$

where $Q^{-1}(\cdot)$ denotes the inverse Q-function. In comparison with the threshold obtained in (6.22), $T'_+$ is an adaptive threshold as it depends on $N_R$ and $\sigma_{S_l}$ as well. With this adaptive $T'_+$, the detection rate $P_{\mathrm{D}}$ can be calculated by

$$\begin{aligned} P_{\mathrm{D}} &= P\{|D| > T'_+|\mathcal{H}_1\} \\ &= \int_{T'_+}^{+\infty} p_{\mathcal{H}_1(D)} dD + \int_{-\infty}^{T'_-} p_{\mathcal{H}_1(D)} dD \\ &= Q\left(Q^{-1}\left(\frac{P_{\mathrm{FA}}}{2}\right) - \sqrt{A^2 \sum_{l=1}^{N_R} \frac{1}{\sigma_{S_l}^2}}\right) \\ &\quad + Q\left(Q^{-1}\left(\frac{P_{\mathrm{FA}}}{2}\right) + \sqrt{A^2 \sum_{l=1}^{N_R} \frac{1}{\sigma_{S_l}^2}}\right). \end{aligned} \tag{6.32}$$

It is noteworthy that the specified $P_{\mathrm{FA}}$ is final effective false alarm rate, and $P_{\mathrm{D}}$ is final effective detection rate in this centralized method, which indicates $P_{\mathrm{EFA}} = P_{\mathrm{FA}}$ and $P_{\mathrm{ED}} = P_{\mathrm{D}}$.

### 6.2.3 Simulation Results

The performance of proposed authentication schemes are evaluated. An OFDM system is considered, in which the number of sub-carriers is 256, the length of cyclic prefix is 32, and the modulation is 4-QAM. Also, the Rayleigh fading channel is employed. For the IQI, simulation setups similar to [22] are considered, in which $(\alpha, \theta, \epsilon, h_i) = (0.244, 5^\circ, [1, 1, 20], [0.01, 1, 0.01])$. In our simulation, the validated transmitter is set to own the IQI parameter as $(\alpha, \theta, \epsilon, h_i)_{\mathcal{H}_0} = (0.05, 1^\circ, [1, 1, 20], [0.01, 1, 0.01])$. As mentioned earlier, this parameter is stored in $N_R$ receivers as validated device fingerprint. Under $\mathcal{H}_0$, the current transmitter is set to own exactly the same IQI parameter with the validated transmitter; while under $\mathcal{H}_1$, the current transmitter is assigned to have IQI parameter as $(\alpha, \theta, \epsilon, h_i)_{\mathcal{H}_1} = (-0.05, 3^\circ, [0.9, 0.9, 18], [0.0095, 0.98, 0.0098])$. As shown, the validated and current transmitter are intentionally set to have close IQI parameters in order to increase the challenge of authentication. $(\alpha, \theta, \epsilon, h_i)_{\mathcal{H}_0}$ and $(\alpha, \theta, \epsilon, h_i)_{\mathcal{H}_1}$ are used to evaluate $P_{\mathrm{EFA}}$ and $P_{\mathrm{ED}}$, respectively, by comparing them with the validated IQI parameter.

Fig.6.2 presents the threshold versus false alarm rate for two methods, and compares the simulated $P_{\mathrm{ED}}$ and $P_{\mathrm{EFA}}$ with corresponding analytical values. In this figure, $P_{\mathrm{FA}}$ denotes $P_{\mathrm{FA}_l}$

and threshold refers to $T_l$ in the distributed method. Furthermore, $P_{\mathrm{FA}_l}$ are set to be the same under different $l$. It is shown that the thresholds of two methods from (6.22) and (6.31) are decreasing with the growth of $P_{\mathrm{FA}}$, which also results in the increase trends of $P_{\mathrm{ED}}$ and $P_{\mathrm{EFA}}$.

Fig.6.3 assesses the $P_{\mathrm{EFA}}$ of two proposed authentication methods in terms of SNR. In distributed method, $P_{\mathrm{EFA}}$ increases with the growth of $P_{\mathrm{FA}}$ and $N_R$. As shown, $P_{\mathrm{EFA}}$ is independent of $N_R$ in centralized method. In addition, $P_{\mathrm{EFA}}$ of both methods are independent of the SNR, which approximately shows steady horizontal lines in this figure.

Moreover, the $P_{\mathrm{ED}}$ vs. $P_{\mathrm{FA}}$ and $P_{\mathrm{ED}}$ vs. SNR are simulated to present the detection capability enhancement of our authentication scheme in Fig.6.4 and Fig.6.5, respectively. As it can be seen, $P_{\mathrm{ED}}$ of both two methods increase with $N_R$ varies from 1 to 5. It means the authentication performance is effectively enhanced by collaborative receivers. Additionally, Fig.6.5 shows that the $P_{\mathrm{ED}}$ of centralized method exceeds the $P_{\mathrm{ED}}$ of distributed method when $N_R > 1$. It is due to the fact that the collaboration of receivers leads to more enhancement in centralized method than the distributed method with the growth of $N_R$.

To evaluate the detection capability of our authentication scheme, a ratio parameter is defined as $R_k = 10\log_{10}\left(\left|\frac{\mu_k}{B'[k]}\right|\right)$ dB, $k = 1, 2, \cdots, N_1$. In fact, $R_k$ shows the minor IQI differences between current and validated transmitters. In Fig.6.6, the $P_{\mathrm{ED}}$ under different $R_k$ is given, and the values of $R_k$ are set to be the same under different $k$. As it can be observed, our scheme is able to show a satisfactory authentication performance even under the small value of $R_k$.

Simulation results demonstrate that with the assistance of the additional collaborative receivers, the detection capabilities of both methods are dramatically enhanced. However, the disadvantage of the distributed method is that the $P_{\mathrm{EFA}}$ also increases in the meanwhile. On the contrary, the $P_{\mathrm{EFA}}$ of the centralized method is totally independent of the number of collaborative receivers. In practice, the centralized method requires more processing and computing capabilities of Rx1. It is because Rx1 should process all estimated IQI data itself in the centralized method, but this procedure is implemented by multiple collaborative receivers in the distributed method. In addition, our simulation only considers one validated transmitter. It is easy to extent it to multiple validated transmitters by storing more validated device fingerprints in receivers.

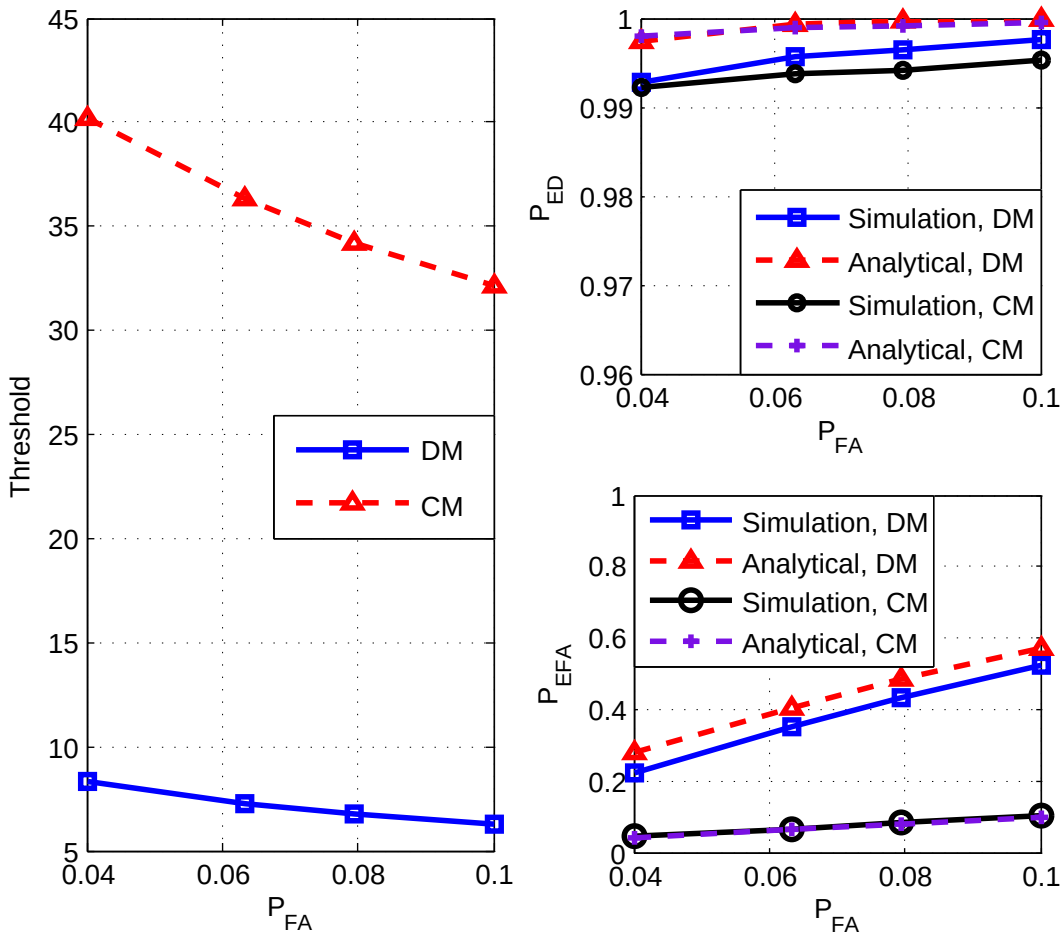


Figure 6.2: Threshold, $P_{\text{EFD}}$ and $P_{\text{EFA}}$ under SNR = 14 dB and $N_R = 8$. DM = Distributed Method, CM = Centralized Method.

## 6.3 Enhanced Physical-Layer Authentication through Combining Diversity

### 6.3.1 Device Fingerprint Estimation using MRC

In wireless communications, the channel fading and noise corruption are inevitable, and unfortunately this can result in worse effect on the RF-AFE imperfection-based device fingerprint estimation. Antenna diversity can be used to overcome this problem. Specifically, we propose adopting maximal-ratio combining, which is one the most commonly used combining diversity, to increase the FNR and further improve the fingerprint estimation accuracy.

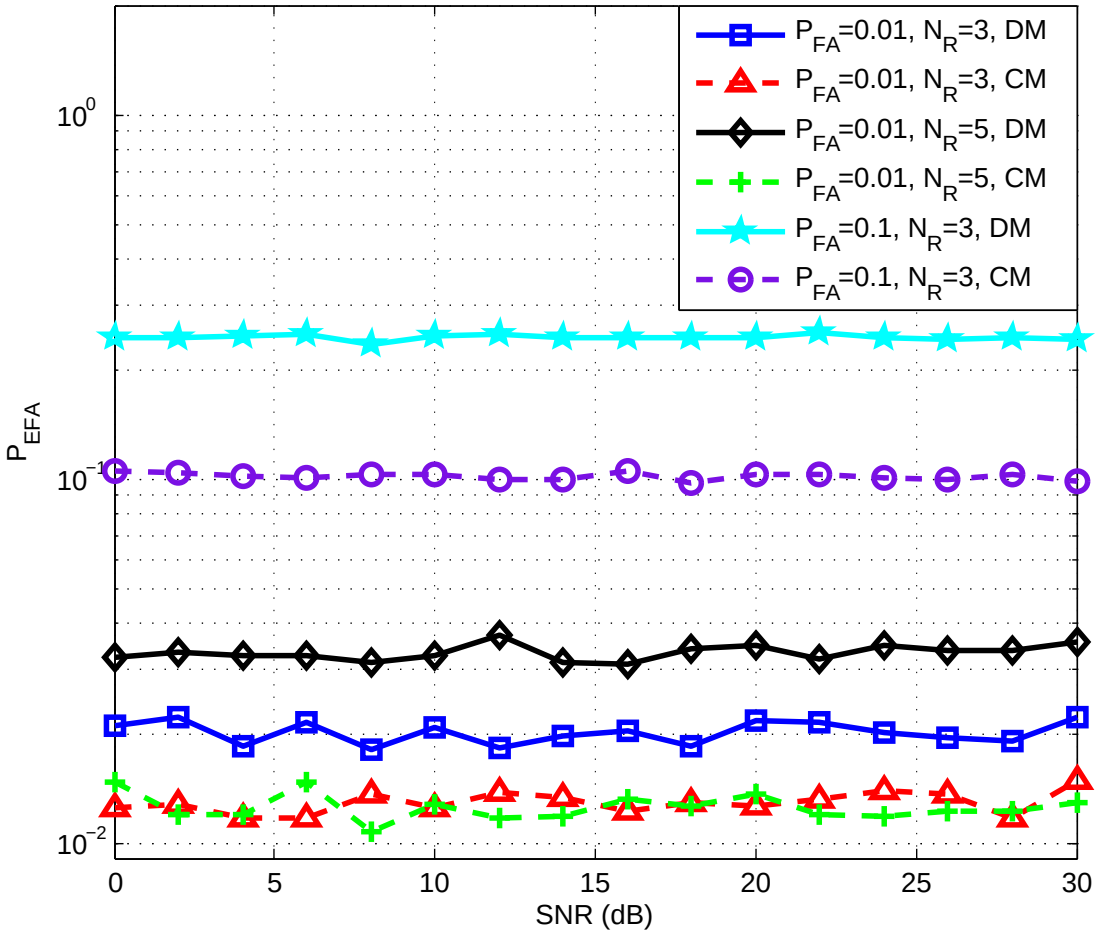


Figure 6.3: $P_{\text{EFA}}$ vs. SNR under different $P_{\text{FA}}$ and $N_R$.

Fig.6.7 shows the physical-layer authentication model using MRC technique. In this model, a receiver equipping with a number of $M$ antennas is considered. The spatial distance between these antennas are assumed to be large enough to guarantee that each antenna is experiencing independent channel, i.e., no correlations between channels are taken into the consideration. Each antenna can receive the signals sent by a transmitter, which is also the authentication target. It is noteworthy that all received signals can be tagged with the identical device-specific fingerprint due to the stability of hardware level RF-AFE imperfections. The initial device fingerprint for each antenna, $l_i$, is first estimated according to the specific fingerprint generation schemes such as proposed in previous chapters. The MRC is then utilized to process all $l$ to obtain one metric, $f$, with maximized FNR. This $f$ is then used in the following process

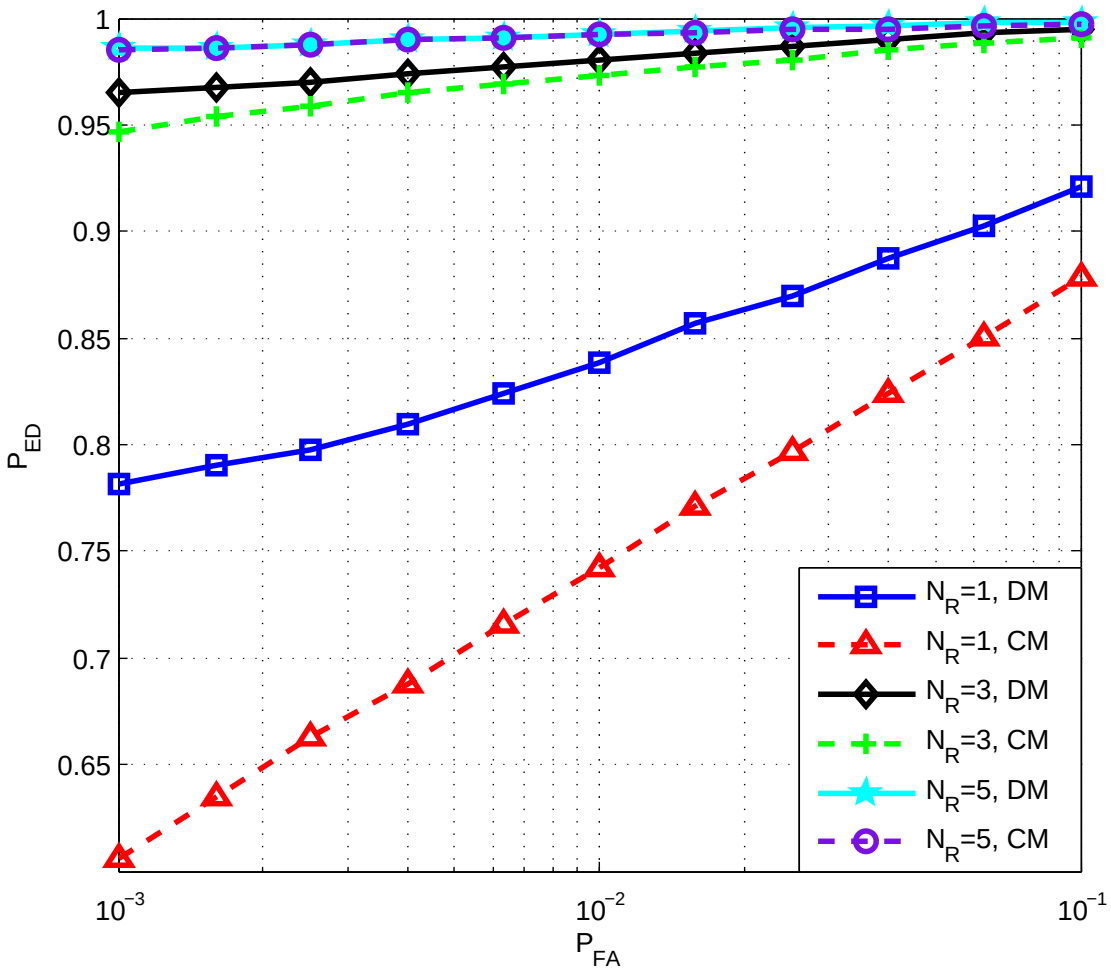


Figure 6.4: $P_{\text{ED}}$ vs. $P_{\text{FA}}$ under SNR = 18 dB and $N_R = 1, 3, 5$.

components for transmitter authentication.

At the $k^{th}$ antenna, we define the obtained $l_k$ as

$$\mathbf{l}_k = \mathbf{f} h_k + \mathbf{n}_k, \tag{6.33}$$

where $\mathbf{f}$ denotes the desired device-specific device fingerprint, $h_k$ is the wireless channel related gain and $\mathbf{n}_k$ denotes the noise with variance $\sigma_r^2$ in this estimate.

Similar to SNR, the corresponding FNR at the $k^{th}$ antenna can be defined as

$$\gamma_{\text{F},k} = \frac{\|h_k \mathbf{f}\|^2}{\|\mathbf{n}_k\|^2} = \frac{P_f |h_k|^2}{\sigma_r^2}, \tag{6.34}$$

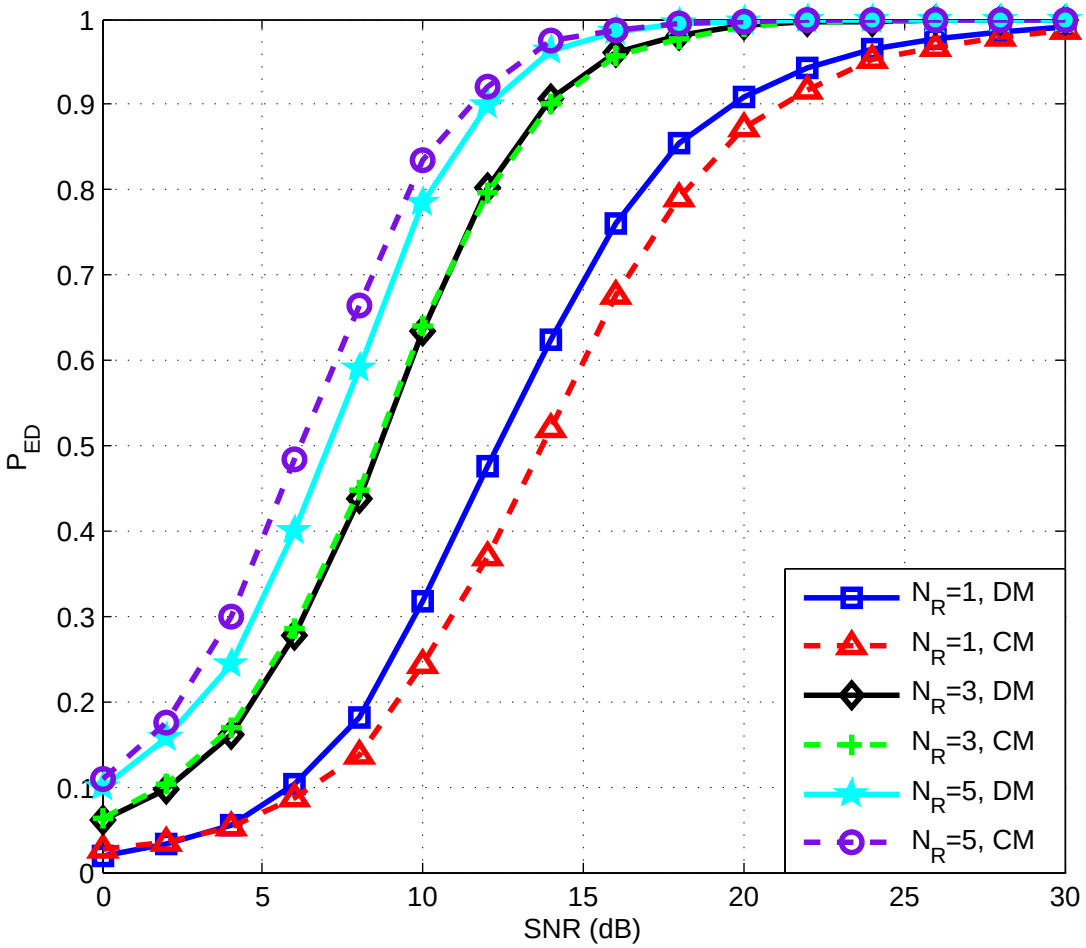


Figure 6.5: $P_{\text{ED}}$ vs. SNR under $P_{\text{FA}} = 0.01$ and $N_R = 1, 3, 5$.

where $P_f$ denotes the average power of $\mathbf{f}$.

In the MRC processing component, as depicted in Fig.6.7, each estimated $l_k$ is multiplied by a weight $w_k^*$. After that, all of the weighted signals are added together to obtain the output of the combiner, which can be given by

$$\sum_{k=1}^{M} w_k^* \mathbf{l}_k = \mathbf{f} \sum_{k=1}^{M} w_k^* h_k + \sum_{k=1}^{M} w_k^* \mathbf{n}_k. \tag{6.35}$$

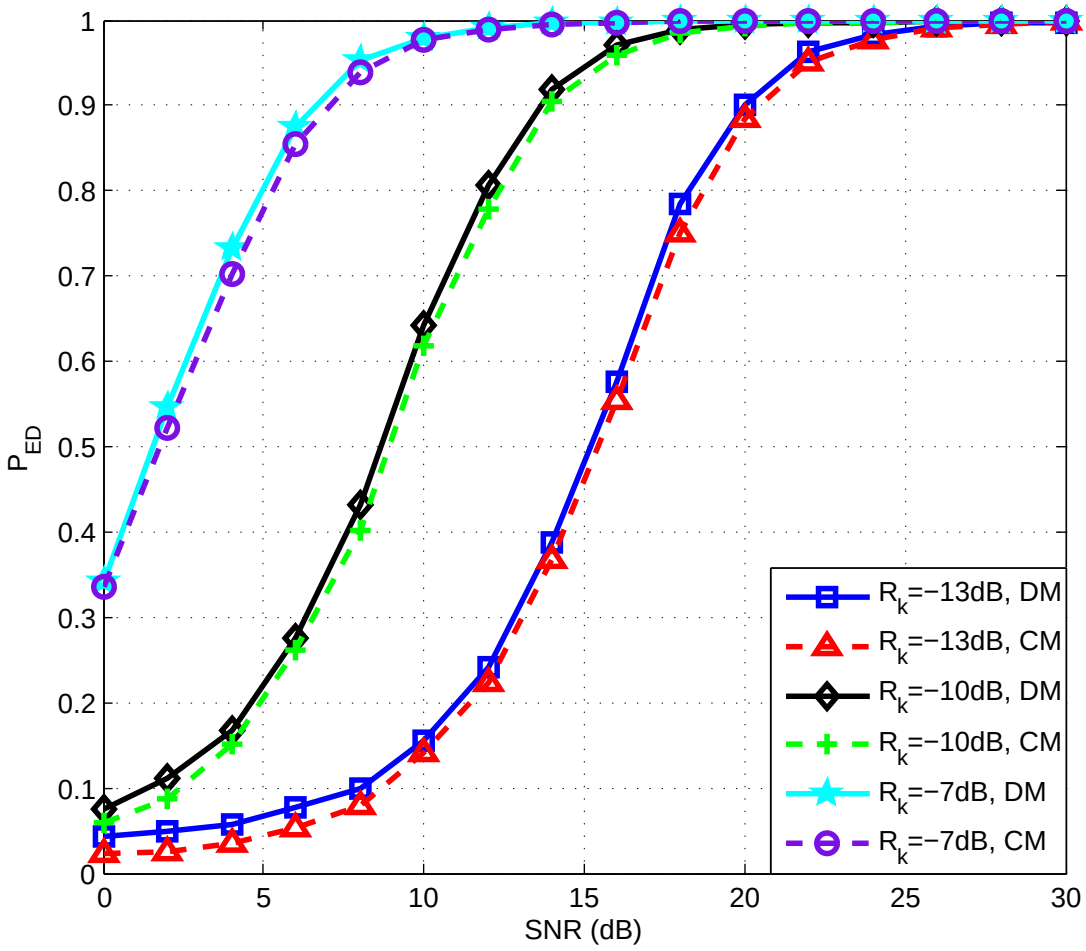


Figure 6.6: $P_{\text{ED}}$ vs. SNR under $R_k = -13$, -10, -7dB, $N_R = 5$ and $P_{\text{FA}} = 0.01$.

Using (6.34) and (6.35), the FNR of the combiner's output can be computed as

$$\gamma_3 = \frac{P_f |\sum_{k=1}^{M} w_k^* h_k|^2}{\sigma_r^2 \sum_{k=1}^{M} |w_k^*|^2}. \tag{6.36}$$

Based on Cauchy-Schwarz inequality, $\gamma_3$ can reach to the maximal value when

$$w_k = h_k. \tag{6.37}$$

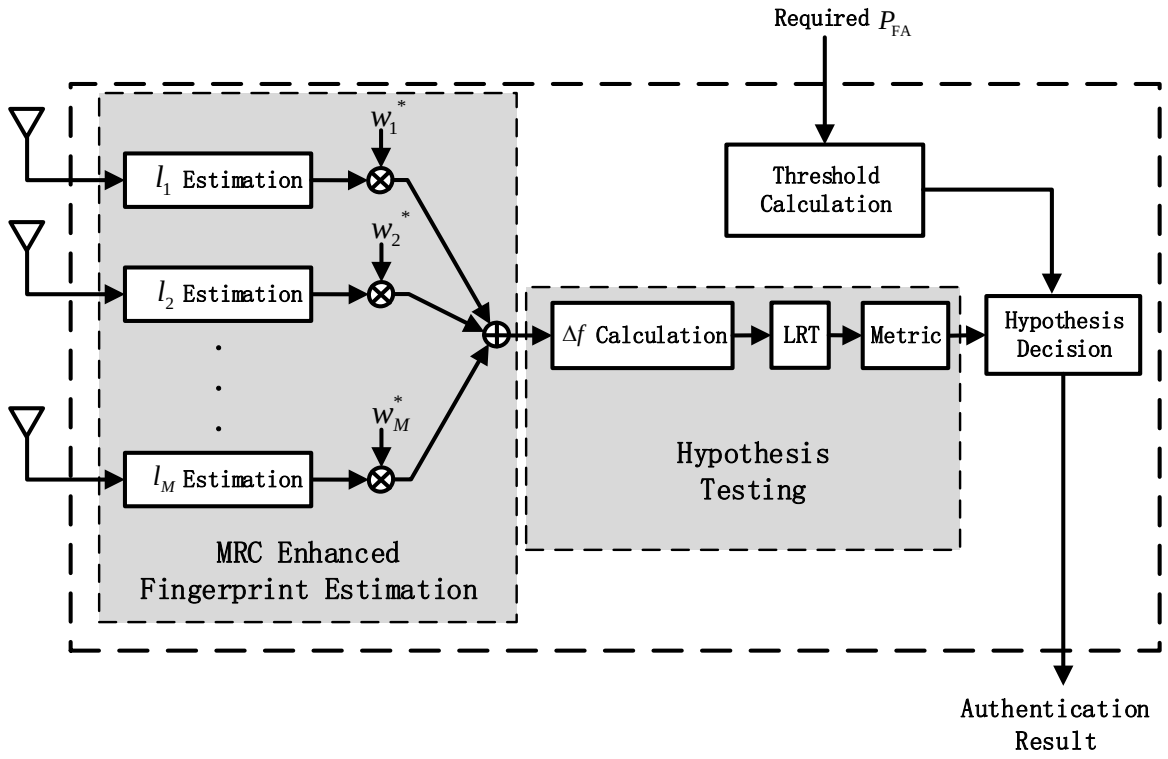


Figure 6.7: Authentication model using MRC technique.

Substituting for $w_k = h_k$ in (6.36), $\gamma_3$ can be maximized as

$$\begin{aligned}\gamma_3 &\leqslant \frac{P_f(\sum_{k=1}^{M} h_k^* h_k)^2}{\sigma_r^2(\sum_{k=1}^{M} h_k^* h_k)} \\ &= \frac{P_f \sum_{k=1}^{M} |h_k|^2}{\sigma_r^2} \\ &= \sum_{k=1}^{M} \gamma_{\mathrm{F},k}. \end{aligned} \tag{6.38}$$

From the result of (6.38), it can be seen that the value of $\gamma_3$ can maximally reach to $\sum_{k=1}^{M} \gamma_{\mathrm{F},k}$. This means that, using MRC, the FNR can increase to the sum of FNRs corresponding to all $M$ antennas. Substituting (6.37) in (6.35), the outputs of the combiner with maximized FNR can be given by

$$\mathbf{f}_{\text{MRC}} = \mathbf{f} \sum_{k=1}^{M} |h_k|^2 + \sum_{k=1}^{M} h_k^* \mathbf{n}_k. \tag{6.39}$$

After obtaining $\mathbf{f}_{\text{MRC}}$, the MRC improved device fingerprint is applied to the hypothesis testing model for fingerprint differentiation.

For representation simplicity, (6.39) is rewritten as

$$\mathbf{f}_{\text{MRC}} = \mathbf{c} + \mathbf{n}_c + j(\mathbf{d} + \mathbf{n}_d), \tag{6.40}$$

where $\mathbf{c} + j\mathbf{d} = \mathbf{f} \sum_{k=1}^{M} |h_k|^2$, $\mathbf{n}_c + j\mathbf{n}_d = \sum_{k=1}^{M} h_k^* \mathbf{n}_k$.

A validated fingerprint set $[\mathbf{f}_{v,1} \quad \mathbf{f}_{v,2} \cdots \mathbf{f}_{v,p}]^T$ is assumed in which the $i^{th}$ element can be expressed as $\mathbf{f}_{v,i} = \mathbf{c}_{v,i} + j\mathbf{d}_{v,i}$. Then, the offset between $\mathbf{f}_{\text{MRC}}$ and $\mathbf{f}_{v,i}$ can be calculated as

$$\begin{aligned} \Delta\mathbf{f} = \mathbf{f}_{\text{MRC}} - \mathbf{f}_{v,i} &= \Delta\mathbf{c} + \mathbf{n}_c + j(\Delta\mathbf{d} + \mathbf{n}_d) \\ &= \Delta\mathbf{f}_I + j\Delta\mathbf{f}_Q, \end{aligned} \tag{6.41}$$

where $\Delta\mathbf{c} = \mathbf{c} - \mathbf{c}_{v,i}$ and $\Delta\mathbf{d} = \mathbf{d} - \mathbf{d}_{v,i}$.

Therefore, a hypothesis testing can be modeled based on (6.41) as

$$\begin{cases} \mathcal{H}_0 : & ||\Delta\mathbf{c}|| = ||\Delta\mathbf{d}|| = 0 \\ \mathcal{H}_1 : & ||\Delta\mathbf{c}|| + ||\Delta\mathbf{d}|| \neq 0 \end{cases}, \tag{6.42}$$

where $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively, represent that the fingerprints $\mathbf{f}_{\text{MRC}}$ and $\mathbf{f}_{v,i}$ belong to the same transmitter or not. More specifically, different wireless transmitter must generate some difference in offsets, $\Delta\mathbf{f}$, implying that at least one of $\Delta\mathbf{c}$ and $\Delta\mathbf{d}$ are non-zero under $\mathcal{H}_1$.

From (6.41), it can be seen that, within the time of authentication, $\Delta f_{I,i}$ and $\Delta f_{Q,i}$ follow the identical distribution $N(0, \sigma^2)$ under hypothesis $\mathcal{H}_0$, where $\sigma^2 = \frac{\sum_{k=1}^{M} |h_k|^2 \sigma_r^2}{2}$; while, $\Delta f_{I,i} \sim N(\Delta c_i, \sigma^2)$ and $\Delta f_{Q,i} \sim N(\Delta d_i, \sigma^2)$ under $\mathcal{H}_1$. Consequently, we are able to separate the fingerprint into two parts and make use of them to build the two-parameter hypothesis testing.

### 6.3.2 Authentication Methods

Regarding the authentication processing, we consider applying the method used in Chapter 3 and briefly present the main results. GLRT is used to deal with the hypothesis decision problem. First, three $2N \times 1$ vectors are composed as

$$\mathbf{a} = [\Delta f_{I,1} \;\; \Delta f_{Q,1} \;\; \Delta f_{I,2} \;\; \Delta f_{Q,2} \cdots \;\; \Delta f_{I,N} \;\; \Delta f_{Q,N}]^{\mathrm{T}}$$

$$\mathbf{b} = [\Delta c_1 \;\; \Delta d_1 \;\; \Delta c_2 \;\; \Delta d_2 \cdots \Delta c_N \;\; \Delta d_N]^{\mathrm{T}}$$

$$\mathbf{w} = [n_{c,1} \;\; n_{d,1} \;\; n_{c,2} \;\; n_{d,2} \cdots n_{c,N} \;\; n_{d,N}]^{\mathrm{T}}.$$

Accordingly, we can obtain

$$\mathbf{a} = \mathbf{b} + \mathbf{w}. \tag{6.43}$$

In this case, the hypothesis testing model is equivalent to

$$\begin{cases} \mathcal{H}_0 : \;\; \mathbf{b} = 0 \\ \mathcal{H}_1 : \;\; \mathbf{b} \neq 0 \end{cases}. \tag{6.44}$$

The the maximum likelihood estimation (MLE) of $\mathbf{b}$ is used to perform the likelihood ratio test as

$$G(\mathbf{a}; \hat{\mathbf{b}}) = \frac{p(\mathbf{a}; \hat{\mathbf{b}}_{\mathcal{H}_1})}{p(\mathbf{a}; \hat{\mathbf{b}}_{\mathcal{H}_0})} > T, \tag{6.45}$$

where $\hat{\mathbf{b}}_{\mathcal{H}_0}$ and $\hat{\mathbf{b}}_{\mathcal{H}_1}$ denote the MLE of $\mathbf{b}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively.

After taking the logarithm of both sides of (6.45) and multiply the result by 2, the likelihood ratio test becomes

$$2 \ln G(\mathbf{a}; \hat{\mathbf{b}}) = \frac{\mathbf{a}^{\mathrm{T}}\mathbf{a}}{\sigma^2} > 2 \ln T = T_h. \tag{6.46}$$

Given that the sum of squares of normal random variables follows different chi-squared

distributions, it can be concluded that

$$z_h = \frac{\mathbf{a}^{\mathrm{T}}\mathbf{a}}{\sigma^2} \sim \begin{cases} \chi^2_{2N}, & \text{under } \mathcal{H}_0 \\ \chi^2_{2N}(\rho), & \text{under } \mathcal{H}_1 \end{cases}, \tag{6.47}$$

where $\chi^2_{2N}$ is the central chi-squared distribution with $2N$ degrees of freedom; while $\chi^2_{2N}(\rho)$ denotes the non-central chi-squared distribution with $2N$ degrees of freedom and non-centrality parameter $\rho$ which is defined as

$$\rho = \frac{\mathbf{b}^{\mathrm{T}}_{\mathcal{H}_1}\mathbf{b}_{\mathcal{H}_1}}{\sigma^2}.$$

The false alarm rate can be calculated as

$$\begin{aligned} P_{\mathrm{FA}} &= P\{z_h > T_h|\mathcal{H}_0\} \\ &= \int_{T_h}^{+\infty} \frac{z_h^{N-1}e^{-\frac{1}{2}z_h}}{2^N\Gamma(N)}dz_h = Q_{\chi^2_N}(T_h), \end{aligned} \tag{6.48}$$

where $Q_{\chi^2_{2N}}(\cdot)$ can be expressed as

$$Q_{\chi^2_{2N}}(T_h) = e^{-\frac{T_h}{2}} \sum_{i=0}^{N-1} \left(\frac{T_h}{2}\right)^i \frac{1}{i!}. \tag{6.49}$$

In practice, $T_h$ is obtained by solving (6.49) according to the required $P_{\mathrm{FA}}$ as $T_h = Q^{-1}_{\chi^2_{2N}}(P_{\mathrm{FA}})$. Eventually, we are able to compute $P_{\mathrm{D}}$ analytically as

$$P_{\mathrm{D}} = \int_{T_h}^{+\infty} \frac{1}{2}(\frac{z_h}{\rho})^{\frac{N-1}{2}} e^{-\frac{1}{2}(z_h+\rho)} I_{N-1}(\sqrt{z_h\rho})dz_h. \tag{6.50}$$

Accordingly, the probability of miss detection can be calculated as

$$P_{\mathrm{MD}} = 1 - P_{\mathrm{D}}. \tag{6.51}$$

### 6.3.3 Simulation Results

This physical-layer authentication system is simulated using our combining diversity enhancement technique. Regarding the device-specific fingerprint, IQI is still selected in this simula-

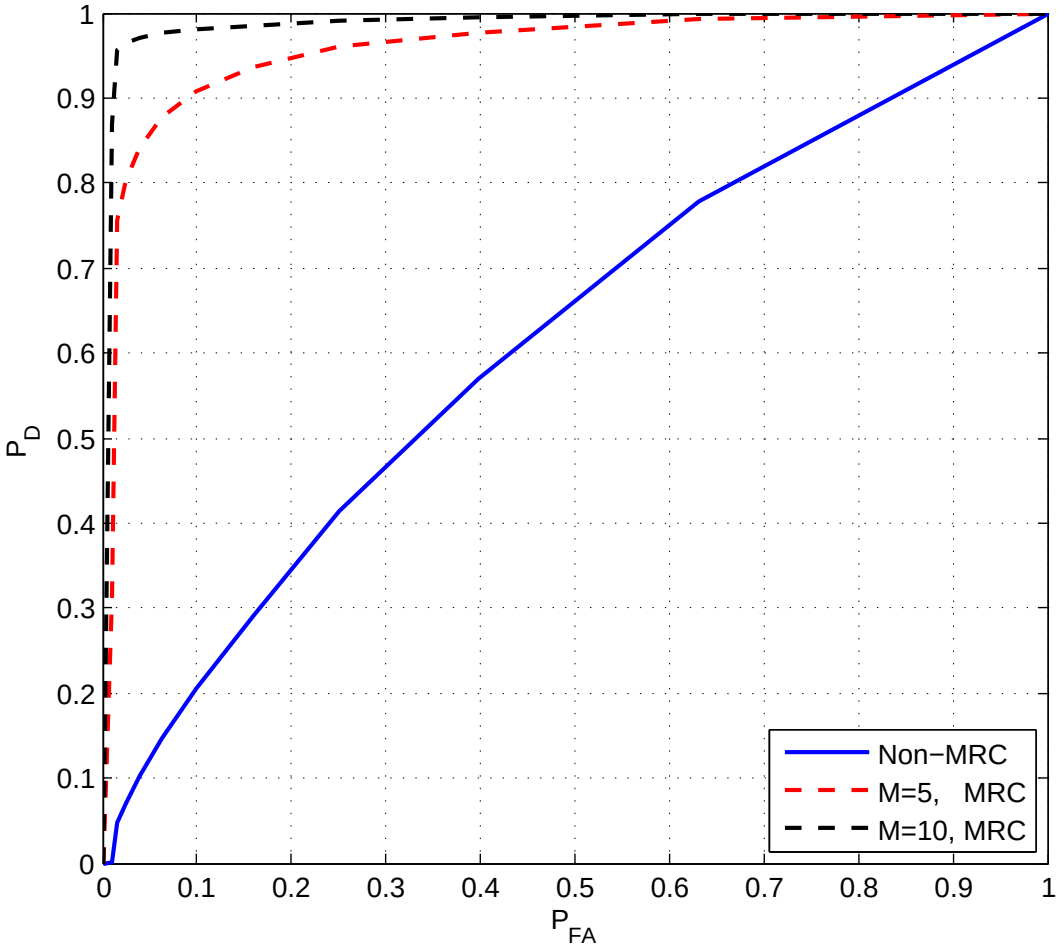


Figure 6.8: Detection probability comparison between non-MRC and MRC with different $M$.

tion. It is noteworthy that only FI IQI of the transmitter is considered. The amplitude and phase imbalances are randomly chosen from $-0.05 \sim 0.05$ and $-5^o \sim 5^o$, respectively. Different $M$ is assumed in the receiver in order to compare the detection probability of using different number of antennas. Fig. 6.8 shows the detection probability enhancement using the proposed authentication system. It can be seen that the detection probabilities of using MRC (dash line) are significantly increased compared with the probability without using MRC (solid line). Besides, the curve of 10 antennas is higher than the curve of 5 antennas as expected. This implies that more diversity gain can be obtained by using more antennas since higher FNR is achieved as shown in (6.38).

## 6.4 Summary

In this chapter, diversity techniques are exploited for the sake of improving physical-layer authentication performance. Specifically, the cooperative diversity and space diversity are applied in the authentication system design. For the former one, the collaboration of multiple receivers is proposed to increase the FNR. In this scheme, the estimated FI and FD IQI of one transmitter is compared with validated device fingerprints by using a binary hypothesis testing. Also, the distributed and centralized authentication methods are proposed to perform this hypothesis testing. Since the data processing capability is enhanced by involving multiple receiver in authentication procedure, the authentication accuracy is improved. On the other hand, the commonly used MRC technique is considered at the receiver side to increase the FNR. It is proved that the FNR under more antennas can achieve higher value, which can significantly enlarge the detection probability.

The works of this chapter can be partially found in my published papers [27]

# Chapter 7

# Cross-Layer Authentication Design in Wireless Networks

## 7.1 Introduction

Physical-layer authentication is emerging as indispensably complementary security technique to guarantee the authenticity of wireless devices. Conventionally, wireless authentication is handled above the physical-layer using key-based cryptography. Although the effectiveness of authentication techniques using pairwise key confirmation has been proven, such as shown in cryptosystem, its implementation in dynamic wireless communication networks still suffers from many problems in key management. The safe and timely symmetric key sharing in highly standardized networks comprised of a large number of mobile and heterogeneous devices is a challenging task. The high computational cost of asymmetric key algorithms generally results in severe latency in large-scale networks which may become intolerable for delay-sensitive communications. More importantly, it is still mathematically unproven that to crack the digital key is computationally infeasible by any devices [3]. In practice, equipping with more powerful processor, the devices are able to crack a digital security key in a shortened time, for example using exhaustive-search attack. However, such attacks are extremely hard to be detected mainly due to the fact that user identifications and access rights in wireless networks are approved to any devices who possess the digital keys including attackers.

Contrary to upper-layer security schemes, wireless transmitters can also be identified at

physical-layer by verifying the unique characteristics of physical communication links and devices, i.e., physical-layer authentication. Compared to digital key based authentication, the possession of specific physical-layer characteristics is directly associated with the communicating devices and the corresponding environment, which are extremely difficult to impersonate. Specifically, the channel between the legitimate transmitter and receiver is only determined by the signal propagation environment between them. The RF-AFE imperfection is a kind of inherent hardware feature, which differs from device to device. Since the communication channel and device can automatically distort transmitted signals, these physical layer attributes, which represents the identity of the current transmitter, are readily available at the receiver side for transmitter authentication. Also, the channel and device imperfection estimation and compensation techniques are basic functions of most present communications receivers. Benefited from this, physical-layer authentication can be accomplished at the receiver without introducing additional security related interaction overhead or throughput reduction to the communication link.

Although physical-layer authentication draws extensive research efforts, it is still far from practical deployment and application due to several challenges. Firstly, the integration of physical-layer authentication techniques with existing upper-layer authentication protocols and standard wireless infrastructure is one significant obstacle of applying such new authentication techniques. Secondly, the fast emerging 5th generation (5G) related techniques, such as the novel millimeter wave (mmWave) transmission, massive deployed small cells and vast heterogeneous devices, are potentially pose urgent technical problems to current physical-layer authentication schemes. Therefore, it is important to explore cross-layer authentication method with full consideration of these challenges.

This chapter is motivated to investigate cross-layer authentication for the future wireless communications. To achieve this goal, we first identify the detailed technical challenges of cross-layer assisted authentication design and 5G communications. Then, two promising directions to overcome these challenges are proposed. Specifically, the inherent physical-layer characteristics are explored for securing encryption key. This key is also used to extend the authentication from device-to-device case to end-to-end case, which is the common requirement in a communication network. In doing so, the physical-layer authentication can be effectively

integrated with existing cryptography-based infrastructures and protocols. In addition, the authentication procedure in 5G heterogeneous network is simplified and enhanced by prediction, pre-sharing and reuse of the physical layer security context.

The rest of this chapter is organized as follows. In Section 7.2, the problems of cross-layer authentication implementation are described, in which the seamless integration and complexity reduction are mainly considered. In Section 7.3, the proposed solutions to the two problems are given. In Section 7.4, the proposed methods are applied into specific case studies in order to evaluate the cross-layer authentication performance. Finally, this chapter is summarized in Section 7.5.

## 7.2 Problem Formulation

### 7.2.1 Integration with Existing Cryptographic Infrastructures and Protocols

Nowadays, a considerable portion of existing communication infrastructures are dealing with the authentication above physical-layer. Since the significant advantages of physical-layer authentication, it is well-accepted that physical-layer authentication can work as an important complement to improve the cryptographic approaches.

In cryptographic system, the encryption algorithm and key distribution (e.g., Diffe-Helman key exchange protocol) are usually used to guarantee these systems are computationally infeasible to break. Nonetheless, this authentication is always accomplished at the expense of rising the computational load and communication delay in wireless systems. Since physical-layer process is inherently faster and some existing physical-layer characteristics are device-specific, the physical-layer technique is expected to be used in the cross-layer authentication design in order to alleviate problems such as delay and high computational load of using cryptography.

However, in practical cross-layer authentication implementations, one of the most challenging tasks is to integrate the physical-layer authentication with existing infrastructures and protocols without occurring conflicts. In [18], the authors mentioned a general framework of cross-layer authentication as the future work of their research. Some of the proposed cross-

layer schemes are based on quantizing the unique physical-layer characteristics to generate a digital signature and forwarding this signature to the upper-layer for match-up verification such as used in [23]. Although the authentication is realized at upper-layer, the principle of this kind of methods and cryptography are divergent so that using it in a cryptosystem will pose additional cost and be likely to produce serious errors. In addition, since this signature is no longer associated with the physical devices, it has no difference from using regularly random numbers so that it no superior to traditional authentication methods. Thus, the seamless integration with authentication performance enhancement is highly demanded.

Another potential obstacle of the practical integration development is the end-to-end authentication extension. In large-scale wireless networks, the authentication and key exchange are always demanded devices who are not directly linked. But most of the current physical-layer authentications are confined to device-to-device authentication as they rely on the characteristics obtained from the direct communication links between the transmitter and receiver. We here take the authentication technique using channel reciprocity as an example. Due to the fast variation, the channel randomness is only temporally available in a specific pair of transmitter and receiver who are currently experiencing this channel. Also, it is extremely difficult to timely share the fast varying channel information in a vast network. As a result, this method is hard to be used in network-wide end-to-end authentication. The crux of accomplishing cross-layer end-to-end authentication is first finding proper physical-layer identities, i.e., shared secret. It is also valuable to find some proper means for upper-layers to extract and process the unique physical-layer identities to ensure that these processed physical-layer information can be used in existing cryptographic schemes. In doing so, the authentication process is not restricted at physical-layers of two direct communicating devices but could be extended to end-to-end authentication with efficient routing and management techniques.

As a summary, two key issues should be ponded to achieve effective integration. Firstly, the physical-layer characteristics selection. Since the upper-layer process as well as end-to-end communication are involved, the time of authentication procedure may be prolonged. Thus, the stable characteristics which at least keep invariant during the authentication procedure should be exploited. Secondly, the way of processing these selected characteristics is another critical concern. For example, the symmetric/asymmetric key generation algorithms using physical-

layer characteristics can be two options.

### 7.2.2 Increasing Authentication Complexity in Complicated Heterogeneous Networks

It is unquestionable that the communication is going forward to 5G phase. Along with extensive 5G technique revolutions, the communication environment is inevitably becoming more complicated. Specifically, the networks of 5G will become more heterogeneous since more diverse types of devices are expected to be served. Another feature of 5G is that the global mobile data traffic will experience a time of explosive growth from 2.5 exabytes/month of 2014 to 24.3 exabytes/month of 2019 as predicted in [97]. To meet the demand of the explosive growth of mobile data traffic, the mmWave transmission and ultra-densification techniques will be a natural choice. As a result, massive smaller cells consisting of femtocells and picocells will be employed. It is predictable that many timely challenges will emerge.

In 5G, some functions of layers may be redefined, e.g., the handoffs may not exist in layer 3 anymore [51]. Hence, to correctly determine the authenticity of various devices operating in diverse upper-layer protocols will be more difficult. Since physical-layer is essential to any devices, it is vital to consider more robust and compatible physical-layer authentication schemes with ever less dependence on particular protocols.

As the cell size is shrinking as well as the number of cells is increasing, the users, especially mobile users, have to oftentimes transfer from different BS/AP covered cells, which results in frequent authentication handover processes in such complex cellular networks. The authentication handover is traditionally based on specially designed cryptographic key and multiple handshakes such as proposed by 3GPP committee in [98]. To transfer the context, the handover has to involve multiple entities including users, APs, BSs and servers. Also, the backhaul processing and multiple handshakes for information or pairwise key exchanges between these entities are generally required. Moreover, additional encryption should be applied to insure that the important exchange is not leaked to unauthorized eavesdroppers. In practice, all of them contribute to the unwelcome latency. It is reported that this procedure takes up to hundreds of milliseconds which goes beyond the tolerance of 5G services [99].

In brief, these new authentication related problems are primarily resulted from the gradually complex communication conditions of 5G. It is believed that making use of the physical-layer characteristics can become the key point to simplify the authentication procedures in the future.

## 7.3 Proposed Solutions

### 7.3.1 Seamless Integration with Existing Protocols using Physical-Layer Security Key

This subsection aims at addressing the problems in seamless integration of the physical-layer and existing upper-layer authentication schemes. It is assumed that the Device B needs to authenticate the claimed identity of Device A, while Device A and B are in end-to-end communication scenario as shown in Fig.7.1. Device C, which can be an access point in practice, is a trusted third party of Device B that shares the direct link with A. For explanation convenience, the open systems interconnection (OSI) layer model is illustrated in this figure.

The physical layer of our design, which is at the bottom of the OSI protocol stack, plays the critical role of providing characteristics including IQI, CFO, and even antenna-specific characteristics to the upper layers. According to existing security protocols, the data link layer authentication and network layer authentication are based on the medium access control (MAC) and Internet protocol (IP) addresses verification with corresponding encryption transformation, respectively; the transport layer authentication relies on the transport layer security (TLS) adopting cryptography such as message authentication code; the most user-defined programmable authentication applications can be implemented at the application layer.

The proposed authentication framework is summarized as follows. As a benefit of direct communication with Device A, Device C becomes capable of evaluating physical-layer characteristics of A. Therefore, the Device A-specific characteristics, such as its IQI and CFO, can be quantized and hashed at Device C for generating specific digital numbers, which are suitable for further upper-layer authentication-related processing. Specifically, these physical-layer characteristic-related numbers of Device A can then be used to generate an asymmetric key for authentication purpose. It is worth noting that security key generation exploiting the

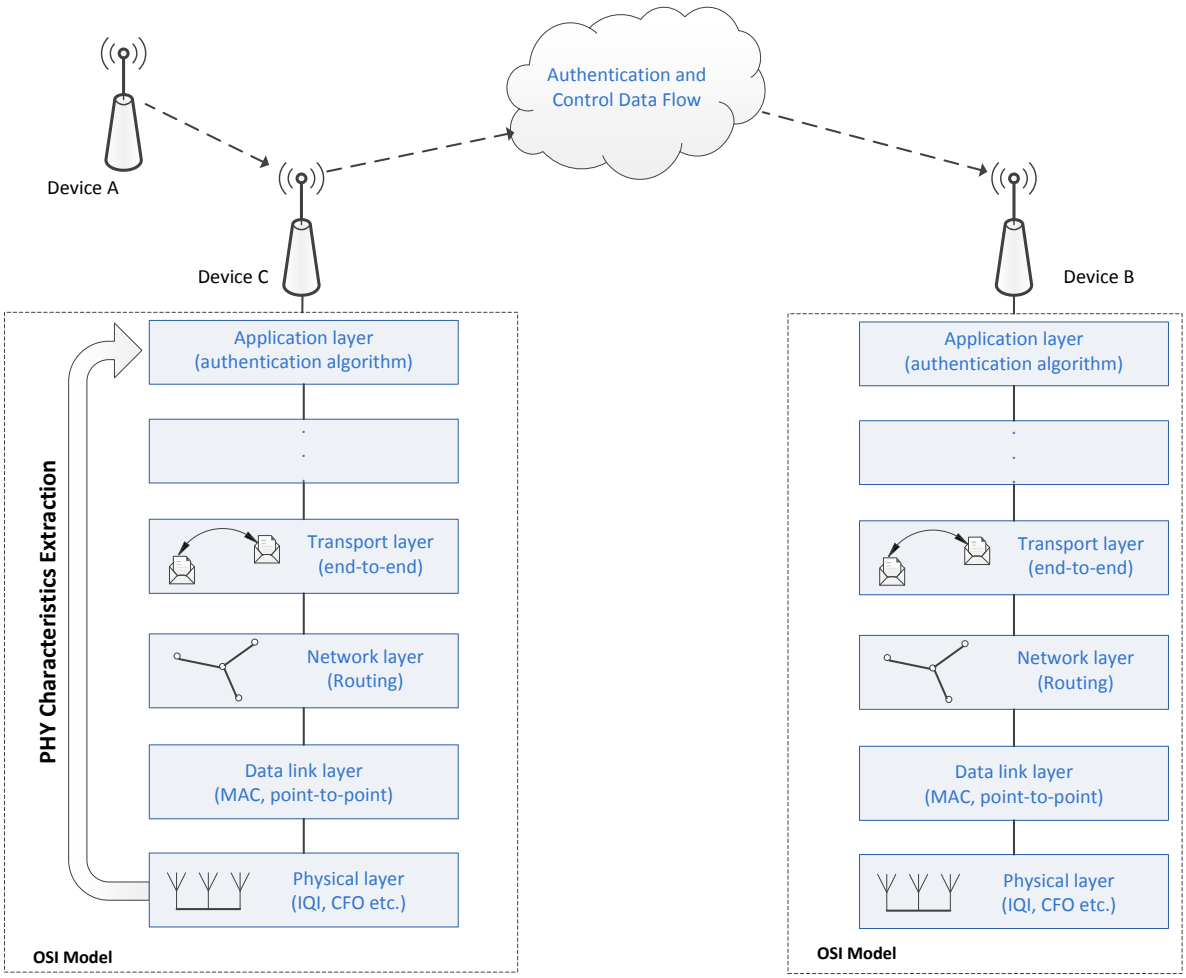


Figure 7.1: Cross-layer design for end-to-end authentication.

hardware-imperfection related attributes are usually more stable than those gleaned from the wireless channels such as argued in [100]. However, the physical-layer characteristics processing techniques - including both the quantization and key reconciliation exploited in these studies can also be considered for enhancing the performance of our authentication technique. These numbers related to Device A can be used as part of the initial input of a function for obtaining the existing public-key by Device C. Please note that, in this step, we can construct a unique mapping relation between these physical-layer characteristics-based numbers and public-key. Also, this mapping relation can be publicly known by any devices. The public-key can be shared with B with the aid of existing encryption algorithms, while the associated private key is only stored in Device A without being shared with any other devices. Basically,

Device A uses its private key to encrypt a plaintext and generate the corresponding ciphertext. Device B attempts to decrypt the ciphertext using the public key, while the authenticity of A is verified only if B is capable of decrypting readable digest, since only A owns the private key. We refer to this method as PHY-key for simplicity. Regarding the PHY-key generation, the physical-layer characteristics can be further combined with existing security key generation mechanisms for the sake of producing a composite security key, which is capable of significantly enhancing the level of wireless security by the introduction of both situation- and device-dependent factors into the key generation process.

There are two main benefits of using the PHY-key. On the one hand, the proposed method could be more efficient. Existing approaches, which directly use these physical-layer characteristics as an authentication tag, will pose additional payload at each layer's data encapsulation and cost additional bandwidth and power in delivering them to Device B. Comparatively, using these characteristics as securing key can eliminate this overhead. On the other hand, the robustness of authentication process is enhanced. Similar to the two-factor authentication strategy in which the physical possession factor and virtual password factor are checked together as a double insurance, the PHY-key are also secured by the intrinsically unforgeable feature of physical-layer characteristics and the computational intractability of asymmetric encryptions. In practice, sophisticated attacker always tries repeatedly to seek for the correct digital key, i.e., using exhaustive/brute-force search attack. However, seeking the key through frequent variation of physical-layer attributes, especially the stable hardware features, is extremely hard in practice. It is worth noting that the PHY-key based authentication could consume more time than typical physical-layer authentication since the encryption processing is inherently more time-consuming than solely physical-layer processing. However, with the utilization of PHY-key, the authentication time in handover procedure can be reduced. The details are summarized in the following subsection.

### 7.3.2 Authentication Procedure Simplification using Physical-Layer Security Information

In this subsection, we focus on simplifying the authentication complexity in the cellular communications. As illustrated in Fig.7.2, it is assumed that a user is moving between cells. To obtain the communication access and be served in the next cell, the user authentication should be first performed again which takes too much time if the handover is very frequent. We here propose the prediction, reuse and pre-sharing of the physical-layer characteristics to simplify this procedure.

While the communication environment is time-varying, the variation trend of physical-layer attributes such as direction of arrival (DOA), RSS, packet round-trip time (RTT) and CSI can be predicted based on their previous observations. This feature is able to play an important role in simplifying authentication preparation session. For example, with the predicted DOA, the authentication-oriented beams of BS or AP can accurately point to the antenna array of the intended user, which actively prevents the impersonation attacker from the highly directional communication link between the user and BS/AP. Besides, these attributes can also be used to monitor and track the real-time moving direction and position of the user. The next cell that the user will enter can be consequently predicted. The authentication server thereby is able to prepare the authentication related information (e.g., the PHY-key information) and send them to the serving AP of the next cell in advance. Once the user enters the new cell, the authentication and association request can be responded immediately by the serving AP.

Although the communication environment complexity is rising, more device-specific physical characteristics are meanwhile conceived, and many of them remain stable and/or predictable. Moreover, the authentication handover may not happen in a completely new context, implying many of the already known information of the stable and/or predictable characteristics can be reused. For example, the PHY-key has high potential to work as an unforgeable key because we involved the physical-layer factor into the key generation. In this case, some repetitive steps such as the frequently repeated pairwise key generation in the solely cryptographic authentication schemes may be reduced. Since PHY-key is also featured as unforgeable, the traditional key exchange protections using multiple handshakes and additional encryptions may

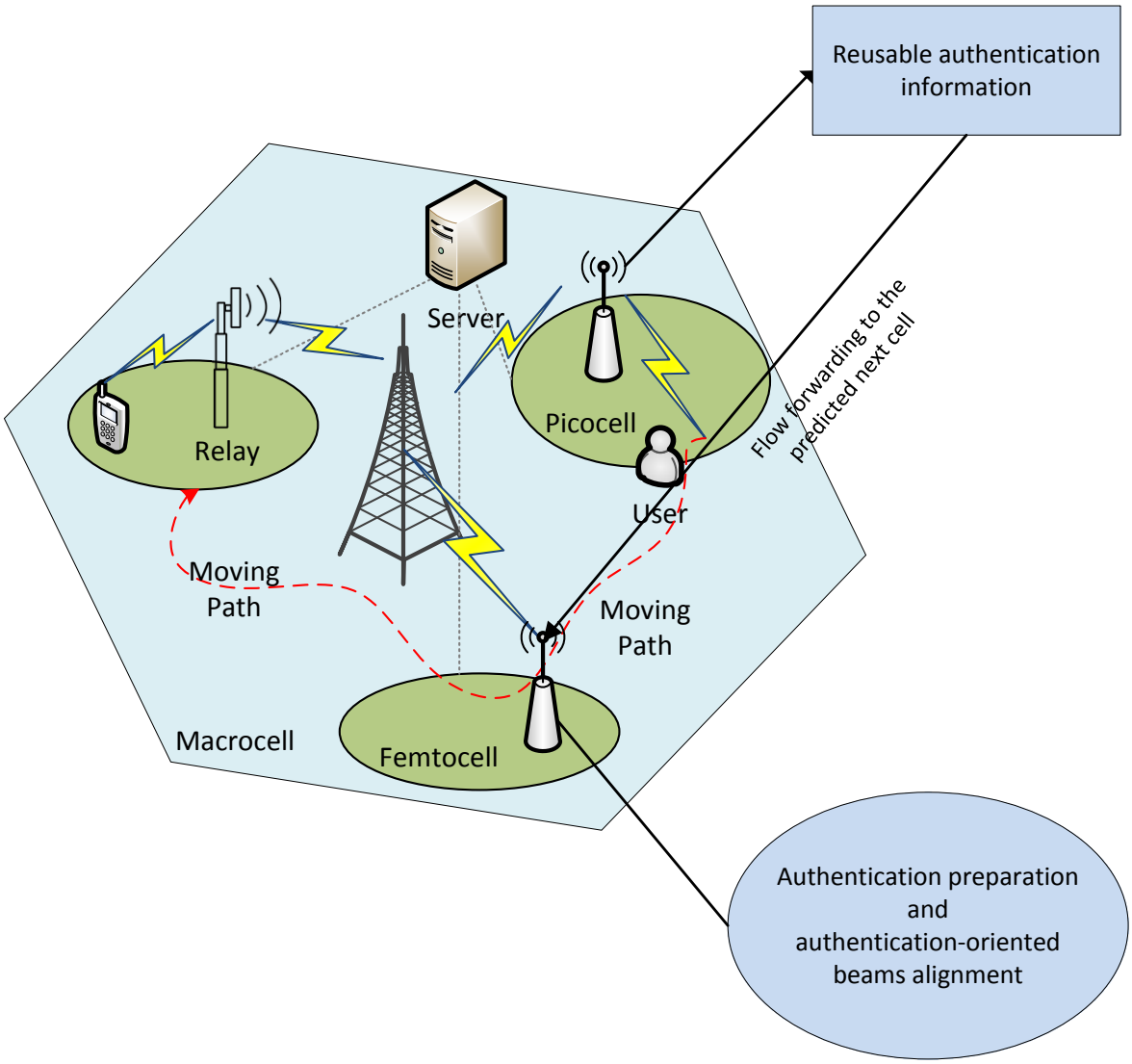


Figure 7.2: The authentication simplification with prediction and reuse of physical-layer characteristics.

even become unnecessary.

In conclusion, the prediction and pre-sharing saves the time of passive response to the authentication request and make the authentication highly directional to the intended user. With the efficient reuse strategy, the authentication can be mainly simplified in terms of the repetitive key generation and time-consuming key exchange.

## 7.4 Case Study and Evaluation

In this case study, our proposed cross-layer authentication is evaluated in terms of correct authentication probability and delay reduction performance.

The proposed PHY-key generation is first applied into the existing one-way hash digital signature scheme, whose block digram is shown in Fig.7.3. There are three entities in this system. One is the source node (S), which is also the authentication target at the same time. One is the destination node (D) who expects to verify the source's authenticity. In this system, S and D are the two ends in the end-to-end authentication implying not direct link is assumed in S and D. The third one is a trusted third party (T), which can directly communicate with S. In this authentication system, we use a pair of keys, one private-key and one public-key, i.e., asymmetric key cryptography. The generation of this key pair is carried out by existing asymmetric key algorithm, e.g., RSA. However, the public-key can also be obtained at T using a function with the device-specific fingerprint of S since T can collect the physical-layer information of S. The secrecy of this private-key can be guaranteed by asymmetric key theory. The public-key can be requested by any authorized entities, while the private-key is only kept in S. The authentication procedure can be presented in the following.

T, who is experiencing the directly link with S, first estimates the device-specific fingerprint, $f$, from the received signals. This procedure can be represented as

$$S \rightarrow T : f \tag{7.1}$$

Then, it processes the quantized estimates with hash function $H_2$ and uses the results of hash function in RSA to generate the private key $K_1$ and public-key $K_2$.

$$S \rightarrow T : (K_1(f), K_2(f)) \tag{7.2}$$

Different from traditional public-key, our $K_2$ is protected by both physical-layer and encryption factors. This public-key can be used to decrypt the signature for getting $y_2$ in D in the future.

At the side of S, S first uses one-way hash function $H_1$ to generate digest $y_1$ and signs $y_1$

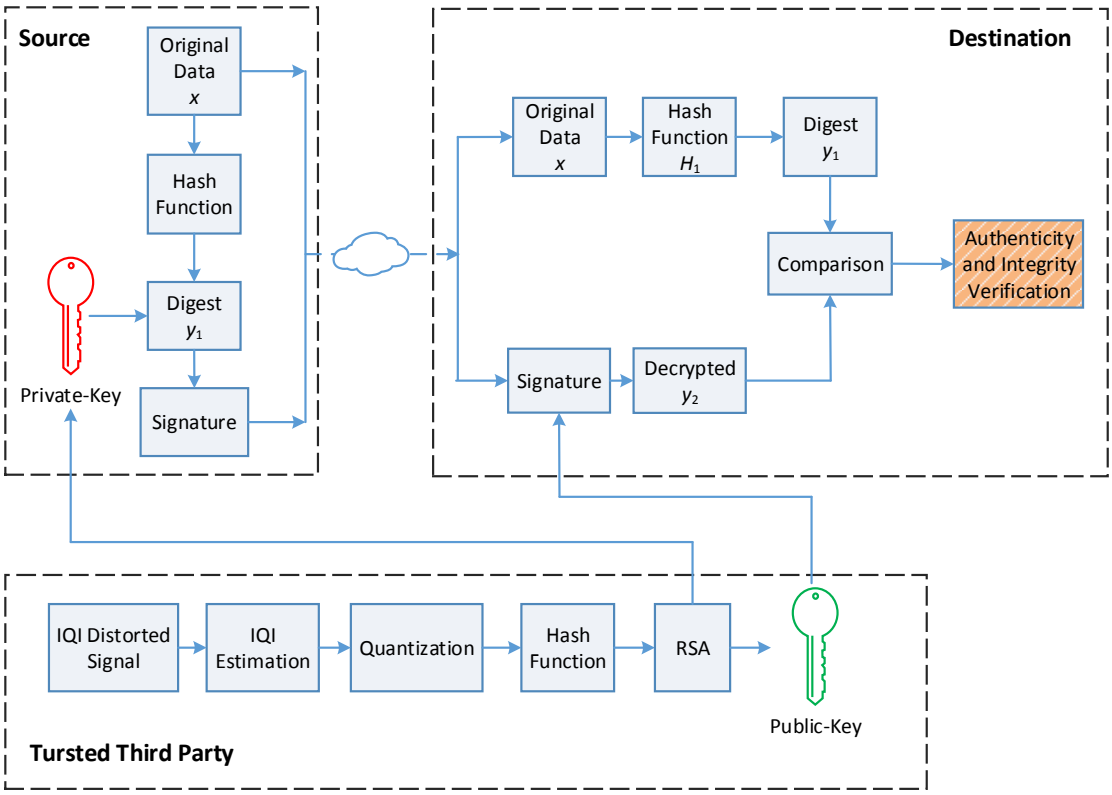


Figure 7.3: One-way hash digital signature using PHY-key generation.

with its own private key $K_1$. This procedure can be expressed as

$$S : y_1(x, H_1) \tag{7.3}$$

$$S_g(y_1, K_1), \tag{7.4}$$

where $S_g$ is the signature of S.

The original data and signature are added in a message and this message is then sent to D using the existing routing protocol. This routing is assumed to be secure, i.e., the integrity of this message is guaranteed.

After receiving, D first request public-key $K_2$ from T. Then, D uses $K_2$ to decrypt the signature and get digest $y_2$. In the meanwhile, D also processes the received $x$ with $H_1$ to obtain

digest $y_1$.

$$S \rightarrow D : y_1(x, H_1) \tag{7.5}$$

$$y_2(S_g, K_2) \tag{7.6}$$

If D can correctly decrypt the readable digest and the content of $y_1$ and $y_2$ can exactly match, the authenticity of S as well as the integrity of data can be verified. This is because only S owns the private-key which can uniquely create the validated $S_g$. In this case, the hypothesis testing can be given by

$$\begin{cases} \mathcal{H}_0 : \ y_1 = y_2 \\ \mathcal{H}_1 : \ y_1 \neq y_2 \end{cases} . \tag{7.7}$$

This authentication system is then simulated as depicted in Fig. 7.3. The commonly used MD5 and RSA algorithms are used to implement the hash function and asymmetric key algorithms, respectively. The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value. RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. Besides, the MRC is also considered in this system to improve the device-specific fingerprint estimation.

Fig. 7.4 shows the simulated correct authentication probability (CAP) vs. SNR. It can be seen that the CAP without using MRC can reach to more than 95% when SNR is larger than 15 dB. It implies a growth of about 20% in CAP compared to those physical-layer authentication method without using any enhancement techniques as shown in the figure. This result shows that, since we make use of both physical-layer and upper-layer encryption methods in the our cross-layer authentication, the higher authentication accuracy is achieved than only authenticating devices in physical layer. It is also observed that our proposed MRC technique can work well in the cross-layer system and raise the CAP. Hence, the space diversity based enhancement technique proposed in Chapter 6 is also applicable in our cross-layer design for additional performance improvement.

We also simulated the proposed authentication simplification in a handover scenario using the PHY-key, and compare its delay performance with traditional handover method. For de-

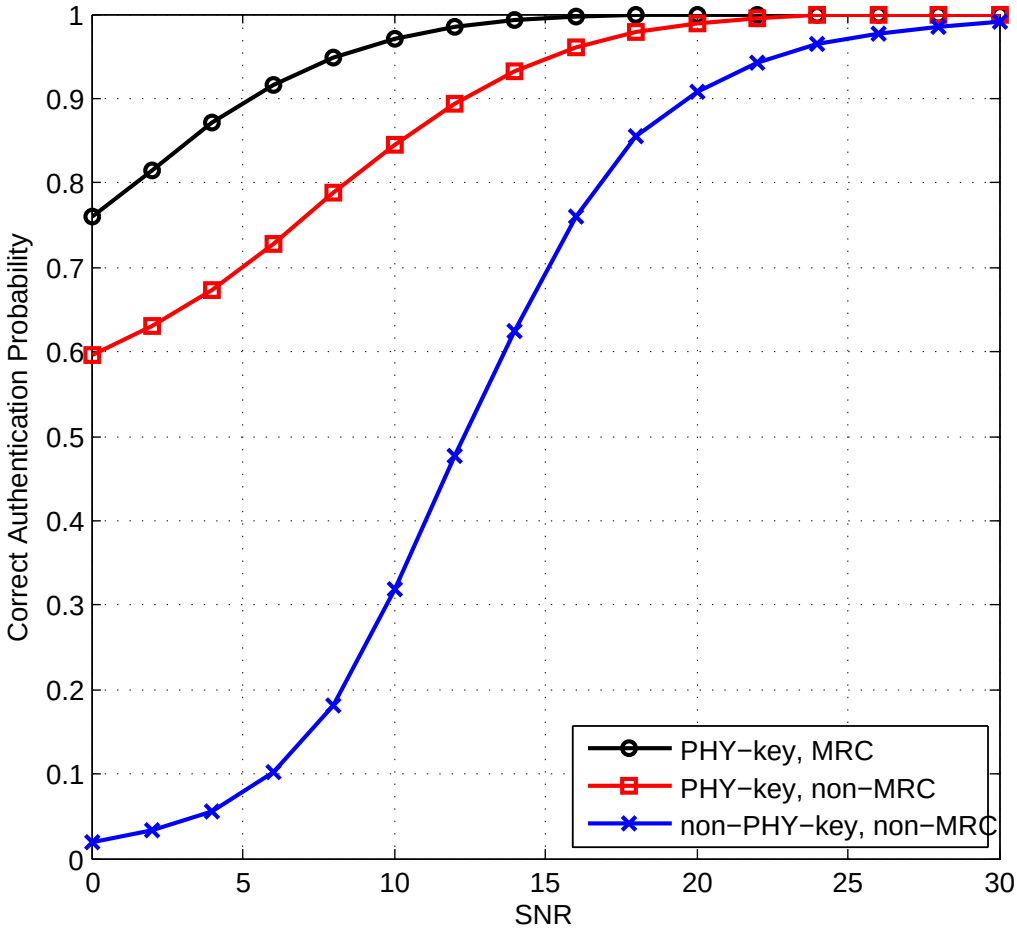


Figure 7.4: Authentication using PHY-key generation.

scription simplicity, it is assumed that a user U moves to a new cell covered by B from the cell covered by A, while A and B are severed by sever S. The identity of U has been authenticated by A, i.e., A has the information of U's identity either as a legitimate user or an impersonation attacker. We also assume a list of authorized devices ($AUTH$) and a list of attackers ($ATTK$), which are kept at A, B and S as $(AUTH, ATTK)_A$, $(AUTH, ATTK)_B$ and $(AUTH, ATTK)_S$, respectively. The lists contain the information of identity, PHY-key and some predicted directions and positions of different users. Our authentication handover procedure with the prediction and reuse of these lists is presented in Algorithm 2.

The simulation results of handover delay using Algorithm 2 and traditional method are shown in Fig.7.5. It can be seen that the delay time is increasing when network utilization rate

**Algorithm 2** PHY-key based authentication handover

1) Start of the authentication handover procedure.

2) A shares the $(AUTH, ATTK)_A$ about U to B directly or via S. B updates $(AUTH, ATTK)_B$.

3) U sends B the association request with claimed identity and signature using the above-mentioned one-way hash digital signature method.

4) B first checks $AUTH_B$. If U is in $AUTH_B$, B uses the corresponding public-key to decrypt the received signature. If it can decrypt correctly, go to step 7); if it is incorrect, go to step 5). If U is not in $AUTH_B$, go to step 5).

5) B generates PHY-key of U and checks $(ATTK)_B$. If U is in $(ATTK)_B$, go to step 7). If U is not in $(AUTH, ATTK)_B$, B sends S the PHY-key of U, then go to step 6).

6) If S decides to grant U the access, go to 7); otherwise, go to 8).

7) B grants U the access in the response, and go to 9).

8) B rejects U in the response.

9) B shares the updated $(AUTH, ATTK)_B$ about U to the next possible cell based the prediction.

10) End of authentication handover.

(NUR) becomes higher, where NUR is defined as the ratio of total packet rate and processing rate. It is also observed that the handover delay of both methods stays low if NUR is below 60%. Once the network does not have enough processing capability remaining, our simplification method shows its superiority in reducing the delay time, which is of high significance to meet the requirements of fast 5G services. Compared to the traditional method, the time is reduced as the $(AUTH, ATTK)$ of user is pre-shared using prediction at step 2) and reuse the shared information at step 4) in the proposed algorithm. Additionally, since our PHY-key is immune to mimicking, the commonly used complicated key exchange protection, e.g., multiple handshakes, may also be saved with proper design in the future.

## 7.5 Summary

This chapter focused on the study of wireless cross-layer authentication in which the physical-layer techniques and upper-layer key-based authentication are considered. We first summarized the main challenges of cross-layer authentication development in terms of the seamless integration with existing upper-layer authentication protocols and the increased authentication

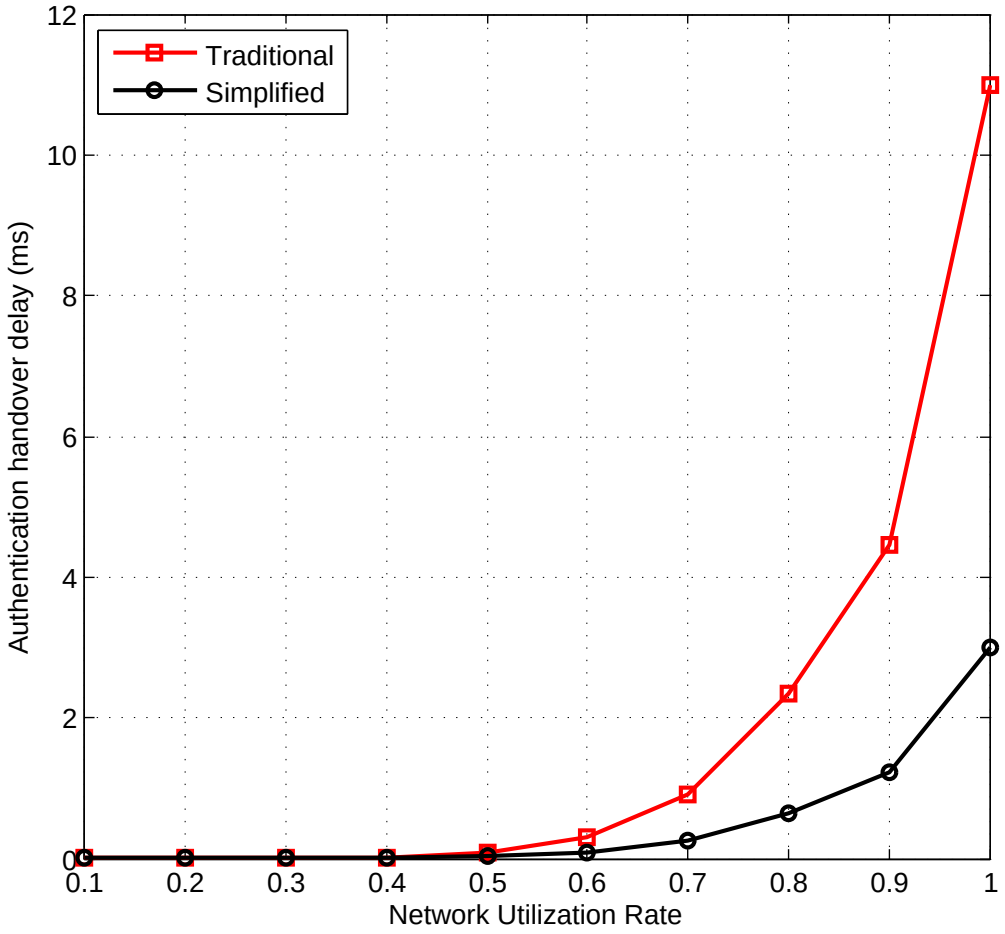


Figure 7.5: Authentication handover delay performance.

complexity problem in complex large-scale networks. Two applicable solutions are then proposed to deal with these problems. Specifically, the cross-layer aided architecture as well as PHY-key are proposed to achieve 1) the seamless integration of physical-layer authentication and cryptography schemes and 2) the simplification of authentication handover procedure. It is noteworthy that the brute-force search attack, which is the fatal weakness of traditional cryptography, can be effectively alleviated by using our PHY-key. Finally, we gave a case study and the corresponding evaluation results showed that the proposed cross-layer authentication system outperforms the traditional authentication in increasing the correct authentication probability and reducing authentication latency.

Honestly speaking, the development of applicable cross-layer design and the network-wide

end-to-end authentication based on layered OSI protocol are still in their infancy. Again, the key point is how to make use of the abundant physical-layer characteristics to complement and enhance the existing upper-layer authentication schemes. Besides, the overwhelming new 5G techniques will bring sharp impacts to current physical-layer authentication, but simultaneously provide more new characteristics for enhancing and simplifying authentication in such a complex communication environment.

# Chapter 8

# Conclusions and Future Works

## 8.1 Conclusions

Since impersonation is a critical attacking method for illegally gaining the access to wireless communication network, wireless device authentication becomes an indispensable security technique to prevent such sophisticated impersonation attackers. Traditional authentication is accomplished above the physical layer. It is vulnerable to identity-based attacks, suffering from high computational complexity and many key management related problems. In light of this, physical-layer authentication, as an effective complement to the upper-layer scheme, is emerging to combat against impersonation attackers for securing wireless communications. This dissertation carries out a comprehensive study on physical-layer authentication related techniques with emphasis on 1) exploring applicable physical-layer authentication method for a special case where the existing upper-layer methods are ineffective, 2) enhancing physical-layer authentication performance, 3) designing cross-layer authentication system.

The contributions of this dissertation in terms of these three aspects are summarized as follows.

***Physical-layer amplify-and-forward relay identification***

In Chapter 3, it is pointed out that the major technical challenge in authenticating AF relay nodes is that all well-defined upper-layer authentication protocol are useless. Therefore, effective physical-layer authentication solutions are are urgently demanded in AF relay scenario. After analyzing the specific working principle of AF relay, it is found that IQI characteristic is a

suitable choice for identifying AF relay nodes. The device fingerprint of AF relay is generated using IQI and wireless channel attributes. Using this device fingerprint, two AF relays can be differentiated with satisfactory accuracy under relatively high SNR condition.

Chapter 4 focuses on investigating optimal AF relay identification scheme. Given the fact that IQI estimation and compensation techniques are basics at most present wireless receivers for improving signal reception, we propose directly using the results of IQI estimation in AF relay identification to avoid the additional fingerprint generation procedure. Benefiting from this method, the authentication performance, especially in low SNR regime, is significantly improved mainly because the unstable factor of wireless link is reduced compared with the method of Chapter 3. Considering that a cooperative system usually consists of multiple relays, the corresponding identification algorithm is proposed to identify multiple AF relays with small IQI values. In addition, the optimal training signal is designed for QAM and PSK modulations to maximize the capability of detecting and tracing the attackers with fixed IQI values. Two more robust suboptimal methods are further proposed and their performances are sufficiently close to the optimal signals. The simulation results validate our comprehensive AF relay identification system and show high correct identification rate even in the case of low SNR and minor IQI.

***Physical-layer authentication enhancement techniques***

Physical-layer authentication is improved in two aspects in this dissertation. First, the device fingerprinting can be enhanced by involving multiple unique physical-layer characteristics. Second, the fingerprint differentiation accuracy can be enhanced using diversity techniques of wireless communications.

In Chapter 5, the multiple wireless channel related attributes and device-specific characteristics are considered in fingerprinting wireless transmitters. Firstly, the IEEE 802.11 WiFi devices are authenticated through verifying PER and RSS. Since both attributes are conveniently accessible in most WiFi platforms without complicated processing, e.g., additional estimation, our authentication system is easy to implement. Besides, more general authentication method using multiple RF-AFE imperfection related characteristics is studied in this chapter. Without loss of generality, a number of $N$ characteristics are considered in the authentication model. A weighted combination of these $N$ characteristics is used in order to achieve higher

authentication accuracy. The optimal weights for each selected characteristics are derived. The theoretical and simulation results are provided to validate the authentication enhancement using multi-characteristics.

Diversity technique is exploited in Chapter 6 as the second method to enhance the reliability of physical-layer authentication. Specifically, the cooperative diversity in the form of using the collaboration of multiple receivers is proposed in an authenticate system. The basic idea is fully making use of the more powerful computation capacity of multiple receivers and gaining better performance in authentication processing. Two processing methods, which are distributed and centralized methods, are proposed in this study. The simulation results show that, by involving in multi-receivers collaboration, the detection probability is increased. In addition, the combining diversity is considered in a receiver with multiple antennas for device authentication. This method aims at increasing the fingerprint-to-noise-ratio through optimal signal combining. The effectiveness of using maximal-ratio combining, which is one of the most commonly used combining strategies, is validated. It is worth noting that the enhancement techniques proposed in Chapter 5 and 6 can also be applied in AF relay authentications which are proposed in Chapter 3 and 4.

***Cross-layer authentication system design in wireless networks***

Chapter 7 mainly focuses on solving the problems in cross-layer authentication implementations. The integration with existing cryptographic infrastructures and protocols as well as the gradually increasing authentication complexity are pointed out as two emerging problems at first. To be specific, as the physical-layer and upper-layer processing are different, the seamless integration of two layers' techniques without any conflict occurring is the first concern. Another concern is the end-to-end authentication extension. Different from the physical-layer authentication, the direct link related characteristics between two authentication ends are usually unavailable in a large-scale network. It is pointed out that the proper physical-layer fingerprint selection and key generation methods play the key role in solving this problem. In addition, due to the more complex 5G communication environment, the authentication processing is becoming more frequent and complicated which will result in intolerable communication latency.

Two effective solutions are then proposed in this chapter. First, the physical-layer key (PHY-key) is proposed, which is suitable for the end-to-end authentication scenario. Using this

PHY-key, the exhaustive-search attack can be effectively mitigated. Second, authentication simplification based on the prediction, pre-sharing and reuse of the physical-layer characteristics is proposed. The two proposed techniques are applied in the case of one-way hash digital signature case and the case of authentication handover in cellular communications, respectively, to evaluate the cross-layer authentication performance. The simulation results show higher correct authentication probability and reduced handover delay as the advantages of using the proposed methods.

## 8.2 Future Works

The contributions presented in this dissertation can be extended and explored to some new related topics as follows.

- In the proposed AF relay identification system, the IQI is considered as the device-specific fingerprint. As discussed in the working principle of AF relaying, the down/up conversions are necessary in the signal relaying. This procedure can inevitably produce some other errors, such as frequency offset, which can be used together with IQI to identify AF relays in physical layer. Furthermore, since the signal distortion from RF-AFE imperfections of AF relays can be accumulated in multiple hops in practice. This feature may be used to identify multiple AF relays in one authentication processing instead of only identifying one AF relay as studied in this dissertation. It is believed that the identification time can be reduced as there is no need to identify the AF relay nodes one by one.

- The multi-characteristics device fingerprinting and diversity techniques are considered as two effective methods to enhance the physical-layer authentication in two separate aspects. In this case, the comprehensive physical-layer authentication system with the consideration of all these enhancement techniques can be further designed. For examples, the optimal characteristics selection and combination in fingerprint generation and the combining diversity enhanced fingerprint differentiation can be used together.

- The authentication simplification is studied in this dissertation to reduce the gradually

increasing authentication complexity in 5G communication networks. However, the 5G related techniques can have some other impacts to existing authentication. For instance, current impacts of RF-AFE imperfections will become severe due to the higher frequency transmission. Since massive MIMO technique will be employed in 5G, the current device-specific characteristic is supposed to become even antenna-specific/RF chain-specific. This new feature can be exploited to identify devices in the future, especially in 5G.

# Bibliography


[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[2] R. Kissel, "Glossary of key information security terms," *National Institute of Standards and Technology*, pp. 1–218, May 2013.

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

[4] A. Polak, S. Dolatshahi, and D. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1469–1479, Aug. 2011.

[5] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channelss," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[6] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Mar. 2010.

[7] W. Hou, X. Wang, and J.-Y. Chouinard, "Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates," in *Proc. IEEE Int. Conf. on Communications (ICC)*, Jun. 2012, pp. 3559 – 3563.

[8] P. Hao, X. Wang, and A. Behnad, "Relay authentication by exploiting I/Q imbalance in amplify-and-forward system," in *Proc. IEEE Conf. on Global Commun. (GLOBECOM)*, Dec. 2014, pp. 613–618.

[9] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 2, pp. 198 – 212, Jun. 2007.

[10] J. R. Douceur, "The Sybil attack," in *Proc. the First International Workshop on Peer-to-Peer Systems*, 2002, pp. 251 – 260.

[11] B. Schneier, "Cryptographic design vulnerabilities," *IEEE Computer*, vol. 31, no. 9, pp. 26–33, 1998.

[12] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656 – 715, Oct. 1949.

[13] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355 – 1387, May 1975.

[14] G. J. Simmons, "Authentication theory/coding theory," in *Proc. Advances in Cryptology*, vol. 196, Aug. 1984, pp. 411 – 431.

[15] L. Lai, H. E. Gamal, and H. V. Poor, "Authentication over noisy channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 906– 916, Feb. 2009.

[16] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1350 – 1356, Jun. 2000.

[17] K. Talbot, P. Duley, and M. Hyatt, "Specific emitter identification and verification," *Technology Review Jounal*, pp. 113 – 133, 2003.

[18] 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.

[19] 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. on Communications (ICC)*, Jun. 2007, pp. 4646 – 4651.

[20] S. Misra, A. Ghosh, A. S. P., and M. S. Obaidat, "Detection of identity-based attacks in wireless sensor networks using signalprints," in *Proc. IEEE/ACM Int. Conf. on Cyber, Physical and Social Computing (CPSCom)*, Dec. 2010, pp. 35 – 41.

[21] H. Wen, P.-H. Ho, C. Qi, and G. Gong, "Physical layer assisted authentication for distributed ad hoc wireless sensor networks," *IET Information Security*, vol. 4, no. 4, pp. 390 – 396, Dec. 2010.

[22] B. Narasimhan, D. Wang, S. Narayanan, H. Minn, and N. Al-Dhahir, "Digital compensation of frequency-dependent joint Tx/Rx I/Q imbalance in OFDM systems under high mobility," *IEEE J. Sel. Topics Signal Process.*, vol. 3, no. 3, pp. 405 – 417, Jan. 2009.

[23] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. ACM Int. Conf. on Mobile Computing and Networking (MobiCom)*, Sep. 2008, pp. 116–127.

[24] P. Rykaczewski, M. Valkama, and M. Renfors, "On the connection of I/Q imbalance and channel equalization in direct-conversion transceivers," *IEEE Trans. Veh. Technol.*, vol. 57, no. 3, pp. 1630 – 1636, May 2008.

[25] N. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric Bayesian method," in *Proc. IEEE Int. Conf. on Computer Commun. (INFOCOM)*, Apr. 2011, pp. 1404–1412.

[26] H. Li, X. Wang, and Y. Zou, "Exploiting transmitter I/Q imbalance for estimating the number of active users," in *Proc. IEEE Conf. on Global Commun. (GLOBECOM)*, Dec. 2013, pp. 3318–3322.

[27] P. Hao, X. Wang, and A. Behnad, "Performance enhancement of I/Q imbalance based wireless device authentication through collaboration of multiple receivers," in *Proc. IEEE Int. Conf. on Communications (ICC)*, Jun. 2014, pp. 939 – 944.

[28] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Trans. Mobile Comput.*, vol. 9, no. 3, pp. 449 – 462, Mar. 2013.

[29] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Proc. IEEE Symposium on VLSI Circuits*, Jun. 2004, pp. 176 – 179.

[30] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. ACM/IEEE Design Automation Conference*, Jun. 2007, pp. 9 – 14.

[31] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of secure watermark-based authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 43 – 55, Mar. 2006.

[32] C. Fei, R. H. Kwong, and D. Kundur, "A hypothesis testing approach to semifragile watermark-based authentication," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 2, pp. 179 – 192, Mar. 2009.

[33] S. Kay, *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*. Prentice Hall, 1998.

[34] V. Aggarwal, L. Lai, A. R. Calderbank, and H. V. Poor, "Wiretap channel type II with an active eavesdropper," in *Proc. IEEE Int. Symposium on Information Theory*, Jun. 2009, pp. 1944 – 1948.

[35] P. Yu, J. Baras, and B. Sadleru, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[36] 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 Int. Conf. on Communications (ICC)*, Jun. 2011, pp. 1 – 5.

[37] 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 Commun.*, vol. 29, no. 2, pp. 431 – 442, Feb. 2011.

[38] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. IEEE Int. Conf. on Communications (ICC)*, May 2008, pp. 1520 – 1524.

[39] L. Xiao, L. J. Greenstein, 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.

[40] F. J. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE Int. Conf. on Communications (ICC)*, Jun. 2013, pp. 4724 – 4728.

[41] 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, May 2014.

[42] V. Bhargava and M. L. Sichitiu, "Physical authentication through localization in wireless local area networks," in *Proc. IEEE Conf. on Global Commun. (GLOBECOM)*, Dec. 2005, pp. 2658 – 2662.

[43] 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, Apr. 2014.

[44] Y. Shi and M. Jensen, "Improved radiometric identification of wireless devices using MIMO transmission," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1346–1354, Dec. 2011.

[45] P. Martin, M. Roman, and P. Jitka, "Wireless device authentication through transmitter imperfections measurement and classification," in *Proc. IEEE Symp. on Personal, Indoor, and Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 497–501.

[46] M. M. Rashid, E. Hossain, and V. K. Bhargava, "Cross-layer analysis of downlink v-blast mimo transmission exploiting multiuser diversity," *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4568 – 4579, Dec. 2009.

[47] K. H. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. on Sensor Networks, Ubiquitous, and Trustworthy Computing*, vol. 1, Jun. 2006.

[48] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," *IEEE Personal Commun. Mag.*, vol. 1, no. 1, pp. 25–31, 1st Qtr 1994.

[49] L. Venkatraman and D. P. Agrawal, "A novel authentication scheme for ad hoc networks," in *Proc. IEEE Int. Conf. on Wireless Communications and Networking Conference*, 2000, pp. 1268 – 1273.

[50] "IEEE draft standard for local and metropolitan area networks part 15.4: Low rate wireless personal area networks (LR-WPANs) amendment: Physical layer (PHY) specifications for low data rate wireless smart metering utility networks," *IEEE P802.15.4g/D5*, 2011.

[51] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065 – 1082, Jun. 2014.

[52] T. Halevi, H. Li, D. Ma, N. Saxena, J. Voris, and T. Xiang, "Context-aware defenses to RFID unauthorized reading and relay attacks," *IEEE Trans. Emerging Topics in Computing*, vol. 1, no. 2, pp. 307–318, Dec. 2013.

[53] Y. Mao and M. Wu, "Security issues in cooperative communications: Tracing adversarial relays," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing(ICASSP)*, vol. IV, May 2006, pp. 69–72.

[54] K. H. Kim, "Analysis of security vulnerability and authentication mechanism in cooperative wireless networks," *Springer IT Convergence and Services*, vol. 107, pp. 3–11, Nov. 2011.

[55] E.-K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 46–52, Aug. 2012.

[56] 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.

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

[58] C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, "Wavelet fingerprinting of radio-frequency identification (RFID) tags," *IEEE Trans. Ind. Electron.*, vol. 59, no. 12, pp. 4843–4850, Dec. 2012.

[59] J. Zhou, J. Shi, and X. Qu, "Landmark placement for wireless localization in rectangular-shaped industrial facilities," *IEEE Trans. Veh. Technol.*, vol. 59, no. 6, pp. 3081–3090, Jul. 2010.

[60] P. Murphy, A. Sabharwal, and B. Aazhang, "On building a cooperative communication system: Testbed implementation and first results," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, Jun. 2009.

[61] M. Mokhtar, A. Gomaa, and N. Al-Dhahir, "OFDM AF relaying under I/Q imbalance: Performance analysis and baseband compensation," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1304–1313, Apr. 2013.

[62] Y. Yao and X. Dong, "Multiple CFO mitigation in amplify-and-forward cooperative OFDM transmission," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3844 – 3854, Dec. 2012.

[63] J. Li, M. Matthaiou, and T. Svensson, "I/Q imbalance in AF dual-hop relaying: Performance analysis in Nakagami-*m* fading," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 836–847, Feb. 2014.

[64] ——, "I/Q imbalance in two-way AF relaying," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2271–2285, Jul. 2014.

[65] ——, "I/Q imbalance in two-way AF relaying: Power allocation and performance analysis," in *Proc. IEEE Int. Conf. on Communications (ICC)*, Jun. 2014, pp. 5042 – 5048.

[66] ——, "I/Q imbalance in two-way AF relaying: Performance analysis and detection mode switch," in *Proc. IEEE Conf. on Global Commun. (GLOBECOM)*, Dec. 2014, pp. 4001 – 4007.

[67] T. Rappaport, R. H. Jr, R. Daniels, and J. Murdock, *Millimeter Wave Wireless Communications*. Pearson Education, 2014.

[68] K.-Y. Sung and C. C. Chao, "Estimation and compensation of I/Q imbalance in OFDM direct-conversion receivers," *IEEE J. Sel. Topics Signal Process.*, vol. 3, no. 3, pp. 438–453, Jun. 2009.

[69] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*. Dover Publications, 1970.

[70] F. Horlin and A. Bourdoux, *Digital Compensation for Analog Front-Ends*. Wiley, 2008.

[71] M. Mokhtar, A.-A. A. Boulogeorgos, G. K. Karagiannidis, and N. Al-Dhahir, "OFDM opportunistic relaying under joint Transmit/Receive I/Q imbalance," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1458–1468, May 2014.

[72] W. Hou and M. Jiang, "Enhanced joint channel and IQ imbalance parameter estimation for mobile communications," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1392–1395, Jul. 2013.

[73] Y. Chung and S. Phoong, "Channel estimation in the presence of transmitter and receiver I/Q mismatches for OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4476–4479, Sep. 2009.

[74] A. Peressini, F. Sullivan, and J. Uhl, *The mathematics of nonlinear programming*. New York : Springer-Verlag, 1988.

[75] R. Horn and C. Johnson, *Matrix Analysis*. Cambridge University Press, 1990.

[76] S. Kenneth, *Complex stochastic processes: An introduction to theory and application*. Addison-Wesley Pub. Co., 1974.

[77] C. Helstrom, *Statistical Theory of Signal Detection, 2nd edition*. New York Pergamon, 1968.

[78] G. Chandrasekaran, J. Francisco, V. Ganapathy, M. Gruteser, and W. Trappe, "Detecting identity spoofs in IEEE 802.11e wireless networks," in *Proc. IEEE Conf. on Global Commun. (GLOBECOM)*, Nov. 2009, pp. 1–6.

[79] Y. Sun, A. Baricz, and S. Zhou, "On the monotonicity, log-concavity, and tight bounds of the generalized Marcum and Nuttall Q-functions," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1166–1186, Mar. 2010.

[80] F. He, H. Man, D. Kivanc, and B. McNair, "EPSON: Enhanced physical security in OFDM networks," in *Proc. IEEE Int. Conf. on Communications (ICC)*, Jun. 2009, pp. 1–5.

[81] F. He, W. Wang, and H. Man, "REAM: RAKE receiver enhanced authentication method," in *Proc. MILITARY COMMUNICATIONS CONFERENCE*, Oct. 2010, pp. 2205 – 2210.

[82] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. MILITARY COMMUNICATIONS CONFERENCE*, Nov. 2011, pp. 538 – 542.

[83] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in *Proc. IEEE Int. Symposium on World of Wireless, Mobile and Multimedia Networks*, Jun. 2006, pp. 566 – 570.

[84] J. H. Lee and R. M. Buehrer, "Characterization and detection of location spoofing attacks," *IEEE Journal of Communications and Networks*, vol. 14, no. 4, pp. 396 – 409, Aug. 2012.

[85] P. Hao and X. Wang, "Performance enhanced wireless device authentication using multiple weighted device-specific characteristics," in *IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP)*, Jul. 2015, pp. 438 – 442.

[86] P. Hao, X. Wang, and A. Refaey, "An enhanced cross-layer authentication mechanism for wireless communications based on PER and RSSI," in *Proc. IEEE Canadian Workshop on Information Theory (CWIT)*, Jun. 2013, pp. 44 – 48.

[87] M. Kim, Y. Maruichi, and J. ichi Takada, "Parametric method of frequency-dependent I/Q imbalance compensation for wideband quadrature modulator," *IEEE Trans. Microw. Theory Tech.*, vol. 61, no. 1, pp. 270 – 280, Jan. 2013.

[88] O. Ozdemir, R. Hamila, and N. Al-Dhahir, "I/Q imbalance in multiple beamforming OFDM transceivers: SINR analysis and digital baseband compensation," *IEEE Trans. Commun.*, vol. 61, no. 5, pp. 1914 – 1925, May 2013.

[89] P.-I. Mak, S.-P. U, and R. P. Martins, "Transceiver architecture selection: Review, state-of-the-art survey and case study," *IEEE Circuits Syst. Mag.*, vol. 7, no. 2, pp. 6–25, Sep. 2007.

[90] D. Tandur and M. Moonen, "Joint compensation of OFDM frequency selective transmitter and receiver IQ imbalance," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing(ICASSP)*, Apr. 2007, pp. 81 – 83.

[91] X. Cai, Y.-C. Wu, H. Lin, and K. Yamashita, "Estimation and compensation of CFO and I/Q imbalance in OFDM systems under timing ambiguity," *IEEE Trans. Veh. Technol.*, vol. 60, no. 3, pp. 1200 – 1205, Mar. 2011.

[92] J. Luo, A. Kortke, W. Keusgen, and M. Valkama, "Efficient estimation and pilot-free online re-calibration of I/Q imbalance in broadband direct-conversion transmitters," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2506 – 2520, Jul. 2014.

[93] L. Anttila, M. Valkama, and M. Renfors, "Frequency-selective I/Q mismatch calibration of wideband direct-conversion transmitters," *IEEE Trans. Circuits Syst. II*, vol. 55, no. 4, pp. 359 – 363, Apr. 2008.

[94] Y. Tsai, C.-P. Yen, and X. Wang, "Blind frequency-dependent I/Q imbalance compensation for direct-conversion receivers," *IEEE Trans. Wireless Commun.*, vol. 9, no. 6, pp. 1976 – 1986, Jun. 2010.

[95] R. Rodriguez-Avila, G. Nunez-Vega, R. Parra-Michel, and A. Mendez-Vazquez, "Frequency-selective joint Tx/Rx I/Q imbalance estimation using golay complementary sequences," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2171 – 2179, May 2013.

[96] B. Narasimhan, S. Narayanan, H. Minn, and N. Al-Dhahir, "Reduced-complexity baseband compensation of joint Tx/Rx I/Q imbalance in mobile MIMO-OFDM," *IEEE Trans. Wireless Commun.*, vol. 9, no. 5, pp. 1720 – 1728, May 2010.

[97] "Cisco visual networking index: Global mobile data traffic forecast update, 20142019," *CISCO, White Paper*, 2015.

[98] "Generation partnership project; technical specification group service and system aspects; 3GPP system architecture evolution (SAE); security architecture (release 11), 2012." *3GPP TS 33.401 version 11.5.0 Release 11*, pp. 1 – 123, Oct. 2012.

[99] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 48 – 53, Jan. 2012.

[100] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33 – 39, Jun. 2015.

# Curriculum Vitae

| | |
|---|---|
| **Name:** | Peng Hao |
| **Post-Secondary Education and Degrees:** | The University of Western Ontario<br>London, ON, Canada<br>2011 - date Ph.D. candidate<br><br>Shandong University<br>Jinan, Shandong, P.R. China<br>2008 - 2011 M.E.Sc.<br><br>Qingdao University<br>Qingdao, Shandong, P.R. China<br>2004 - 2008 B.E.Sc. (Hons) |
| **Related Work Experience:** | Teaching Assistant<br>The University of Western Ontario<br><br>Research Assistant<br>The University of Western Ontario |

**Publications:**

1. P. Hao, X. Wang, and A. Refaey, "An Enhanced Cross-Layer Authentication Mechanism for Wireless Communications Based on PER and RSSI," *in Proc. IEEE Canadian Workshop on Information Theory (CWIT)*, Jun. 2013, pp.44-48.

2. P. Hao, X. Wang, and A. Behnad, "Performance Enhancement of I/Q Imbalance Based Wireless Device Authentication Through Collaboration of Multiple Receivers," *in Proc. IEEE International Conference on Communications (ICC)*, Jun. 2014, pp.945-950.

3. P. Hao, X. Wang, and A. Behnad, "Relay Authentication by Exploiting I/Q Imbalance in Amplify-and-Forward System," *in Proc. IEEE Conference on Global Communications (Globecom)*, Dec. 2014, pp.613-618.

4. P. Hao and X. Wang, "Performance Enhanced Wireless Device Authentication using Multiple Weighted Device-Specific Characteristics," *in Proc. IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP)*, Jul. 2015, pp.438-442.

5. X. Wang, P. Hao and Lajos Hanzo, "Physical-Layer Authentication for Wireless Security Enhancement: Current Challenges and Future Development," *IEEE Communications Magazine under minor revision*, Jul. 2015.

6. P. Hao, A. Behnad and X. Wang, "A Novel Cross-Layer Authentication Based on Exploiting CFO, I/Q Imbalance and Interference in Wireless Communications," *to be Submitted to IEEE Journal of Selected Topics in Signal Processing*.

7. P. Hao, A. Behnad and X. Wang, "Enhanced Amplify-and-Forward Relay Identification using I/Q Imbalance Based Device Fingerprinting," *Submitted to IEEE Transactions on Information Forensics and Security*.