

July 2019

Wireless Physical Layer Design for Confidentiality and Authentication

Tao Wang

University of South Florida, smiling_tao@hotmail.com

Follow this and additional works at: <https://scholarcommons.usf.edu/etd>



Part of the [Computer Sciences Commons](#)

Scholar Commons Citation

Wang, Tao, "Wireless Physical Layer Design for Confidentiality and Authentication" (2019). *Graduate Theses and Dissertations*.

<https://scholarcommons.usf.edu/etd/7985>

This Dissertation is brought to you for free and open access by the Graduate School at Scholar Commons. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Scholar Commons. For more information, please contact scholarcommons@usf.edu.

Wireless Physical Layer Design for Confidentiality and Authentication

by

Tao Wang

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy in Computer Science and Engineering
Department of Computer Science and Engineering
College of Engineering
University of South Florida

Major Professor: Yao Liu, Ph.D.
Jay Ligatti, Ph.D.
Xinming Ou, Ph.D.
Huseyin Arslan, Ph.D.
Lei Zhang, Ph.D.

Date of Approval:
June 12, 2019

Keywords: Pinpoint waveforming, Far proximity identification, USRP, Channel state information

Copyright © 2019, Tao Wang

ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor Dr. Yao Liu for her continuous support of my Ph.D study, for her patience, motivation, and immense knowledge. She is super nice, and her guidance helped me in all the time of my research and writing of this dissertation. I am very fortunate to have her as my advisor.

I would like to thank all my committee members, Dr. Jay Ligatti, Dr. Xinming (Simon) Ou, Dr. Huseyin Arslan, and Dr. Lei Zhang, for their time and efforts reviewing and discussing my research. I would also like to thank Dr. Zhuo Lu for his insightful comments and encouragement on my research. Besides, I would like to express my gratitude for the support of the National Science Foundation (NSF).

Thank you to my lab-mates with whom I've had the opportunity to work, and talk. They are Tao Hou, Song Fang, Dakun Shen, Zi Li, Yan Albright, Cagri Cetin, Xiaoshan Wang, Chengbin Hu, Ahmad Alagil, Abed Alanazi, Jean Baptists Subils and Shamaria Engram.

Last but not the least, I would like to give my special thanks to my parents and my partner for their love, support and encouragement throughout my PhD study and my life.

TABLE OF CONTENTS

LIST OF TABLES	iv
LIST OF FIGURES	v
ABSTRACT	vii
CHAPTER 1 INTRODUCTION	1
1.1 Location-restricted Service Access Control	2
1.2 Far Proximity Identification in Wireless Systems	6
1.3 Summary of Contributions	9
1.4 Dissertation Roadmap	10
CHAPTER 2 LOCATION-RESTRICTED SERVICE ACCESS CONTROL	11
2.1 Synchronization	11
2.1.1 Clock and Propagation Synchronization	12
2.1.2 Channel Synchronization	12
2.1.2.1 Signal Modulation	13
2.1.2.2 Basic Channel Synchronization	14
2.1.2.3 Refined Channel Synchronization	16
2.2 Multipath Channel Calibration	17
2.2.1 Preliminary	18
2.2.2 Advanced Channel Calibration	19
2.2.2.1 Obtaining Calibrate Symbols	19
2.2.2.2 Reducing Channel Estimation Errors	21
2.3 Jamming Entanglement	21
2.4 Tolerable Time Shift	22
2.4.1 Impact of the Time Shift on SNR	22
2.4.2 Impact of the Time Shift on Jamming Signals	24
2.5 Service Area Size	26
2.5.1 Channel Uncorrelation Property	26
2.5.2 Power Attenuation by the Channel Uncorrelation	27
2.5.3 Power Attenuation of Multiple Transmitters	29
2.5.3.1 Impact of SNR on Service Area Size	31
2.5.4 Security Discussion	32
2.6 Multi-user Mode	34

2.6.1	CDMA Integrated Pinpoint Waveforming	34
2.6.2	TDMA Integrated Pinpoint Waveforming	35
2.6.3	FDMA Integrated Pinpoint Waveforming	36
2.7	Performance Evaluation	37
2.7.1	System Design	37
2.7.2	Example Pinpoint Service	38
2.7.3	Evaluation Metrics	39
2.7.4	Measuring Channel Cross-decorrelation	40
2.7.4.1	Cross and Auto-variance	41
2.7.4.2	Channel Cross-decorrelation	42
2.7.5	Jamming Signal Entanglement	43
2.7.6	Service Area Size	45
2.7.6.1	Impact of Distance	45
2.7.6.2	Impact of Central Frequency	46
2.7.6.3	Impact of Signal to Jamming Power Ratio	47
2.7.7	Pinpoint Accuracy	48
2.8	Related Work	49
2.9	Summary	49
CHAPTER 3	FAR PROXIMITY IDENTIFICATION IN WIRELESS SYSTEMS	51
3.1	System and Threat Models	51
3.2	Far Proximity Verification	52
3.2.1	Proximity Fingerprints	53
3.2.1.1	Key Features of Proximity Fingerprints	55
3.2.1.2	Impact of Directional Antennas	56
3.2.1.3	Proximity Fingerprint with Single or Many Peaks	57
3.2.2	Far Proximity Identification Using Proximity Fingerprints	57
3.2.2.1	Outdoor Signal Propagation	59
3.2.2.2	Indoor Signal Propagation	61
3.2.2.3	Far Proximity Identification	61
3.2.2.4	Fine-grained Proximity Identification	63
3.2.2.5	Choosing α	65
3.2.2.6	Experimental Examples	66
3.2.3	System Design	68
3.2.3.1	Dealing with the Wireless Uncertainty	69
3.2.4	Implication	70
3.3	Attacks and Countermeasures	71
3.3.1	Dealing with Jam-and-replay Attacks	72
3.3.1.1	Attack Methodology	72
3.3.1.2	Defense Approach	72
3.3.2	Dealing with Flipping Attacks	73
3.3.2.1	Attack Methodology	73

3.3.2.2	Defense Approach	75
3.3.3	Dealing with Spoofing Attacks	78
3.3.3.1	Attack Methodology	78
3.3.3.2	Defense Approach	79
3.3.4	Impact of a Cloned Prover	80
3.4	Experimental Evaluation	80
3.4.1	Experiment Setup	81
3.4.1.1	Data Set	81
3.4.1.2	Evaluation Metrics	82
3.4.2	Experiment Results	83
3.4.2.1	Proximity Fingerprint vs. Distance	83
3.4.2.2	Error Rate vs. Pathloss	84
3.4.2.3	Error Rate vs. Distance	85
3.4.2.4	Tightness of the Proximity Bound	87
3.4.2.5	Experiment for a Longer Distance Scenario	88
3.5	Related Work	89
3.5.1	Distance Bounding Protocols	89
3.5.2	Close Proximity Identification	90
3.5.3	CSI Based Distance Tracking Scheme	91
3.6	Summary	92
CHAPTER 4	FUTURE WORK	93
4.1	Light-weight Encryption Schemes	93
4.2	Security Evaluation on Current Third-party Script over the Internet	94
CHAPTER 5	CONCLUSION	95
REFERENCES		96
APPENDIX A:	COPYRIGHT PERMISSIONS	102

LIST OF TABLES

Table 2.1	Impact of the distance	46
Table 2.2	Impact of the central frequency (1.2Ghz)	47
Table 2.3	Impact of the power ratio of desired signal to jamming signal (ratio = 0.5)	47
Table 2.4	Pinpoint accuracy	48

LIST OF FIGURES

Figure 1.1	Constructive interference of two waves.	4
Figure 1.2	A naive idea	4
Figure 2.1	Without channel synchronization	13
Figure 2.2	With channel synchronization	13
Figure 2.3	Basic channel synchronization	15
Figure 2.4	Refined channel synchronization against the multipath effect	17
Figure 2.5	Received pictures at different positions	38
Figure 2.6	USRP 1	41
Figure 2.7	USRP 2	41
Figure 2.8	Distribution of different variance	42
Figure 2.9	Floor plan: Service area size	43
Figure 2.10	Floor plan: pinpoint accuracy	43
Figure 2.11	Jamming signal entanglement	44
Figure 3.1	An example of the multipath effect	54
Figure 3.2	An example of the real-measured channel impulse response obtained from the CRAWDAD data set	63
Figure 3.3	The estimated lower bound of the proximity as a function of the proximity fingerprint f	66
Figure 3.4	Estimated lower bound v.s. the real distance regarding different path loss exponent α	67
Figure 3.5	Example of flipping attacks: the mixed channel impulse response reflects proximity features of both the transmitter A and B	74
Figure 3.6	Channel impulse response measured in normal scenario	76

Figure 3.7	Channel impulse response measured in the scenario of flipping attacks	76
Figure 3.8	Relationship between the distance and the proximity fingerprint	84
Figure 3.9	Error rate as a function of pathloss exponent α	84
Figure 3.10	Error rate as a function of various distances in the LoS scenario	85
Figure 3.11	Error rate as a function of various distances in the NLoS scenario	85
Figure 3.12	The empirical CDF curves of the tightness	87
Figure 3.13	Empirical CDF of tightness with a distance of 50 meters	87

ABSTRACT

As various of wireless techniques have been proposed to achieve fast and efficient data communication, it's becoming increasingly important to protect wireless communications from being undermined by adversaries. A secure and reliable wireless physical layer design is essential and critical to build a solid foundation for upper layer applications. This dissertation present two works that explore the physical layer features to secure wireless communications towards the data confidentiality and user authentication.

The first work builds a reliable wireless communication system to enforce the location restricted service access control. In particular, the work proposes a novel technique named pinpoint waveforming to deliver the services to users at eligible locations only. The second work develops a secure far proximity identification approach that can determine whether a remote device is far away, thus preventing potential spoofing attacks in long-haul wireless communications. This dissertation lastly describes some future work efforts, designing a light-weight encryption scheme to facilitate sensitive data encryption for applications which cannot support expensive cryptography encryption operations such as IoT devices.

CHAPTER 1

INTRODUCTION

In the past decades, wireless techniques have been remarkably evolved, and pervasively adopted in our daily life and critical applications. Therefore, it is becoming increasingly important to design defense approaches to protect emerging wireless techniques from being undermined by adversaries. Unlike traditional communication, a wireless device can communicate with any other device within its power range [1]. This makes wireless communication vulnerable to multiple potential attacks: (1) Eavesdropping becomes one of the major security problems to wireless systems, because any devices within the power range of a wireless transmitter can receive the signal from this transmitter through the open public air; (2) Attackers may also attempt to intercept, jam or even manipulate the transmitted signals to take over the communication between the transmitter and receiver and further launch spoofing attacks.

This dissertation presents two works that renovate the wireless physical layer design towards improvement of the aforementioned security issues. As the physical layer is the first and fundamental layer underlying the higher level functions in the computer networking, a secure and reliable wireless physical layer design is critical and essential to provide a solid foundation to facilitate the implementation of upper layer applications. The first work builds a reliable wireless communication system to enforce the location restricted service access control, so as to preserve the confidentiality of the data traffic against eavesdropping attacks. The second work develops a secure far proximity identification approach that can determine whether a remote device is far away, thus preventing potential spoofing attacks in long-haul wireless communications.

1.1 Location-restricted Service Access Control

As the rapid development of wireless technologies, it is highly desirable to enforce location-oriented service access control that provides wireless services to users at eligible locations only. For example,

- To focus limited resources on legitimate customers, restaurants and coffee shops may offer internet access to wireless users only when they are sitting at tables.
- Companies may allow wireless network access only to employees working in select office cubicles, in order to comply export control policies.
- In wireless surveillance system, the monitor cameras may need to deliver their video streams to specific users at specific locations, e.g, personnel in the security control room, to reduce the privacy leakage.

Surprisingly, existing techniques fail to achieve this goal in a secure and efficient manner. We discuss existing techniques and their shortcomings below.

- User account control: The service access control can be achieved by creating individual accounts for each user, where a user can obtain the wireless service by providing a correct username and password. However, this may be insufficient for secure access control to location-oriented services, as a user might share account information with friends. This method also requires active account administration which is impractical for location-oriented services with high turnover such as in the restaurant example.
- MAC address binding: MAC address binding is a variant of the user account control. A wireless router allows the access of wireless users only when they have valid Media Access Control (MAC) addresses. Nevertheless, the users may share their MAC addresses with others who are not at the desired locations.

- Beamforming techniques: Beamforming techniques (e.g., [2, 3]) use antenna arrays for directional signal transmission or reception. These techniques may be utilized to send the service data to the wireless users at the specified directions, but again they cannot enable the location-oriented service access control, because all other wireless users are able to receive the service data as long as they reside in the signal coverage range of the antenna arrays.
- Localization plus encryption: Service providers may use existing localization algorithms like time-of-arrival (TOA) and angle-of-arrival (AOA) to find the locations of wireless users, and encrypt the service data so that users at target locations can use appropriate keys to decrypt it. However, cryptographic encryption may cause a significant latency, and thus fail to support common services like high-speed downloading and online video watching. Also, like the password case, with compromised cryptographic keys, undesired receivers at other locations can still obtain the service.

In this work, we would like to develop a novel and practical wireless system that achieves the aforementioned location-oriented service access control to support emerging wireless technologies. Our basic idea is to leverage the effect of *constructive interference* as shown in Figure 1.1. The crests of two identical waves meet at the same point, and then both waves form a new wave with the same shape but the magnitude is boosted to twice of that of an individual wave.

This observation inspires us to propose a new wireless system that pinpoints wireless services to users at eligible locations only. Intuitively, we can set up a naive system as illustrated in Figure 1.2. The service provider concurrently sends identical service packets (e.g., down-link internet data) using two (or more) transmitters. Assume an ideal synchronization algorithm is in use and these packets arrive at the receiver at the service location simultane-

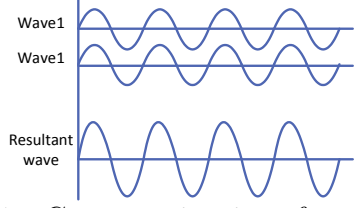


Figure 1.1: Constructive interference of two waves.



Figure 1.2: A naive idea

ously. Thus, they constructively interfere with each other to form a boosted received packet whose magnitude is twice of that of an individual packet.

In practice, a small time shift among the packet arrival times may exist due to synchronization imperfections. At the service location, such a time shift should be less than a certain threshold, so that the constructive interference still exists and the receiver is able to decode the received packet. To prevent leaking the service to undesired wireless receivers, including receivers close to the service provider, an intuitive way is to transmit at a weak power so that receivers at undesired locations (where the constructive interference vanishes) will experience a low signal-to-noise ratio (SNR), and hence a high bit error rate that retards the correct decoding of the received messages. At the desired location (where the constructive interference happens), the receiver obtains a boosted SNR that enables the correct message decoding.

However, how to select an appropriate signal transmit power becomes a challenging question. If the transmit power is too small, the constructive interference may not incur enough power to allow the receivers at the service location to correctly decode the received data. On the other hand, if the transmit power is too large, receivers outside of the service location may recognize the signal and thus can decode the received data. To avoid the difficulty of determining the transmit power, we propose to entangle the original transmit signals by jamming signals, so that the jamming signals can significantly reduce the SNR at the undesired receivers but cancel each other at the desired receiver to cause no impact.

Specifically, for a pair of transmitters T_1 and T_2 , we generate a pair of jamming signals j_1 and j_2 , where j_1 and j_2 are of the opposite phase (i.e., $j_1 = -j_2$). The transmitter T_1 then adds the jamming signal j_1 to its transmit signal. Similarly, T_2 adds the jamming signal j_2 to its transmit signal. Finally, T_1 and T_2 send $s + j_1$ and $s + j_2$ to the wireless channel respectively, where s is the original signal to be sent by both transmitters. At the service location, due to the constructive interference, the original signal s boosts, but the jamming signals j_1 and j_2 cancel each other (they are of opposite phase). At other locations where constructive interference vanishes, j_1 and j_2 do not cancel each other, and instead they serve as jamming signals to decrease the SNR at receivers at these locations. Consequently, the receivers will experience a service of bad quality.

We point out that in an ideal free space propagation environment, constructive interference of the electromagnetic wave occurs whenever the phase difference between the waves is a multiple of a half period. This means that there exist multiple locations, where the constructive interference may happen. However, in a practical wireless environment, because wireless channels are uncorrelated every a half wavelength, the original transmit signals sent by different transmitters may experience different channel distortions when they propagate to the receiver. Therefore, at the locations where the constructive interference should happen, signals received from different transmitters show different shapes due to the distortion and thus achieve a poor constructive interference. To solve this problem and pinpoint the service to the desired location only, we propose a channel synchronization technique that compensates the channel distortion at the desired constructive interference location, so that received signals exhibit the same wave shape when they arrive at this location. The channel synchronization technique is customized for the desired location only. For other constructive interference locations, the arrived signals still show different shapes, thereby yielding the same low SNR as other non constructive interference locations as proved in Section 2.5.2.

We name the proposed system as the *pinpoint waveforming* system. Figure 1.2 is a naive example of this system. Nevertheless, to transform this naive system to a real-world system, non-trivial effort should be done to answer the following basic questions:

- Synchronization: How can the system achieve propagation synchronization, so that signals sent by multiple transmitters can arrive at the service location concurrently? Moreover, how can we achieve the aforementioned channel synchronization?
- Tolerable time shift: Signals sent by transmitters are expected to arrive at the desired receiver simultaneously to form the constructive interference, but in practice a small time shift among them might exist due to the processing delay and synchronization imperfections. What is the tolerable time shift that can still enable the constructive interference at the desired receiver?
- Service area size: The service area is defined as the neighborhood area, within which the constructive interference happens and a receiver can receive the service data with a good quality. It should be hard for receivers outside of the service area to obtain the service data. To ensure the accurate service access control, a critical question is how large the service area is.

1.2 Far Proximity Identification in Wireless Systems

As mobile platforms are more and more pervasive and adopted in critical applications, it is becoming increasingly important to measure the physical proximity of mobile devices in a secure way. For example, Implantable Medical Devices (IMDs) like pacemakers may grant access to an external control device only when that device is close enough [4]. As another example, contactless-payment systems (like Google Wallet), which enable users to make payments by placing a mobile device in the close proximity of a payment terminal,

may require the mobile devices to be within several centimeters or even millimeters of the payment terminals.

Thus, verifying the *close proximity* has triggered significant attention and activity from the research community, and multiple techniques have been proposed to achieve the efficient identification of close proximity (e.g., [5, 6, 7, 8, 9, 10, 11]), including the well-known distance bounding protocols and their variants (e.g., [8, 9, 10]).

Although various techniques have been developed to identify whether a device is close, the problem of identifying the *far proximity* (i.e., a target is at least a certain distance away) has been neglected by the research community. Meanwhile, verifying the far proximity is desirable and critical to enhance the security of emerging wireless applications. By enforcing far proximity, in addition to traditional access control and cryptographic approaches, we can enhance the security of various critical wireless applications, such as satellite communication, long-haul wireless TV, radio, and alarm broadcasting, and Marine VHF radio for rescue and communication services [12].

For example, GPS devices receive signals, presumably from satellites in space, to determine their locations. Ideally, the GPS devices could verify that received signals are from far-away sources, to avoid being deceived by a nearby adversary's signals. In cellular networks, mobile phones may at times expect to receive signals from particular cell towers. It has been demonstrated that adversaries can set up a fake short-range cell tower to fool nearby mobile phones [13, 14]. To avoid being deceived by such a fake cell tower, it is desirable that mobile phones can authenticate that the signals they receive originate from a tower at an expected, further distance away.

Existing close proximity identification techniques (e.g., [5, 6, 7]) qualitatively decide whether or not a target is nearby, but they cannot be directly extended to address the far proximity identification problem. The qualitative decision that a target is not nearby

doesn't quantitatively guarantee that the target is at least a certain distance away (i.e., in the far proximity).

Distance bounding protocols (e.g., [8, 9, 10]) demonstrated their success in quantitatively estimating the distance between two wireless devices. However, they cannot be directly applied to enforce far proximity identification. In distance bounding protocols, a local device sends a challenge to a remote device, and the remote device replies with a response that is computed as a function of the received challenge. The local device then measures the round-trip time between sending its challenge and receiving the response, subtracts the processing delay from the round-trip time, and uses the result to calculate the distance between itself and the remote device. However, by delaying its response to a challenge, a dishonest remote device can appear to be arbitrarily further from the local device than it actually is.

In this paper, we develop a secure far proximity identification approach that can determine whether a remote device is far away. The key idea of the proposed approach is to estimate the proximity from the unforgeable "fingerprint" of the proximity. We develop a technique that can extract the fingerprint of a wireless device's proximity from the physical-layer features of signals sent by the device (i.e. channel impulse response). Since channel estimation is mandatory for all wireless systems to achieve reliable communications, mobile devices can easily extract a proximity fingerprint from an estimated channel impulse response. The proximity fingerprints are closely related to the distance between the local and remote devices. They are easy to extract but difficult to forge. We also develop a novel technique that uses the proximity fingerprint to identify the lower bound of the distance between the local and the remote devices. We further propose a fine-grained proximity identification algorithm and derive both lower and upper bounds of the proximity between the local and the remote devices. Besides, we identify typical types of attacks against proposed schemes and propose the corresponding defense approaches.

1.3 Summary of Contributions

The contributions of the dissertation are summarized herein:

- Location-restricted Service Access Control towards Wireless Communications: (1) We propose the concept of pinpoint entanglement, which exploits the constructive interference to enable the location-oriented service access control; (2) We propose to entangle the original signals by specifically designed jamming signals to significantly reduce the SNR at undesired receivers for the service exclusiveness; (3) We demonstrate the feasibility of the proposed pinpoint entanglement system by answering the two essential concerns about the tolerable time shift and the service area size; (4) We implement a prototype of pinpoint entanglement system on top of the Universal Software Radio Peripherals (USRPs), and evaluate the performance of the prototype system through comprehensive experiments. Our results show that the receiver obtains a high throughput that ranges between 0.90 and 0.93 when it is at the desired location, but this throughput dramatically decreases when the receiver is moved from the desired location. In particular, at a distance of 0.3 meter, the throughput of the eavesdropper approaches to 0.
- Far Proximity Identification in Wireless Systems: (1) we develop a novel fingerprinting technique that enables the local device to extract the fingerprint of a wireless device's proximity from the physical-layer features of signals sent by the device; (2) we discover the theoretical relationship between the proximity and its fingerprint, and we developed a technique that can use such a relationship to estimate the lower and upper bounds of the distance between the local and remote devices; and (3) we validate and evaluate the effectiveness of the proposed far proximity identification method through experiments on the real-world data. The experiment results show that the proposed approach can detect the far proximity with a success rate of 0.85 for the non-Line-of-sight (NLoS)

scenario, and the success rate can be further increased to 0.99 for the Line-of-sight (LoS) scenario.

1.4 Dissertation Roadmap

The aforementioned projects are contained in the following chapters. Chapter 2 describes the physical layer design to enforce the location-restricted service access control in wireless networks. The far proximity identification against spoofing attack in long-haul wireless communications is presented in Chapter 3. Then, Chapter 4 discusses the preliminary future work of light-weight encryption schemes in IoT devices, followed by the Conclusion in Chapter 5. The text for Chapters 2 and 3 is taken from their respective publications, [15], [16], and [17] respectively.

CHAPTER 2

LOCATION-RESTRICTED SERVICE ACCESS CONTROL

In this chapter¹, we demonstrate the feasibility of the pinpoint waveforming system by answering essential concerns about synchronization, tolerable time shift, and the service area size. We implement a prototype of pinpoint entanglement system on top of the Universal Software Radio Peripherals (USRPs), and evaluate the performance of the prototype system through comprehensive experiments. Our results show that the receiver obtains a high throughput that ranges between 0.90 and 0.93 when it is at the desired location, but this throughput dramatically decreases when the receiver is moved from the desired location. In particular, at a distance of 0.3 meter, the throughput of the eavesdropper approaches to 0.

2.1 Synchronization

We discuss synchronization first, because synchronization is the basis for the proposed pinpoint waveforming system to achieve the constructive interference of original signals and the cancelation of the jamming signals. Synchronization includes three components, and they are *clock synchronization*, *propagation synchronization*, and *channel synchronization*.

¹This chapter was published in ACM CCS 2015 [16], and IEEE Transactions on Dependable and Secure Computing 2016 [15]. Permission is included in Appendix 5.

2.1.1 Clock and Propagation Synchronization

Clock synchronization deals with the discrepancy of the clocks of multiple transmitters, so that they transmit service packets at the same time. In the proposed system, all transmitters are connected to the same service provider, and thereby their clocks are roughly the same.

The distances between the receiver and each transmitter may be different. Accordingly, signals sent by these transmitters may arrive at the receiver at different time even if they are sent at the same time. To compensate the propagation difference, the service provider needs to perform propagation synchronization through adjusting the transmit time of each transmitter. Propagation synchronization has been extensively studied in the context of wireless sensor networks (e.g., [18, 19]). In a traditional way, the receiver broadcasts a beacon signal, and the transmitter (service provider) adjusts each transmitter's transmit time based on beacon arrival time recorded at this transmitter[20]. Since transmitter clocks are inherently the same, the proposed system is compatible with the traditional synchronization approach.

Note that after clock and propagation synchronization, due to the processing delay and synchronization imperfections, the time shift will still exist between the signal arrival times. In section 2.4, we show the impact of the time shift and the maximum time shift that can be tolerated by the system.

2.1.2 Channel Synchronization

The impact of channel effect cannot be neglected. The signals sent by different transmitters may undergo different channel effect. When the signals arrive at the receiver, their shapes accordingly exhibit different distortions, and thus the constructive interference may diminish due to the wave shape discrepancy. The transmit (jamming) signals should be calibrated so that they have the same (reverse) shapes when they arrive at the receiver.

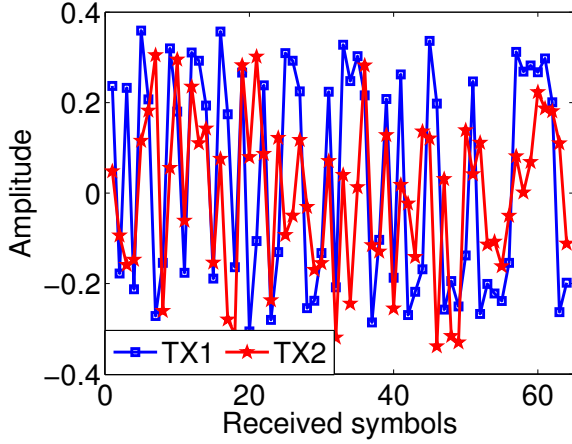


Figure 2.1: Without channel synchronization

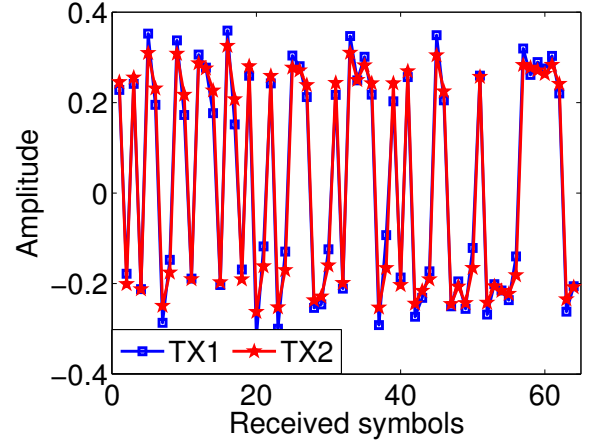


Figure 2.2: With channel synchronization

Figure 2.1 shows a real measured example of the channel impact without the channel synchronization. Two transmitters are separated by a certain distance to result in uncorrelated channels (i.e., 0.75 meter for a 2.4 Ghz channel). The receiver is 3 meters away from both transmitters. Each device is a USRP connected to a PC. Both transmitters send the same sequence of 64 symbols (i.e., the transmission unit at the wireless physical layer) to the receiver. As seen in Figure 2.1, the amplitude of symbols received from both transmitters are different from each other due to the different channel distortions. Figure 2.2 shows the amplitude of received symbols after the channel synchronization. Both received symbols then become similar to each other.

2.1.2.1 Signal Modulation

Before we discuss the proposed channel calibration algorithm, we first introduce the signal modulation/demodulation to facilitate the reader's understanding. We focus our discussion on I/Q modulation, because it is widely used in modern wireless systems. In I/Q modulation, signals are transmitted in the form of symbols, which are the transmission unit at the wireless

physical layer. We use Quadrature Phase-Shift Keying (QPSK) modulation, a typical I/Q modulation, as an example to show how I/Q modulation works.

QPSK encodes two bits into one symbol at a time. In Figure 2.3 (a), bits 00, 01, 10, and 11 are represented by points whose coordinates are (-1,-1), (-1,1), (1,-1), and (1,1) in an I/Q plane, respectively. The I/Q plane is called a *constellation diagram*. A symbol is the coordinate of a point on the constellation diagram. Due to the channel noise, a received symbol is not exactly the same as the original symbol sent by the sender. To demodulate, the receiver outputs the point that is closest to the received symbol on the constellation diagram as the demodulation result.

2.1.2.2 Basic Channel Synchronization

Same signals from different transmitters will exhibit distinct wave shapes when they come to the receiver, because they undergoes different channel distortion. Thus, on the constellation diagram, the receiver not only receives multiple symbols from the multiple transmitters at the same time, but these symbols have different phases and amplitudes. As an example shown in Figure 2.3 (a), the receiver receives four symbols from four transmitters and these symbols are at different positions on the constellation diagram. The received symbols can interfere with each other, and consequently it becomes difficult for the receiver to correctly decode the received packets. Hence, channel synchronization is required in the proposed scheme so that the received symbols can converge to the same ideal point to form a good constructive interference.

In our basic idea, we propose to calibrate the symbols before they are transmitted to offset the channel distortion. As shown in Figure 2.3 (b), the original symbol sent by the transmitter is (1,1) and the corresponding received symbol is at point A on the constellation diagram. For QPSK, the angle between the ideal point (1, 1) and the horizontal axis is $\frac{\pi}{4}$. Thus, the coordinate of the received symbol can be represented by $(\sqrt{2}a \cos(\theta + \frac{\pi}{4}),$

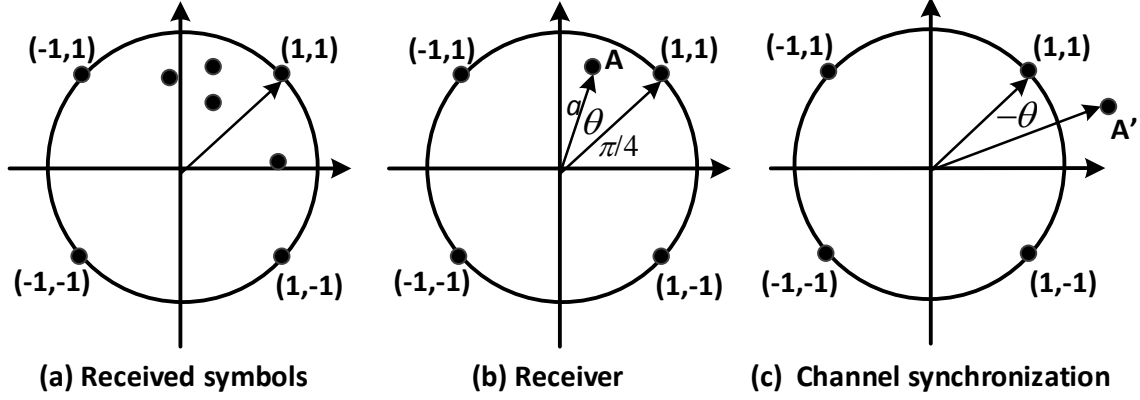


Figure 2.3: Basic channel synchronization

$\sqrt{2}a \sin(\theta + \frac{\pi}{4})$), where a is amplitude attenuation factor, and θ is the phase shift between the received symbol and the ideal point $(1, 1)$.

Channel synchronization aims to calibrate the received symbols to the corresponding ideal points. Toward this end, rather than transmitting the ideal points, the transmitter transmits symbols that deviate from the ideal points in a way that offset the channel distortion. As shown in Figure 2.3 (c), the transmitter transmits a symbol A' , whose phase shift from the ideal point $(1,1)$ is $-\theta$ and the magnitude is $\frac{1}{a}$, in lieu of the ideal point $(1, 1)$. Thus, the coordinate of the calibrated symbol is $(\frac{1}{a}\sqrt{2}\cos(\frac{\pi}{4} - \theta), \frac{1}{a}\sqrt{2}\sin(\frac{\pi}{4} - \theta))$. When this symbol arrives at the receiver, the calibration offset cancels the channel effect, and thereby the received symbol will converge to the ideal point.

The transmitter needs to know θ and a for the channel synchronization. Due to the channel reciprocity property, the wireless channel remains the same if the roles of the transmitter and the receiver are exchanged[21]. Thus, training stages can be utilized for the transmitter to measure θ and a from the training symbols sent by the receiver. To further reduce the communication overhead, the transmitter can obtain θ and a in the piggyback way. Specifically, it can measure them from the symbols that are contained in the existing up-link packets (e.g., service request packets and acknowledgement packets) sent by the receivers,

2.1.2.3 Refined Channel Synchronization

Multipath effect is the phenomena that signals sent by the transmitter travel along multiple paths to reach the receiver. Thus, the receiver can receive multiple copies of the original signal from the multiple paths. These signal copies can interfere with each other and confuse the receiver to obtain an incorrect message decoding results.

The signal propagation paths can be generally classified as unresolvable and resolvable paths. For a transmitted symbol, the copies traveling on unresolvable paths arrive at the receiver with an arrival time difference less than one symbol duration, i.e., the transmission time of one symbol. Thus, they form one symbol on the constellation diagram. For resolvable paths, the copies traveling on these paths arrive at the receiver with a time difference larger than one symbol duration, and therefore on the constellation diagram they form separate symbols that interfere future transmitted symbols. In this paper, we only consider the impact of signal copies from resolvable paths, because they are the major factors that contribute to the inter-symbol interference and the decoding failures. Specifically, for L resolvable paths, the receiver will then receive L copies of subsequently transmitted symbols.

Figure 2.4 (a) shows an example of a 3-path channel. The transmitter transmits three symbols S_0 , S_1 , and S_2 . At time t_0 , the receiver receives S_0 from Path 1. At time t_1 , the receiver receives S_1 from Path 1 and a delayed copy of S_0 from Path 2. At time t_2 , the receiver receives S_2 from Path 1, the delayed copy of S_1 from Path 2, and the delayed copy of S_0 from Path 3.

We propose to cancel the interference caused by multipath symbols via adding a complementary symbol to the transmitted symbol. Specifically, Figure 2.4 (b) shows the snapshot of the constellation diagram at time t_2 for the aforementioned 3-path channel, the superposed impact of the delayed copies of S_0 and S_1 can be represented by an equivalent symbol S_m , which is the vector sum of S_0 and S_1 . To eliminate the multipath symbols, in addition to

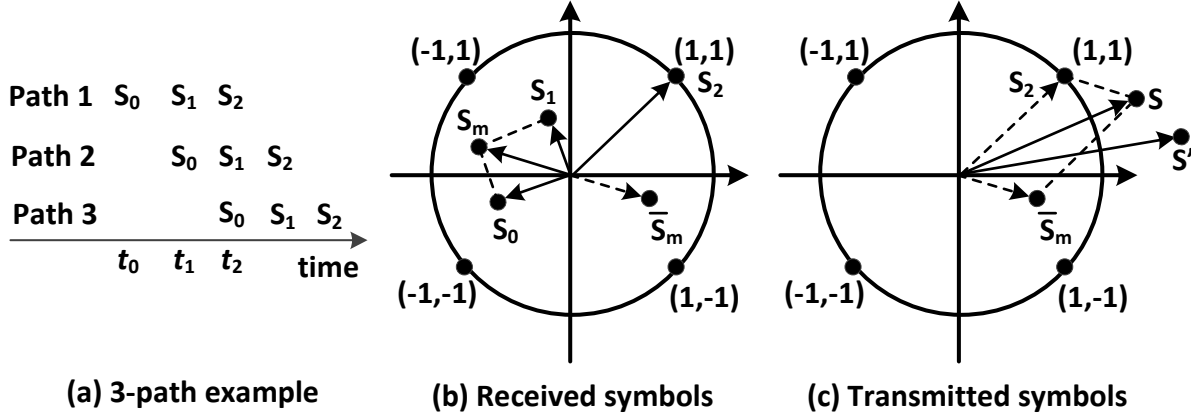


Figure 2.4: Refined channel synchronization against the multipath effect

sending the desired symbol S_2 , the transmitter also needs to send a cancelation symbol \bar{S}_m that is at the reverse position of S_m . The magnitude of S_m and \bar{S}_m are the same but \bar{S}_m shifts from S_m by an angle of π . As shown in figure 2.4 (c), the vector sum of the desired symbol S_2 and \bar{S}_m is S . Thus, the transmitter performs the basic synchronization to calibrate S to S' to resist against the channel noise, and the actually transmitted symbol is S' .

We would like to point out that \bar{S}_m can only eliminate the multipath effects from previous symbols S_0 and S_1 . However, subsequent symbols will still be interfered by the calibrated \bar{S}_m due to the multipath effects. So all these symbols should be calibrated in the same way, and the i -th symbol can be calibrated only after all its previous $L - 1$ symbols are already calibrated. We discuss the details Section 2.2.

2.2 Multipath Channel Calibration

To achieve the channel calibration, the transmitter must first get the channel impulse response (CIR), which includes the amplitude attenuation coefficient, phase shift, and the effects of the multipath propagation. Traditionally, channel estimation algorithms[22] are applied at the receiver to adapt received signals to the current channel conditions. However, we cannot directly use these methods in the proposed scheme, because we require that signals

to reach the receiver with same shapes to gain the constructive interference. Inspired by the channel reciprocity that the channel effects observed by the transmitter and the receiver are the same during the communication, we propose to directly estimate the CIR at the transmitter and then use this information to calibrate the transmit signals.

2.2.1 Preliminary

To facilitate the presentation of the proposed technique, we first give the preliminary knowledge about the channel estimation. Channel is usually estimated using a predefined training sequence that are composed of multiple symbols. Specifically, the training sequence is known to both the transmitter and the receiver prior to their communication. The transmitter sends the training sequence to the receiver through the wireless channel, and upon receiving, the receiver uses the original training sequence and the received copy to estimate the channel.

In general, the received training sequence is distorted by both channel effects and the noise. It can be expressed by $\mathbf{r} = \mathbf{h} * \mathbf{d} + \mathbf{n}$, where \mathbf{h} is the channel state information, \mathbf{d} is the original training sequence, $*$ is the convolution operator, and \mathbf{n} is the channel noise that is normally considered as a zero-mean Gaussian noise. We can rewrite this equation in the matrix form below.

$$\mathbf{r} = \begin{bmatrix} d_1 & 0 & \cdot & 0 \\ d_2 & d_1 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot \\ d_L & d_{L-1} & \cdot & d_1 \\ \cdot & \cdot & \cdot & \cdot \\ d_K & d_{K-1} & \cdot & d_{K-L+1} \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \\ \cdot \\ \cdot \\ h_L \end{bmatrix} + \mathbf{n},$$

where the vector $[d_1, d_2, \dots, d_k]^t$ denotes the known training data \mathbf{d} , vector $[h_1, h_2, \dots, h_L]^t$ denotes the unknown channel \mathbf{h} , and $[n_1, n_2, \dots, n_k]^t$ denotes the unknown channel noise \mathbf{n} . Note that k is the length of the training sequence and it must be larger than L to enable the estimation of the channel.

To facilitate our analysis, we rewrite the above matrix equation into the compact form and we can obtain $\mathbf{r} = \mathbf{D}\mathbf{h} + \mathbf{n}$. Normally, least-square (LS) estimator can be used to solve \mathbf{h} from the compact equation for channel estimation[23], yielding the estimation result $\hat{\mathbf{h}} = \{\mathbf{D}^H \mathbf{D}\}^{-1} \mathbf{D}^H \mathbf{r}$, where H denotes the complex conjugate transpose operator.

In our scheme, channel estimation is done at the transmitter, and the training sequence is sent from the receiver. Due to the channel reciprocity property, the channel estimated by the transmitter will represent the channel between itself and the receiver. To cope with the channel changes, the training sequence can be sent periodically so that the transmitter can capture the current CIR.

2.2.2 Advanced Channel Calibration

As discussed earlier, we propose to construct a complementary symbol for each transmitted symbol to cancel the multipath effect. The complementary symbol for the i -th transmitted symbol is constructed not only based on the i -th transmitted symbol but also based on $L - 1$ previously transmitted symbols.

2.2.2.1 Obtaining Calibrate Symbols

Let $\hat{\mathbf{h}} = [\hat{h}_1, \hat{h}_2, \dots, \hat{h}_L]^T$ denote the estimated channel, and $\mathbf{d}_r = [d_{1_r}, d_{2_r}, \dots, d_{k_r}]^T$ denote the desired, interference-free received symbols. Further let $\mathbf{d}_t = [d_{1_t}, d_{2_t}, \dots, d_{k_t}]^T$ denote the calibrated symbols to be transmitted to the receiver. Note that \mathbf{d}_t combines both complementary and original symbols. At time t_0 , d_{1_t} is sent and it arrives at the receiver through the first path. The corresponding received symbol is $d_{1_r} = d_{1_t} \cdot \hat{h}_1$. At time t_1 , d_{2_t}

is sent, it arrives at the receiver through the first path, and meantime the multipath copy of d_{1_t} arrives through the second path. The second received symbol can hence be presented as $d_{2_r} = d_{1_t}\hat{h}_2 + d_{2_t}\hat{h}_1$. Finally, at time t_k , the receiver will receive both the symbol d_{k_t} via the first path and the multipath copies of the previous $L - 1$ symbols. The received symbol d_{k_r} is $d_{k_r} = \sum_{i=1}^L d_{k-i+1_t}\hat{h}_i$. We rewrite this linear relation using the matrix form and we obtain:

$$\begin{bmatrix} d_{1_r} \\ d_{2_r} \\ \cdot \\ \cdot \\ d_{k_r} \end{bmatrix} = \begin{bmatrix} d_{1_t} & 0 & \cdot & 0 \\ d_{2_t} & d_{1_t} & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot \\ d_{L_t} & d_{L-1_t} & \cdot & d_{1_t} \\ \cdot & \cdot & \cdot & \cdot \\ d_{k_t} & d_{k-1_t} & \cdot & d_{k-L+1_t} \end{bmatrix} \begin{bmatrix} \hat{h}_1 \\ \hat{h}_2 \\ \cdot \\ \cdot \\ \hat{h}_L \end{bmatrix}$$

We use the compact matrix form $\mathbf{d}_r = \mathbf{D}_t \hat{\mathbf{h}}$ to represent the above equation. Because \mathbf{D}_t includes the calibrated symbols to be sent by transmitters, we would like to solve \mathbf{D}_t from this equation. Intuitively, it can be computed by $\mathbf{D}_t = \mathbf{d}_r \hat{\mathbf{h}}^H \{\hat{\mathbf{h}} \hat{\mathbf{h}}^H\}^{-1}$. However, since $\hat{\mathbf{h}}$ is a column vector, $\hat{\mathbf{h}} \hat{\mathbf{h}}^H$ is always a singular matrix and it's not feasible to find its matrix reverse $\{\hat{\mathbf{h}} \hat{\mathbf{h}}^H\}^{-1}$.

In the proposed scheme, the desired data $[d_{1_r}, d_{2_r}, \dots, d_{k_r}]$ and channel impulse response $[\hat{h}_1, \hat{h}_2, \dots, \hat{h}_L]$ are known. We can thus find \mathbf{D}_t by recursively solving linear equations. Specifically, the first calibrated symbol d_{1_t} can be directly calculated by $d_{1_t} = \frac{d_{1_r}}{\hat{h}_1}$. With d_{1_t} , we can then compute the second calibrated symbol d_{2_t} by $d_{2_t} = \frac{d_{2_r} - d_{1_t}\hat{h}_2}{\hat{h}_1}$. In general, the k -th calibrated symbol can be computed by $d_{k_t} = \frac{d_{k_r} - \sum_{i=2}^L \hat{h}_i d_{k-i+1_t}}{\hat{h}_1}$ ($k > L$), where $-\sum_{i=2}^L \hat{h}_i d_{k-i+1_t}$ is the complementary component to eliminate the previous multipath copies, and $\frac{1}{\hat{h}_1}$ is the basic calibration component to compensate the power attenuation and phase shift of the current symbol.

2.2.2.2 Reducing Channel Estimation Errors

To eliminate the channel noise and accommodate normal temporal variance, we would like to utilize the zero-mean property of the channel noise, i.e., to use the average values of multiple channel estimations to reduce the estimation error. Specifically, we set a window of size N , and advance the window so that it always keeps the most recent N channel estimations. The ultimate output channel impulse response is the average of the N channel estimations in the window. Since the channel estimation is given by $\hat{\mathbf{h}} = \{\mathbf{D}^H \mathbf{D}\}^{-1} \mathbf{D}^H \mathbf{r}$, and the estimated error is thus $\{\mathbf{D}^H \mathbf{D}\}^{-1} \mathbf{D}^H \mathbf{n}$. The average $\hat{\mathbf{h}}_{\text{avg}}$ of the N estimations is $\frac{1}{N} \sum_{i=1}^N \mathbf{h}_i = \frac{1}{N} \sum_{i=1}^N \{\mathbf{D}^H \mathbf{D}\}^{-1} \mathbf{D}^H \mathbf{r}_i$, and the average estimation error becomes $\{\mathbf{D}^H \mathbf{D}\}^{-1} \mathbf{D}^H \sum_{i=1}^N \mathbf{n}_i$. When N is chosen large, due to the zero mean property of the channel noise, this error approximates to a zero vector.

2.3 Jamming Entanglement

Signal to noise ratio (SNR) is always a key metric to evaluate the reliability of a wireless communication system. According to Shannon Theorem [2], a large SNR can support a high speed service than a small SNR on the same channel bandwidth. Thus, we would like to enable a receiver at the desired location to always achieve a large SNR, and an eavesdropper at an undesired location to encounter a low SNR, so that it cannot distinguish the received signal from the background noise and fails to decode received data.

The basic idea is to intentionally introduce noise to the raised transmit signal, so that the noise can significantly reduce the SNR at the eavesdroppers but cancel each other at the desired receiver to cause no impact.

In order to generate such noise signals for all transmitters, we randomly divide the N transmitters into $\frac{N}{2}$ pairs. For each pair, we assign one transmitter with a randomly generated sequence, whose length is the same as the message length. Then, we generate the

opposite sequence for the other transmitter. For example, if the randomly generated sequence is $1, 1, -1, 1$, then the corresponding opposite sequence is $-1, -1, 1, -1$. The pair of transmitters add the corresponding noise sequences to the message and send the combined signals to the wireless channel. Because the noise signals are embedded in the combined signals, which can synchronize at the desired receiver, the noise signals naturally achieve the synchronization to enable the cancelation. However, for the eavesdroppers, due to the lack of the time synchronization and channel calibration, the noise signals fail to cancel each other and the sum of them still confuse the eavesdroppers. Moreover, the noise sequences are randomly generated for each message, and thus the eavesdroppers cannot guess and pre-determine them.

On the other hand, for a receiver that is not located at the desired service location, due to the lack of channel synchronization, it will experience distorted received signals in various shapes, and consequently the jamming signals cannot cancel each other, yielding a low SNR at the undesired location. In Section 2.5.2, we show how the channel distortion affects the SNR at the undesired location.

2.4 Tolerable Time Shift

In the above discussion, we consider the ideal case where the arrival signals are perfectly synchronized. In practice, as mentioned, after clock and propagation synchronization, a slight time shift may still exist among the received signals due to the processing delay and synchronization imperfections. In the following, we identify the tolerable time shift, within which received signals can achieve the constructive interference to obtain a boosted SNR.

2.4.1 Impact of the Time Shift on SNR

SNR is the ratio of the received signal power to the noise power. Because the noise power is independent from the time shift, the received signal power remains as the key metric to

determine the SNR at the desired receiver. Lemma 1 gives the threshold of the time shift based on the received signal power. Without loss of generality, we assume that there are two arrival signals to facilitate the presentation.

Lemma 1 *The constructive interference does not happen if $\delta_t > \frac{1}{4f_0}$, where δ_t is the time shift between two arrival signals and f_0 is the frequency and the baseband signal.*

Proof: The modulated transmit signal $S(t)$ can be written as $S(t) = \text{Re}[\sqrt{2}A_m g(t)e^{j\theta_m}] = \sqrt{2}A_m g(t) \cos \theta_m$, where A_m and θ_m are the amplitude and the phase of the transmit signal respectively, and $g(t)$ is the baseband signal. Typically, $g(t)$ is a sine, cosine or rectangle wave[22]. Assume $g(t) = \sin(2f_0 t)$, $S(t)$ then equals to $\sqrt{2}A_m \sin(2f_0 t) \cos \theta_m$, and its power is $A_m^2 \cos^2 \theta_m$. When two signals arrive at the receiver with a time shift of δ_t , the combined signal power P_c becomes as,

$$\begin{aligned} P_c &= \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} 2\{A_m \sin(2f_0 t) \cos \theta_m \\ &\quad + A_m \sin[2f_0(t + \delta_t)] \cos \theta_m\}^2 dt \\ &= \frac{2A_m^2 \cos^2 \theta_m}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} \{[1 + \cos(2\pi f_0 \delta_t)] \sin(2\pi f_0 t) \\ &\quad + \sin(2\pi f_0 \delta_t) \cos(2\pi f_0 t)\}^2 dt \\ &= 2A_m^2 \cos^2 \theta_m [1 + \cos(2\pi f_0 \delta_t)]. \end{aligned}$$

We can see that P_c is highly associated with the time shift δ_t . When $\delta_t = \frac{1}{4f_0}$, the combined signal power P_c is $2A_m^2 \cos^2 \theta_m$. On the other hand, the SNR is $\frac{A_m^2 \cos^2 \theta_m}{N_c}$ at each transmitter, where N_c is the noise power. Because two arrival signals bring twice of the noise power to the receiver, the received signal power P_c must be larger than $2A_m^2 \cos^2 \theta_m$ to achieve a boosted SNR (i.e., the constructive interference). Thus, the tolerable time shift should be less than $\frac{1}{4f_0}$ so that $P_c > 2A_m^2 \cos^2 \theta_m$.

As a practical example, for the 1Mbps and 10Mbps transmission speed with the QPSK modulator, a tolerable time shift of $\frac{1}{4f_0}$ equals to 500 and 50ns respectively.

2.4.2 Impact of the Time Shift on Jamming Signals

In Section 2.3, we propose to increase the SNR through transmitting jamming signals that can cancel each other at the receiver. In what follows, we will investigate the impact of the tolerable time shift on the effectiveness of this scheme. We present Lemma 2 below.

Lemma 2 *After the jamming entanglement, the expected SNR at the desired receiver is $\frac{2\{\frac{N}{2} + \sum_{i=1}^N \sum_{j=1, j>i}^N \cos[2\pi f_0 \frac{\Delta(j-i)}{N-1}]\}}{N[1 - \cos(2\pi f_0 \frac{\Delta}{2})]}$, where N is the number of transmitters, and Δ is the maximum tolerable time shift.*

Proof: The modulated signal $S(t)$ is $Re[\sqrt{2}A_m g(t)e^{j\theta_m}] = \sqrt{2}A_m g(t) \cos \theta_m$, where A_m and θ_m are the amplitude and the phase of the transmit signal respectively, and $g(t)$ is the baseband signal. Typically, $g(t)$ is a sine, cosine or rectangle wave[22]. Assume $g(t) = \sin(2f_0 t)$, $S(t)$ then equals to $\sqrt{2}A_m \sin(2f_0 t) \cos \theta_m$, and its power is $A_m^2 \cos^2 \theta_m$. Assume the signal arrival times for N transmitters are t_0, \dots, t_{N-1} . For the tolerable time shift Δ , all signals arrive the receiver within the range $t_0 \sim t_0 + \Delta$. The boosted power at the receiver can be represented by

$$\begin{aligned} P_{cN} &= \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} \left\{ \sum_{i=1}^N \sqrt{2}A_m \sin[2f_0(t + t_i)] \cos \theta_m \right\}^2 dt \\ &= 2A_m^2 \cos^2 \theta_m \left\{ \frac{N}{2} + \sum_{i=1}^N \sum_{\substack{j=1 \\ j>i}}^N \cos[2\pi f_0(t_j - t_i)] \right\} \end{aligned}$$

Further assume that the arrival time of all the signals follows the uniform distribution between 0 and Δ . The expected time shift between any two signals is thus $\frac{\Delta}{N-1}$. The expected

boosted power $E(P_{cN})$ can be derived by $2A_m^2 \cos \theta_m^2 \{ \frac{N}{2} + \sum_{i=1}^N \sum_{\substack{j=1 \\ j>i}}^N \cos[2\pi f_0 \frac{\Delta(j-i)}{N-1}] \}$. We can see that $E(P_{cN})$ increases as N increases.

As discussed in Section 2.3, the boosted SNR is $\frac{a^2 N P'_t}{N_c}$ in the ideal case when the jamming signals are totally canceled out. When the jamming signals cannot completely cancel each other, their combined power dominates the actual noise because the jamming signal power as well as the transmit power are usually chosen much higher than the channel noise power to result in a satisfiable SNR at the receiver. Hence, we neglect the channel noise to facilitate the following analysis. Assume the modulated jamming signal for one transmitter is $\sqrt{2}A_m \sin(2f_0 t) \cos \theta_m$. The corresponding opposite counterpart is thus $-\sqrt{2}A_m \sin(2f_0 t) \cos \theta_m$. Then the combined power of both signals is $2A_m^2 \cos \theta_m^2 [1 - \cos(2\pi f_0 \delta_t)]$, and the expected SNR can be derived by

$$E(SNR) = \frac{2\{ \frac{N}{2} + \sum_{i=1}^N \sum_{\substack{j=1, j>i}}^N \cos[2\pi f_0 \frac{\Delta(j-i)}{N-1}] \}}{N[1 - \cos(2\pi f_0 \frac{\Delta}{2})]},$$

where $\frac{\Delta}{2}$ is the expected time shift between the arrival times of camouflage signals.

$E(SNR)$ increases as N increases or Δ decreases. For example, with 4 transmitters and a tolerable time shift of $\frac{1}{4f_0}$, the expected SNR at the receiver reaches approximately 10 dB. When the number of transmitters is 8, the expected SNR can be boosted to approximately 13 dB. For a reduced tolerable time shift of $\frac{1}{8f_0}$, the achieved SNR is about 20 dB. In a conclusion, for a service system with the maximum tolerable time shift Δ , the jamming signals still significantly help to boost the SNR at the desired receiver.

Because signals travel at the speed of light, it seems that a small tolerable time shift may result in a large service area (e.g. 50ns indicates a distance of 15m). In this section, we attempt to obtain a fine-grain service area using the channel uncorrelation property, which states that two receivers will observe different channels from the same transmitter if they are separate by a couple of wavelength away[24]. In particular, [25] indicates that a distance

of half wavelength can lead to uncorrelated channels. In the following part, we investigate how uncorrelated channels affect the boosted SNR.

2.5 Service Area Size

Because signals travel at the speed of light, it seems that a small tolerable time shift may result in a large service area (e.g. 50ns indicates a distance of 15m). In this section, we attempt to obtain a fine-grain service area using the channel uncorrelation property, which states that two receivers will observe different channels from the same transmitter if they are separate by a couple of wavelength away[24]. In particular, [25] indicates that a distance of half wavelength can lead to uncorrelated channels. In the following part, we investigate how uncorrelated channels affect the boosted SNR.

2.5.1 Channel Uncorrelation Property

We first describe the channel uncorrelation property and explore the distance required to generate the uncorrelated channels. Channel correlation coefficient is normally used to indicate the similarity between two channels. When two channels are fully correlated, the coefficient approximates to 1; while when two channels are uncorrelated from each other, the coefficient is 0. Theoretically, the multipath channel is usually modeled as the Rayleigh fading channel[26]. In a rich, isotropic scattering environment, multipath components arrive at the receiver from all the directions, and the corresponding channel correlation coefficient can be described as a zeroth order Bessel function [27]: $\rho(d, f) = J_0(2\pi d/\lambda)$, where d is the distance between the receiver and the eavesdropper, f is the carrier frequency of the signal, and $\lambda = \frac{c}{f}$ is the wavelength of the signal. When we substitute $d = \frac{\lambda}{2}$ into this function, the channel correlation coefficient approximates to 0, which indicates that two channels are uncorrelated. In practice, [28] presents that a longer distance (e.g. a couple of wavelength) may be required to get the uncorrelated channels when there are less scatterings.

2.5.2 Power Attenuation by the Channel Uncorrelation

In this part, we discuss how the uncorrelated channels affect the boosted SNR. As mentioned earlier, channels observed by the eavesdropper are uncorrelated from the calibrated ones. Thus, channel effects cannot be eliminated and signals will exhibit different shapes when they arrive at the eavesdropper. Lemma 3 gives the SNR at the desired location and undesired location respectively.

Lemma 3 *The SNR at desired location and undesired location are $\frac{2P_h \cdot P_t}{N_c}$ ($P_t \gg \frac{N_c}{P_h}$) and $\frac{P_t}{P_j}$ respectively, where P_t is the transmit power of original signal, N_c is the channel noise power, P_j is the jamming signal power and P_h is the channel variance.*

Proof: Without loss of generality, we assume two transmitters. The calibrated signals from two transmitters are denoted as S_1 and S_2 respectively. Let P_t be the transmit power for both signals. Assume the receiver observes two channels $h_1(\tau)$ and $h_2(\tau)$. According to [2], Multipath channel is described as $h(\tau) = \sum_{l=1}^L a_l e^{j\phi_l} \delta(\tau - \tau_l)$, where a_l and $e^{j\theta_l}$ are the amplitude attenuation and phase shift of the signal copy that travel along the i -th path. At time τ_l , channel $h_1(\tau_l)$ and $h_2(\tau_l)$ can be modeled as the random variables with zero mean and a variance that is usually denoted as P_h [29]. Thus, at this time, the received signal is $S_1 \cdot h_1(\tau_l) + S_2 \cdot h_2(\tau_l)$. Since the mean value of the received signal is 0, we can get the received power by calculating its variance. Specifically, for a random variable x with the zero mean, its power $P = \int x^2 f(x) dt = Var(x)$, where $Var(\cdot)$ donates the variance. Thus, the combined transmit power at the receiver is as follows,

$$\begin{aligned} P_s &= Var[S_1 \cdot h_1(\tau_l) + S_2 \cdot h_2(\tau_l)] \\ &= P_t E[|h_1(\tau_l)|^2 + 2|h_1(\tau_l) \cdot h_2(\tau_l)^*| + |h_2(\tau_l)|^2] \\ &= 2P_h \cdot P_t + 2\rho P_h \cdot P_t, \end{aligned}$$

where ρ is defined as the channel correlation coefficient and equals to $\frac{|h_1(\tau_l) \cdot h_2(\tau_l)^*|}{\sqrt{\text{Var}(|h_1(\tau_l)|) \text{Var}(|h_2(\tau_l)|)}} = \frac{|h_1(\tau_l) \cdot h_2(\tau_l)^*|}{P_h}$ [30], and $*$ denotes the complex conjugate operator.

At the undesired location, the channels of two transmitters are uncorrelated from each other. Thus, their coefficient ρ equals to 0 and the received power is $P_s = 2P_h \cdot P_t$. On the other hand, two channels observed by the desired receiver are calibrated and are quite correlated with each other. So their coefficient ρ equals to 1 and thus the received power is $P_s = 4P_h \cdot P_t$.

The power of jamming signals can be derived in the same way. Assume two calibrated jamming signals are denoted as C_1 and C_2 ($C_1 = -C_2$) with the power P_j for each of them. Assume the receiver observes two channels $h_1(\tau)$ and $h_2(\tau)$. At time τ_l , the combined power of two jamming signals is given by $P_c = \text{Var}[C_1 \cdot h_1(\tau_l) + C_2 \cdot h_2(\tau_l)] = 2P_h \cdot P_j - 2\rho P_h \cdot P_j$.

At the desired location, the receiver observes two correlated channels. Thus, ρ equals to 1 and the combined power equals to 0. At undesired location, two channels observed by the receiver are uncorrelated. Thus, ρ equals to 0, and the combined power equals to $2P_h \cdot P_j$, which can significant affect the SNR of the receiver.

Note that SNR is represented as the ratio of the original signal power (given by P_s) to the sum of jamming signal power (given by P_c) and channel noise power N_c (i.e. $SNR = \frac{P_s}{P_c + 2N_c}$). Note that the power of channel noise is doubled at the receiver, because channel noise from two received signals combines together. At the desired location, channels are synchronized, and original signals get boosted and jamming signals cancel each other, yielding an SNR that equals to $\frac{2P_h \cdot P_t}{N_c}$. The transmit power P_t as well as the jamming signal power P_j are usually chosen much higher than the channel noise power N_c to result in a satisfiable SNR at the receiver ($P_t \gg \frac{N_c}{P_h}$). So N_c is negligible compared to the jamming power. Accordingly, at the undesired location, the channel is not synchronized (i.e. ρ is close to zero) and the SNR is represented by $SNR = \frac{P_s}{P_c + N_c} \approx \frac{P_t}{P_j}$. If $P_j = P_t$, SNR approximates to 0dB and the receiver cannot distinguish between the original and jamming signals.

2.5.3 Power Attenuation of Multiple Transmitters

In this section, we extend Lemma 3 from a two-transmitter scenario to the multi-transmitter one, where N transmitters are connected to the same service provider, and each one transmits a signal that is calibrated based on the channel between the transmitter and the desired location. The SNR at desired location and undesired locations are given by

Lemma 4 *With multiple transmitters, the SNR at desired location and undesired location are $\frac{NP_h \cdot P_T}{N_c}$ ($P_T \gg \frac{N_c}{P_h}$) and $\frac{P_T}{P_J}$ respectively, where P_T is the power of transmit signals, N_c is the power of channel noise, P_J is the power of the jamming signal, and P_h is the channel variance.*

Proof: We assume N transmit signals $[S_1, S_2, \dots, S_N]$ have the same transmit power P_T . The signal S_i will propagate through the channel $h_i(\tau)$ and each channel $h_i(\tau)$ ($0 \leq i \leq N$) has the same channel variance P_h . Therefore, the combined signal power P_{ms} at time t_τ is as follows,

$$\begin{aligned} P_{ms} &= \text{Var} \left[\sum_{i=1}^N S_i \cdot h_i(\tau_l) \right] \\ &= P_T E \left[\sum_{i=1}^N |h_i(\tau_l)|^2 + \sum_{i=1}^N \sum_{\substack{j=1 \\ j \neq i}}^N |h_i(\tau_l) \cdot h_j(\tau_l)^*| \right] \\ &= NP_h \cdot P_T + \sum_{i=1}^N \sum_{\substack{j=1 \\ j \neq i}}^N \rho_{ij} P_h \cdot P_T, \end{aligned}$$

where ρ_{ij} is the channel correlation coefficient between i^{th} channel and j^{th} channel. At the desired location, all the transmitted signals are calibrated and channels observed by the receiver are correlated. Thus, ρ_{ij} equals one and P_{ms} becomes $N^2 P_h \cdot P_T$. On the other hand, channels are not calibrated at undesired locations, and thus the receiver observes

uncorrelated channels and ρ_{ij} decreases to zero. P_{ms} then becomes $NP_h \cdot P_T$, which is N times less than the combined power when all the channels are synchronized.

To enable the jamming signal entanglement, N jamming signals $[C_1, C_2, \dots, C_N]$ are transmitted with the same power P_J and propagate through different channels $[h_1, h_2, \dots, h_N]$. As mentioned in Section 2.3, all the transmitters are randomly divided into pairs and each pair is assigned with a pair of randomly generated jamming signals, whose phases are opposite to each other. Therefore, if two jamming signals C_i and C_j belong to the same pair, then $C_j = -C_i$ and their combined power is $Var[C_i \cdot h_i(\tau_l) + C_j \cdot h_j(\tau_l)] = 2P_h \cdot P_J - 2\rho P_h \cdot P_J$. Otherwise, C_i and C_j are from different pairs and independent to each other. Thus, the combined power becomes $2P_h \cdot P_J$, and we can get the combined power of jamming signals as shown below:

$$\begin{aligned}
P_{mc} &= Var\left[\sum_{i=1}^N C_i \cdot h_i(\tau_l)\right] \\
&= \sum_{\substack{i=1 \\ j \neq i}}^{N/2} Var[C_i \cdot h_i(\tau_l) + C_j \cdot h_j(\tau_l)], \text{ where } C_i = -C_j \\
&= NP_h \cdot P_J - \sum_{i=1}^{N/2} 2\rho_i P_h \cdot P_J
\end{aligned}$$

At the desired location, all the channels observed by the receiver are correlated, ρ_i then becomes 1, and jamming signals cancel each other. However, receivers at undesired locations observe uncorrelated channels due to channel uncorrelation property. Thus jamming signals still exist at the receiver and can interfere with transmit signals. The combined power of jamming signals is $NP_h \cdot P_J$.

The SNR of the receiver is the ratio of the combined transmit power to the combined noise (i.e. $SNR = \frac{P_{ms}}{P_{mc} + N \cdot N_c}$). At the desired location, channels are synchronized, transmit

signals boost each other and jamming signals cancel each other. Thus, the maximum SNR obtained by the receiver is $\frac{NP_h \cdot P_T}{N_c}$, which is dominated by the transmit signal power, and the receiver can get the desired SNR if appropriate transmit signal power is selected. At the undesired location, constructive interference vanishes and channels become uncorrelated to each other. Accordingly, the SNR at the receiver is $\frac{P_h \cdot P_T}{P_h \cdot P_J + N_c}$. In general, the power of jamming signals is chosen much larger than the channel noise N_c . Thus, the SNR is approximately to $\frac{P_T}{P_J}$. Furthermore, if jamming signal power is chosen at the same level as the transmit signal power, the SNR at undesired receivers approximately reaches 0dB, which means transmit signals cannot be recognized from the noise.

2.5.3.1 Impact of SNR on Service Area Size

As the above discussion, when channels are uncorrelated to each other (i.e. $\rho = 0$), the SNR at the receiver will achieve the minimum value and the receiver can hardly distinguish transmit signals from jamming signals. Theoretically, $\rho = 0$ happens when the receiver is half wavelength far from the desired location. For example, modern wireless devices like WIFI, Bluetooth devices usually uses $2.4GHz$ as their central frequency to transmit signals. The corresponding wavelength is $0.125m$ (i.e. $(3 \times 10^8)/(2.4 \times 10^9) = 0.125m$), and the service area size is $6.125 \times 6.125cm^2$, when real signal and jamming signal have the same power.

In practice, a couple of wavelength may be required to gain such uncorrelated channels. For example, if the uncorrelation is caused by 4 wavelengths, the service size will be $0.5 \times 0.5m^2$. SNR at the undesired location also shows that SNR decreases as the jamming signal power P_j increases. Thus, if we require a smaller service area size in this scenario, we may properly increase the jamming signal power to meet the requirements.

2.5.4 Security Discussion

An attacker against the proposed system can be either active or passive. An active attacker tries to create, interrupt, intercept, block or overwrite the transmit signals to prevent the receiver from obtaining the legitimate service. The active attacker may launch multiple attacks. For example, It may impersonate as an authorized service provider to gain the trust of a receiver; It may inject malicious information into the channel to mislead the receiver; It may jam the receiver so that the receiver cannot obtain the service. However, these active attackers are not unique to our scheme. Existing approaches have been proposed to deal with these attacks. For example, the receiver can establish the cryptographic authentication protocol with the service provider to deal with impersonation attacks and confirm the message integrity[31][32], and spread spectrum techniques like Frequency Hopping Spread Spectrum(FHSS) and Direct Sequence Spread Spectrum (DSSS) can be designed to defend against jamming attacks[33][34].

A specific active attack in the proposed scheme is the replay attack. It seems that an attacker may intentionally introduce a time shift of the received signal at the desired location by duplicating and transmitting the received signal with a small delay. Nevertheless, we can consider such replay attacks as the traditional jamming attacks. Because even the attacker can replay the delayed signal, it cannot disrupt the alignment and cancellation of the original transmit signals at the desired location, which means the receiver will obtain both desired signal and replayed signal. The replayed signal will be served as the noise to decrease the SNR at the receiver and interfere the decoding process. Such attack is different from the scenario when the receiver is located at undesired locations. First, at undesired location, desired signals are distorted and can only achieve poor alignment due to lack of channel and time synchronization. Therefore, the desired signal itself at the undesired location is distorted and may be not able to decode. In addition, jamming signals in the undesired

locations cannot cancel each other. Since the jamming signals are usually chosen the same level as the desired signals, the SNR at the undesired locations will always remain small and can hardly provide a good service.

Therefore, we can apply traditional methods to defend against such replay attacks. First, we may increase the power of transmit signals (both desired signal and jamming signal at the transmitter) to increase the SNR at the desired locations. In addition, we may also apply FHSS or DSSS to increase the robustness of received signals against the replayed signals.

A passive attacker is usually an eavesdropper, which attempts to obtain the legitimate service from the service provider. For a basic eavesdropper, as shown in Lemma 3, when the eavesdropper's channel is totally uncorrelated from the receiver's channel, it will not achieve a boosted SNR to decode the received service data. It seems that multiple eavesdroppers with high-gain, directional antennas may collaborate to add their received signals together to form a boosted signal, with which they can decode the original service data. Nevertheless, even collaborated attackers can obtain jamming entangled signals from different transmitters respectively, these transmit signals are calibrated to accommodate the distinct channels between transmitters and the desired receiver only, and consequently received signals are uncorrelated to each other at attackers. Therefore, the sum of received signals is equivalent to that of multiple random signals, and both channel distortions and jamming signals can significantly interfere the correct decoding of the combined signal. Thus, no matter how many eavesdroppers exist, signals received by these eavesdroppers always suffer from the distortion from jamming signals and the wireless channel fading, and exhibit different shapes as long as their channels are not calibrated for homomorphism at the service provider side. As such, a boosted SNR cannot be obtained for correct decoding.

2.6 Multi-user Mode

Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), and Frequency Division Multiple Access (FDMA) are three typical methods adopted by modern wireless communication systems to support multi-user access. For CDMA, users are assigned with special designed codes that are orthogonal to each other, and an individual user can extract its own data by correlating received signals with the assigned codes. For TDMA and FDMA, users are assigned with distinct, non-overlapping time slots/frequency bands to send and receive wireless signals. By utilizing different codes, time slots, and frequencies, the interferences among wireless users can be eliminated.

In the following, we demonstrate how to integrate traditional multiple access techniques into the pinpoint system to support multiple users. Because the location-restricted service is delivered from the service provider to the receiver, we only discuss how to implement the pinpoint system for the downlink flow of these multiple access techniques.

2.6.1 CDMA Integrated Pinpoint Waveforming

With CDMA, the transmitter can pinpoint the service to each user using their assigned CMDA code. In particular, service provider first assigns each user with a unique code $A^{(n)}$ and the transmitter can then directly encode original signals using the CDMA codes to deliver information to all users. In addition, because users are located at different locations, transmit signals of different users may need to be sent at distinct times to compensate the time difference of arrivals. The following equation exhibits the transmit signals of N users at the m^{th} transmitter.

$$S_m = \sum_{n=1}^N [(D^{(n)} + J^{(n)}) \sum_{k=1}^L a_k^{(n)} g(t - kT_c - T_{md}^{(n)})],$$

where $D^{(n)}$ and $J^{(n)}$ are the desired signal and jamming signal of the n^{th} user respectively. $a_k^{(n)}$ is the k^{th} chip in the code $A^{(n)}$ and T_c is chip time. $T_{md}^{(n)}$ is the time delay of transmit signal of the n^{th} user at m^{th} transmitter. In general, each specific code $A^{(n)}$ is designed to be orthogonal to each other, so that users can extract the desired information by correlating the received signals with their assigned codes. However, in the proposed scheme, because M transmitters cooperate together to pinpoint the service to N users at different positions, time delay $T_{md}^{(n)}$ may vary from different transmitters and different users. Thus, the orthogonality between codes cannot be maintained due to the time difference, and information decoding is significantly interfered by transmit signals of other users.

To eliminate such interference, asynchronous coding scheme is required at the transmitter. In particular, we may apply the pseudo-noise (PN) code adopted by the uplink flow of the traditional CDMA. PN code is a binary sequence that appears random but can be generated in a deterministic manner. Different PN codes are nearly orthogonal and statistically uncorrelated to each other. Therefore, if signals are encoded by different PN codes, their correlation always remains small even when there exists time shift between them. This means undesired signals can only slightly interfere the decoding, and the correct information can be recovered by using the appropriate error correction code.

2.6.2 TDMA Integrated Pinpoint Waveforming

With TDMA, the transmitter can pinpoint the service to each user during its time slot. Specifically, the service provider divides each signal frame into time slots and assigns each user with a particular slot. The transmitter then sends entangled signal of each user at their corresponding time slot. Transmit signal of n^{th} user at m^{th} transmitter is described as follows:

$$S_m^{(n)} = (D^{(n)} + J^{(n)})[u(t - T_{md}^{(n)}) - u(t - T_{md}^{(n)} - T_s - T_g)],$$

where $D^{(n)} + J^{(n)}$ are the jamming entangled signals of the n^{th} user. $u(t)$ is the step function (i.e. $u(t) = 1$, when $t \geq 0$). $T_{md}^{(n)}$ is the delay time of corresponding transmit signals and it is used to compensate for the time difference of arrivals caused by the distinct propagation distance between different transmitters and users. T_s is the time period of each slot. T_g is the guard time to avoid the interference from undesired transmit signals. In particular, the propagation synchronization may introduce overlapping time slots due to the varying time shifts experienced by different users. To solve this, transmitters can insert an appropriate time guard T_g between time slots to eliminate the overlaps and avoid the interference among multiple users.

2.6.3 FDMA Integrated Pinpoint Waveforming

With FDMA, the transmitter can pinpoint the service to each user at the assigned frequency band. If the Orthogonal Frequency-division Multiplexing (OFDM) is enforced, each user will be assigned with a particular sub-carrier and jamming entangled signals of each user will be sent within the corresponding sub-carrier. The transmit signals generated by the OFDM system can be represented by

$$S_m = \frac{1}{\sqrt{T}} \sum_{n=1}^N (D^{(n)} + J^{(n)}) e^{j \frac{2\pi}{T} n(t - T_{md}^{(n)})},$$

where T is the symbol duration, $D^{(n)} + J^{(n)}$ are the corresponding jamming entangled signals, and $T_{md}^{(n)}$ is the time delay of the n^{th} transmit signal. $e^{j \frac{2\pi}{T} n}$ is the assigned subcarrier of the n^{th} user and the whole bandwidth is divided into N pieces in an OFDM system, and accordingly the spectrum assigned to each user is limited. Thus, the receiver may experience a weak multipath effect that causes less distortion to jamming entangled signals. Nevertheless, the amplitude attenuations and phase shifts are different from different locations, without channel synchronization, the jamming entangled signals still exhibit random shapes when

arriving at an undesired receiver, and consequently the jamming portion cannot cancel each other.

2.7 Performance Evaluation

We develop a prototype pinpoint service system on top of the Universal Software Defined Radio Peripherals (USRP), which are radio frequency (RF) transceivers with high bandwidth and high dynamic range processing capability. The USRPs use SBX broadband daughter boards operating in the 400 - 4400 Mhz range as RF front ends. The software toolkit implementing the prototype is the GNURadio [35].

2.7.1 System Design

The receiver is a standalone USRP, and the transmitter (i.e., the service provider) consists of two USRPs connected by an multiple-input and multiple-output (MIMO) cable. Both USRPs follow the master and slave protocol. Specifically, the master USRP connects to both the slave USRP and the host computer, and the slave USRP only connects to the master USRP. The master provides the clock scale and the time reference to the slave USRP through the MIMO cable. The master and slave USRPs are separated by about 0.75 meter to achieve uncorrelated channels between each USRP and the receiver.

Our software program is developed from the Benchmark TX/RX Program, which is the communication tool provided by GNURadio for data transmission and file transfer between two USRPs. The source codes are located at `gnuradio/gr-digital/examples`. For the transmitter, we redesign the modulation block of the Benchmark TX program by adding two new modules, namely jamming signal entanglement and channel calibration modules. We also add a delay compensation module to compensate the difference of signal arrival times measured at the master and slave USRPs. An input bit sequence is first modulated into physical layer symbols, then entangled with jamming signals, and finally transmitted to the receiver



Figure 2.5: Received pictures at different positions

after channel calibration and delay compensation. Because the receiver requires no specific changes, we directly run the Benchmark RX Program at the receiver but add a constellation sink to observe the real time constellation diagram for analyzing the performance.

2.7.2 Example Pinpoint Service

We choose two typical types of service data, pictures and videos, to visually validate the effect of the pinpoint prototype. Figure 2.5 shows the received pictures at different positions. At the desired location, the receiver can successfully download the original picture sent by the transmitter. We then move the receiver 0.1, 0.2, and 0.3 meter away from the desired location, and find a drastic worsening of the packet delivery rate. When the receiver is 0.3 meter away, the picture cannot be displayed at all due to the huge number of packet loss.

We also implement the real-time video transmission that sends a live scene captured by a web camera to the receiver. Specifically, a web camera is connected to the transmitter to surveillance the surrounding of the transmitter. We encode the video stream using MPEG-4 AVC, which is the most commonly used format for video compression, and input the stream into the USRPs through the Linux socket interface. We then pinpoint the stream to the receiver at the desired location. The receiver downloads and decodes packets from the transmitter and displays them on a video player. We observe a clear and fluent video when the receiver is located at the desired position, and the video quality deteriorates when the receiver moves away from undesired locations. In particular, we encounter frequent video sticks while

playing, and severely distorted images. At the physical layer, we find that received symbols significantly deviate from the ideal points on the constellation diagram, thereby yielding a huge amount of demodulation errors. We recorded the video deterioration process and an anonymous demo video on youtube can be found at <https://youtu.be/lJ64bxYP5SM>. In the following, we discuss the details of the evaluation results.

2.7.3 Evaluation Metrics

We evaluate the prototype system using the following typical metrics for measuring the service of quality:

- Signal to noise ratio (SNR): This is the ratio of the received signal power to the noise power, which is the sum of both the jamming signal power and the channel noise power.
- Packet delivery rate: This is the ratio of the number of correctly received packets to the total number of received packets. In the prototype implementation, each packet is appended with a 32-bit cyclic redundancy check (CRC) code for error detection, and prefixed with a 64-bit access code for packet synchronization. The length of each packet is 500 bytes. The receiver detects packets by correlating received bits with the access code. A high correlation indicates the arrival of a packet, and the receiver verifies this packet by looking at the CRC. We consider a packet to be received correctly only if the packet passes CRC check.
- Throughput: Throughput is the number of correctly received packets per unit time. To facilitate the comparison, we normalize the throughput into the range of $0 - 1$. If the throughput is close to 1, the bit rate at the receiver is close to that at the transmitter, and thus the service delay is near zero. If the throughput is 0, no information bits are received at the receiver and the service delay is regarded as infinity.

In addition to the pervious metrics, we also introduce a fourth metric, channel cross-decorrelation, which quantifies disparity between two channels. A small cross-decorrelation value indicates a strong correlation between two channels, and a large value indicates two channels are uncorrelated with each other. We include channel cross-decorrelation as an extra evaluation metric, because the service quality is also highly relevant with this metric. The cross-decorrelation between the channels of desired and undesired locations should be large, so that a receiver at a undesired location cannot obtain a service of good quality.

2.7.4 Measuring Channel Cross-decorrelation

SNR values, packet delivery rate and throughput can be easily measured from the communication traffic based on their definitions above. However, how to measure the last metric channel cross-decorrelation is not as straightforward as the pervious three metrics, because it reflects the disparity among wireless channels that cannot be directly observed. In the following, we discuss our methodology to measure this metric.

To achieve the channel calibration, an accurate channel estimation between the transmitter and the receiver is required. We estimate the channel in a training stage, where the receiver broadcasts a beacon signal to the transmitter, and transmitter then measures the corresponding channel impulse response from the received beacon signal. At the training stage, we measure the channel for 500 times and took the average value as the current channel impulse response. Thus, we can eliminate the impact of the unexpected disturbance caused by the channel noise, normal temporal variations, and other interferences.

Figures 2.6 and 2.7 plot the magnitude (i.e. amplitude attenuation) and phase (i.e phase shift) of the average channel impulse response measured at the two USRPs respectively. The system operates on the central frequency of 2.4 GHz and adopts the binary phase shift keying (BPSK) modulation. The unit of the X-axis is a symbol duration, which is approximately the minimum time required to resolve two paths. We can see that the channels of both

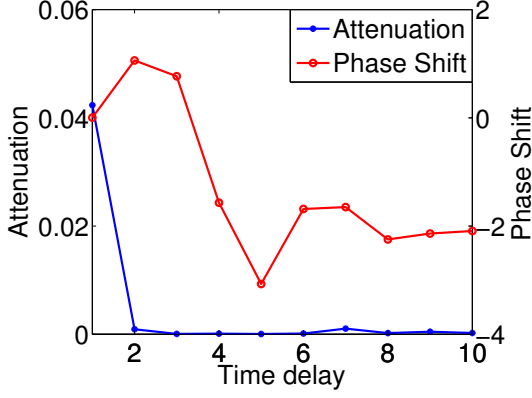


Figure 2.6: USRP 1

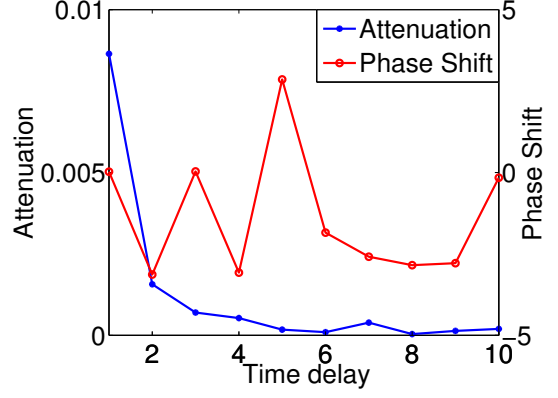


Figure 2.7: USRP 2

USRPs are quite different in shape and magnitude. This observation is consistent with the basic experiment setting, in which both USRPs are separated by a certain distance to ensure the uncorrelated channels.

2.7.4.1 Cross and Auto-variance

Before we introduce how to measure the channel cross-decorrelation to quantize such channel difference, we first define two terms *cross-variance* and *auto-variance* that will be involved in calculating the channel cross-decorrelation. The cross-variance is defined as the Euclidean distance between two different channels. For channels i and j , their average cross-variance V_{ij} is calculated by $\frac{1}{N} \sum_{n=1}^N |h_{in} - h_{avgj}|$, where N is the total number of channel measurements, h_{in} is the n -th estimated channel impulse response of channel i , and h_{avgj} is the average channel impulse response of channel j . When $i = j$, the cross-variance degenerates to the auto-variance V_{ii} , which is the Euclidean distance between an one-time channel measurement and the average of multiple channel measurements for the same channel. In the experiment, we use the average value of the auto-variance over all the channel estimations. Figure 2.8 plots the distributions of the cross and auto-variance of previous channels measured at two USRPs. In addition, we also plot the cross variance of two channels measured after the channel calibration. The cross-variance before the calibration is

much larger than the auto-variance, because the channels of both USRPs are uncorrelated from each other. After the calibration, the cross-variance is closed to the auto-variance within one channel that indicates two channel are quite correlated.

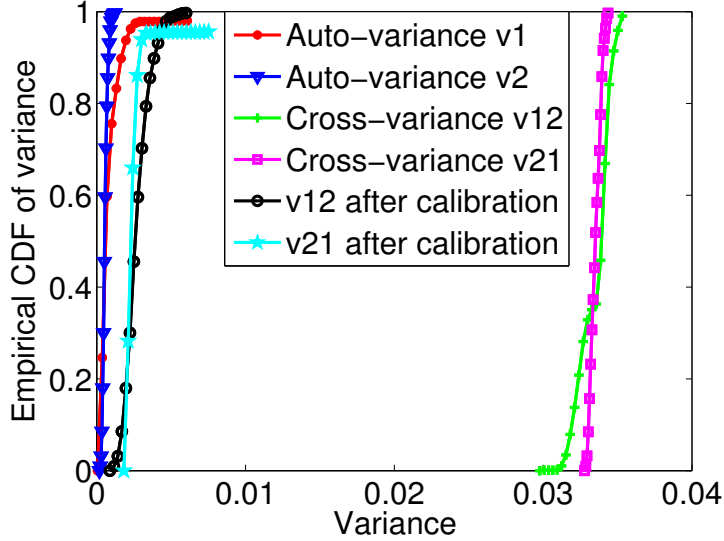


Figure 2.8: Distribution of different variance

2.7.4.2 Channel Cross-decorrelation

We use channel cross-decorrelation to normalize the cross-variance to facilitate the comparisons of the similarity and difference among wireless channels, and the cross-decorrelation R_{ij} between channels i and j is defined as $R_{ij} = \frac{|V_{ij} - V_{jj}|}{\frac{1}{2}|h_{avg i} + h_{avg j}|}$.

A cross-decorrelation value of 0.5 means that the channel difference is as large as 50% of the magnitude of the averages of the two channels. The cross-decorrelation ranges between 0 and 2. If it is larger than 1, the channel difference is even larger than the magnitude of the averages of the two channels. In Figure 2.8, for USRP 1 (master) and USRP 2 (slave), their cross-decorrelations are $R_{12} = 1.28$ and $R_{21} = 1.30$, which indicate that the channels measured at both USRPs are quite different from each other. In addition, after

the calibration, their cross-decorrelations measured are $R_{12} = 0.040$ and $R_{21} = 0.043$, which indicates two channels after the calibration are highly correlated.

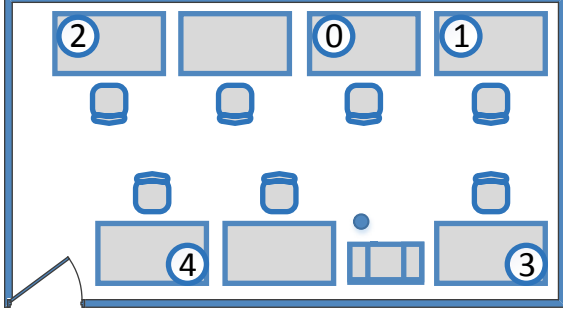


Figure 2.9: Floor plan: Service area size

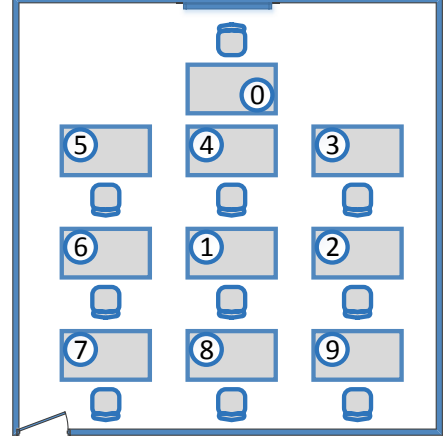
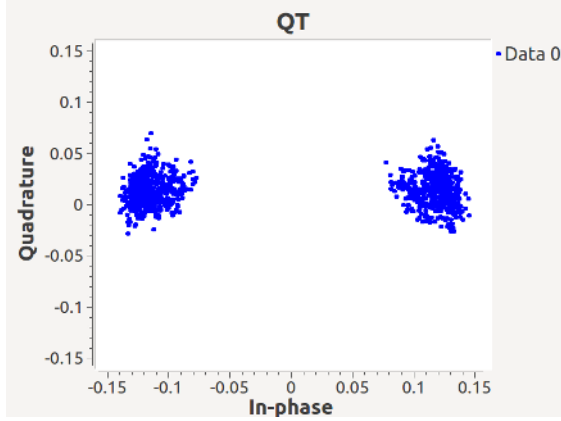


Figure 2.10: Floor plan: pinpoint accuracy

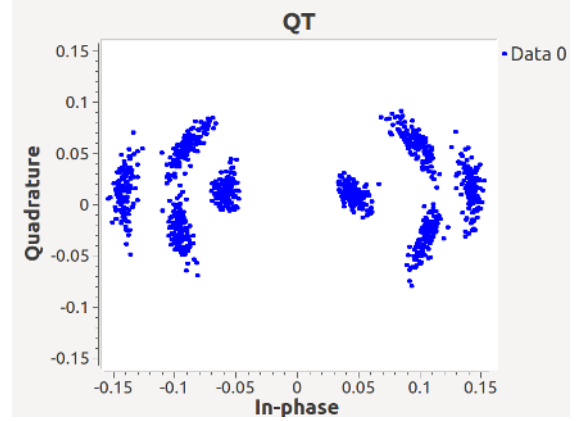
2.7.5 Jamming Signal Entanglement

As mentioned earlier, we entangle the jamming signals into transmit signals to conceal the real information. The jamming signals should cancel each other at the desired location but jam the original signals at undesired locations, so that eavesdroppers at those locations cannot distinguish the original signals from the jamming signals, and thus fail to decode the data.

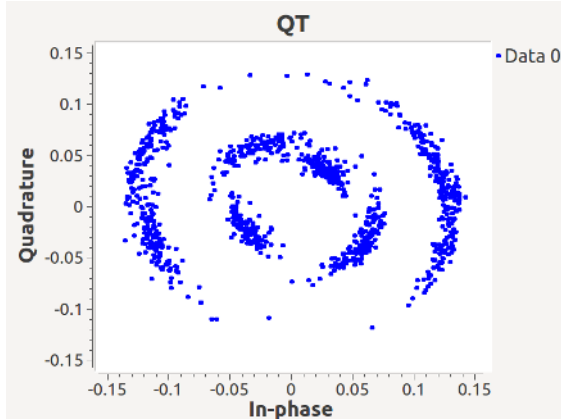
We randomly choose an indoor location, namely Position 1, to place the receiver and calibrate the channel between the receiver and the transmitter. We mark this location as the desired location. We then randomly choose three other locations, namely Positions 2, 3, and 4, that are about 0.1, 0.2, and 0.3 meter away from the desired location respectively. We mark these locations as the undesired locations. Figure 2.11(a) plot the symbols on the constellation diagram with jamming signal entanglement for the desired location, i.e., Position 1. We can see that received symbols converge to the ideal points at Position 1.



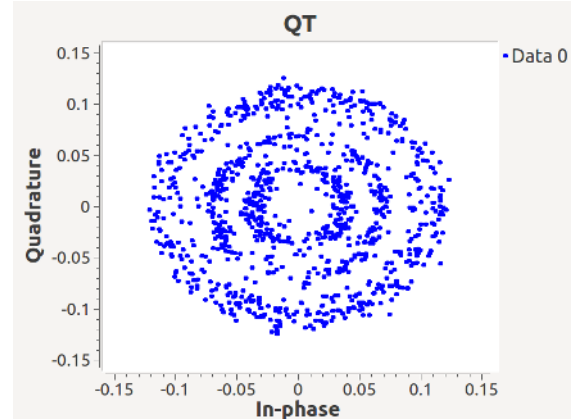
(a) Position1



(b) Position2 (0.1 meter from Position1)



(c) Position3 (0.2 meter from Position1)



(d) Position4 (0.3 meter from Position1)

Figure 2.11: Jamming signal entanglement

Due to slightly imperfect synchronization and normal oscillator shift, jamming signals may not exactly cancel each other and the residue introduces an additional noise that cause the deviation of the received symbols. Nevertheless, such noise is too small to impact the decoding accuracy and the received symbols still closely fluctuate around the ideal points.

Figures 2.11(b), 2.11(c), and 2.11(d) plot received symbols at undesired locations, i.e., Positions 2, 3, and 4, when jamming signal entanglement is enforced. As mentioned earlier, for undesired locations, transmit signals are not calibrated and they arrive at the receiver in different shapes and thus the jamming signals do not cancel each other, leading to a high demodulation error rate. As seen in these figures, received symbols randomly scatter around

the entire constellation diagram, and become more and more difficult to decode with the increasing distance from Position 1, the desired location.

2.7.6 Service Area Size

We would like to explore the service area size achieved by the prototype system in the real world. The experiment environment is a typical indoor room with wooden doors, metal and wooden obstacles, and electronic devices. Figure 2.9 shows the positions of the transmitter and the receiver. The transmitter is placed at Position 0 and we pinpoint the service to Positions 1, 2, 3, and 4. For each test, the transmitter sends 3000 packets to the receiver.

2.7.6.1 Impact of Distance

Without loss of generality, we choose four moving directions for the four positions. For Positions 1, 2, 3, and 4, the receiver moves towards(\Uparrow), backwards(\Downarrow), to the right(\Rightarrow), and to the left(\Leftarrow) of the transmitter. Table 2.1 shows the impact of the distance between the receiver and the desired location on the aforementioned four evaluation metrics, i.e., SNR, packet delivery rate, throughput, and the channel cross-decorrelation. In this test, the system operates on the central frequency of 2.4Ghz and the ratio of desired signal power to jamming signal power is set to 1. In this table, Pos., Dir., D, Corr., and PDR denote position, moving direction, distance between the receiver and the desired location, cross-decorrelation, and packet delivery rate respectively. These abbreviations are also applied for the subsequent tables. As seen in Table 2.1, moving directions cause no noticeable impact on the four metrics. For each of the four desired locations, when the receiver is located at this location, i.e., distance is equal to 0, the receiver achieves the maximum SNR, packet delivery rate, and throughput. When the receiver moves away from this location, the channel cross-decorrelation increases and the corresponding SNR, packet delivery rate, and throughput

decrease significantly. In particular, when the distance reaches 0.3 meter, the throughput at all four positions approximately reaches to 0 and thus no service is received.

Table 2.1: Impact of the distance

Pos.	Dir.	D(cm)	Corr.	SNR	PDR	Throughput
1	↑	0	0.038	14.0	99.71%	0.93
1	↑	10	0.33	5.1	68.75%	0.53
1	↑	20	0.66	3.5	57.41%	0.35
1	↑	30	1.25	-1.4	6.28%	0.012
2	↓	0	0.039	14.0	99.18%	0.93
2	↓	10	0.30	7.0	80.65%	0.61
2	↓	20	0.76	3.4	39.70%	0.17
2	↓	30	1.12	0	19.74%	0.031
3	⇒	0	0.012	14.9	97.61%	0.92
3	⇒	10	0.31	8.2	74.79%	0.47
3	⇒	20	0.72	3.5	41.57%	0.26
3	⇒	30	1.10	0.8	20.08%	0.078
4	⇐	0	0.013	14.9	96.53%	0.90
4	⇐	10	0.25	9.5	85.85%	0.64
4	⇐	20	0.77	4.4	58.95%	0.30
4	⇐	30	1.15	1.5	21.43%	0.062

2.7.6.2 Impact of Central Frequency

Theoretically, reducing the central frequency can enlarge the service area, because it can increase the signal wavelength and therefore raise the distance required for the channel uncorrelation. In this test, we reduce the central frequency from 2.4 Ghz to 1.2 Ghz to remeasure the four metrics at Positions 1 and 2, the ratio of desired signal power to jamming signal power remains unchanged (i.e 1), and the results are shown in Table 2.2. For the 2.4 Ghz central frequency shown in table2.1, when the receiver is moved 0.3 meter away from the desired location, the channel cross-decorrelation is 1.21 and 1.16 at Positions 1 and 2 respectively. For the 1.2 Ghz central frequency shown in table2.2, a similar channel cross-decorrelation, i.e., 1.25 at Positions 1 and 1.12 at position 2, is achieved with an increased

distance of 0.45 meter. Thus, a lower frequency can cause a larger service area. This experimental observation is consistent with the theoretical conclusion.

Table 2.2: Impact of the central frequency (1.2Ghz)

Pos.	Dir.	D(cm)	Corr.	SNR	PDR	Throughput
1	↑	0	0.018	26.0	99.42%	0.96
1	↑	15	0.29	10.45	88.33%	0.77
1	↑	30	0.65	4.1	63.93%	0.33
1	↑	45	1.21	0	20.66%	0.089
2	↓	0	0.025	22.5	99.33%	0.98
2	↓	15	0.34	8.0	88.75%	0.56
2	↓	30	0.74	4.4	62.27%	0.35
2	↓	45	1.16	0	14.45%	0.055

2.7.6.3 Impact of Signal to Jamming Power Ratio

As discussed in Section 2.5.2, we can reduce the service area size by decreasing the ratio of desired signal power to jamming signal power. Unlike previous experiment settings that use a ratio of 1, we decrease the ratio from 1 to 0.5 to test the impact in position 1 and 2, and our experimental observation matches the previous discussion result. Specifically, as shown in table2.1 with a ratio of 1, the throughput reduces to approximately 0 when the receiver is 0.3 meter away from a desired location. However, with a ratio of 0.5, the throughput reaches zero when the receiver is 0.2 meter away from the desired location as shown in table2.3. So the service area shrinks with the decreasing signal to jamming power ratio.

Table 2.3: Impact of the power ratio of desired signal to jamming signal (ratio = 0.5)

Pos.	Dir.	D(cm)	Corr.	SNR	PDR	Throughput
1	↑	0	0.042	10.1	90.33%	0.72
1	↑	10	0.36	1.3	25.76%	0.12
1	↑	20	0.67	-1.15	4.78%	0.01
2	↓	0	0.039	11.0	96.28%	0.69
2	↓	10	0.35	1.9	32.33%	0.13
2	↓	20	0.74	-1.3	23.93%	0.024

2.7.7 Pinpoint Accuracy

We test how accurate the prototype system can pinpoint the service to a desired location in a meeting room. Figure 2.10 shows the positions of the transmitter and receivers. We place the transmitter in the front of the room (i.e. position 0) and the desired receiver in the middle of the room (i.e. Position 1). We also place 8 eavesdroppers scattering around the desired receiver (i.e. at Positions 2 to 9). The wireless communication system operates on the central frequency of 2.4GHz and adopts the binary phase shift keying (BPSK) modulation. The power ratio of the desired signal to jamming signal is set to 1 and the bit rate is 1Mbps.

The pinpoint accuracy is displayed in Table 2.4. The receiver at the desired location can approximately achieve a SNR of 14dB, a packet delivery rate of 99.27%, and a throughput of 0.98, while eavesdroppers at undesired locations get a much worse performance. For example, an eavesdropper at position 5 can only achieve a SNR of 1.6dB, a packet delivery rate of 23.26%, and a throughput of 0.03. In addition, even an eavesdroppers is located closer to the transmitter than the receiver (e.g. position 4), its performance is still quite limited (e.g., a SNR of 0.8dB, a packet delivery rate of 13.70%, and a throughput of 0.02) due to the poor jamming signal cancelation.

Table 2.4: Pinpoint accuracy

Pos.	Cross-decorrelation	SNR	PDR	Throughput
1	0.026	14.0	99.27%	0.98
2	0.65	2.4	31.68%	0.20
3	0.81	2.4	19.39%	0.12
4	0.92	0.8	13.70%	0.02
5	1.14	1.6	23.26%	0.03
6	0.91	1.9	23.71%	0.07
7	1.66	-1.5	2.69%	0.003
8	1.62	-1.0	24.72%	0.02
9	0.96	0	29.69%	0.04

2.8 Related Work

The proposed pinpoint system utilizes multiple antennas to deliver the service data to desired locations. The existing Multiple Input Multiple Output (MIMO) techniques (e.g., [36, 24, 37, 2]) also explore multiple antennas to achieve high transmission efficiency. The antennas used in MIMO systems can send same signals to enhance the reliability of the data transmission (e.g., [36]), or different signals to increase the capacity of the wireless channel (e.g., [2]). With the proliferation of beamforming techniques [3], multiple directional antennas have been recently integrated into MIMO systems to grant the wireless accesses to different users simultaneously. This technique is known as MU-MIMO. However, MIMO and MU-MIMO techniques do not aim to pinpoint service data to desired locations. For these techniques, any user residing in the signal coverage range of the antennas can hear the transmit data.

There exist two other recent papers that are relevant to this one. The scheme proposed in [38] utilizes multiple directional antennas to deliver the service to desired locations. Specifically, each antenna sends different portion of an original message, and thus this message can be reconstructed at locations where transmit signals overlap each other. However, due to the lack of channel calibration, an attacker with high-gain, directional antennas can still capture the transmit signals to recover the original information, even if they are not at the desired locations. The scheme presented in [39] proposes to jam undesired locations to prevent illegal accesses to the confidential data, whereas this paper provides service to desired locations through jamming entanglement. Both papers are complementary to each other.

2.9 Summary

In the paper, we propose the pinpoint waveforming system to enable location-oriented service access control. To design such a system, we create the channel calibration technique

that compensates the channel distortion and enables signals sent by different transmitters to arrive at the desired receiver with the same shapes. We also created the jamming entanglement technique that introduces jamming signals to significantly reduce the SNR at the eavesdropper but raise the SNR at the desired receiver. We develop a prototype system using USRPs and the experiment evaluation results validate the feasibility of the proposed system.

CHAPTER 3

FAR PROXIMITY IDENTIFICATION IN WIRELESS SYSTEMS

In this chapter¹, we develop a novel fingerprinting technique that enables the local device to extract the fingerprint of a wireless device’s proximity from the physical-layer features of signals sent by the device. We also present a theoretical analysis to demonstrate the feasibility of the far proximity identification using the proposed fingerprint. We validate and evaluate the effectiveness of the proposed far proximity identification method through experiments on the real-world data. The experiment results show that the proposed approach can detect the far proximity with a success rate of 0.85 for the non-Line-of-sight (NLoS) scenario, and the success rate can be further increased to 0.99 for the Line-of-sight (LoS) scenario.

3.1 System and Threat Models

To facilitate the presentation, we refer to the local device, which verifies the proximity, as the *verifier* and the remote device, whose proximity is being verified, as the *prover*. The verification system consists of a verifier and a prover. Both are equipped with radio interfaces that can transmit and receive wireless signals.

The verifier aims to determine whether or not a prover is at least a certain distance away, and it analyzes the signals emitted by the prover to achieve this goal. The verifier can work in both *active* or *passive* modes. In the active mode, the verifier sends a message to the prover to initialize the proximity identification, and the prover cooperates with the verifier

¹This chapter was published in ESORICS 2014 [17]. Permission is included in Appendix 5.

by sending wireless signals back to the verifier to enable the verification. In the passive mode, instead of actively sending out signals, the verifier monitors the wireless channel to capture the prover’s signal. Once the prover’s signals are captured, the verifier can identify the prover’s proximity.

We assume that the prover is untrusted. The prover may provide the verifier with fake messages and wrong configuration information regarding its hardware and software settings, such as device type, signal processing delay, and protocols in use. The prover may intentionally delay its replies to the verifier’s messages or send bogus replies at any time to mislead the verifier. However, we assume that the verifier can receive wireless signals sent by the prover. As the long-haul wireless applications (e.g., space communications and TV broadcasting) usually have the stronger LoS feature, we assume that there are no metal shields on the straight line between the verifier and the prover to block wireless signals from the prover.

3.2 Far Proximity Verification

A simple and naive method to identify whether a prover is far away is to examine the received signal strength (RSS). A signal decays as it propagates in the air. Thus, it seems that strong RSS indicates a short signal propagation length and a close transmitter, whereas weak RSS strength implies a far-away transmitter. However, a dishonest prover can increase or decrease its transmit power to pretend to be close to, or far from, the verifier. The root reason for the failure of the naive method is that RSS can be easily forged. In this paper, we discover unforgeable and unclonable *fingerprints* of the proximity and propose techniques that can identify the far proximity based on these fingerprints.

3.2.1 Proximity Fingerprints

Because of the multipath effect [40], a signal sent by the prover generally propagates to the verifier in the air along multiple paths due to reflection, diffraction, and scattering. Each path has an effect (e.g., distortion and attenuation) on the signal traveling on it [41]. A *channel impulse response* characterizes the overall effects imposed by the multipath propagation, and it reflects the physical feature of a wireless link [40]. Because it is difficult to change the physical feature, channel impulse responses have been used as "link signatures" to uniquely identify the wireless link between a wireless transmitter and a receiver [42, 41, 43].

Figure 3.1 (a) shows a simple example of multipath propagation. The signal sent by the prover is reflected by an obstacle (i.e., a building), and thus it travels along Path 1 (the direct path from the prover to the verifier), and Path 2 (the reflection path). The signal copy that travels along one path is usually referred to as a *multipath component* [40]. Let r_1 and r_2 denote the multipath components that travel along Path 1 and Path 2 respectively. Figure 3.1 (b) is an example of the corresponding channel impulse response, which shows that r_1 arrives at the verifier first and the peak of the signal amplitude of r_1 is A_{r_1} , and r_2 arrives after r_1 , and its peak is A_{r_2} .

Intuitively, if the prover increases (decreases) the transmit power, both A_{r_1} and A_{r_2} will increase (decrease), but the prover cannot adjust its transmit power such that it arbitrarily manipulates only one of A_{r_1} and A_{r_2} , because it is difficult for the prover to identify and modify the physical paths over which multipath components propagate [41]. On the other hand, the length of the signal propagation path is closely related to the amplitude of the received signal. A far-away prover results in weaker A_{r_1} and A_{r_2} than a close prover. Based on this intuition, we give the definition of proximity fingerprint below.

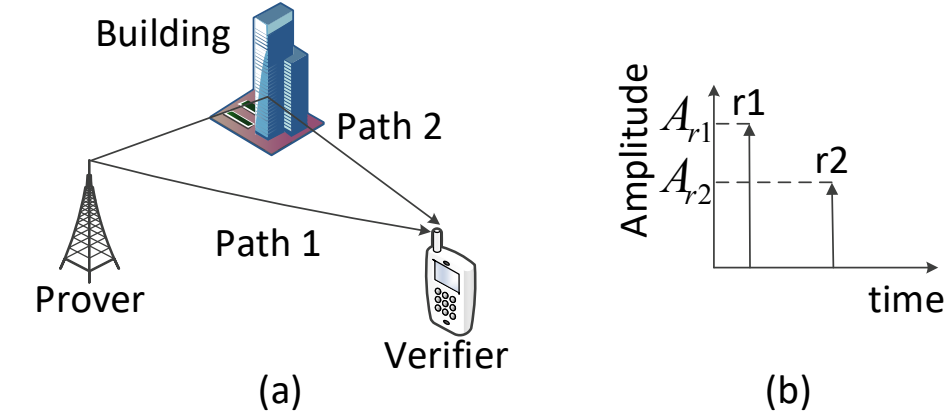


Figure 3.1: An example of the multipath effect.

Definition 1 (Proximity Fingerprint) *Let A_{r1} and A_{r2} be the amplitudes of the first and the second received multipath components, respectively. The proximity fingerprint f is the ratio of A_{r1} to A_{r2} , i.e., $f = \frac{A_{r1}}{A_{r2}}$.*

In Lemma 5, we prove that increasing or decreasing the transmit power does not affect the proximity fingerprint.

Lemma 5 *Let P_t denote the transmit power. Let P_{r1} and P_{r2} be the amplitudes of the first and the second received multipath components. If the prover changes P_t to nP_t ($n > 0$), then both P_{r1} and P_{r2} will change to $\sqrt{n}P_{r1}$ and $\sqrt{n}P_{r2}$.*

Proof: The amplitude P_r of a received signal can be modeled as [40]

$$P_r = \begin{cases} \sqrt{P_t k (\frac{d_0}{d})^\alpha} & d > d_0, \\ \sqrt{P_t k} & d \leq d_0, \end{cases} \quad (3.1)$$

where P_t is the transmit power, d is the length of the path along which the signal propagates from the transmitter to the receiver ($d > d_0$), k is a scaling factor whose value depends on the antenna characteristics and the average channel attenuation, d_0 is a reference distance for the antenna far-field, and α is the path loss exponent. The values of k , d_0 , and α can

be obtained either analytically or empirically [40]. Assume $d_1 > d_0$ and $d_2 > d_0$. Thus, according to Equation 3.2.2.2, P_{r1} and P_{r2} can be approximated by

$$P_{r1} = \sqrt{P_t k \left(\frac{d_0}{d_1}\right)^\alpha}, \quad P_{r2} = \sqrt{P_t k \left(\frac{d_0}{d_2}\right)^\alpha}, \quad (3.2)$$

where d_1 and d_2 are the lengths of the path along which the first and the second received multipath components travel respectively. If P_t is changed to nP_t ($n > 0$), then P_{r1} and P_{r2} will accordingly change to $\sqrt{n}P_{r1}$ and $\sqrt{n}P_{r2}$, and the proximity fingerprint (the ratio of P_{r1} to P_{r2}) remains the same.

Note that due to the bandwidth limitation, the verifier can only distinguish two signals when their arrival time difference is larger than the resolvable time (i.e., $1/B$, where B is the channel bandwidth). Therefore, P_{r1} and P_{r2} may not be the amplitude of received signals from exact first and second paths. Nevertheless, Lemma 5 always holds as long as the prover cannot modify P_{r1} and P_{r2} simultaneously.

3.2.1.1 Key Features of Proximity Fingerprints

Lemma 5 shows that the prover cannot adjust its transmit power to arbitrarily manipulate the proximity fingerprint, but it appears that an attacker (i.e., a dishonest prover or a third-party adversary against benign provers) could affect the proximity fingerprint by intentionally placing a reflector nearby the prover to generate a fake path, in addition to the direct signal path from the prover to the verifier.

However, at the verifier's view, the direct and fake paths are still one unresolvable path if the difference between the arrival times of the signals traveling on both paths is much smaller than the symbol duration, which is the transmission time of a wireless physical-layer unit [40]. To be successful, an attacker has to place the reflector far enough away from the prover (i.e., δc meters, where δ is the symbol duration and c is the speed of light [40]), such

that the difference between the two path arrival times is resolvable at the verifier. More crucially, at this distance the attacker must make sure that the prover’s signal can exactly hit his reflector and be bounced back to the target verifier. However, it is quite uncertain for the prover’s signal to be delivered to the reflector, then reflected by the reflector to the verifier due to the random scattering effect caused by long distance propagation [40].

For example, GPS satellites have a typical symbol duration of 0.01 second [44]. It is impractical for the satellite’s signal to exactly hit a reflector that is 3,000,000 meters away, and moreover be reflected by the reflector to hit a target GPS navigation device on earth.

To summarize, proximity fingerprints are caused by wireless reflections somewhere, which the verifier does not need to know and identify. The verifier can easily extract A_{r1} and A_{r2} from the channel impulse response and compute the proximity fingerprint as A_{r1}/A_{r2} . Note that estimating the channel impulse responses is a must-have function for most modern wireless systems [40, 45]. But in order for the attacker to be successfully, the attacker has to know (1) how to pinpoint a far-away place to put a reflector or an active wireless device, and (2) exactly where to direct the reflector to shoot a needle in a haystack. Thus, significant practical hurdles exist for attacking proximity fingerprints. In this way, verifiers can easily extract proximity fingerprints, but it is difficult for attackers to forge or manipulate a specific fingerprint.

The attacker may also launch active attacks to undermine the verification of proximity fingerprints. In later section (3.3), we will discuss these active attacks and the corresponding countermeasures.

3.2.1.2 Impact of Directional Antennas

When directional antennas are used, the multipath effect may be reduced. However, directional antennas cannot provide perfect laser-like radio signals. For example, the beamwidth of a 3-element Yagi Antenna, the most common type of directional antenna, is 90 degrees

in the vertical plane and 54 degrees in the horizontal plane [46]. Thus, it is not possible to completely eliminate the multipath effect, and accordingly the multipath propagation has been also considered in designing wireless communication systems equipped with directional antennas (e.g., [47, 48]). The proximity fingerprint can be calculated based on a very limited number of paths (i.e., two paths), and thus it is compatible to wireless systems with directional antennas in use.

3.2.1.3 Proximity Fingerprint with Single or Many Peaks

In cases where channel has more than two resolvable peaks, we still select the first two peaks to estimate the distance. That's because the first two peaks are usually largest ones in channel and more resilient to the channel noise.

The scheme cannot be applied to the scenario where CIR only has one peak. But such situation happens only when the signals are transmitted through the ideal environment (e.g. free space propagation) or within a narrow bandwidth. Practical GPS or cellular networks do not assume free space propagation. In addition, even the transmit signals have a narrow bandwidth (e.g. 5MHz or 10MHz), it's still highly likely that the CIR has multiple resolvable peaks due to the long propagation distance (e.g. thousands of meters). For example, if the signal bandwidth is 5MHz, the resolvable time is about 0.2 microsecond and thus the minimum path difference required to distinguish two peaks is about 60 meters. Since the transmitter is usually thousands of meters away from the receiver, it's highly possible that there exist two propagation paths whose distance difference is larger than 60 meters.

3.2.2 Far Proximity Identification Using Proximity Fingerprints

Based on the study of proximity fingerprint, we now reveal the relationship between the proximity fingerprint and the actual proximity, and we propose far proximity identification

techniques that can provide fine granularity and lower bounds on proximity (i.e., the prover is at least a certain distance away from the verifier) using the proximity fingerprint.

To calculate the proximity of the prover, we first model the fingerprint of the proximity. We consider signal propagation in two typical wireless environments, i.e., the outdoor and the indoor environments.

There are multiple signal propagation models that characterize the path loss of wireless signals, such as the free space path loss model, ray tracing path loss models, the simplified path loss model, and empirical path loss models [40]. The common feature of these models is that they all indicate that the power of the transmitted signal decreases as the propagation distance increases. In the channel impulse response, each resolvable multipath component is the superposition of multiple non-resolvable signals arriving within the resolvable time. Because the empirical path loss model is able to characterize the path loss in complex propagation environments, we would like to apply the empirical model to quantitatively estimate the amplitude of resolvable multipath component in channel response. In the following discussion, without loss of generality, we focus on two well-known propagation models (Okumura Model [40] and ITU Indoor Propagation Model [45]) for both outdoor and indoor environments.

We assume that there are no large metallic obstacles that can significantly block the straight line propagation between the verifier and the prover. Thus, the first received multipath component normally travels along the straight line due to the penetration and diffraction-around-object effect, and the propagation distance is approximately d meters, where d is the distance between the verifier and the prover. The second received multipath component travels along a reflection path. Assume that the difference between the arrival times of the first and the second multipath components is Δt . The propagation distance of the second arrived multipath component is thus $d + \Delta t c$ meters, where c is the speed of light.

3.2.2.1 Outdoor Signal Propagation

One of the most common models for outdoor signal propagation in urban, suburban, and rural areas is the Okumura Model [40]. According to the Okumura model, the signal path loss in decibels (dB) in urban areas can be modeled as

$$\begin{aligned} L(\text{dB}) &= 69.55 + 26.16 \log_{10}(f_c) - 13.82 \log_{10}(h_{te}) \\ &- a(h_{re}, f_c) + (44.9 - 6.55 \log_{10}(h_{te})) \log_{10}(d), \end{aligned}$$

where d is the length of the path along which the signal propagates from the transmitter to the receiver, f_c is the central frequency, h_{te} and h_{re} are the transmitter's and the receiver's antenna heights respectively, and $a(h_{re}, f_c)$ is a correction factor computed using h_{re} and f_c [40]. Based on the Okumura Model, we give Lemma 6

Lemma 6 *The proximity fingerprint in the outdoor environment is $\sqrt{(\frac{d_2}{d_1})^{\frac{\gamma}{10}}}$, where d_1 and d_2 are the lengths of the paths along which the first and the second received multipath components travel respectively, $\gamma = 44.9 - 6.55 \log_{10}(h_{te})$, and h_{te} is the transmitter's antenna height.*

Proof: The received signal power P_r can be represented as $P_r(\text{dB}) = P_t(\text{dB}) - L(\text{dB})$, where P_t is the transmit power. To facilitate the calculation, we change the unit of P_r from dB to watt (W). The relationship between $P_r(\text{dB})$ and $P_r(\text{W})$ is $P_r(\text{dB}) = 10 \log_{10} P_r(\text{W})$. Thus, we can derive

$$P_r(\text{W}) = 10^{\frac{1}{10}(P_t(\text{dB}) - L(\text{dB}))} = \frac{10^{\frac{1}{10}P_t(\text{dB})}}{10^{\frac{1}{10}L(\text{dB})}} = \frac{P_t(\text{W})}{L(\text{W})}.$$

Similarly, we can derive $L(\text{W})$ as

$$L(\text{W}) = 10^{\frac{1}{10}L(\text{dB})} = 10^{\frac{1}{10}(\beta + \gamma \log_{10}(d))},$$

where $\beta = 69.55 + 26.16 \log_{10}(f_c) - 13.82 \log_{10}(h_{te}) - a(h_{re}, f_c)$ and $\gamma = 44.9 - 6.55 \log_{10}(h_{te})$.

The amplitude of a signal is the square root of the received signal power. Thus, the amplitudes A_{r1} and A_{r2} of the first and the second received multipath components can be represented by

$$A_{r1} = \sqrt{P_{r1}(W)} = \sqrt{\frac{P_t(W)}{10^{\frac{1}{10}(\beta + \gamma \log_{10}(d_1))}}},$$

$$A_{r2} = \sqrt{P_{r2}(W)} = \sqrt{\frac{P_t(W)}{10^{\frac{1}{10}(\beta + \gamma \log_{10}(d_2))}}},$$

where d_1 and d_2 are the lengths of the paths along which the first and the second received multipath components travel respectively. Note that both multipath components have the same values for γ and β , because they are from the same signal source (i.e., the prover) and exhibit the same frequency f_c . Thus, the proximity fingerprint f can be written as

$$f = \frac{A_{r1}}{A_{r2}} = \sqrt{\left(\frac{d_2}{d_1}\right)^{\frac{\gamma}{10}}}. \quad (3.3)$$

According to the Okumura model, the signal path loss models in suburban and rural areas are, respectively,

$$L_{suburban}(\text{dB}) = L(\text{dB}) - 2[\log_{10}(f_c/28)]^2 - 5.4,$$

and

$$L_{rural}(\text{dB}) = L(\text{dB}) - 4.78[\log_{10}(f_c)]^2 + 18.33 \log_{10}(f_c) - K,$$

where K ranges from 35.94(countryside) to 40.94 (desert). By using the same analytical approach, we can obtain the similar result that the proximity fingerprint in the suburban and rural areas is $\sqrt{\left(\frac{d_2}{d_1}\right)^{\frac{\gamma}{10}}}$.

3.2.2.2 Indoor Signal Propagation

The path loss in the indoor environment can be usually represented by the ITU Indoor Propagation Model [45] as shown below

$$L(\text{dB}) = 20 \log f_c + \lambda \log d + P_f(N_f),$$

where λ is the empirical path loss at the same floor, N_f denote the number of floors between the transmitter and receiver, and $P_f(N_f)$ denotes the floor penetration loss. Based on the ITU indoor model, we give Lemma 7

Lemma 7 *The proximity fingerprint in the indoor environment is $\sqrt{(\frac{d_2}{d_1})^{\frac{\lambda}{10}}}$, where d_1 and d_2 are the lengths of the paths along which the first and the second received multipath components travel respectively, and λ is the empirical floor penetration loss factor.*

Proof: As discussed earlier, the received signal power P_r can be represented as $P_r(\text{dB}) = P_t(\text{dB}) - L(\text{dB})$. By converting the unit of P_r from dB to W, we can obtain

$$P_r(\text{W}) = \frac{P_t(\text{W})}{L(\text{W})} = \frac{P_t(\text{W})}{10^{\frac{1}{10}(20 \log f_c + \lambda \log d + P_f(N_f))}}.$$

The proximity fingerprint, the ratio of A_{r1} to A_{r2} can be written as

$$f = \frac{\sqrt{P_{r1}(\text{W})}}{\sqrt{P_{r2}(\text{W})}} = \sqrt{(\frac{d_2}{d_1})^{\frac{\lambda}{10}}}. \quad (3.4)$$

3.2.2.3 Far Proximity Identification

Assume there are no large metallic obstacles that can significantly block the signal propagation between the verifier and the prover. The path that the first received multipath component usually travels along (i.e., Path 1) is roughly straight between the verifier and the prover due to penetration and diffraction-around-obstacles features of wireless signals [40].

Thus, d_1 approximately equals to the distance between the verifier and the prover. The lower bound of d_1 is given in Lemma 8.

Lemma 8 *Let d be the distance between the prover and the verifier. We have $d \geq \frac{c}{B(f^{\frac{2}{\alpha}} - 1)}$, where c is the speed of light, B is the bandwidth of the communication system, α is the path loss exponent, and f is the proximity fingerprint.*

Proof: Let t denote the time at which the prover's signal starts to propagate to the verifier. Let t_1 and t_2 denote the arrival times of the first and the second received multipath components, respectively. Therefore, $d_1 = (t_1 - t)c$ and $d_2 = (t_2 - t)c$, and we have the following:

$$d_2 = (t_2 - t)c = (t_1 - t)c + (t_2 - t_1)c = d_1 + \Delta c,$$

where $\Delta = t_2 - t_1$. From Equations 3.3 and 3.4, we know that for both the outdoor and indoor environments, the proximity fingerprint f can be generalized by the same expression $f = \sqrt{(\frac{d_2}{d_1})^\alpha}$, where α equals to $\frac{\gamma}{10}$ and $\frac{\lambda}{10}$ for the outdoor and indoor propagation respectively. The first received multipath component travels along the straight line between the verifier and the prover. Hence, the distance d between the verifier and the prover is equal to d_1 . According to [40], for resolvable multiple path components, $\Delta \geq \frac{1}{B}$, where B is the bandwidth of the wireless communication system. Thus,

$$f = \sqrt{(\frac{d_2}{d_1})^\alpha} = \sqrt{(\frac{d + \Delta c}{d})^\alpha}$$

and we have

$$f \geq \sqrt{(\frac{d + \frac{c}{B}}{d})^\alpha},$$

and

$$d \geq \frac{c}{B(f^{\frac{2}{\alpha}} - 1)}. \quad (3.5)$$

3.2.2.4 Fine-grained Proximity Identification

A more accurate time difference estimation between arrivals can be obtained from the measured channel impulse response. Figure 3.2 shows an example of a real-measured channel impulse response obtained from the CRAWDAD data set [49], which contains channel impulse responses collected in an indoor environment with obstacles (e.g., cubicle offices and furniture) and scatters (e.g., windows and doors). As shown in Figure 3.2, the time difference between the first and second peaks is about 75 nanoseconds. Since signals arriving within the resolution time cannot be distinguished from each other, the estimation error is considered as $\pm \frac{1}{2B}$, where B is the bandwidth of the communication system. Assume the time difference observed from the channel impulse response is δt , we can model the time difference range as $(\delta t - \frac{1}{2B}, \delta t + \frac{1}{2B})$.

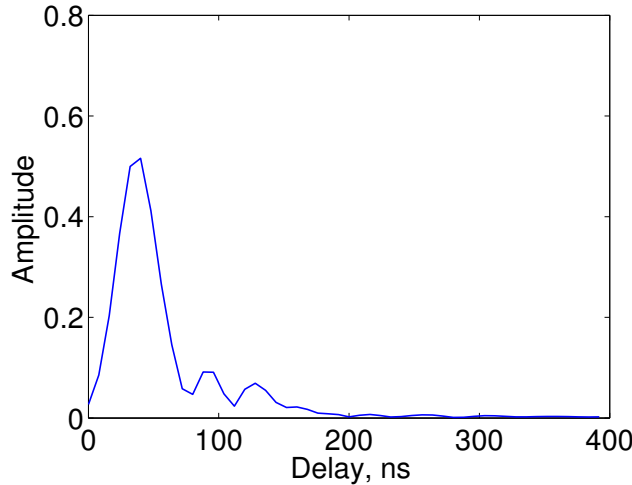


Figure 3.2: An example of the real-measured channel impulse response obtained from the CRAWDAD data set

We would like to utilize such fine-grained time difference to further refine the proximity identification. In addition, with the range of the time difference, we can yield both lower and upper bounds of the proximity between the verifier and the prover. Assume the estimated time difference is within $(\delta t - \frac{1}{2B}, \delta t + \frac{1}{2B})$. We have Lemma 9 as stated below:

Lemma 9 *Let d be the distance between the prover and the verifier. d can be estimated within the range of $(\frac{(\delta t - \frac{1}{2B})c}{f^{\frac{2}{\alpha}} - 1}, \frac{(\delta t + \frac{1}{2B})c}{f^{\frac{2}{\alpha}} - 1})$, where c is the speed of light, α is the path loss exponent, and f is the proximity fingerprint.*

Proof: In the proof of Lemma 8, we generalize the proximity fingerprint f as $f = \sqrt{\frac{d_2}{d_1}^\alpha}$, where d_1 and d_2 are the propagation distance of the first and second multipath components respectively. Since the first received multipath component approximately travels along the straight-line between the verifier and the prover, we have $d = d_1$.

Assume the time difference between two multipath components is Δt . We have the relationship between d_1 and d_2 as $d_2 = d_1 + \Delta t c$, where c is the speed of light. By substituting the relationship into the proximity fingerprint, we can derive the distance as the following equation 3.6:

$$d = \frac{\Delta t c}{f^{\frac{2}{\alpha}} - 1}. \quad (3.6)$$

Since the time difference Δt is within the range of $(\delta t - \frac{1}{2B}, \delta t + \frac{1}{2B})$, where δt is the time difference observed from the corresponding channel impulse response, we can have the upper bound of the distance between the prover and verifier by substituting $\Delta t \leq \delta t + \frac{1}{2B}$.

$$d \leq \frac{(\delta t + \frac{1}{2B})c}{f^{\frac{2}{\alpha}} - 1}.$$

Similarly, lower bound of the proximity can be obtained by substituting $\Delta t \geq \delta t - \frac{1}{2B}$ into the equation 3.6.

$$d \geq \frac{(\delta t - \frac{1}{2B})c}{f^{\frac{2}{\alpha}} - 1}.$$

Therefore, we have the proximity range between the prover and the verifier as $(\frac{(\delta t - \frac{1}{2B})c}{f^{\frac{2}{\alpha}} - 1}, \frac{(\delta t + \frac{1}{2B})c}{f^{\frac{2}{\alpha}} - 1})$.

3.2.2.5 Choosing α

For the outdoor signal propagation, according to the Okumura model, $\gamma = 44.9 - 6.55 \log_{10}(h_{te})$, where h_{te} is the height of the transmitter's antenna. If the verifier has specific types of targets, for example, the verifier aims to verify the proximity of a satellite, a cellular base station, or a TV tower, then the verifier can directly compute γ by looking up the typical values of h_{te} from the corresponding wireless device handbooks. Alternatively, the verifier can also get an estimate of γ by using the typical transmitter antenna height in the outdoor environment (e.g., the typical transmitter antenna height ranges between 1 to 200 meters [45], and thus γ approximately lies between 44.9 and 29.83). After obtaining γ , the verifier can compute $\alpha = \frac{\gamma}{10}$. For the indoor signal propagation, $\alpha = \frac{\lambda}{10}$, where λ is the indoor path loss factor that doesn't rely on the antenna height and it can be obtained through empirical experiments.

Note that the path loss exponent α for both outdoors and indoors can be actually regarded as an attenuation factor that reflects the attenuation caused by the propagation path [50]. Previous studies have performed extensive empirical experiments to measure typical values of such an attenuation factor in different wireless environments [40]. For example, the attenuation factor is 2.0 for vacuum free space, 2.7–3.5 for urban areas, 3.0–5.0 for suburban areas, and 1.6–1.8 for indoors [40]. In the following discussion, without loss of generality, we use these typical empirical values of the attenuation factor as the example α . Nevertheless, the verifier can obtain α empirically using existing readily-available approaches (e.g., [51, 52]),

and a real-measured attenuation factor can help to improve the accuracy of the proximity lower bound estimation.

3.2.2.6 Experimental Examples

Figure 3.3 shows the estimated lower bound of the proximity as a function of the proximity fingerprint f . The speed of light c is 2.99792458×10^8 , and the bandwidth B is 20 Mbps. From Figure 3.3, we can see that the proximity lower bound of the prover decreases as the proximity fingerprint f increases. The indoor environment has the smallest α , and with $f = 5$ the verifier can know that the prover is at least 3.01 meters away. The suburban environment has the largest α , and with $f = 5$ the verifier can know that the prover is at least 16.59 meters away.

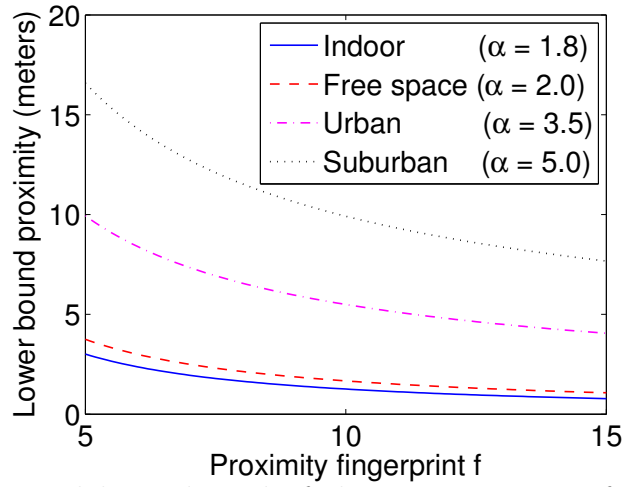


Figure 3.3: The estimated lower bound of the proximity as a function of the proximity fingerprint f . The indoor environment has the smallest α , and with $f = 5$ the verifier can know that the prover is at least 3.01 meters away. The suburban environment has the largest α , and with $f = 5$ the verifier can know that the prover is at least 16.59 meters away.

As mentioned, figure 3.2 shows an example of a real-measured channel impulse response obtained from the CRAWDAD data set. The channel impulse response was measured when the distance between the transmitter and the receiver is 4.09 meters. From Figure 3.2, we can

see that each received multipath component leads to a triangle in shape with a peak [41]. The second multipath component arrives at the receiver about 75 nanoseconds after the arrival of the first one. The proximity fingerprint is 5.6499. The channel impulse response was measured indoors, and thus α ranges between 1.6 and 1.8.

We use Lemma 8 to estimate the lower bound of the proximity of the transmitter, and Figure 3.4 shows the result. We can observe that the estimated lower bound increases as α increases. However, when α reaches the maximum value (i.e., 1.8) of the indoor environment, the real distance is still bounded by (i.e., greater than) the estimated lower bound. Specifically, when $\alpha = 1.8$, the lower bound of the proximity is 3.84 meters. This means the transmitter should be at least 3.84 meters away from the receiver. The actual distance between the transmitter and the receiver is 4.09 meters, which is slightly greater than the lower bound 3.84 meters.

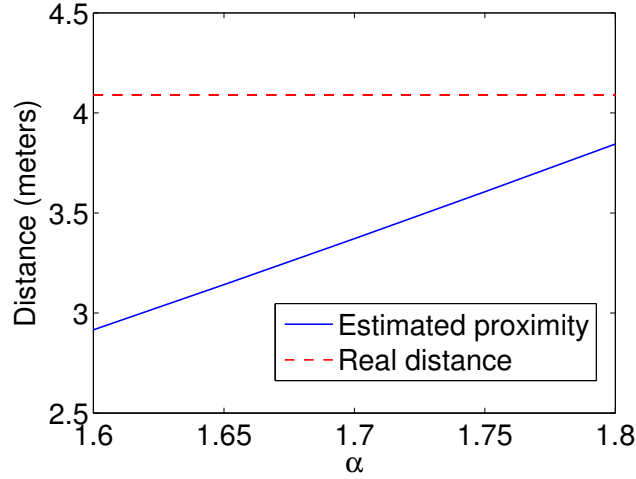


Figure 3.4: Estimated lower bound v.s. the real distance regarding different path loss exponent α

Note that long-haul communications may desire a much relaxed tightness of the proximity lower bound. For example, GPS satellites running on the Low Earth Orbit have an altitude of approximately 2,000,000 meters (1,200 miles). With a proximity lower bound of 1,000,000 meters (i.e., the bound is less than the actual proximity by 50%), it would be possible to

prevent most attackers from impersonating the satellites, because it is usually very difficult for the attacker to achieve such a long transmission range.

3.2.3 System Design

In what follows, we show how the theoretical result of Lemma 8 can be used in a practical communication system to achieve the far proximity identification.

The verifier's objective is to find out the proximity lower bound of the prover, i.e., to verify that the prover is at least a certain distance away. According to Lemma 8, the proximity lower bound is computed by $\frac{c}{B(f^{\frac{2}{\alpha}} - 1)}$. Thus, the verifier can simply compute this bound with the knowledge of the speed of light c , the system bandwidth B , the path loss exponent α , and the proximity fingerprint f . The speed of light c is a universal physical constant and the bandwidth B is a system configuration parameter, and both of them are known to the verifier. The path loss exponent α can be either obtained empirically, or can be determined using the typical values. The proximity fingerprint f is the only remaining factor that the verifier needs to decide to compute the lower bound.

As we discussed earlier, the fingerprint f is the ratio of A_{r1} to A_{r2} , where A_{r1} and A_{r2} are the amplitudes of the first and the second received multipath components. A_{r1} and A_{r2} can be extracted from the channel impulse response. A wireless packet is usually preceded by a preamble, a special data content that indicates the beginning of an incoming packet. When the prover sends a packet to the wireless channel, the verifier will first capture the preamble using the match filtering technique [53]; then the verifier knows that there is an incoming packet and continues to receive the payload. The preamble not only enables packet capture, but also enables the estimation of the channel impulse response at the verifier.

After receiving the preamble, the verifier can use existing channel estimation techniques (e.g., least-square (LS) and linear minimum mean squared error (LMMSE) estimators [54]) to estimate the channel impulse response from the preamble, and thereby obtain the values

of A_{r1} and A_{r2} and the proximity fingerprint $f = A_{r1}/A_{r2}$. It is worth pointing out that using the preamble is not the only way to obtain A_{r1} and A_{r2} . The verifier can also use blinding estimation methods (e.g., [55]) to estimate the channel impulse response from the entire content of the preamble and the payload. In addition, the verifier can use hybrid methods (e.g., [56]) that combine preamble-based estimation and blind estimation together to improve the estimation accuracy. After obtaining the proximity fingerprint f and demodulating the payload and authentication information, the verifier then verifies the prover's proximity using Lemma 8.

3.2.3.1 Dealing with the Wireless Uncertainty

Wireless channels can be affected by random environmental factors like temperature, humidity, and vegetation. Thus, the estimated channel impulse response may be time-varying and fluctuate around a center value. To improve the proximity authentication accuracy, instead of using only one channel impulse response to estimate the proximity, we propose to estimate the proximity based on multiple channel impulse responses, which are collected over a certain time window. Each channel impulse response can yield a set of amplitude ratios, and the corresponding set of estimated proximity. Suppose there are L multiple paths and n channel impulse responses, the verifier will obtain a total of $L * n$ estimates of the prover's proximity. The verifier then uses the mean value of these estimates as the proximity authentication output, so that the impact of random noises can be mitigated with the boosted size of the sample space.

In addition, the path loss exponent α plays an important role in authenticating the proximity. To make α resilient against environmental changes, we propose to use training phases to calibrate α periodically. In a training phase, the verifier estimates the proximity of an authenticated beacon transmitter, whose real distance is already known to the verifier. The verifier compares the estimated proximity with the real distance between the beacon

transmitter and itself. Based on the comparison result, the verifier adjusts α so that the difference between the estimation output and real distance can be minimized. After the training phase, the verifier uses calibrated α to identify the proximity of an unknown wireless device.

By averaging over multiple channel measurements and using a real time α , the verifier can cope with environment changes and improve the proximity authentication performance.

3.2.4 Implication

Lemma 8 indicates that the prover is at least $\frac{c}{B(f^{\frac{2}{\alpha}}-1)}$ meters away from the verifier. This range is determined by the speed of light c , the system bandwidth B , the path loss exponent α , and the proximity fingerprint f . Note that c , α , and B are system constants that are determined by the physical features of the propagation medium. Thus, they are not manipulatable. Also, there are significant practical hurdles to manipulate the proximity fingerprint f , as described in Section III-A. Therefore, the provers can prove (or cannot repudiate) that it is at least $\frac{c}{B(f^{\frac{2}{\alpha}}-1)}$ meters away.

On the other hand, Lemma 8 reveals a good feature of the proposed technique, i.e., it supports passive proximity identification. As we discussed earlier, c , α , and B are system constants that are already known to the verifier. The proximity fingerprint f is computed based on channel impulse responses. Existing channel estimation techniques are typically passive, and they do not rely on active two-way interactions between the prover and the verifier to estimate channel impulse responses. With the knowledge of c , α , B , and f , the verifier can directly compute the proximity lower bound of the prover. The passive verification not only reduces communication overhead, but also increases the difficulty for an adversary to recognize an on-going proximity identification activity.

3.3 Attacks and Countermeasures

A proximity fingerprint itself is unforgeable, because it is extracted from channel impulse responses, which have been regarded as "signatures" to uniquely identify the wireless link between a transmitter and a receiver. However, an attacker may launch attacks targeting at the verification decision process such that the verifier gets an incorrect verification decision. Specifically, the attacker is able to intercept, interfere, or even jam the signal transmission between the prover and verifier, and aims at causing false negative/positive errors to fool the verifier to get a wrong decision on a dishonest/benign prover. In addition, a dishonest prover may manipulate the channel estimation process to create a fake channel impulse response at the verifier or collaborate with attackers to generate a mixed received signal to fool the verifier with a wrong decision.

To fool the verifier, the attacker may try to collaborate with another active wireless device or equip with multiple antennas to create a fake second path by transmitting signals from a different direction. In this case, the attacker must make sure that there is no multipath effect for the signals traveling on the direct path (e.g., the path from the prover to the verifier) and the fake path (e.g., the path from the active wireless device to the verifier). Otherwise, the attacker cannot control and guarantee that the fake path is exactly the second received path at the verifier side. Eliminating the multipath effect completely is normally regarded as infeasible.

In this paper, we focus on three other major attacks against the far proximity fingerprinting and they are:

- Jam-and-replay attack: The attacker may jam the prover and replay an intercepted signal to fool the verifier taking the attacker's proximity as the prover's proximity.

- Flipping attack: The attacker may collaborate with malicious provers to generate mixed received signals at the verifier, and thus result in the false negative and positive errors.
- Spoofing attack: A dishonest prover may try to create a fake channel impulse response at the verifier by manipulating the channel estimation process.

3.3.1 Dealing with Jam-and-replay Attacks

3.3.1.1 Attack Methodology

In the jam-and-replay attack, the attacker first intercepts the transmit signal from the prover, and at the same time jams the transmission to prevent the verifier from receiving the original signal from the prover. Then the attacker replays the intercepted signal from the prover at the attacker's own location, such that the verifier is fooled into taking the attacker's proximity as the prover's proximity. Because the attacker jams the original transmission between the prover and verifier, traditional anti-replay mechanisms such as sequence numbers do not work.

3.3.1.2 Defense Approach

A common method to address jam-and-replay attacks is to explore timestamps (e.g., [7]). In such a method, the sender includes a timestamp in the transmitted message, which indicates the time when a particular bit or byte called the anchor (e.g., the start of the message header) is transmitted over the air. Upon receiving a frame, the receiver can use this timestamp and its local message receiving time to estimate the message traverse time. An overly long time indicates that the message has been forwarded by an intermediate attacker.

Timestamps-based method requires clock synchronization between the sender and the receiver, but it generally has a low synchronization requirement in common wireless appli-

cations. For example, in an 11 Mbps 802.11g wireless network, the transmission of a typical 1500-byte TCP message requires 1.09 (i.e., $\frac{1500 \times 8}{11 \times 10^3}$) milliseconds. Thus, the attacker at least doubles the transmission time of the message to 2.18 milliseconds. As long as the verifier and the prover have coarsely synchronized clocks that differ in the order of milliseconds, the verifier can detect jam-and-replay attacks. In practice, multiple schemes can be applied to satisfy such clock synchronization requirement to detect the attack [57]. For example, in IEEE 802.11 standard, it specifies the timing synchronization function (TSF) to fulfill timing synchronization among users. Since the TSF is based on a 1 MHz clock and "ticks" in microseconds, it can achieve the time accuracy in the range of few microseconds (us), which is orders of magnitude smaller than milliseconds (ms). Note that the synchronization requirement can be further relaxed in GPS applications. GPS satellites have a transmission rate ranging between 20 bits/s and 100 bits/s [44]. The transmission of a standard 1500-bits GPS navigation message [44] takes 15 – 75 seconds, and accordingly the synchronization accuracy can be reduced to the order of seconds.

In addition, to launch jam-and-replay attacks, the attacker must send jamming signals to jam the wireless transmission. Jamming attacks have been extensively studied in the literature, and various techniques regarding jamming detection and countermeasures have been proposed (e.g., [58, 40, 59]). The prover and the verifier can also use existing jamming detection or anti-jamming techniques to discover the presence of jam-and-replay attacks, or to defend against such attacks.

3.3.2 Dealing with Flipping Attacks

3.3.2.1 Attack Methodology

The attacker can collaborate with malicious provers or interfere legitimate provers to generate a mixed received signals at the verifier, and thus result in a flipped decision (i.e.,

in far proximity \rightarrow out of far proximity and out of far proximity \rightarrow in far proximity). Specifically, the attacker uses its own proximity to “pollute” the prover’s proximity. Assume the prover and the attacker are d_p and d_a meters away from the verifier respectively, where $d_p \gg d_a$ or $d_a \gg d_p$. The attacker sends signals to the verifier along with the transmission of the prover. Suppose the attacker and the prover do not overwrite each other’s signal (e.g., by using a very high transmission power). Thus, the verifier receives a mixed signal formed by both the prover and the attacker’s signals. Intuitively, the proximity fingerprint extracted from the mixed signal will reflect proximity features of both the attacker and the prover, and thus the corresponding proximity lower bound d estimated based on the proximity fingerprint can greatly deviate from the real proximity lower bound d_p of the prover.

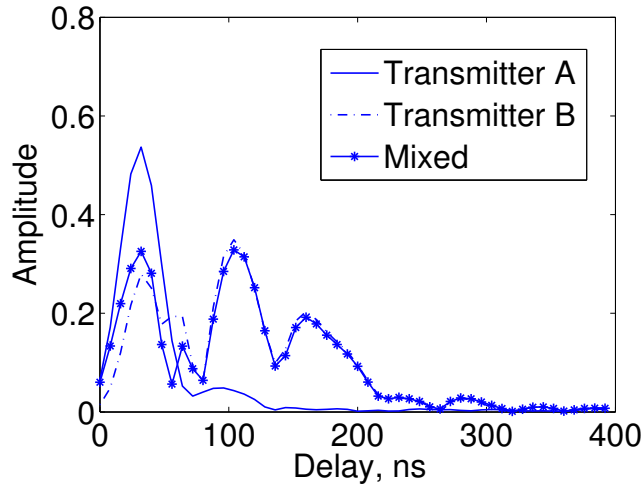


Figure 3.5: Example of flipping attacks: the mixed channel impulse response reflects proximity features of both the transmitter A and B.

We conducted experiments using the CRAWDAD dataset to examine the impact of the attacker. The dataset includes over 9,300 real channel impulse response measurements in a 44-node wireless network [49]. Two transmitters (nodes 31 and 35) and a receiver (node 44) from the data set are used for the experiments. Figure 3.5 shows the real measured channel impulse responses between the transmitters and the receiver. Transmitter A is positioned 1.83 meters away from the receiver. The proximity fingerprint, the amplitude ratio of the

first received multipath component to that of the second one, is about 11.06. Accordingly, the estimated lower bound of the transmitter’s proximity is 1.67 meters. Compared to transmitter A, transmitter B is farer away from the receiver. The distance between transmitter B and the same receiver is 14.15 meters. Transmitter B’s proximity fingerprint is about 1.80 and the estimated proximity lower bound is 12.99 meters. We let transmitters A and B send signals to the receiver at the same time. Thus, the receiver receives a mixed signal from both transmitters. The mixed signal can result in a channel impulse response as shown in Figure 3.5. The proximity fingerprint estimated from this channel impulse response is 2.44, and the corresponding estimated proximity lower bound is 8.85 meters, which falls between the true bounds of transmitter A (1.67) and transmitter B (12.99).

The experiment results show that it is possible for an attacker to use its own proximity to significantly affect the estimated proximity lower bound of the prover. Consequently, a nearby attacker may fool the receiver into believing that a far-away prover is not far away, and vice versa.

3.3.2.2 Defense Approach

A basic solution to deal with flipping attacks is to use existing jamming detection approaches. The attacker’s signals cause the wireless interference to the transmission, and thus they can be regarded as jamming signals. Jamming attacks have been extensively studied in the literature, and various techniques regarding jamming detection have been proposed (e.g., [58, 60, 59, 61, 62, 63, 64, 65]). The verifier may use existing jamming detection techniques to discover the presence of flipping attacks.

However, one drawback of jamming detection techniques is that they require the attacker to constantly jam the prover’s transmission for a relatively long time, such that the receiver can collect enough jammed signal samples. By analyzing those samples, the receiver can obtain important statistical values, including packet loss rate, bit error rate, and received

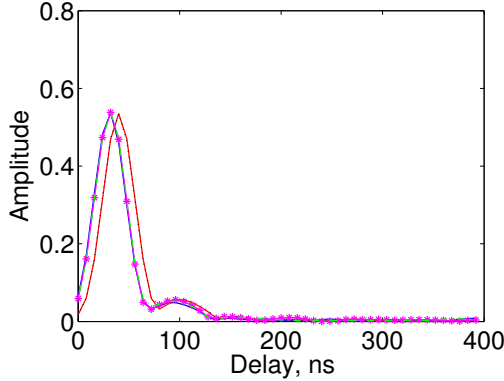


Figure 3.6: Channel impulse response measured in normal scenario

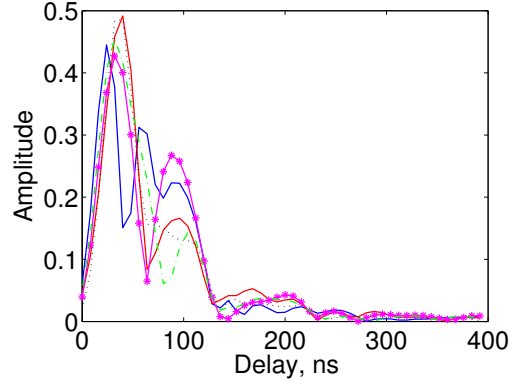


Figure 3.7: Channel impulse response measured in the scenario of flipping attacks

signal strength. Those values enable the receiver to make a decision regarding whether or not the communication system is under jamming attacks. However, if the attacker jams the transmission for a short time, the receiver may not be able to get an accurate estimate of those statistical values, thereby reporting an incorrect decision.

We propose advanced defense techniques to deal with flipping attacks. Traditional jamming detection techniques require constant long-term jamming, because the detection decision is based on statistical values obtained from a certain amount of jammed signal samples. To deal with a short-term flipping attacker, we design defense techniques without relying on statistical values. Intuitively, due to the absence or imperfect synchronization, there exists a tiny clock discrepancy between the attacker and the prover. This clock discrepancy is actually a time-varying random variable. When there exist flipping attacks, the attacker's and the prover's signals mix together, and the clock discrepancy introduces randomness to the mixed signal.

We performed experiments using the CRAWDDAD dataset to compare the channel impulse responses obtained from non-mixed and mixed signals. We considered a normal scenario and an attack scenario. In the first scenario, only the prover transmits signals to the verifier, while in the second one, the attacker launches flipping attacks by interfering the prover's

transmission. Figure 3.6 shows 5 channel impulse responses in the normal scenario and each of them is extracted from a short-term signal that lasts for about 250 nanoseconds. We can observe that those channel impulse responses are similar to each other in shape. Figure 3.7 shows 5 channel impulse responses extracted from the mixed signals in the attack scenario. Unlike the normal scenario, the channel impulse responses exhibit random shapes and they are quite different from each other.

Therefore, we can detect the presence of flipping attacks through checking the consistency among channel impulse responses. Specifically, we can compute the difference between successive channel estimations. The channel is considered as polluted, if two successive estimated channels change significantly. Specifically, assume we have two successive channel estimations \mathbf{h}_i and \mathbf{h}_j , their difference is denoted as the Euclidean distance $d_{ij} = \|\mathbf{h}_i - \mathbf{h}_j\|$. Then we compare d_{ij} with a threshold τ , for a constant $\tau > 0$. When $d_{ij} > \tau$, the channel is considered as polluted and a flipping attack is detected.

The flipping attack detection can be viewed as a choice between two events F_0 and F_1 , where F_0 indicates the event of a normal scenario, while F_1 indicates the event of a flipping attack. The density functions conditioned on F_0 and F_1 can be denoted as $f_{d_{ij}}(d_{ij}|F_0)$ and $f_{d_{ij}}(d_{ij}|F_1)$ respectively. Accordingly, we can obtain the probability of false alarm and missed detection as $P_f = \int_{x=\tau}^{\infty} f_{d_{ij}}(x|F_0)dx$ and $P_m = \int_{x=0}^{\tau} f_{d_{ij}}(x|F_1)dx$ respectively. As both probabilities are functions of the threshold τ , there is a tradeoff between the false alarm rate and missed detection rate. In practice, we may empirically select a threshold τ to achieve a high detection rate and at the same time, maintain a relatively low false alarm rate. In addition, to further minimize the false alarm caused by the normal channel fading, we compare the differences among n channel estimations ($n > 2$). The channel will be treated as polluted, only when p out of n channel estimations are dramatically changed, where p is the threshold of the flipping attack indicator.

3.3.3 Dealing with Spoofing Attacks

3.3.3.1 Attack Methodology

Instead of creating real-world fake paths, the attacker may target the channel estimation process, such that the verifier obtains a fake impulse response specified by the attacker. Let \mathbf{S}_v denote the symbols (i.e. transmission units in physical layer) received by the verifier, and \mathbf{S}_v can be represented as $\mathbf{S}_v = \mathbf{h} * \mathbf{S}_p + \mathbf{n}_v$, where \mathbf{S}_p are the preambles, \mathbf{h} is the actual channel impulse response between the verifier and the prover, and \mathbf{n}_v is the channel noise, respectively. Upon receiving \mathbf{S}_v , the verifier uses \mathbf{S}_p and \mathbf{S}_v as the input of the channel estimation algorithm (e.g., LS and LMMSE), and the output of the algorithm is the estimated channel impulse response.

In general, the prover and the verifier must agree on the same preambles to achieve the accurate channel estimation. However, it is possible for a dishonest prover to specify a fake channel impulse response by modifying the transmit preambles. Let \mathbf{S}'_p denote the preambles to be transmitted by a dishonest prover, and let \mathbf{S}'_v denote the corresponding received symbols. \mathbf{S}'_v can be represented by $\mathbf{S}'_v = \mathbf{h} * \mathbf{S}'_p + \mathbf{n}'_v$ [66]. Further let \mathbf{h}_a denote the fake channel estimation result chosen by the dishonest prover. The goal of the dishonest prover is to find symbols \mathbf{S}'_p , such that when \mathbf{S}'_p arrive at the verifier, the corresponding received symbols \mathbf{S}'_v can result in an estimated channel impulse response that is equal to \mathbf{h}_a . To achieve this goal, the prover let $\mathbf{S}'_v = \mathbf{h}_a * \mathbf{S}_p + \mathbf{n}_v$, i.e., $\mathbf{h} * \mathbf{S}'_p + \mathbf{n}'_v = \mathbf{h}_a * \mathbf{S}_p + \mathbf{n}_v$.

Upon receiving \mathbf{S}'_v , the verifier uses \mathbf{S}_p and \mathbf{S}'_v to estimate the channel impulse response. Because $\mathbf{S}'_v = \mathbf{h}_a * \mathbf{S}_p + \mathbf{n}_v$, the estimated channel impulse response will be equal to \mathbf{h}_a . We rewrite the equation $\mathbf{h} * \mathbf{S}'_p + \mathbf{n}'_v = \mathbf{h}_a * \mathbf{S}_p + \mathbf{n}_v$ as $\mathbf{h} * \mathbf{S}'_p + \mathbf{n} = \mathbf{S}$, where $\mathbf{S} = \mathbf{h}_a * \mathbf{S}_p$ and $\mathbf{n} (= \mathbf{n}'_v - \mathbf{n}_v)$ is the white Gaussian channel noise. By using the standard least square approach [54], we can obtain that $\mathbf{S}'_p = (\mathbf{H}^H \mathbf{H})^{-1} \mathbf{H}^H \mathbf{S}$, where \mathbf{H} is the Toeplitz matrix of \mathbf{h} . By sending \mathbf{S}'_p to the verifier, the prover can fool the verifier to obtain a fake channel

results \mathbf{h}_a . Because all elements in \mathbf{h}_a are chosen by the dishonest prover, the verifier will obtain fake amplitude ratios that are specified by the prover.

3.3.3.2 Defense Approach

To launch a successful spoofing attack, the dishonest prover must first know the actual channel \mathbf{h} between the prover and the verifier. Otherwise, the attacker can only generate a unpredictable channel estimation by randomizing the preambles. To defend against the attack, we propose to introduce a passive auxiliary node, which we refer to as the helper. Specifically, the prover and the verifier agree on two different preambles \mathbf{S}_{p1} and \mathbf{S}_{p2} , and the verifier and the helper use \mathbf{S}_{p1} and \mathbf{S}_{p2} to estimate the channel impulse responses from two successive transmissions of the prover. The basic idea is that the dishonest prover cannot maintain the consistent channel impulse responses at both the verifier and the helper with two different preambles \mathbf{S}_{p1} and \mathbf{S}_{p2} , especially when the prover has no idea of the channel between the prover and the passive helper.

To facilitate the presentation, without loss of generality, we omit the noise part in the following equations. To generate a fake channel impulse response \mathbf{h}_a , the prover solves the fake preamble \mathbf{S}'_{p1} from the equation $\mathbf{h} * \mathbf{S}'_{p1} = \mathbf{h}_a * \mathbf{S}_{p1}$, so that the verifier will regard \mathbf{h}_a as the channel impulse response when uses \mathbf{S}_{p1} to estimate the channel. The helper also uses \mathbf{S}_{p1} to estimate its channel impulse response from $\mathbf{h}_h * \mathbf{S}'_{p1} = \mathbf{h}_{ah} * \mathbf{S}_{p1}$, where \mathbf{h}_h and \mathbf{h}_{ah} are the actual and the estimated channel impulse response between the helper and the prover. For the attacker's next transmission, both the verifier and the helper will use the preamble \mathbf{S}_{p2} to estimate the channel. Similarly, to fool the verifier, the attacker must generate another fake preamble \mathbf{S}'_{p2} such that it satisfies $\mathbf{h} * \mathbf{S}'_{p2} = \mathbf{h}_a * \mathbf{S}_{p2}$. However, the attacker can hardly fool the verifier and the helper at the same time. Because the attacker cannot know the channel between the attacker and the helper, the fake preamble \mathbf{S}'_{p2} will not necessary satisfy the helper node's equation $\mathbf{h}_h * \mathbf{S}'_{p2} = \mathbf{h}_{ah} * \mathbf{S}_{p2}$. Thus, the channel

estimation result at the helper will be different from the previous channel estimation result \mathbf{h}_{ah} .

If the successive estimated channel impulse responses show dramatic changes in a short time at the helper, the spoofing attacks are detected and the helper triggers an alert at the verifier. To avoid false alarms caused by normal channel fading, we can further increase the number of preambles. The verifier and the helper agree on n preambles ($n > 2$), and the alert will be triggered only when p out of n channel estimations are detected as inconsistent, where p is the threshold of the spoofing attack alerts.

3.3.4 Impact of a Cloned Prover

In an extreme scenario, a dishonest prover may use a collaborator at a different location to forge the proximity. The collaborator claims to be the prover and sends signals to the verifier. As a result, the verifier will take the collaborator's proximity as the prover's proximity. In this case, the verifier will send the data to a higher layer for authenticity verification. Such verification will fail if the prover does not disclose its personal information (e.g., user ID, network address, private key) to the collaborator. However, the verification does succeed if the collaborator has all the information of the prover, in which case the collaborator is essentially a full copy of the prover. Therefore, it is not practical to detect such a same-identity attack in any proximity detection system, including all distance bounding protocols. To defeat such attacks, the verifier needs to enforce existing security mechanisms like duplicated nodes detection (e.g., [67]) or hardware biometrics authentication (e.g., [42]), which are orthogonal to this work.

3.4 Experimental Evaluation

The proposed far proximity identification approach identifies whether a prover is at least a certain distance away from the verifier. To evaluate the performance of the proposed far

proximity detection approach, two key questions are of particular interest. The first question is how likely it is that the detection method makes an error. An error happens when a prover is identified as at least β meters away, while the real distance d between the verifier and the prover is less than the identified lower bound β . The second question is how tight the estimated lower bound is. Let ϵ denote the difference between the real distance d and the lower bound β , i.e., $\epsilon = d - \beta$. Ideally, to obtain a good estimation accuracy, one would like to achieve a small ϵ . In this section, we perform experiments using real-world channel data to evaluate the performance of the proposed approach in a real wireless environment.

3.4.1 Experiment Setup

Wireless propagation can be either line-of-sight (LoS) or non-LoS (NLoS). In LoS scenarios, there exist no major or very few obstacles residing between the transmitter and receiver, and thus LoS scenarios usually feature better signal quality. In NLoS scenarios, there exist a number of major obstacles between the transmitter and receiver, and NLoS scenarios are more complicated with higher signal distortion and sharper changes in signal strength.

Far proximity identification often applies to long-haul wireless communications (e.g., GPS) in outdoor environments, which are usually open and have a much stronger feature in LoS than NLoS. Compared to outdoor environments, indoor environments like offices, residential homes, and shops, are more complicated due to the frequent occurrences of walls, people, furniture, cubicles, etc. Thus, indoor environments usually have a fairly large number of NLoS propagation paths. In our experiment, we choose the more challenging indoor environment for our evaluation to examine the worst-case performance of the proposed method.

3.4.1.1 Data Set

We validate the proposed far proximity identification technique using the CRAWDAD data set [68], which contains more than 9,300 real channel impulse response measurements

(i.e., link signatures) in a 44-node wireless network [49]. There are $44 \times 43 = 1,892$ pairwise links between the nodes, and multiple measurements are provided for each link [49]. The map of the 44 node locations is shown in [41]. The measurement environment is an indoor environment with obstacles (e.g., cubicle offices and furniture) and scatters (e.g., windows and doors). More information regarding the CRAWDAD data set can be found in [68, 49].

3.4.1.2 Evaluation Metrics

We herein use *error rate* and *tightness of the bound* as metrics to evaluate the performance of the proposed technique in the real world. In addition, the proximity lower bound is computed based on a key factor, the proximity fingerprint. Thus, the proximity fingerprints plays a vital role in proximity identification. To further validate the the feasibility of using proximity fingerprints for proximity identification, we also perform experiments to reveal the relationship between the real distance and the proximity fingerprints. Our evaluation metrics are summarized below.

- **Error rate:** The error rate is the ratio of the number of failed trials (i.e., error happens in the trail) to the total number of trials. An error happens when the real distance between the verifier and the prover is less than the identified proximity lower bound. The error rate indicates how possible a nearby adversary will be considered as a remote legitimate device. A small error rate indicates a nearby adversary can hardly pretend to be far away from the prover, and vice versa.
- **Tightness of the bound:** Tightness is the normalized difference between the estimated lower bound and the real distance (i.e., $\frac{d-\beta}{d}$, where β is the estimated proximity lower bound, and d is the real distance between the verifier and the prover).

Tightness indicates how close between the estimated result and the real distance. A small tightness indicates a remote device will not be falsely considered as a nearby adversary, and vice versa.

- Proximity Fingerprints: The proximity fingerprint is the ratio of the amplitude of the first received multipath component to that of the second one.

3.4.2 Experiment Results

Based on the CRAWDAD data set, we perform experiments under both LoS and NLoS scenarios to show the error rate, tightness of the bound, and the relationship between the proximity fingerprint and the distance.

We distinguish two types of channel impulse responses: if a LoS path exists and there are no obstacles between the transmitter and the receiver, we mark the corresponding channel impulse responses as LoS channel impulse responses. Otherwise, we mark them as NLoS channel impulse responses. Thus, we obtain two sets of data. The first set is formed by all LoS channel impulse responses, and the second one is formed by all NLoS channel impulse responses. We perform our experiments using both sets.

3.4.2.1 Proximity Fingerprint vs. Distance

The proximity fingerprint is an important parameter in computing the proximity lower bound. According to Lemma 8, the theoretical proximity lower bound is calculated as $\frac{c}{B(f^{\frac{2}{\alpha}} - 1)}$. From this formula, we can easily derive that as the proximity fingerprint f increases (other parameters remain the same), the proximity lower bound decreases and vice versa. Note that the proximity lower bound reveals the least distance between the verifier and the prover. Thus, the increase of the proximity fingerprint f may also indicate the decrease of the real distance and vice versa. We plot the proximity fingerprint as a function of the distance

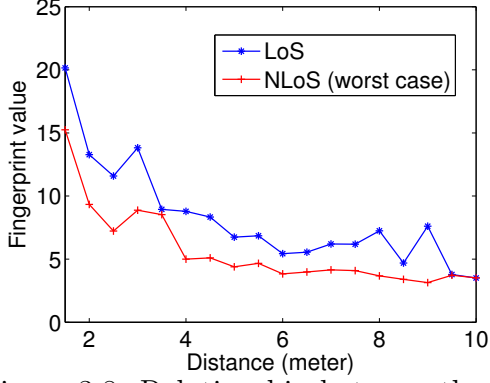


Figure 3.8: Relationship between the distance and the proximity fingerprint.

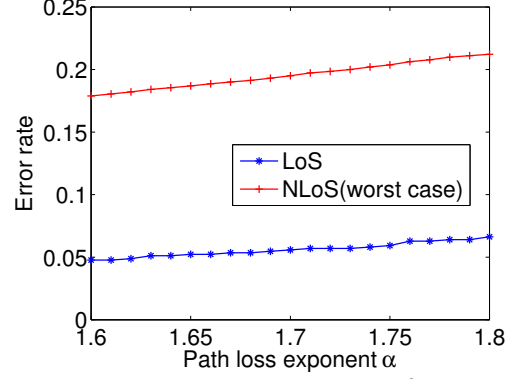


Figure 3.9: Error rate as a function of pathloss exponent α .

in Figure 3.8. We can see that the proximity fingerprint in the NLoS scenario slightly differs from that of the LoS scenario in magnitude due to the reflection loss. However, for both scenarios, their proximity fingerprints exhibit the same tendency, i.e., they both decrease as the distance increases. This observation is consistent with our theoretical result.

3.4.2.2 Error Rate vs. Pathloss

To obtain the error rate, we experiment as follows. Let N_{LoS} denote the number of channel impulse responses in the LoS data set. For each channel impulse response in the data set, we compute the proximity fingerprint and the corresponding proximity lower bound using Lemma 8. We also compute the real distance between the transmitter and the receiver based on their coordinates. If the lower bound is less than the real distance, we mark the trial as successful. Otherwise, we mark the trial as failed. Accordingly, the error rate is calculated as $\frac{N_f}{N_{LoS}}$, where N_f is the number of failed trails and N_{LoS} is the total number of trials. We perform the experiment again using the NLoS data set and obtain the corresponding error rate for the NLoS scenario.

The channel impulse responses are collected from an indoor environment, and the corresponding pathloss exponent α empirically ranges between 1.6 and 1.8. Thus, we perform

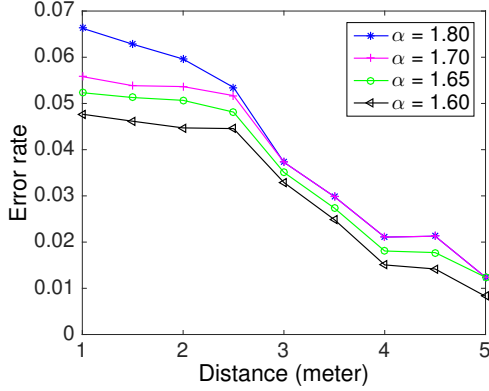


Figure 3.10: Error rate as a function of various distances in the LoS scenario

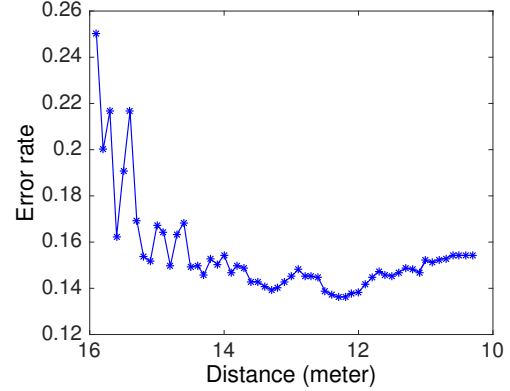


Figure 3.11: Error rate as a function of various distances in the NLoS scenario

our experiment for different values of α in this range. Figure 3.9 plots the error rate as a function of α . The pathloss exponent α reflects how a signal is distorted and attenuated during its propagation, and a large α can result in higher signal distortion and attenuation. Accordingly, from Figure 3.9 we can observe that the error rate increases as α increases. However, when α reaches the maximum value for indoor environments, the achieved error rate in the LoS scenario is as low as 0.075. For the minimum α of 1.6, the proposed approach has a reduced error rate of 0.05.

For the NLoS scenario, we can still achieve an error rate between 0.17 and 0.22. Note that NLoS scenarios are the worst-case scenarios. Far proximity identification is typically used in outdoor environments, which have the stronger LoS feature. As shown in Figure 3.9, the error rate of LoS scenarios is much lower than that of the NLoS scenarios.

3.4.2.3 Error Rate vs. Distance

We then perform experiments to examine how the real distance affects the error rate. For each channel impulse response in the LoS data set, we compute the distance between the corresponding transmitter and the receiver. Let d_{max} and d_{min} denote the maximum and minimum distance among all computed distances. We calculate the error rate using

the set formed by channel impulse responses whose corresponding distance are larger than a threshold distance. The threshold is initially set as d_{min} and increases each time until it reaches d_{max} . We perform the experiments again using the NLoS set.

Figure 3.10 shows the error rate as a function of various distances in the LoS scenario. The error rate decreases as distance increases. The obvious reason is that a larger distance indicates a longer distance between the transmitter and the receiver, and thus a higher chance that the estimated proximity lower bound is less than the distance. When distance approaches the maximum distance between the sender and the receiver, the corresponding error rate is 0.01. When distance approaches the minimum distance, the error rate slightly increases but it is still a small rate that ranges between 0.05 and 0.07 for different α .

Figure 3.11 plots the error rate of the NLoS scenario for $\alpha = 1.80$, which results the worst error rate as compared to other values of α . Contrary to the LoS scenario, the error rate of the NLoS scenario increases as distance increases. That's because in the NLoS scenario a longer distance between the transmitter and the receiver indicates a higher chance that there are more obstacles, and thus a reduced proximity detection accuracy. The “worst worst case” happens when distance approaches the maximum distance d_{max} for the worst case NLoS scenario. However, as we can observe from Figure 3.11, the achieved error rate of the “worst worst case” is about 0.25. This means that we can successfully obtain the proximity lower bound for a majority number (75%) of verifiers. As distance decreases, the error rate decreases quickly. When distance approaches the minimum distance, the achieved error rate is about 0.15. Again, the experiment is performed in an indoor environment (e.g., WiFi and Bluetooth), which has a short signal propagation distance. Outdoor wireless applications (e.g., space communications and TV broadcasting) usually have the stronger LoS feature, and therefore can substantially benefit from the proposed method in terms of significantly reducing the error rate.

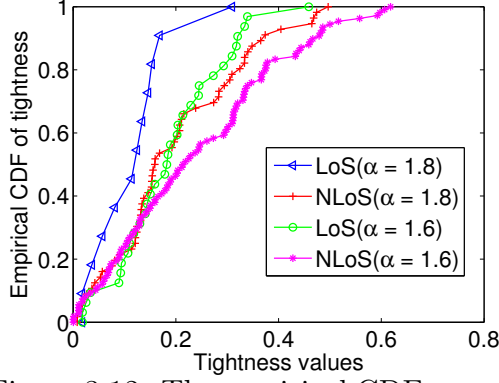


Figure 3.12: The empirical CDF curves of the tightness.

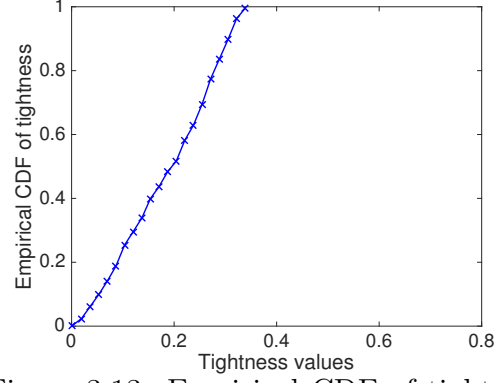


Figure 3.13: Empirical CDF of tightness with a distance of 50 meters

3.4.2.4 Tightness of the Proximity Bound

Our second evaluation metric is the tightness of the bound. To evaluate the tightness, we perform the following experiments using LoS and NLoS data sets. In all experiments, the pathloss exponent α is set to the minimum and maximum values of 1.6 and 1.8. For each channel impulse response in the LoS data set, we compute the distance between the corresponding transmitter and the receiver and the proximity lower bound. Based on the bound and the actual distance, we can calculate the tightness of the bound. We then sort all the tightness values and compute the empirical cumulative distribution function (CDF) for them. We perform the experiment again using NLoS data set and obtain the CDFs of the NLoS tightness values.

Figure 3.12 shows the CDF curves of the tightness computed using channel impulse responses collected in LoS and NLoS scenarios. For the LoS scenario with $\alpha = 1.8$, we can observe that 95% of the tightness values are less than 0.2. The indoor environment typically features a short propagation path, and thus a 0.2 tightness indicates a small absolute difference in distance. For example, if the distance between the transmitter and receiver is 5 meters, the achieved tightness can be around 1 meter. In particular, the maximum distance

d_{max} between the transmitter and the receiver is about 11 meters, and the corresponding proximity bound is 9.56 meters, which is very close to the actual distance.

For the NLoS scenario with $\alpha = 1.8$, we can observe from Figure 3.12 that 90% of the tightness values are less than 0.3. Compared to the LoS Scenario, the NLoS scenario has a reduced performance due to the existence of obstacles. Again, the experiment is conducted based on short-range communications, and a 0.3 tightness still suggests a small absolute difference in distance. When α decreases to 1.6, the achieved tightness increases. That's because the corresponding estimated proximity lower bound decreases, and a decreased bound grows the difference between the bound and the real distance, and thus augments the tightness. However, for $\alpha = 1.6$, we can still observe that a great majority of the tightness values are fairly small, e.g., 95% and 80% of the tightness values are less than 0.25 and 0.3 in the LoS and the NLoS (worst-case) scenarios respectively. Note that such tightness is usually sufficient to prevent attackers from impersonating the transmitters in typical long-haul outdoor wireless applications. For example, GPS satellites running on the Low Earth Orbit have an altitude of approximately 2,000,000 meters (1,200 miles). With a proximity lower bound of 1,000,000 meters (i.e., a tightness of 0.5), it would be possible to prevent most attackers from impersonating the satellites, because it is usually very difficult for the attacker to achieve such a long transmission range.

3.4.2.5 Experiment for a Longer Distance Scenario

We further conduct an experiment to evaluate the performance of the proposed scheme in the scenario of a longer distance between the prover and the verifier on top of the Universal Software Radio Peripherals (USRPs), which are the radio frequency transceivers.

In the experiment, the transmit rate is set as 10 Mbps and the distance between the prover and the verifier is set as 50 meters, which are the maximum rate and largest distance we can achieve due to the hardware limitations of USRPs (i.e. processing capability and

transmission power). The experiment is done in the outdoor scenario, and the corresponding path loss exponent α is chosen as 5.0. We measure the channel impulse response for 1000 times, and for each measurement we estimate the corresponding lower bound proximity. Note that during the measurements, the environment may change since there are people walking between the transmitter and receiver.

From the experiment results, we can observe an error rate of 0.0939. We also draw the empirical CDF of tightness in Figure 3.13. As shown in this figure, the maximum tightness value is 0.3385. As discussed earlier, such tightness is usually sufficient to prevent attackers from impersonating a nearby transmitters in typical long-range outdoor wireless applications.

3.5 Related Work

Related work falls into the following areas.

3.5.1 Distance Bounding Protocols

Distance bounding protocols are a class of protocols that determine an approximate distance between a local device and a remote device. (e.g., [8, 9, 10]). Distance bounding protocols and their variants are based on the common observation that the distance between the local and the remote devices is equal to the product of the speed of electromagnetic wave and the one-way signal propagation time. The approximate distance is obtained from a series of wireless packets exchanged between the local device and the remote device. Specifically, the local device sends a challenge to the remote device, which then replies with a response that is generated based on the challenge. The local device measures the round-trip time between sending the challenge and receiving the response, subtracts the processing delay from the round-trip time, and uses the result to compute the distance. Because the response is generated based on the challenge, the distance bounding protocol can prevent the remote

device from pretending to be closer than it actually is by sending a fake response before it receives the challenge.

However, by delaying its response to a challenge, a remote device can appear to be arbitrarily further from the local device than it actually is. Hence, distance-bounding protocols cannot enforce lower bounds on proximity (i.e., requirements that the remote device be *at least* a certain distance from the local device). For this reason, the GPS-device and mobile-phone examples used for motivation cannot be enforced by distance-bounding protocols.

3.5.2 Close Proximity Identification

There also exist traditional close proximity detection techniques (e.g., [69, 70]) that can detect the presence of nearby objects without any physical contact. These techniques use electromagnetic field changes to identify a close object. A proximity sensor generates an electromagnetic field or a beam of electromagnetic radiation (e.g., infrared). If an object moves into the field range of the sensor, a field change can result, and thus the sensor senses the presence of the object. For example, a sound alert is triggered when a vehicle moves into the close proximity of a worker or an obstacle. However, traditional techniques cannot identify the proximity of a specific object, because the proximity sensor reports all nearby objects as long as those objects are in the field range.

Researchers later developed techniques that identify the close proximity of an individual target if the target can emit wireless signals (e.g., [71, 5, 6]). For example, based on the observation that a strong received signal usually indicates a close transmitter, Macii et al developed approaches that determine the proximity of the remote wireless device by measuring received signal strength [71]. However, the use of signal strength to determine proximity was found to be insecure, as a dishonest remote device can easily pretend to be close to the local device by boosting its transmit power.

More recent efforts overcome this drawback with the assistance of special hardware [5, 6]. Cai et al. proposed a scheme that identifies the presence of a close wireless device by using multiple antennas [5]. Halevi et al. proposed to use ambient sensors to detect whether a Near-Field-Communication (NFC) device is nearby or not [6]. Although those approaches can prevent attackers manipulating transmit power to deceive the local device, they cannot be directly extended to address the far proximity identification problem. They output a decision regarding whether a target is nearby, but such a decision cannot guarantee that the target is at least a certain distance away. Also, the requirement of special hardware such as multiple antennas and ambient sensors introduces extra cost and may reduce their compatibility.

Liu et al. proposed a new close proximity identification approach that does not rely on special hardware [7]. By using the wireless physical features that uniquely identify a wireless link between a transmitter and a receiver, the proposed technique enables the local device to distinguish between a nearby and a far-away remote device. An attacker cannot manipulate such physical features to pretend to be close to the local device. However, similar to all previous approaches, this approach is a decision-based, i.e. outputs a simple “yes” or “no” to indicate whether the remote device is very close or not. Hence, it does not provide the quantitative lower bound of the proximity, which is the primary contribution of this paper.

3.5.3 CSI Based Distance Tracking Scheme

Existing CSI distance tracking ideas mainly focus on providing accurate distance estimation schemes. For example, Sen et al. proposed a distance estimation scheme that can extract the signal strength and the angle of only the direct path utilizing the channel state information, and thus provide an accurate estimation result in WiFi based localization systems [72]. On the other hand, the proposed scheme aims to estimate the lower bound of the proximity and focus on preventing a nearby adversary from impersonating a remote legiti-

mate device. Existing CSI distance tracking schemes (e.g. [72]) may be vulnerable to such attacks, since attackers can pretend to be a further distance away from the receiver if they reduce the transmit power. In this way, the proposed scheme is complementary to existing schemes to provide an accurate and secure distance estimation scheme.

3.6 Summary

In this paper, we proposed a far proximity identification approach that determines the lower bound of the distance between the verifier and the prover. The key idea of the proposed approach is to estimate the proximity lower bound from the unforgeable fingerprint of the proximity. We developed a technique that can extract the fingerprint of a wireless device's proximity from the channel impulse response of the signals sent by the device. We also developed a technique that uses proximity fingerprint to calculate the proximity lower bound. We have examined the proposed approach through the real-world experimental evaluation using the CRAWDAD data set [68]. Our results indicate that the proposed approach is a promising solution for enforcing far proximity policies in wireless systems.

CHAPTER 4

FUTURE WORK

I would like to discuss two possible future works that can further improve the system and network security.

4.1 Light-weight Encryption Schemes

Traditional cryptography encryption schemes have been widely applied to preserve the confidentiality of users' privacy and sensitive data [73]. However, traditional cryptography schemes are usually computational-capability dependent. They are time and energy consuming, and cannot be applied in applications with limited processing capability. For example, IoT devices nowadays are widely deployed in our daily life and may collect our privacy. It's essential to build a covert channel when IoT devices communicate with others. However, since many IoT devices are battery limited and integrated with simple chips, they may not be able to afford expensive cryptography encryption operations. Simply applying the traditional cryptography schemes may significantly reduce the life time of the IoT devices.

We attempt to design a light-weight encryption scheme that can achieve the confidentiality of the data traffic, and at the same time consumes few processing capabilities. The intuitive idea is to utilize the physical layer features to implement a practical light-weight encryption scheme.

4.2 Security Evaluation on Current Third-party Script over the Internet

As Internet now involves various of our privacy information, privacy disclosure has becoming a main concern when surfing the Internet. It's essential to reveal potential security risks over the Internet. JavaScript, as a popular client-side programming language has been widely applied in modern web applications to achieve fast and responsive user interactions. For example, it can be utilized to gather and manage web cookies, track users' activities, and can also be utilized to create a login form to validate user access to other resources. However, we find that web developers nowadays heavily depend on third-party JavaScript providers (e.g., jQuery and Google Analytics) to facilitate the web development, which means the security of the web application will depend on the reliability of third-party service providers.

Therefore, we would like to present a measurement study to learn existing third-party JavaScript deployment within the websites and identify insecure practices of web developers.

CHAPTER 5

CONCLUSION

This dissertation presents two works to renovate the wireless physical layer design towards the improvement of wireless network security.

In the first work, we developed a novel and practical wireless technique named pinpoint waveforming to achieves the location-restricted service access control. We also implemented a real-time video streaming service to validate the proposed scheme. Compared to traditional access control techniques, this work allows the system to securely deliver the service to eligible locations without incurring expensive cryptographic encryption operations.

The second work develops a secure far proximity identification approach that can determine whether a remote device is far away. We propose to extract a physical layer fingerprint that is quite related with the proximity, and is unique and unforgeable. We also developed a technique that uses the proximity fingerprint to calculate the proximity lower bound, thus preventing potential spoofing attacks in long-haul wireless communications.

REFERENCES

- [1] Tao Wang, Yao Liu, and Athanasios V Vasilakos. Survey on channel reciprocity based key establishment techniques for wireless systems. *Wireless Networks*, 21(6):1835–1846, 2015.
- [2] A. Goldsmith. *Wireless communications*. Cambridge university press., 2005.
- [3] R. R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaidya. Using directional antennas for medium access control in ad hoc networks. In *Proceedings of the MobiCom '02*, 2002.
- [4] K.B. Rasmussen, C. Castelluccia, T.S. Heydt-Benjamin, and S. Čapkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*, 2009.
- [5] L. Cai, K. Zeng, H. Chen, and P. Mohapatra. Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas. In *Proceedings of the Annual Network and Distributed System Security Symposium (NDSS 2011)*, 2011.
- [6] T. Halevi, D. Ma, N. Saxena, and T. Xiang. Secure proximity detection for nfc devices based on ambient sensor data. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS 2012)*, 2012.
- [7] Y. Liu, P. Ning, and H. Dai. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In *Proceedings of 2010 IEEE Symposium on Security and Privacy (S&P '10)*, pages 286–301, May 2010.
- [8] S. Brands and D. Chaum. Distance bounding protocols. In *Proceedings of EURO-CRYPT*, pages 344–359, 1994.
- [9] N. O. Tippenhauer and S. Čapkun. Id-based secure distance bounding and localization. In *Proceedings of 2009 European Symposium on Research in Computer Security (ESORICS'09)*, 2009.
- [10] K. B. Rasmussen and S. Čapkun. Realization of rf distance bounding. In *Proceedings of the USENIX Security Symposium*, 2010.

- [11] G. P. Hancke and M. G. Kuhn. An RFID distance bounding protocol. In *Proceedings of SecureComm'05*, pages 67–73, 2005.
- [12] Marine vhf radio. http://en.wikipedia.org/wiki/Marine_VHF_radio. [Online; accessed 13-July-2013].
- [13] R. Weinmann. The baseband apocalypse. *BlackHat DC*, 2011.
- [14] C. Paget. Practical cellphone spying. *DEF CON 18*, 2010.
- [15] Tao Wang, Yao Liu, Tao Hou, Qingqi Pei, and Song Fang. Signal entanglement based pinpoint waveforming for location-restricted service access control. *IEEE Transactions on Dependable and Secure Computing*, 15(5):853–867, 2018.
- [16] Tao Wang, Yao Liu, Qingqi Pei, and Tao Hou. Location-restricted services access control leveraging pinpoint waveforming. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 292–303. ACM, 2015.
- [17] Tao Wang, Yao Liu, and Jay Ligatti. Fingerprinting far proximity from radio emissions. In *European Symposium on Research in Computer Security*, pages 508–525. Springer, 2014.
- [18] F. Sivrikaya and B. Yener. Time synchronization in sensor networks: a survey. *Network, IEEE*, 2004.
- [19] J. E. Elson and D. Estrin. *Time synchronization in wireless sensor networks*. PhD thesis, University of California, Los Angeles, 2003.
- [20] J Elson, L Girod, and D Estrin. Fine-grained network time synchronization using reference broadcasts. *SIGOPS Oper. Syst. Rev.*, 2002.
- [21] C. A. Balanis. *Antenna Theory: Analysis and Design*. Wiley-Interscience, 2005.
- [22] J Proakis and M Salehi. *Digital Communications*. McGraw-Hill Education, 2007.
- [23] M. Biguesh and A.B. Gershman. Training-based mimo channel estimation: a study of estimator tradeoffs and optimal training signals. *Signal Processing, IEEE Transactions on*, 2006.
- [24] Song Fang, Yao Liu, Wenbo Shen, Haojin Zhu, and Tao Wang. Virtual multipath attack and defense for location distinction in wireless networks. *IEEE Transactions on Mobile Computing*, 16(2):566–580, 2016.
- [25] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam. Proximate: proximity-based secure pairing using ambient wireless signals. In *Proceedings of the MobiSys'11*, 2011.

- [26] M. K. Simon and M. S. Alouini. *Digital communication over fading channels*. John Wiley & Sons, 2005.
- [27] J. Salz and J.H. Winters. Effect of fading correlation on adaptive arrays in digital mobile radio. *Vehicular Technology, IEEE Transactions on*, 1994.
- [28] X. He, H. Dai, W. Shen, and P. Ning. Is link signature dependable for wireless security? In *INFOCOM, 2013 Proceedings IEEE*, 2013.
- [29] Kai Yu and Björn Ottersten. Models for mimo propagation channels: a review. *Wireless communications and mobile computing*, 2(7):653–666, 2002.
- [30] Julius S Bendat and Allan G Piersol. *Random data: analysis and measurement procedures*. John Wiley & Sons, 2011.
- [31] C. Boyd and A. Mathuria. *Protocols for authentication and key establishment*. Springer Science & Business Media, 2003.
- [32] H. Krawczyk, R. Canetti, and M. Bellare. *HMAC: Keyed-hashing for message authentication*. RFC Editor, 1997.
- [33] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential dsss: Jamming-resistant wireless broadcast communication. In *Proceedings of the INFOCOM'10*, 2010.
- [34] M. Strasser, C. Pöpper, and S. Čapkun. Efficient uncoordinated fhss anti-jamming communication. In *Proceedings of the MobiHoc'09*, 2009.
- [35] Gnu radio. <http://gnuradio.org/redmine/projects/gnuradio/wiki>.
- [36] A. Lozano and N. Jindal. Transmit diversity vs. spatial multiplexing in modern mimo systems. *Wireless Communications, IEEE Transactions on*, 2010.
- [37] Song Fang, Tao Wang, Yao Liu, Shangqing Zhao, and Zhuo Lu. Entrapment for wireless eavesdroppers. 2019.
- [38] S. Sheth, A. Seshan and D. Wetherall. Geo-fencing: Confining wi-fi coverage to physical boundaries. *Pervasive Computing*, 2009.
- [39] Y. S. Kim, P. Tague, H. Lee, and H. Kim. Carving secure wi-fi zones with defensive jamming. In *Proceedings of the ASIACCS '12*, 2012.
- [40] A. Goldsmith. *Wireless Communications*. Cambridge University Press, New York, NY, USA, 2005.
- [41] N. Patwari and S. K. Kasera. Robust location distinction using temporal link signatures. In *MobiCom '07: Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pages 111–122, New York, NY, USA, 2007. ACM.



- [42] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom '08)*, pages 116–127, 2008.
- [43] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera. Advancing wireless link signatures for location distinction. In *MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking*, New York, NY, USA, 2008. ACM.
- [44] Gps signals. http://en.wikipedia.org/wiki/GPS_signals. [Online; accessed 27-July-2013].
- [45] A. F. Molisch. *Wireless Communications, 2nd Edition*. Wiley India Pvt. Limited, 2007.
- [46] L. B. Kuechle. Selecting receiving antennas for radio tracking. <http://www.atstrack.com/PDFFiles/receiverantrev6.pdf>.
- [47] S. Sud. A low complexity spatial rake receiver using main beam multipath combining for a cdma smart antenna system. In *Proceedings of 2007 IEEE Military Communications Conference (MILCOM)*, pages 1–6, 2007.
- [48] L. Yu, W. Liu, and R. J. Langley. Robust beamforming methods for multipath signal reception. *Digital Signal Processing*, 20(2):379–390, 2007.
- [49] SPAN. Measured channel impulse response data set. <http://span.ece.utah.edu/pmwiki/pmwiki.php?n=Main.MeasuredCIRDataSet>.
- [50] Tao Wang and Yao Liu. Secure distance indicator leveraging wireless link signatures. In *2014 IEEE Military Communications Conference*, pages 222–227. IEEE, 2014.
- [51] G. Mao, B. D. O. Anderson, and B. Fidan. Path loss exponent estimation for wireless sensor network localization. *The International Journal of Computer and Telecommunications Networking*, 51(10):2467–2483, 2007.
- [52] N. Alam, A. T. Balaie, and A. G. Dempster. Dynamic path loss exponent and distance estimation in a vehicular network using doppler effect and received signal strength. In *Proceedings of 2010 Vehicular Technology Conference Fall (VTC 2010-Fall)*, pages 1–5, 2010.
- [53] K. Gunnam, G. Choi, M. Yeary, and Y. Zhai. A low-power preamble detection methodology for packet based rf modems on all-digital sensor front-ends. In *In Proceedings of the IEEE Instrumentation and Measurement Technology Conference*, 2007.
- [54] M. Biguesh and A. B. Gershman. Training-based mimo channel estimation: A study of estimator tradeoffs and optimal training signals. *IEEE Transaction on Signal Processing*, 54(3):884–893, March 2006.


- [55] M. K. Tsatsanis and G. B. Giannakis. Blind estimation of direct sequence spread spectrum signals in multipath. *IEEE Transactions on Signal Processing*, 5(45):1241 – 1252, 1997.
- [56] C. Jinho. Equalization and semi-blind channel estimation for space-time block coded signals over a frequency-selective fading channel. *IEEE Transactions on Signal Processing*, 52(3):774 – 785, 2004.
- [57] A. Mahmood, R. Exel, H. Trsek, and T. Sauter. Clock synchronization over iee 802.11—a survey of methodologies and protocols. *IEEE Transactions on Industrial Informatics*, 13(2):907–922, April 2017.
- [58] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang. Defending DSSS-based broadcast communication against insider jammers via delayed seed-disclosure. In *Proceedings of the 26th Annual Computer Security Applications Conference ACSAC '10*, December 2010.
- [59] Robert A. Scholtz. *Spread Spectrum Communications Handbook*. McGraw-Hill, 2001.
- [60] A. Goldsmith. *Wireless Communications*. Cambridge University Press, August 2005.
- [61] Pöpper, M. Strasser, and S. Čapkun. Anti-jamming broadcast communication using uncoordinated spread spectrum techniques. *IEEE Journal on Selected Areas in Communications: Special Issue on Mission Critical Networking*, 2010.
- [62] R. Poisel. *Modern Communications Jamming Principles and Techniques*. Artech House Publishers, 2006.
- [63] C. Pöpper, M. Strasser, and S. Čapkun. Jamming-resistant broadcast communication without shared keys. Technical report, ETH Zurich, September 2008. ETH Zurich D-INFK Technical Report 609.
- [64] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '05)*, 2005.
- [65] J. Chiang and Y. Hu. Extended abstract: Cross-layer jamming detection and mitigation in wireless broadcast networks. In *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '07)*, 2007.
- [66] N. Patwari and S. K. Kasera. Temporal link signature measurements for location distinction. *IEEE Transactions on Mobile Computing*, 10(3):449–462, March 2011.
- [67] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In *Proceedings of the IEEE Symposium on Security and Privacy (oakland'05)*, pages 49–63, 2005.


- [68] N. Patwari and S. K. Kasera. CRAWDAD utah CIR measurements. <http://crawdad.cs.dartmouth.edu/meta.php?name=utah/CIR>.
- [69] Z. Chen and R.C. Luo. Design and implementation of capacitive proximity sensor using microelectromechanical systems technology. *IEEE Transactions on Industrial Electronics*, 45(6):886–894, 1998.
- [70] P. H. Lo, C. Hong, S. C. Lo, and W. Fang. Implementation of inductive proximity sensor using nanoporous anodic aluminum oxide layer. In *Proceedings of 2011 International Solid-State Sensors, Actuators and Microsystems Conference (TRANSDUCERS)*, pages 1871–1874, 2011.
- [71] D. Macii, F. Trenti, and P. Pivato. A robust wireless proximity detection technique based on rss and tof measurements. In *Proceedings of 2011 IEEE International Workshop on Measurements and Networking (M&N’11)*, pages 31–36, 2011.
- [72] Souvik Sen, Jeongkeun Lee, Kyu-Han Kim, and Paul Congdon. Avoiding multipath to revive inbuilding wifi localization. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, pages 249–262. ACM, 2013.
- [73] Yuexin Zhang, Yang Xiang, Tao Wang, Wei Wu, and Jian Shen. An over-the-air key establishment protocol using keyless cryptography. *Future Generation Computer Systems*, 79:284–294, 2018.

APPENDIX A: COPYRIGHT PERMISSIONS

The following permission is for the content in Chapter 3.





[Home](#) [Account Info](#) [Help](#) 


**Title:** Fingerprinting Far Proximity from Radio Emissions
Author: Tao Wang, Yao Liu, Jay Ligatti
Publication: Springer eBook
Publisher: Springer Nature
Date: Jan 1, 2014
Copyright © 2014, Springer International Publishing Switzerland


Logged in as:
Tao Wang
[LOGOUT](#)

Order Completed
Thank you for your order.
This Agreement between Tao Wang ("You") and Springer Nature ("Springer Nature") consists of your license details and the terms and conditions provided by Springer Nature and Copyright Clearance Center.
Your confirmation email will contain your order number for future reference.
[printable details](#)
License Number 4607481239013
License date Jun 14, 2019
Licensed Content Publisher Springer Nature
Licensed Content Publication Springer eBook
Licensed Content Title Fingerprinting Far Proximity from Radio Emissions
Licensed Content Author Tao Wang, Yao Liu, Jay Ligatti
Licensed Content Date Jan 1, 2014
Type of Use Thesis/Dissertation
Requestor type academic/university or research institute
Format electronic
Portion full article/chapter
Will you be translating? no
Circulation/distribution <501
Author of this Springer Nature content yes
Title Wireless Physical Layer Design for Confidentiality and Authentication
Institution name University of South Florida
Expected presentation date Aug 2019
Requestor Location Tao Wang
4202 E. Fowler Avenue
TAMPA, FL 33620
United States
Attn: Tao Wang
Total 0.00 USD
[ORDER MORE](#) [CLOSE WINDOW](#)
Copyright © 2019 [Copyright Clearance Center, Inc.](#) All Rights Reserved. [Privacy statement](#). [Terms and Conditions](#).
Comments? We would like to hear from you. E-mail us at customer@copyright.com

The following two permissions are for the content in Chapter 2.



[Home](#) [Account Info](#) [Help](#) 



Requesting permission to reuse content from an IEEE publication

Title: Signal Entanglement Based Pinpoint Waveforming for Location-Restricted Service Access Control

Author: Tao Wang

Publication: Dependable and Secure Computing, IEEE Transactions on

Publisher: IEEE

Date: 1 Sept.-Oct. 2018

Copyright © 2018, IEEE

Logged in as:
Tao Wang

[LOGOUT](#)

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

[BACK](#) [CLOSE WINDOW](#)

Copyright © 2019 [Copyright Clearance Center, Inc.](#) All Rights Reserved. [Privacy statement](#). [Terms and Conditions](#).
Comments? We would like to hear from you. E-mail us at customer care@copyright.com



RightsLink®

Account
Info

Help



Title: Proceedings, Association for
Computing Machinery
Article ID: PJC02
Publication: Publication1
Publisher: CCC Reproduction
Date: Jan 1, 1900
Copyright © 1900, CCC Reproduction

Logged in as:
Tao Wang
Account #:
3001469185

LOGOUT

Order Completed

Thank you for your order.

This Agreement between Tao Wang ("You") and ACM (Association for Computing Machinery) ("ACM (Association for Computing Machinery)") consists of your order details and the terms and conditions provided by ACM (Association for Computing Machinery) and Copyright Clearance Center.

License number	Reference confirmation email for license number
License date	Jun, 14 2019
Licensed content publisher	ACM (Association for Computing Machinery)
Licensed content title	Proceedings, Association for Computing Machinery
Licensed content date	Jan 1, 1900
Type of use	Thesis/Dissertation
Requestor type	Academic institution
Format	Electronic
Portion	chapter/article
The requesting person/organization	Tao Wang
Title or numeric reference of the portion(s)	Chapter 2
Title of the article or chapter the portion is from	Location-restricted Services Access Control Leveraging Pinpoint Waveforming
Editor of portion(s)	N/A
Author of portion(s)	Tao Wang, Yao Liu, Qingqi Pei, and Tao Hou
Volume of serial or monograph	N/A
Page range of portion	
Publication date of portion	OCT, 2015
Rights for	Main product
Duration of use	Life of current edition
Creation of copies for the disabled	no
With minor editing privileges	yes
For distribution to	Worldwide
In the following language(s)	Original language of publication
With incidental promotional use	no
Lifetime unit quantity of new product	Up to 499
Title	Wireless Physical Layer Design for Confidentiality and Authentication
Institution name	other
Expected presentation date	Aug 2019
Requestor Location	Tao Wang 4202 E. Fowler Avenue TAMPA, FL 33620 United States Attn: Tao Wang
Billing Type	Invoice
Billing address	Tao Wang 4202 E. Fowler Avenue TAMPA, FL 33620 United States Attn: Tao Wang
Total (may include CCC user fee)	0.00 USD
Total	0.00 USD

CLOSE WINDOW

Copyright © 2019 Copyright Clearance Center, Inc. All Rights Reserved. [Privacy statement](#). [Terms and Conditions](#).
Comments? We would like to hear from you. E-mail us at customer@copyright.com