Wireless Network Physical Layer Security with Smart Antenna

Ting Wang

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Computer Engineering

Yaling Yang, Chair
Y. Thomas Hou
Jung-Min Park
Sandeep K. Shukla
Danfeng Yao

May 7, 2013
Blacksburg, Virginia

Keywords: Wireless Network Security, Localization, Location privacy, Anti-eavesdropping,
Smart Antenna, Beamforming, Location Spoofing

Wireless Network Physical Layer Security with Smart Antenna

Ting Wang

(ABSTRACT)

Smart antenna technique has emerged as one of the leading technologies for enhancing the quality of service in wireless networks. Because of its ability to concentrate transmit power in desired directions, it has been widely adopted by academia and industry to achieve better coverage, improved capacity and spectrum efficiency of wireless communication systems. In spite of its popularity in applications of performance enhancement, the smart antenna's capability of improving wireless network security is relatively less explored. This dissertation focuses on exploiting the smart antenna technology to develop physical layer solutions to anti-eavesdropping and location security problems.

We first investigate the problem of enhancing wireless communication privacy. A novel scheme named "artificial fading" is proposed, which leverages the beam switching capability of smart antennas to prevent eavesdropping attacks. We introduce the optimization strategy to design a pair of switched beam patterns that both have high directional gain to the intended receiver. Meanwhile, in all the other directions, the overlap between these two patterns is minimized. The transmitter switches between the two patterns at a high frequency. In this way, the signal to unintended directions experiences severe fading and the eavesdropper cannot decode it. We use simulation experiments to show that the artificial fading outperforms single pattern beamforming in reducing the unnecessary coverage area of the wireless transmitter.

We then study the impact of beamforming technique on wireless localization systems from the perspectives of both location privacy protection and location spoofing attack.

For the location privacy preservation scheme, we assume that the adversary uses received signal strength (RSS) based localization systems to localize network users in Wireless LAN (WLAN). The purpose of the scheme is to make the adversary unable to uniquely localize the user when possible, and otherwise, maximize error of the adversary's localization results. To this end, we

design a two-step scheme to optimize the beamforming pattern of the wireless user's smart antenna. First, the user moves around to estimate the locations of surrounding access points (APs). Then based on the locations of the APs, pattern synthesis is optimized to minimize the number of APs in the coverage area and degenerate the localization precision. Simulation results show that our scheme can significantly lower the chance of being localized by adversaries and also degrade the location estimation precision to as low as the coverage range of the AP that the wireless user is connected to.

As personal privacy preservation and security assurance at the system level are always conflictive to some extent, the capability of smart antenna to intentionally bias the RSS measurements of the localization system also potentially enables location spoofing attacks. From this aspect, we present theoretical analysis on the feasibility of beamforming-based perfect location spoofing (PLS) attacks, where the attacker spoofs to a target fake location by carefully choosing the beamforming pattern to fool the location system. The PLS problem is formulated as a nonlinear feasibility problem, and due to its intractable nature, we solve it using semidefinite relaxation (SDR) in conjunction with a heuristic local search algorithm. Simulation results show the effectiveness of our analytical approach and indicate the correlation between the geometry of anchor deployment and the feasibility of PLS attacks. Based on the simulation results, guidelines for guard against PLS attacks are provided.

This work is supported in part by National Science Foundation fund number ECCS-0802112 and the Institute for Critical Technology and Applied Science (ICTAS).

To my beloved family

- parents Lisuo Wang, Yuping Zhang and husband Min Li

Acknowledgments

First and foremost, I would like to thank my advisor Dr. Yaling Yang for her guidance, inspiration and continuous support throughout my Ph.D study. She encourages me to explore the topics of my interest and is always there to help. She is nice and patient, discussing my research works with me and helping me to improve my paper writing and presentation skills. Outside of work, she has always been a good friend, which makes our research group a big happy family. It is my fortune and honor to have her as my advisor.

I would like to thank all my committee members, Dr. Y. Thomas Hou, Dr. Jung-Min Park, Dr. Sandeep K. Shukla and Dr. Danfeng Yao, for spending their precious time on the dissertation review and providing me helpful suggestions.

I also extend my gratitude to my colleagues of the SHINE lab, Bo Gao, Chuan Han, Chang Liu, Jingyao Zhang, Zhenhua Feng, Zhenhe Pan, Yi Tang, Xiangwei Zheng and Kexiong Zeng, for all the inspiring discussions and brainstorming.

I must thank all my friends at Blacksburg for making my life here wonderful and memorable. Qing He, Yue Yan, Xiaoxing Li, Xiaojing Long, Tao Jia and Yuan Shen have been my friends since the first year of my life here. Because of them, I was not lonely when I started a life far away from home. I feel lucky that later I found more and more lovely friends here: Jiajia Li, Huijun Xiong, Guanying Wang, Kaigui Bian, Hao Wu, Hua Lin, Liguang Xie, Canming Jiang, Shengzhi Shao, Yi Deng.

Last but not least, I give my dedicated thanks to my parents and my husband Min Li. Without their

love and support, I would not be able to make this work completed. I would like to express my heart-felt gratitude to all of them.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Smart antenna technique has emerged as one of the leading technologies for enhancing the overall performance of wireless communication systems. It utilizes the diversity created by the multiple antenna elements of the antenna array to perform spatial filtering on both the transmitted and received signals, which cannot be done by conventional omnidirectional antennas. This unique advantage of the smart antenna enables signal processing in the spatial domain in addition to the time and frequency dimensions. Numerous studies have been done to explore the use of smart antenna technique to improve the quality of service in wireless networks. Some of the existing wireless communication infrastructures have already implemented smart antennas to achieve better coverage, improved capacity and higher transmission quality. However, the ability of the smart antenna technique in the field of wireless network security is comparatively less explored. Until very recently, the utilization of smart antenna in communication security has been mostly focused on spatially concentrating transmit power and using multiple-input and multiple-output (MIMO) to create artificial noise for the purpose of anti-eavesdropping. This dissertation aims to exploit novel applications of the smart antenna technique to the security of wireless network physical layer.

1.2 Smart Antenna Meets Network Security and Privacy

Most of the security problems in network physical layer are related to the fact that in wireless communication, information is exchanged over the air and may be captured or interfered by adversaries. The aim of physical layer security is to ensure reliable delivery of information to the intended receiver and, at the same time, prevent malicious access and interferences. Both these two aspects are highly influenced by the status of the wireless communication channel. While the channel variation due to the natural environment is beyond our control, the powerful smart antenna technology makes signal tuning at the transmitters and receivers a possible solution to get control over the wireless communication links.

Smart antenna techniques are known for their capabilities in increasing communication range, interference reduction, spatial reuse, etc. In the area of wireless network security, the most popular application of smart antenna is anti-eavesdropping. In [12] and [43], the authors propose to use a collaboration of multiple APs equipped with smart antenna arrays to reduce the region exposed to eavesdroppers. In [46] and [48] antenna array redundancy is utilized to create random interference to the eavesdropping channel. In [26] and [97], the authors introduce artificial noise produced by smart antenna to confuse the eavesdroppers with carefully designed noise signals, which can be canceled at the intended receiver. Other than anti-eavesdropping, directional antenna also has been used to prevent wormhole attacks in [35]. The authors in [91] developed a system named "SecureAngle" which leverages angle-of-arrival (AoA) information measured by antenna array to construct signatures that uniquely identify wireless users and set up virtual fences to enhance network security.

All the above applications show the effectiveness of smart antenna in enhancing security of wireless networks. However, things that we can do with smart antenna are absolutely not limited to these applications. This dissertation proposes three novel security approaches based on smart antenna in wireless network physical layer. The topics include potential threats and security solutions for the communication privacy and radio positioning based on beamforming of the smart antenna.

1.3 Scope of the Dissertation

According to the layered model of network architecture, security issues vary in different network layers. This dissertation concentrates on the security and privacy issues in the wireless network physical layer. Physical layer security approaches are independent of and can be complementary to upper layer security approaches such as data encryption. Particularly, the goal of this dissertation is to exploit the capability of smart antenna to solve problems of anti-eavesdropping and location security.

Anti-eavesdropping aims at securing the confidentiality of the transmitted data and has always been an active research topic in wireless communication. We revisit this old topic and develop a novel scheme to tackle this problem using beamforming of smart antenna.

Comparatively, location security involves new issues raised after the development of localization technique. On one hand, the localization systems are targeting accurate location estimation of all wireless nodes in civil and military applications. The location estimation results may be used by location based service (LBS), location based access control (LBAS) and other critical systems. Ambiguous or unrevealed location information will degenerate the performance of the localization systems or even fail the functionality of the system. On the other hand, accurate localization conflicts with the users' interests of privacy protection. Especially if the control of the localization system or the location estimation results can be potentially taken over by malicious parties, the location privacy of the users is in danger and further attacks based on the users' location information can be threatening. This is a reflection of the contradiction between security and privacy. In this dissertation, both the security and privacy aspects of the location related issues in wireless networks are studied.

1.4 Contributions and Dissertation Organization

This dissertation presents novel solutions to the problems of anti-eavesdropping and location security in the network physical layer by leveraging the smart antenna technology.

First, we present a novel physical layer security strategy named "artificial fading" to enhance privacy of wireless communication [86]. It employs a smart antenna array at the sender to periodically switch the radiation pattern between a pair of predesigned beamforming patterns at a high frequency. These two patterns are designed to both have high constant directional gain towards the intended receiver. However, in all the other directions, the overlapping area between them is minimized. In this way, the double-beam switching process intentionally creates a fast fading effect, named artificial fading, to severely degenerate the signal in the unintended directions and hence reduce the unnecessary coverage. Therefore, there is little space where an eavesdropper can get the signal and, hence, the transmitted information is protected. Simulation experiments show that our anti-eavesdropping scheme outperforms single pattern beamforming in reducing the unnecessary coverage area exposed to eavesdroppers.

Second, we propose a location privacy protection scheme against received signal strength (RSS) based localization systems using beamforming [85]. We use a smart antenna array to change the wireless terminal's radiation pattern from omnidirectional to an optimized beamforming pattern. The radiation pattern reduces the number of valid RSS measurements that can be obtained by the localization system and also introduces large bias to the location estimation results. At the same time, the proposed pattern synthesize scheme ensures that the wireless terminal's communication quality is intact. To our best knowledge, our work is the first application of pattern synthesis for the purpose of protecting location privacy of wireless network users.

Third, we investigate the feasibility of location spoofing attacks using transmit beamforming. Specifically, this study focuses on the location spoofing attack that is targeting a particular fake location, and we name it perfect location spoofing (PLS) [87, 84]. The problem of PLS feasibility is formulated as a nonlinear programming problem, which is proven to be NP-hard. We solve it

using semidefinite relaxation combined with a heuristic local search algorithm. The effectiveness of the proposed solution is validated by simulation experiments. In addition, by analyzing the simulation results, the following questions are explored: how is the feasibility of PLS attacks related to the density and geometry of the anchor deployment of the location system? What kind of anchor deployment is good for guard against PLS attacks? Given certain anchor deployment and a specific fake location, where could the attacker be hiding to launch a PLS attack? The answers to the above questions provide a means to evaluate the robustness of RSS based localization system in terms of attack resistance and give insightful guidance for spoof resistant anchor deployment.

This dissertation is structured as follows:

- Chapter 2 introduces the preliminary knowledge related to this dissertation, which includes physical layer security and privacy in wireless networks, smart antenna fundamentals and localization techniques.
- Chapter 3 presents the novel idea of artificial fading, which is produced by smart antenna beam-switching. The method for designing optimal switched beamforming patterns to generate artificial fading is introduced in detail and the evaluation of the performance of the proposed scheme is provided.
- Chapter 4 proposes the smart antenna based location privacy protection scheme against RSS localization systems. Simulation results are provided to show the effectiveness of the proposed scheme.
- Chapter 5 investigates the feasibility of PLS attacks using beamforming. The formulation and solution to the PLS problem are introduced throughly. Strategies for defence against PLS attacks are also discussed.
- Chapter 6 concludes the dissertation.

Chapter 2

Preliminaries

This chapter introduces the background knowledge that is related to this dissertation, which covers wireless network physical layer security and privacy as well as smart antenna and localization techniques. Information in this chapter will facilitate the understanding of the concepts that are used throughout this dissertation.

2.1 Physical Layer Security Threats

Most of the physical layer attacks target the open peer-to-peer network architecture and the shared wireless medium of wireless networks. An exhaustive overview of physical layer security can be found in [89, 93, 90]. We group physical layer attacks roughly into three categories according to their direct impacts, which are attacks to network infrastructure, attacks to communication content and attacks to user identity information.

2.1.1 Attacks to Network Infrastructure

The most straightforward way to attack a wireless network is by tampering the network devices. If a node of the network is compromised, the attacker can steal whatever information that is generated by this node or sent to this node. Moreover, the attacker can further launch denial-of-services (DOA) attacks to damage the network. Especially when the tampered node is the access point of the network, the damage caused by the attack is even more severe.

2.1.2 Attacks to Communication Content

Attacks to communication content aim at either stealing confidential data, which is realized by eavesdropping attacks, or intercepting the data communication, which is realized by jamming attacks.

Eavesdropping

Eavesdropping attacks exist in both wired and wireless networks. For wired networks, the attackers need to physically intrude into the network to wiretap the communication data. Whereas, in wireless networks, the signal is broadcasted over the air and as long as the attackers are located inside the coverage area of the transmitter, they can hear the signal. In addition, the more sensitive the attackers' receivers are, the more capable they are to capture weak signals. Therefore, wireless networks are more prone to eavesdropping attacks.

Jamming

Jamming attacks disrupt wireless communication without physical intrusion to the network infrastructures. The logic of the attack is to introduce intense interference to occupy the frequency bands used by the wireless network, and the regular communication between legitimate wireless nodes is disrupted due to the strong interference.

2.1.3 Attacks to Identity Information

Identity attacks in wireless networks cover two types of attacks. One is user privacy violation and the other is identity spoofing.

Location Privacy Violation

From the user privacy point of view, identity attacks can be any illegal access to the personal information of wireless network users. For upper layers of wireless networks, privacy is considered related to the user account, IP address, MAC address, etc. However, in physical layer, user identity is linked to location and can be revealed by the radio signal [8]. Physical layer localization technology takes advantage of the broadcast nature of radio signal to pinpoint the location of wireless transmitters. With localization systems, the attackers can localize a particular user and track the movement of the user. Given the location and movement information, it is not difficult for the attackers to figure out the user's identity and even more confidential information.

Location Spoofing

From the system security aspect, forged identity is often the basis for other forms of attacks. In the upper layers of networking, identity spoofing can be IP spoofing and MAC address spoofing. In the physical layer, identity spoofing can be realized by location spoofing. For self-localization systems, the attackers may report fake location information to the system. In passive location systems, the attackers can manipulate the features of the radio signal and masquerade to be at fake locations [45] to forge their identities.

Due to the open nature of wireless networks, wireless localization is vulnerable to malicious attacks. In [17], it is experimentally shown that by attenuating or amplifying the RSS readings at the anchors, the localization system may conclude in false location estimation. Bauer et al. show that attackers with directional antennas [7] have the ability to bias the location estimation to a direction of their choice in addition to introducing significant localization errors. The requirements for

successful GPS spoofing attacks are analyzed in [80].

2.2 Physical Layer Security Approaches

In this part, we briefly introduce existing security approaches for solving the attacks mentioned in last section.

Infrastructure Protection

In order to protect network infrastructures from attacks, hardware based schemes are a straightforward choice. In [13], defense techniques based on processor monitoring are proposed to prevent attacks to routers. Upper layer authentication and authorization protocol can also be helpful. A centralized provisioned management structure is proposed in [33] to disseminate network policies and administration privileges to all the devices that make up the network infrastructure.

Anti-eavesdropping

Besides the smart antenna-based anti-eavesdropping schemes that are summarized in Section 1.2, cryptographic [55] is also widely used to make it extremely difficult for the eavesdroppers to understand the transmitted data even if they can hear it. In this way, the data carried by the wireless signal stays secured.

Anti-jamming

The most commonly used anti-jamming technique is spread spectrum which has two kinds of implementation. One is frequency-hopping spread spectrum (FHSS), which changes the frequency band of the wireless signal randomly, so that it is quite difficult for the attackers to capture the signal. The other is direct-sequence spread spectrum (DSSS), which spreads the signal energy to

cover a wide rage of frequency bands, such that the signal is indistinguishable from noise [78].

Privacy Preservation

To protect location privacy of wireless network users, in [37] Jiang et al. use intelligent transmit power control (TPC) to reduce the APs in range to reduce the chance of being localized. In [88], a physical layer location privacy scheme with beamforming against AOA based localization systems is proposed. An approach named "Phantom" is proposed in [57] which leverages synchronized transmissions among multiple close-by mobile devices to create forged locations and obfuscate adversary's location systems.

Secure Localization

A few robust localization schemes have been proposed to countermeasure malicious attacks. A secure localization and key distribution scheme named "Secure Walking GPS" is introduced in [54] to cope with the Dolev-Yao, the wormhole, and the GPS-denial attacks. The authors in [23] design an attack-resistant fingerprinting based localization algorithm using a probabilistic inclusive disjunction model. Bao and Liang propose an algorithm that uses the sensor node votes to improve the safety performance of node positioning in wireless sensor networks [6]. Statistical analysis is also a powerful tool to detect and eliminate biased RSS measurements under signal strength attacks [17, 45, 47].

2.3 Smart Antenna Fundamentals

A smart antenna generally represents any antenna array that is capable of adjusting or adapting its radiation pattern according to application requirements, such as enhancing signals of interest and minimizing interferences [30]. Figure 2.1 illustrates the basic idea of smart antenna pattern synthesis. Each of the antenna elements contributes to the final output based on its associated

complex weight, which adjusts the amplitude and phase of the antenna element. The combination of all the weighted excitations determines the total radiation gain of the antenna array. Following the same principle, a smart antenna array can be constructed with a variety of geometries, like linear array, circular array, planar array and 3-dimensional array.

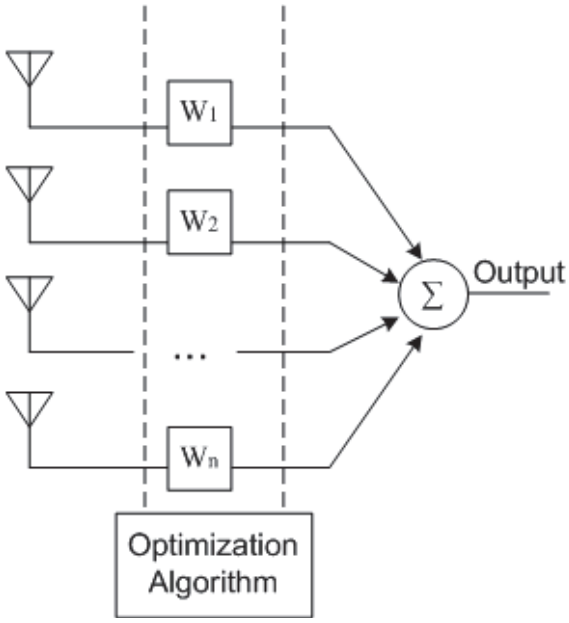


Figure 2.1: Pattern synthesis of smart antenna.

2.3.1 Types of Smart Antenna

Basically there are two ways to realize smart antennas, which are switched beam and fully adaptive array. Although both of them have the functionality of adjusting the beam patterns, their degrees of "smartness" are different according to the flexibility in pattern synthesis.

Switched Beam Antenna

The switched beam is an easy implementation of smart antennas. In this approach, an antenna array has several fixed beam patterns with a narrow beamwidth. Usually, these beam patterns are

obtained by shifting one directional beam pattern. For application in either the transmitter or the receiver, simple algorithm can be used to adjust the phase of the antenna elements and steer the beam pattern to point to the optimum direction. Switched beam antennas can provide significant improvement in signal coverage and channel capacity compared with traditional omnidirectional antennas. However, its performance is limited due to lack of flexibility in tuning the beam patterns.

Adaptive Array Antenna

Fully adaptive antenna arrays are much more powerful than switched beam antennas. Sophisticated signal processing algorithms are adopted to dynamically optimize the synthesized beam pattern. In this way, it can perform rapid reactions to the changing wireless channel condition and system requirement. For transmitter beamforming, it is able to track the mobility of the desired user to provide consistent high quality signal to the mobile user, while at the same time minimize the interference to other users by forming nulls in their directions. For receiver beamforming, adaptive antennas can mitigate the interferences as well as multipath effects to get a better signal-to-interference ratio. However, all these nice features are achieved at the cost of high complexity of the signal processing algorithm and high computational requirement.

2.3.2 Applications of Smart Antenna

Smart antenna is a promising technique which has already fundamentally boosted multiple applications in wireless communication [81]. In this part, we present several representative applications of the smart antenna technique.

Power Efficiency Enhancement

Conventional antennas transmit wireless signal with omnidirectional patterns even if the intended receivers are only in a particular direction. As a result, most of the transmit energy is actually wasted. With a smart antenna, the transmitter can selectively concentrate the transmit power to the

directions of the intended receivers. Thus, compared with conventional antennas, smart antennas are capable of serving the same users with less power consumption and reaching users in longer distances using the same power consumption.

Channel Capacity Enhancement

There are several advantages of using smart antenna for communication to improve wireless channel capacity. First, the use of directional beams results in reduced interference, better signal-to-interference ratio and hence, improved capacity [10]. Second, the smart antenna is a helpful tool to mitigate multipath effects [75]. Third, the smart antenna enables multiple-input multiple-output (MIMO) and thus achieves better communication performance with spatial diversity.

Spatial Division Multiple Access (SDMA)

With the advanced spatial processing capability, the smart antenna is able to locate multiple users and create a separated sector for each user. In this way, multiple users can share the same frequency band at the same time with an angular separation. This technology significantly improves the frequency reuse and hence, increases the system capacity and reduces the infrastructure cost [9].

Direction Finding

Direction finding is another important application of smart antennas [65, 68]. On one hand, it is helpful for targeting the intended receiver when adjusting and steering the directional beam patterns. On the other hand, direction finding is the fundamental requirement of Direction of Arrival (DOA) based localization techniques.

Security Enhancement

One straightforward security benefit of using smart antennas in communication is that the wireless signal will be more concentrated to the intended receiver. The reduced signal radiation to other directions results in lower chances of eavesdropping attacks. In this dissertation, we will further exploit the potential of smart antennas in security aspects. We will investigate the cases where smart antennas are utilized to ensure physical layer security, as well as launch attacks to wireless networks.

2.4 Localization Techniques

Wireless localization has been a long standing research topic and the recent location based services (LBSs) have greatly promoted the rapid development of localization techniques. In this section, we first provide a brief overview of the existing location schemes. Then, we introduce the potential attacks to localization systems and the countermeasures that have been developed for attack-resistant localization.

Based on the mechanisms used for position estimation, we group the existing localization schemes roughly into four categories: range-based, fingerprinting-based, connectivity-based and hybrid positioning.

2.4.1 Range-based Positioning

In range-based localization systems, the distance information can be obtained from RSS and time of arrival (TOA) measurements. For RSS based schemes, the distance from the transmitter to the receiver is estimated using radio signal propagation and attenuation models [63, 39, 94]. Similarly, TOA based schemes use the signal propagation delay to calculate the distance [59, 19, 27]. With these estimated distances, the localization result is obtained geometrically by trilateration. Besides trilateration, another range-based mechanism of positioning is triangulation, where the wireless

signal's angle of arrival (AOA) is measured by receivers equipped with antenna arrays [56, 64]. Positioning using triangulation is based on the principle that in a triangle graph, if the positions of the vertices are already known and the angles from a point inside this triangle to the vertices are given, the position of the interior point can be determined.

2.4.2 Fingerprinting-based Positioning

Fingerprinting-based schemes follow a common two-phase framework for location estimation, although they may use different kinds of signal measurements. Before the positioning system can operate, an off-line phase is necessary to collect sensing data that carries location dependent features and create the fingerprint database. During the on-line phase, the location of the wireless radio is estimated using classification algorithms based on the fingerprint database. RSS of Wireless LAN signals is the most widely used measurement for fingerprinting-based schemes [4, 5, 38, 25, 71, 70]. In addition, in [16], FM broadcast radio signals are used for indoor fingerprinting because they are less susceptible to human presence, multipath and fading. The authors in [3] construct fingerprint by combining the optical, acoustic and motion attributes captured by sensors on a mobile phone.

2.4.3 Connectivity-based Positioning

As the name suggests, connectivity-based algorithms use merely the connectivity information to estimate the position of wireless radios. In [11], a node calculates the centroid of its proximate reference points to localize itself using a simple connectivity metric. An approximate point-in-triangle test (APIT) positioning scheme is presented in [34]. Location algorithms using multidimensional scaling are introduced in [73, 72].

2.4.4 Hybrid Positioning

Recently, smartphone localization has attracted tremendous interest, and the variety of sensors in smartphones enable new hybrid positioning schemes, which take advantage of multimodal sensing to achieve better location accuracy and independence from infrastructure. Constandache et al. develop a war-driving free human localization system which uses the accelerometer and compass readings from smartphones to capture users' movement traces [20, 21]. The authors in [96] propose a technique called EV-Loc which integrates electronic and visual signals to improve the accuracy of wireless localization. Acoustic ranging estimates among peer phones are utilized to assist WiFi based localization for improved accuracy in [49]. Other location schemes based on multimodal sensing can be found in [69, 83, 52].

Chapter 3

Enhancing Wireless Communication Privacy with Artificial Fading

This chapter addresses the problem of anti-eavesdropping in wireless network physical layer. The main contribution of this chapter is twofold. First, we propose a novel concept of *artificial fading* that is produced by double-beam switching of smart antenna array to intentionally corrupt unwanted wireless communication links. Second, we develop a physical layer anti-eavesdropping scheme to minimize the unnecessary coverage area, and hence, lower the chance of being eavesdropped. Our anti-eavesdropping scheme employs smart antenna with two synthesized radiation patterns, which are optimized to provide good signal quality to the intended receiver, while their overlap apart from the intended direction is minimized. During the transmission, the transmitter periodically alternates between the two optimized patterns at a high frequency, which produces severe fading to the received signal in undesired directions. Since such signals are corrupted and cannot be decoded, eavesdropping is prevented. Simulation experiments show that our anti-eavesdropping scheme outperforms single pattern beamforming in reducing the unnecessary coverage area exposed to eavesdroppers.

3.1 Introduction

With the advances in wireless data networking, the amount of confidential information communicated through "free medium" is greater than ever. However, leaving those important data floating in the space is dangerous and vulnerable to eavesdropping attack.

Generally, there are two complementary types of schemes to combat eavesdropping attack. The first type includes cryptographic techniques which are based on the premise that deciphering without knowledge of the secret key is computationally infeasible [55]. The second type is physical layer security schemes that aim at hiding the protected radio signal to the passive eavesdroppers. In this chapter, we focus on the latter.

Physical layer security schemes are usually following two concepts: intentionally adding interference to the eavesdropping channels or reducing the coverage region of the transmitter. To generate interference to the eavesdropping channels, the authors in [46] and [48] use antenna array redundancy to create random interference to the eavesdropping channel, while in [26] and [97], artificial noise is introduced to confuse the eavesdropper with carefully designed noise signals which can be canceled at the intended receiver. These schemes require that the channel response from the transmitter to the receiver is perfectly estimated and known to the transmitter. This is realized by either assuming that the communication channel is reciprocal or the transmitter gets feed back about the channel information from the receiver. On the other hand, methods that reduce coverage region lower the chances of eavesdropping by stopping the eavesdroppers from hearing the transmitted signal. In [12] and [43], the authors propose to use collaboration of multiple Access Points (APs) equipped with smart antenna arrays to reduce the region exposed to eavesdroppers. These schemes modify the network protocol to segment the original network packets into fragments. These fragments then are sent by different APs. These schemes are only applicable to network infrastructures with high density of APs.

In this chapter, we present a novel physical layer security strategy named "artificial fading" to reduce the coverage region of a transmitter. We employ smart antenna array at the sender to

periodically switch the radiation pattern between a pair of predesigned beamforming patterns at a high frequency. These two patterns are designed to both have high constant directional gain towards the intended receiver. However, in all the other directions, the overlapping area between them is minimized. In this way, the double-beam switching process intentionally creates a fast fading effect, named artificial fading, to severely degenerate the signal in the unintended directions and hence reduce the unnecessary coverage. Therefore, there is little space where an eavesdropper can get the signal and, hence, the transmitted information is protected. The detailed contributions of our work are as follows:

- We present the novel concept of artificial fading to support physical layer anti-eavesdropping.
- We propose the method for designing optimal switched beamforming patterns to generate artificial fading.
- We provide insightful evaluation of the performance of the proposed artificial fading scheme.

Comparing to existing approaches, artificial fading has the following benefits: *First, it does not require special deployment of the network infrastructures; Second, it does not require collaboration from other nodes in the network.* Our work shows that when single pattern beamforming scheme already reaches the optimum of minimizing unnecessary coverage area, we are still able to further reduce the unnecessary coverage area using artificial fading.

The rest of this chapter is organized as follows. The backgrounds about terminologies, threat model and smart antenna are introduced in Section 3.2. Section 3.3 describes the proposed scheme, artificial fading, and analyze its effectiveness for anti-eavesdropping. The modeling of antenna pattern optimization is presented in section 3.4. Experimental results are reported in Section 3.5. Section 3.6 discusses and Section 3.7 concludes the chapter.

3.2 Background

In this section we present the important definitions used throughout this chapter and introduce the threat model of eavesdropping attacks.

3.2.1 Definitions of Different Signal Coverages

Generally, the "coverage area" can be understood as the locations where the radiated signal can be heard, or, the area within which a wireless network user can successfully use the network service. However, the coverage areas can be classified into various levels which require different signal qualities. Thus, to be specific, we present the definitions of coverage areas under different signal quality requirements and use different names to differentiate them throughout this chapter.

Effective Coverage

The region within which the signal quality is good enough for successful decoding of the transmitted signal.

Invalid Coverage

The region where the existence of the transmitted signal can be detected but the signal quality is not good enough for decoding the signal.

Unnecessary Coverage

The region apart from the target receiver within the effective coverage area. It has little contribution to the wireless link between the transmitter and the receiver. However, it brings the risk of eavesdropping. Our proposed scheme aims at reducing this unnecessary coverage area, and hence, lowers the chance of being eavesdropped.

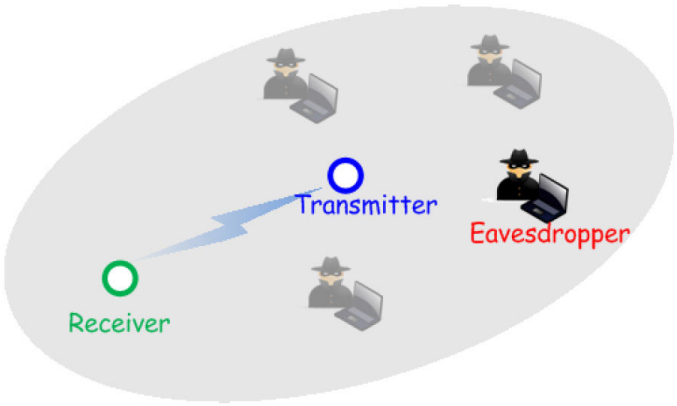


Figure 3.1: Eavesdropping threat.

3.2.2 Eavesdropping Threat Model

We assume that a communication link is set up between a pair of legitimate nodes. Packets carrying confidential information are broadcasted over the air. As an example illustrated in Figure 3.1, the effective coverage region of the transmitter is represented by the shaded area. A node, either the receiver or an adversarial eavesdropper, can receive the packets as long as it is located within the effective coverage of the transmitted signal. Thus an eavesdropper within the effective coverage can silently sniff the transmitted packets. Even if the leaked packets are encrypted, the eavesdropper may take effort to crack the encryption to extract the original data, or do data mining to obtain valuable information.

As we can see, the larger the effective coverage, the higher the risk of eavesdropping. Thus in this chapter, the objective of our strategy is to reduce the unnecessary coverage apart from the direction to the receiver. By using smart antenna array at the transmitter to concentrate the transmit power towards the receiver, the unnecessary coverage can be reduced. However, the reduction is limited by the directivity of a antenna array. In this work, we propose the concept of "artificial fading", which is realized by double-beam switching of smart antenna array, to break the limit of coverage reduction supported by a single beamforming pattern and therefore make much larger reduction on unnecessary coverage.

3.2.3 Smart Antenna Beamforming

A smart antenna array consists of multiple antenna elements. The geometric arrangement of the antenna elements varies according to different designs. However, the common idea of smart antenna arrays is that the amplitudes and phases of the current excitations to the antenna elements are controlled to obtain a desired synthesized radiation pattern. Mathematically, the current excitations are modeled as a complex weight vector. The process of adjusting the complex weight vector to synthesize a desired pattern is called beamforming [30]. Traditionally, beamforming is considered more suitable to be implemented at the APs or base stations in wireless networks. However, recent studies show that beamforming can also be realized on mobile devices [66, 95].

A fully adaptive smart antenna array has both static and dynamic capabilities of beamforming. The static beamforming capability is the ability to produce a specific pattern that satisfies the application requirement, such as minimizing the side lobe level when given a fixed main beam width, and vice versa. On the other hand, the dynamic capability means that the smart antenna is able to vary the synthesized pattern dynamically to meet the changing requirement. One metric for the dynamic performance of smart antennas is the transition time between two radiation patterns. Currently, advanced smart antenna products are able to switch beam patterns in sub-microsecond given the predefined beamforming patterns [58]. Some of them can even finish the pattern reconfiguration in tens of nanoseconds [12]. Thus using the advanced smart antenna hardware, the operation of our artificial fading scheme can be fulfilled within a very short period.

3.3 Artificial Fading

This section provides detailed introduction to the effectiveness of artificial fading.

3.3.1 Concept

Traditional beamforming based anti-eavesdropping methods based on smart antenna reduce the unnecessary coverage by simply reducing the transmit power to unintended directions, whereas the suppression capability is quite limited, especially for antenna array with fewer elements. This bottleneck is caused by the tradeoff between the side lobe level and the main beam width of a synthesized beamforming pattern, which means that if we want to decrease either the side lobe level or the main beam width, we have to increase the other. To break this bottleneck, we employ a smart antenna array at the transmitter end to produce two switched beamforming patterns. These two beamforming patterns are designed to satisfy two requirements. First, in the direction to the receiver, they both have persistent high directional gain to ensure good signal quality to the receiver. Second, in all the other directions, the overlap between these two patterns is minimized, meaning that the high gain directions of one beamforming pattern correspond to the null directions of the other beamforming pattern. Figure 3.2 is a simple illustration of the described pattern pair. During the transmission, the smart antenna array alternates between these two patterns at a high frequency. As a result, the receiver is getting persistent high quality signal, while in other directions, the RSS is changing dramatically and only incomplete frame fractions can be detected, which cannot be used to successfully recover the original signal. This periodical severe variation of the signal strength acts similarly to signal fading in wireless communication channels. Thus we name such signal variation intentionally produced by beam switching of smart antenna as "***Artificial Fading***". The locations where only incomplete frame fractions can be received are actually within the invalid coverage region. We will show that by means of artificial fading, we are able to produce larger reduction of unnecessary coverage comparing to single beamforming pattern.

3.3.2 Feasibility

In physical layer data transmissions, signal outage happens when deep fading causes the RSS falling below the radio sensitivity level. Burst of bit errors occurs during the signal outage period.

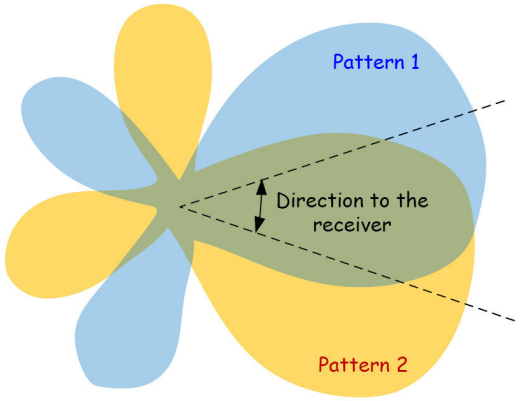


Figure 3.2: Illustration of a pattern pair for beam switching.

When the bit error rate goes beyond the capability of the error correction code, the whole frame is corrupted. The role of artificial fading is to create high-frequency periodical signal outage to the unintended transmit directions. To this end, we define the switching period as T_{sw}, which is set to be half of the physical layer data frame duration. State-of-the-art smart antennas can perform beam switching in less than one microsecond [12][58]. Thus, as long as the transition time of beam switching is negligible compared with the frame duration, it is feasible to carry out artificial fading during signal transmission.

To analyze the effectiveness of artificial fading, we use WLAN as an example. The minimum Physical Layer Convergence Protocol (PLCP) frame duration in WLANs is from tens of microseconds to more than 100 microseconds. Thus, a beam switching transition time less than one microsecond is negligible compared with the PLCP frame duration. Suppose at a specific location around the transmitter, while the path losses to the location are the same for two beamforming patterns 1 and 2, the antenna directional gains of these two patterns are different, which results in different average RSSs, denoted as $\overline{R}_1$ and $\overline{R}_2$ for these two patterns. Figure 3.3 shows how the signal strength fluctuates at this location when the two patterns are switched. When either $\overline{R}_1$ or $\overline{R}_2$ is lower than the radio sensitivity threshold, signal outage happens periodically at this location and causes bursts of bit errors. Next, we will show that such signal outage is beyond the tolerance of the error correction algorithm used in WLANs.

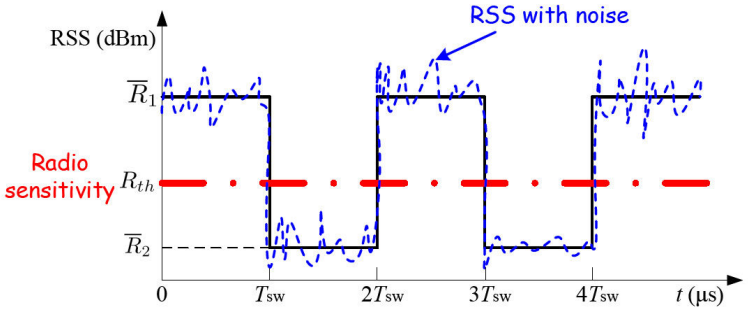


Figure 3.3: RSS fluctuation under artificial fading.

The error correction capability of an error correction code is defined as the number of bit errors (t_{ecc}) within a code word that can be corrected. For convolutional code, t_{ecc} is bounded by the free distance (d_{free}) following the relationship [60]

$$t_{ecc} = \lfloor \frac{d_{free} - 1}{2} \rfloor. \tag{3.1}$$

IEEE 802.11 standards use $K = 7$ convolutional code with a minimum code rate $\frac{1}{2}$ [1]. Higher code rate can be achieved by puncturing the "basic" rate $\frac{1}{2}$ code. Additionally, interleaving is used to avoid burst bit errors. Thus, we can consider that the bit errors caused by signal outage are randomly scattered across the whole frame. The largest d_{free} of $K = 7$ convolutional code is 10, which is reached under code rate $\frac{1}{2}$ by adding 7 redundant bits to the 7 information bits. So a code word of $K = 7$ rate $\frac{1}{2}$ convolutional code contains totally 14 bits. By plugging in $d_{free} = 10$ into equation (3.1), we can get that the 14 bits convolutional code word is able to correct up to 4 bit errors. In other words, the $K = 7$ convolutional code does not work when the bit error rate goes higher than $\frac{5}{14}$. While under the intentioned artificial fading, the signal outage probability is approximately $\frac{1}{2}$, which is out of the error correction capability of $K = 7$ convolutional code. Thus, we are safe to say that at a specific location, as long as the RSS under one of the two switched beamforming patterns is below the radio sensitivity threshold, no PLCP frame can be correctly decoded, and hence, this location is under invalid coverage.

It is worth mentioning that our artificial fading scheme is not limited to WLAN networks. It can also be applied to other wireless networks as long as the transition time between the switched

beamforming pattern is much less than the duration of the physical layer data frame and the signal outage produced by artificial fading is beyond the error correction capability of the coding scheme used by the wireless network protocol.

As a result of the proposed artificial fading scheme, the effective coverage area of the transmitter only includes the locations where under both of the two switched beamforming pattern, the RSS is higher than the radio sensitivity. In the following sections, we use this conclusion to calculate the effective coverage area of double-beam switching transmission.

3.4 Minimization of Unnecessary Coverage

In this section, we first describe the prediction of effective coverage area under our artificial fading scheme. Then we formulate the problem of minimizing unnecessary coverage based on the mathematical relationship between the antenna array weight vector and the effective coverage area.

3.4.1 Smart Antenna Model

In the remainder of this chapter, we assume that the radio station is equipped with a circular smart antenna array, which consists of N_{ant} isotropic elements placed over a circle with radius R. The i^{th} antenna element is located with the phase angle ϕ_i. The beamforming pattern of this circular smart antenna array is expressed as below [82]

$$G(\theta) = \sum_{i=1}^{N_{ant}} w_i \exp[j\frac{2\pi}{\lambda} R\cos(\theta - \phi_i)], \tag{3.2}$$

where λ is the signal wavelength, θ represents the direction and $\mathbf{w} = [w_1, w_2, \cdots w_{N_{ant}}]^H$ is the complex weight vector that can be tuned to change the radiation pattern.

We choose circular antenna array as an example to illustrate the design of our scheme because it can produce flexible asymmetric beamforming patterns and easily deflect a beam through 2π [30]. However, it is important to note that our scheme also works with antennas with other geometric

forms, such like planar arrays. Although their beamforming functions differ from equation (5.1), since their radiation patterns are also determined by the complex weight vectors, they can still work with our scheme by simply replacing equation (5.1) with their corresponding beamforming functions.

3.4.2 Prediction of Effective Coverage Area

In order to minimize the unnecessary coverage area of the transmitted signal, we use log-distance path loss model to predict the mean RSSs at given distances and calculate the predicted effective coverage area. Although the practical wireless communication channels can be more complicated and the real coverage area is extremely hard to predict, we believe that the log-distance path loss model is effective in providing predictions and guidance in an average sense and is the best option when accurate channel condition information cannot be obtained.

Effective Coverage Area of Single Pattern Beamforming

According to the log-distance path loss model, the mean path loss at distance d is given by

$$\overline{PL}(d)(\text{dB}) = 10\alpha \log_{10} d + PL_0(\text{dB}), \tag{3.3}$$

where PL_0 is the path loss at the reference distance $d_0 = 1$ m, α is the path loss exponent and d is the distance from the transmitter to the interested location. In order to calculate the signal coverage area, we let r be the distance from the transmitter to the location where the signal strength is the radio sensitivity threshold. Hence we have

$$\overline{PL}(r)(\text{dB}) = P_0(\text{dBm}) - R_{th}(\text{dBm}). \tag{3.4}$$

Here P_0 is the required transmit power to keep good connection with the receiver if omnidirectional antenna is used. R_{th} denotes the radio sensitivity threshold. By combining (3.3) and (3.4), we get

$$10\alpha \log_{10} r = P_0(\text{dBm}) - PL_0(\text{dB}) - R_{th}(\text{dBm}), \tag{3.5}$$

$$r = \left(\frac{P_0}{R_{th} P L_0}\right)^{\frac{1}{\alpha}}. \tag{3.6}$$

For smart antenna, the radiation power at direction θ is also determined by the directional gain $|G(\theta)|^2$ in addition to P_0. So we rewrite equation (3.6) as

$$r(\theta) = \left(\frac{P_0 |G(\theta)|^2}{R_{th} P L_0}\right)^{\frac{1}{\alpha}}. \tag{3.7}$$

According to the area integral formula in polar coordinates, the predicted effective coverage area A is calculated by

$$\begin{aligned} A &= \tfrac{1}{2} \int_0^{2\pi} r^2(\theta)\, \mathrm{d}\theta \\ &= \tfrac{1}{2} \int_0^{2\pi} \left(\tfrac{P_0 |G(\theta)|^2}{R_{th} P L_0}\right)^{\frac{2}{\alpha}} \mathrm{d}\theta \\ &= \tfrac{1}{2} \left(\tfrac{P_0}{R_{th} P L_0}\right)^{\frac{2}{\alpha}} \int_0^{2\pi} |G(\theta)|^{\frac{4}{\alpha}}\, \mathrm{d}\theta. \end{aligned} \tag{3.8}$$

If we uniformly divide the space $[0, 2\pi)$ into M small sectors, we are able to transform equation (3.8) into discret form.

$$A \approx \frac{\pi}{M} \left(\frac{P_0}{R_{th} P L_0}\right)^{\frac{2}{\alpha}} \sum_{m=0}^{M-1} |G(\theta_m)|^{\frac{4}{\alpha}},\ \theta_m = \frac{2\pi m}{M}. \tag{3.9}$$

Effective Coverage Area Under Double-beam Switching

Because a pair of radiation patterns are employed in the proposed anti-eavesdropping scheme, we use a superscript to differentiate the patterns. Thus, according to (5.1), the n^{th} beamforming pattern is determined by the complex weight vector $\mathbf{w}^{(n)}$ and the beamforming pattern is given by

$$\begin{aligned} &G^{(n)}(\theta) = \sum_{i=1}^{N_{ant}} w_i^{(n)} \exp[j \tfrac{2\pi}{\lambda} R \cos(\theta - \phi_i)], \\ &n = 1, 2. \end{aligned} \tag{3.10}$$

Therefor, the effective coverage radius of the n^{th} beamforming patterns is

$$r^{(n)}(\theta) = \left(\frac{P_0 |G^{(n)}(\theta)|^2}{R_{th} P L_0}\right)^{\frac{1}{\alpha}},\ n = 1, 2. \tag{3.11}$$

As shown in Section III, a wireless communication link is unusable when its RSS under at least one of the two beamforming patterns is lower than the radio sensitivity level. Thereby, we define the effective coverage radius under double-beam switching as

$$r_{sw}(\theta) = min\{r^{(1)}(\theta), r^{(2)}(\theta)\}. \tag{3.12}$$

Thus, the effective coverage area of double-beam switching transmission is described by

$$A_{sw} = \frac{1}{2}\int_0^{2\pi} r_{sw}^2(\theta)\,\mathrm{d}\theta. \tag{3.13}$$

By dividing the space $[0, 2\pi)$ into M small sectors, A_{sw} can be approximately expressed as:

$$\begin{aligned} &A_{sw} \approx \tfrac{\pi}{M}\left(\tfrac{P_0}{R_{th}PL_0}\right)^{\frac{2}{\alpha}} \sum_{m=0}^{M-1} |G_{sw}(\theta_m)|^{\frac{4}{\alpha}}, \\ &|G_{sw}(\theta_m)| = min\{|G^{(1)}(\theta_m)|, |G^{(2)}(\theta_m)|\}, \\ &\theta_m = \tfrac{2\pi m}{M}. \end{aligned} \tag{3.14}$$

3.4.3 Double-pattern Optimization

Since the signal towards the intended receiver should have a high quality, we assume that the main beam of the two beamforming patterns should overlap for at least a certain width in the direction to the intended receiver. This beamwidth of the overlapped main beams is defined as BW. The effective coverage outside BW is unnecessary coverage since it has little contribution to quality of the intended communications, while it provides space for hidden eavesdroppers.

Assuming the receiver's direction is $\theta = 0°$, the desired main beam region is $[-\frac{BW}{2}, \frac{BW}{2}]$ and directions outside this region are unwanted transmit directions which cause unnecessary coverage. In order to simplify the formulas in discrete form, we define $\Delta = \frac{2\pi}{M}$, which represents the size of every discrete sector. Letting

$$l = \lfloor \frac{BW}{2\Delta} \rfloor, \tag{3.15}$$

the unnecessary coverage area for single beamforming pattern can be derived from (3.9) as:

$$U \approx \frac{\pi}{M}\left(\frac{P_0}{R_{th}PL_0}\right)^{\frac{2}{\alpha}} \sum_{m=l}^{M-1-l} |G(\theta_m)|^{\frac{4}{\alpha}},\ \theta_m = m\Delta. \tag{3.16}$$

For the artificial fading scheme, according to (3.14), the unnecessary coverage area of double-beam switching transmission can be expressed as:

$$\begin{aligned} &U_{sw} \approx \tfrac{\pi}{M}\left(\tfrac{P_0}{R_{th}PL_0}\right)^{\frac{2}{\alpha}} \sum_{m=l}^{M-1-l} |G_{sw}(\theta_m)|^{\frac{4}{\alpha}}, \\ &|G_{sw}(\theta_m)| = min\{|G^{(1)}(\theta_m)|, |G^{(2)}(\theta_m)|\}, \\ &\theta_m = m\Delta. \end{aligned} \tag{3.17}$$

We model the problem of optimal artificial fading as a problem of minimizing the predicted unnecessary coverage area expressed in (3.17) under double-beam switching transmission. This problem is a nonlinear programming problem with the complex antenna array weight vectors $\mathbf{w}^{(1)}$ and $\mathbf{w}^{(2)}$ as optimization variables. Without loss of generality, we normalize the antenna array directional gain with respect to $G^{(n)}(0) = 1$. Since $\frac{\pi}{M}\left(\frac{P_0}{R_{th}PL_0}\right)^{\frac{2}{\alpha}}$ is a constant, we can remove it from the objective function without affecting the optimal solution, and get the problem formulation below:

$$\begin{aligned} \min_{\mathbf{w^{(1)}},\mathbf{w^{(2)}}} \quad & \sum_{m=l}^{M-1-l} |G_{sw}(\theta_m)|^{\frac{4}{\alpha}} \\ \text{s. t.} \quad & |G_{sw}(\theta_m)| = min\{|G^{(1)}(\theta_m)|, |G^{(2)}(\theta_m)|\} \\ & G^{(n)}(0) = 1,\ n = 1, 2 \\ & l = \lfloor \tfrac{BW}{2\Delta} \rfloor. \end{aligned} \tag{3.18}$$

The problem in (3.18) is non-convex and it is generally impossible to directly solve it and get a rigorous optimal solution. So we need to seek approximation algorithms based on the practical properties of smart antenna beamforming. As shown in formulation (3.18), in a specific direction, only the smaller directional gain between the two beamforming patterns contributes to the objective function, and hence, needs to be minimized. Therefore, a good solution set to (3.18) is to divide the whole range of undesired transmit directions into two sets. Each beamforming pattern is tuned only to minimize the coverage area within one set while having freedom to transmit larger power on the other set. In other words, one pattern's minimized direction set is always overlapped with the other pattern's non-minimized direction set, except the direction towards the receiver, where main beams of the two pattern are overlapped. The pattern pair in Figure 3.2 also shows this idea. To determine the allocation of direction sets to be minimized for each pattern for the above type

of solutions, note that, from the aspect of antenna pattern synthesis, for an antenna array with N elements, at most $N-1$ nulls can be formed according to the the antenna array's degree of freedom [51]. Also, it has been shown that by combining multiple nulls (placing them closely), a wider or deeper total null space can be formed [51][77]. Hence, this indicates that we should combine multiple nulls of a single synthesized pattern to form a wide null which covers a relatively large phase range. Thus, we divide the range of undesired transmit directions into two continuous sectors with equivalent size. We let each beamforming pattern form a wide null in one sector by tuning the complex weight vectors. Thus, along every undesired transmit direction, the transmitted signal is nulled out at least in every other pattern switching period, which is exactly how artificial fading works. Then, the problem is reformulated as the following convex optimization problem which can be directly solved using existing nonlinear optimization software such like cvx [29].

$$\begin{aligned} \min_{\mathbf{w^{(1)},w^{(2)}}} \quad & \sum_{m=l}^{\lfloor \frac{M-1}{2} \rfloor} |G^{(1)}(\theta_m)|^{\frac{4}{\alpha}} + \sum_{m=\lceil \frac{M-1}{2} \rceil}^{M-1-l} |G^{(2)}(\theta_m)|^{\frac{4}{\alpha}} \\ \text{s. t.} \quad & G^{(n)}(0) = 1,\ n = 1, 2 \\ & \theta_m = m\Delta \end{aligned} \tag{3.19}$$

3.4.4 Limited Total Transmit Power

Taking into account the potential transmit power restriction to the artificial fading scheme, the total transmit power P_{sw} can be expressed as:

$$P_{sw} = \frac{P_0}{2M} \sum_{m=0}^{M-1} |G^{(1)}(\theta_m)|^2 + |G^{(2)}(\theta_m)|^2. \tag{3.20}$$

Suppose the transmit power limit is P_{th}. By combining this constraint into the double-beam optimization problem in (3.19), we get the form of our artificial fading optimization problem under

limited total transmit power:

$$\begin{aligned} \min_{\mathbf{w^{(1)}},\mathbf{w^{(2)}}} \quad & \sum_{m=l}^{\lfloor \frac{M-1}{2} \rfloor} |G^{(1)}(\theta_m)|^{\frac{4}{\alpha}} + \sum_{m=\lfloor \frac{M-1}{2} \rfloor}^{M-1-l} |G^{(2)}(\theta_m)|^{\frac{4}{\alpha}} \\ \text{s. t.} \quad & G^{(n)}(0) = 1,\ n = 1, 2 \\ & \sum_{m=0}^{M-1} |G^{(1)}(\theta_m)|^2 + |G^{(2)}(\theta_m)|^2 \leq \frac{2MP_{th}}{P_0} \\ & \theta_m = m\Delta. \end{aligned} \tag{3.21}$$

3.5 Simulation Evaluation

To evaluate the performance of the proposed artificial fading scheme in reducing the unnecessary coverage area, we optimize the double-pattern synthesis by solving problems (3.19) and (3.21), and simulate the signal propagation under artificial fading in Matlab environment. We first show an example of the optimized pattern pair and compare the performance with single pattern beamforming using log-distance path loss model. Then we employ Monte Carlo simulation to compare the reduced unnecessary coverage areas using single pattern beamforming and the proposed artificial fading scheme with the presence of shadow fading and multipath Rayleigh fading.

The setting of the parameters is as below. The path loss exponent is $\alpha = 3.5$. Radio sensitivity is $R_{th}(\text{dBm}) = -70$ dBm. The required transmit power, when omni directional antenna is used, is $P_0(\text{dBm}) = 10$ dBm and the path loss at $d_0 = 1m$ is $PL_0(\text{dB})$ =30 dB.

3.5.1 Example of Optimized Beamforming Pattern Pair

Figure 3.4(a) illustrates a simple example of the optimized beamforming pattern pair for maximizing the effect of artificial fading. In this case, we assume that the receiver is in the direction of $\theta = 0^\circ$. The smart antenna array consists of $N_{ant} = 6$ omni antenna elements and the width of the required main beam towards the receiver is $BW = 30^\circ$. As shown in Figure 3.4(a), pattern 1 and pattern 2 both have a wide main lobe, which contains the direction of the receiver, and a wide null that spans a separate direction sector. Thus, in the undesired directions, at least one

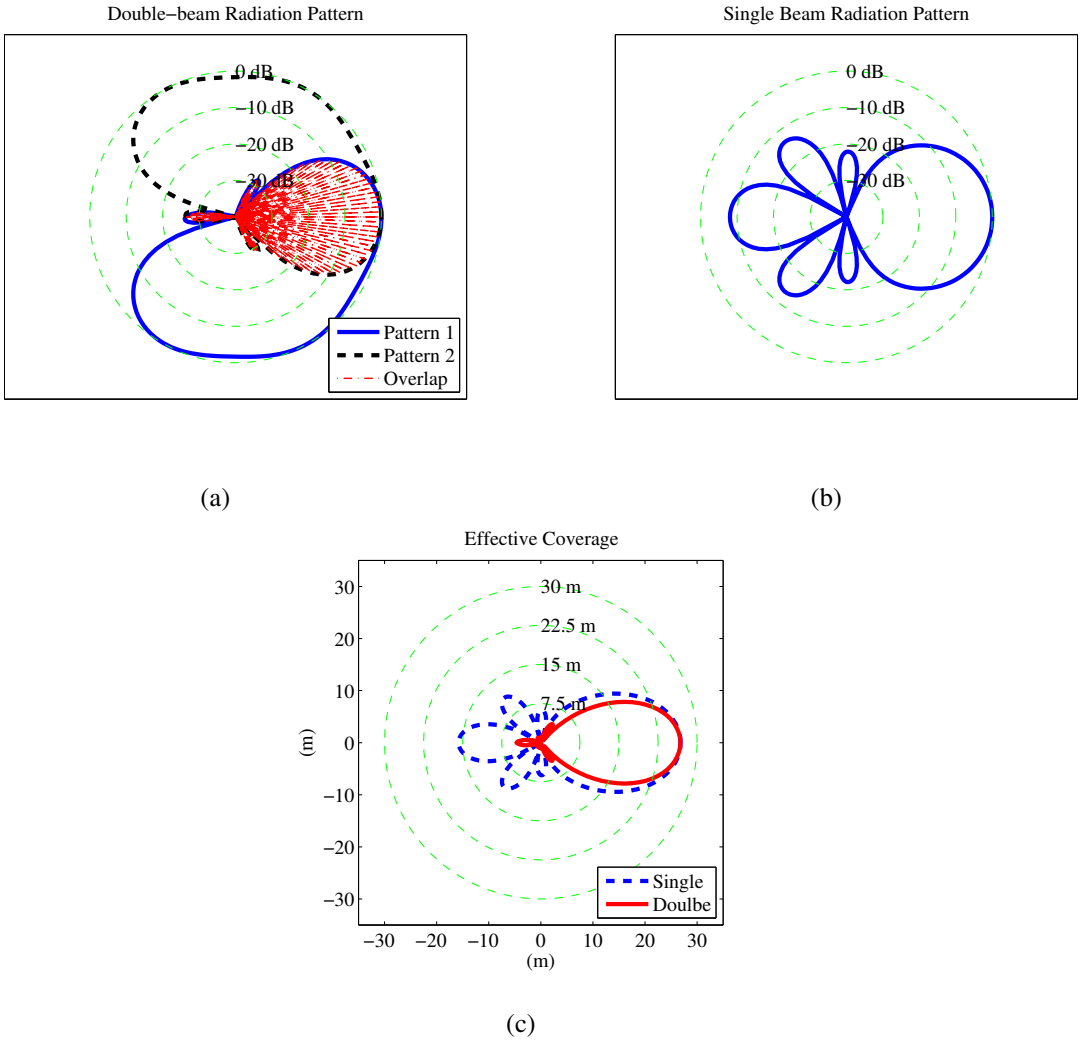


Figure 3.4: Radiation patterns and predicted effective coverage of single beamforming pattern and double-beam switching.

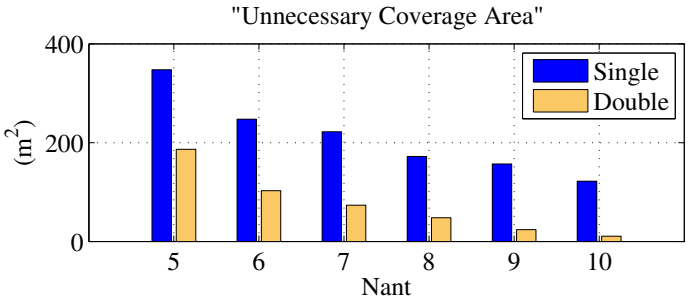
pattern can null out the transmitted signal during its operation period. While in the direction to the intended receiver, the antenna has a constant high gain. As a comparison, the optimal radiation pattern using single-pattern beamforming is shown in Figure 3.4(b), which is also synthesized by the smart antenna array with $N_{ant} = 6$ elements. Although this pattern has already been optimized to minimize the unnecessary coverage area, it still has considerable side lobes which result in unnecessary coverage. Differently, the overlapped pattern in Figure 3.4(a) has much smaller side lobes, due to the cooperation between the two patterns. As a result, the predicted effective coverage area of double-beam switching has a much smaller unnecessary portion compared with single beamforming pattern as shown in Figure 3.4(c).

3.5.2 Analysis in Ideal Channel

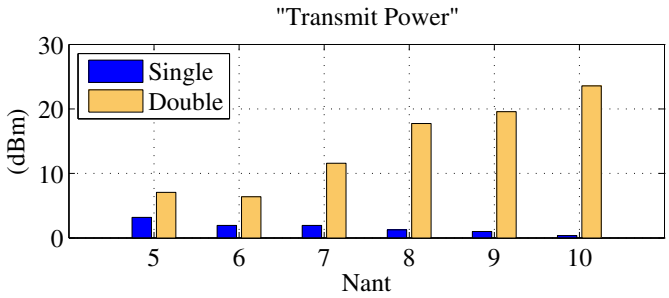
In this part, we analyze the performance of the proposed artificial fading scheme and single pattern beamforming scheme using log-distance path loss model by changing the number of antenna elements (N_{ant}) and the total transmit power constraint (P_{th}).

Figure 3.5(a) illustrates the minimized unnecessary coverage area of single-pattern beamforming and double-beam switching. The double-beam patterns are generated from the formulation in (3.19). Transmit power constraint is not considered yet in order to find the best capability of artificial fading scheme in trading power consumption for enhancing anti-eavesdropping. It is indicated in the figure that as N_{ant} increases, the minimum unnecessary coverage area decreases under both schemes. This is because the smart antenna array with more antenna elements has more flexibility in tuning the radiation pattern. Comparatively, for a given number of antenna elements, double-beam switching transmission can reduce more than half the unnecessary coverage area of single pattern beamforming.

We also compare the power consumption under the two schemes in Figure 3.5(b). We discover that for single pattern beamforming, as N_{ant} increases, the total transmit power for achieving the minimum unnecessary coverage is decreasing. The reason is that for single pattern beamform-



(a)



(b)

Figure 3.5: Performance comparison without transmit power limit.

ing, the main strategy for anti-eavesdropping is reducing the transmit power in undesired directions. However, the proposed artificial fading scheme, realized by double-beam switching, reduces the unnecessary coverage area by corrupting wireless signals in undesired directions. Thus it will trade power consumption for further reduction of unnecessary coverage area whenever it is possible. Therefore, we can observe in Figure 3.5(b) that the total transmit power consumed by double-beam switching is higher than single pattern beamforming. This observation implies that the performance of the proposed artificial fading scheme is related to the allowed total transmit power.

To analyze how the performance of the artificial fading scheme is related to the total transmit power limit, we set $N_{ant} = 6$ and $BW = 30°$. The constraint on max total transmit power is added to the optimization problem defined in (3.21). The result is shown in Figure 3.6. The horizontal coordinate represents the upper bound constraint of the transmit power for the artificial fading scheme and the vertical coordinate shows the minimum unnecessary coverage area using optimized

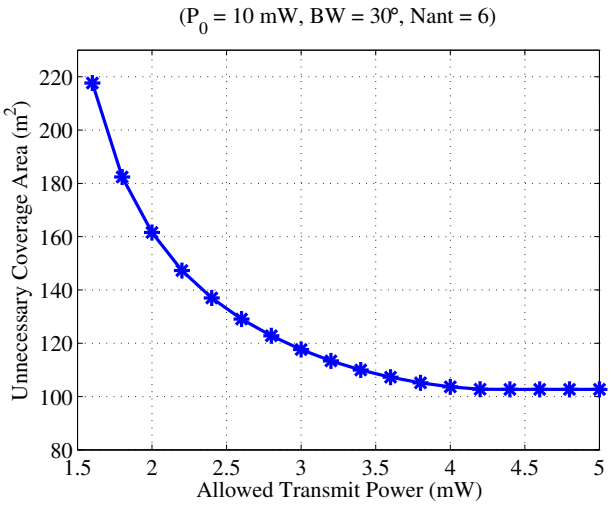
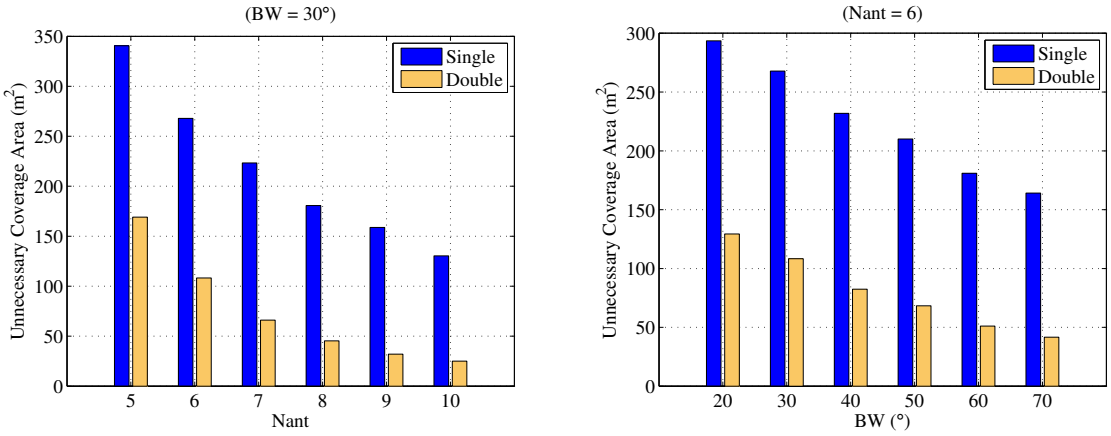


Figure 3.6: Minimum unnecessary coverage area v.s. transmit power limit.



(a) (b)

Figure 3.7: Performance comparison under transmit power limit defined by the required transmit power when omni-directional antenna is used (10 mW).

beamforming pattern pair. Generally, the minimum unnecessary coverage area decreases when allowed transmit power increases. However, when the transmit power limit reaches a certain value, (4.2 mW in this example), the minimum unnecessary coverage area cannot be further reduced, because the artificial fading scheme already reaches its optimum under this antenna array geometry.

In order to compare the performance of the single pattern beamforming scheme and the proposed artificial fading scheme under a practical transmit power constraint, we assume that the transmit power limit in problem (3.21) is P_{th} =10mW, which equals the required transmit power when omni directional antenna is used, and run simulations with different value of N_{ant} and BW. The minimized unnecessary coverage area under different parameter settings is illustrated in Figure 3.7(a) and Figure 3.7(b). We can see that the artificial fading scheme significantly outperforms the single pattern beamforming scheme when its power consumption is no more than the transmit power consumed by an omni directional antenna.

3.5.3 Evaluation in Shadow Fading Channel

In this part, we evaluate the performance of the proposed artificial fading scheme under shadow fading. We assume that the standard deviation of the log normal shadow fading is $\sigma = 5$ (dB). For each parameter setting, 1000 beam switching periods are simulated.

First, with the same parameter settings as the case in Section 3.5.1, Figure 3.8(a) and Figure 3.8(b) show the outage probabilities (P_{out}) of single pattern beamforming and double-beam switching under shadow fading in a $80 * 80$ m^2 area, respectively. Each color represents a level of P_{out} as shown on the right side of the figure. For both schemes, we set $N_{ant} = 6$ and $BW = 30°$. Following the example of IEEE 802.11 discussed in Section 3.3.2, because signal outage with probability larger than 0.4 is beyond the capability of the error correction code, the effective coverage region should be inside the area with $P_{out} \leq 0.4$. Since we assume that the intended receiver is in the $0°$ direction, the covered regions of both single- and double-beamforming schemes according to $P_{out} \leq 0.4$ point to the right side. We find that for $P_{out} \leq 0.4$, the covered region in Figure

Table 3.1: Unnecessary coverage area of single pattern beamforming under **shadow fading**. (m^2)

P_{out}	N_{ant} = 6	N_{ant} = 8	N_{ant} = 10
0.1	336	242	181
0.2	443	315	244
0.3	555	394	303
0.4	664	477	372

3.8(a) is almost without side lobes, and is apparently smaller than the covered region in Figure 3.8(b). This is consistent with the result in Figure 3.4(c) which is obtained under idea channel condition. The only difference is that due to the shadow fading and the outage tolerance capability of the error correction code, the real effective coverage area might differ from the value in ideal communication environments. However, the shape of the effective coverage area is still roughly the same with the predicted effective coverage in ideal channel. Also, as shown in Figure 3.8(c), the curve segments from $P_{out} = 0$ to $P_{out} = 0.4$ implie that the proposed artificial fading scheme creates smaller unnecessary coverage area than single pattern beamforming scheme. Although for $P_{out} > 0.5$, double-beam switching transmission has larger covered area, within the regions where signal outage probability is larger than 0.5, the eavesdropper in those regions cannot successfully decode the signal and there is no information leakage concern.

Next, we change the value of N_{ant} and simulate the performance of the proposed artificial fading scheme with different total transmit power limits (P_{th}). The unnecessary coverage area using single pattern beamforming is listed in Table 3.1 as reference. The performance of the artificial fading scheme is provided in Table 3.2. By comparing the two tables, we can see that the proposed artificial fading scheme can achieve greater reduction of unnecessary coverage area against the single pattern beamforming scheme in shadow fading environment and its performance tends to improve when higer transmit power consumption is allowed.

Table 3.2: Unnecessary coverage area of double-beam switching under **shadow fading**. (m^2)

P_{th} (mW)	P_{out}	N_{ant} = 6	N_{ant} = 8	N_{ant} = 10
2	0.1	308	193	136
	0.2	420	279	197
	0.3	531	354	264
	0.4	653	466	356
6	0.1	200	150	108
	0.2	284	219	151
	0.3	374	298	213
	0.4	501	409	295
10	0.1	229	143	95
	0.2	321	217	150
	0.3	426	288	204
	0.4	545	415	287

Table 3.3: Unnecessary coverage area of single pattern beamforming under **multipath Rayleigh fading**. (m^2)

P_{out}	N_{ant} = 6	N_{ant} = 8	N_{ant} = 10
0.1	152	116	90
0.2	250	184	149
0.3	343	256	199
0.4	448	334	262

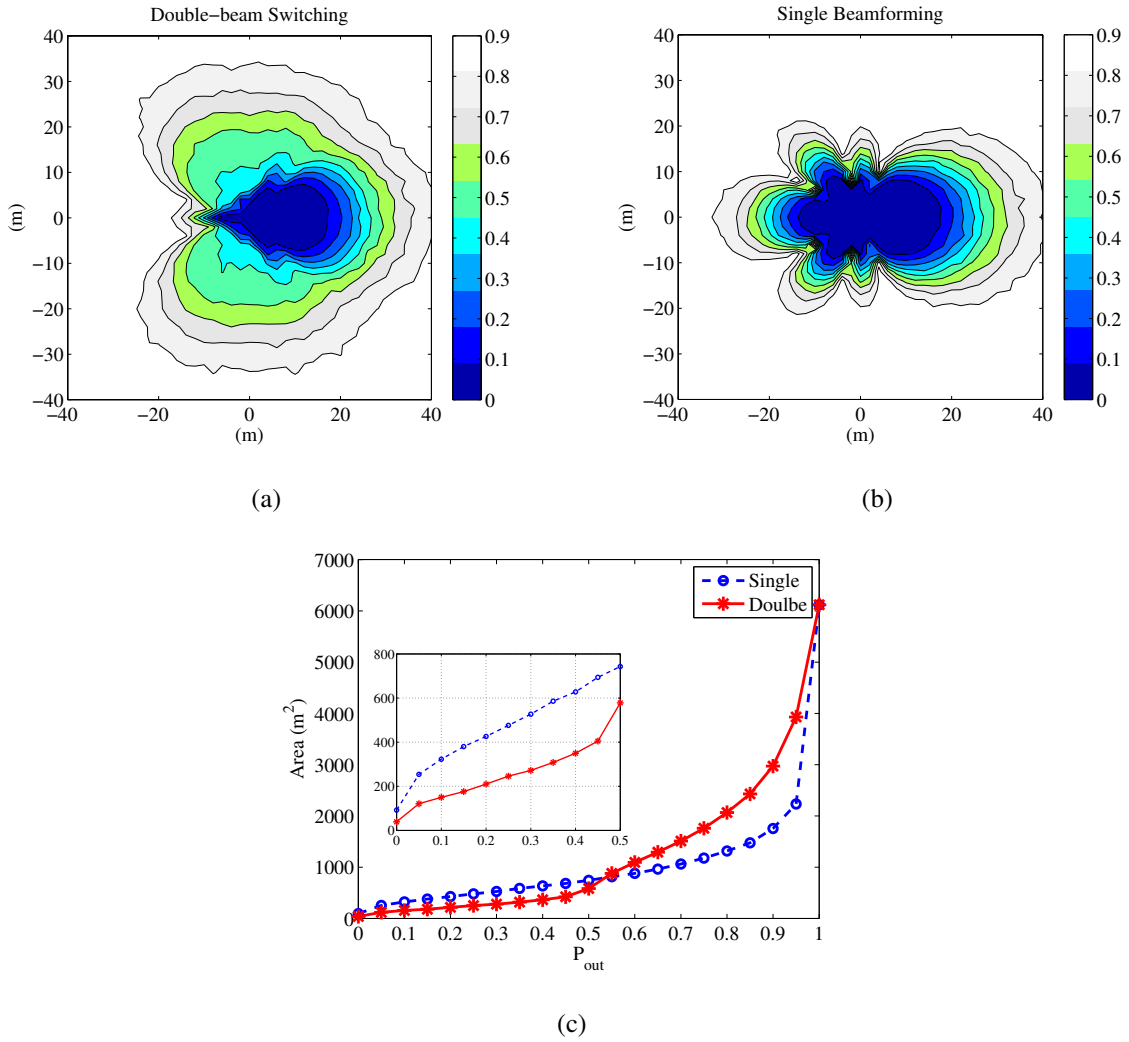


Figure 3.8: Outage Probability under single pattern beamforming and double-beam switching in shadow fading channel.

3.5.4 Evaluation in Multipath Rayleigh Fading Channel

This part shows the simulation results under multipath Rayleigh fading. For the same values of N_{ant} and BW, the spacial distribution of outage probability under Rayleigh fading has the same shape and trend with the results under shadow fading, which are shown in Figure 3.8, even though the exact size of each region corresponding to a given outage probability might be slightly different. Thus, we omit the figure of spacial outage probability distribution for Rayleigh fading channel due to space limitations. Table 3.3 and Table 3.4 list the unnecessary coverage under multipath Rayleigh fading for the single pattern beamforming scheme and the artificial fading scheme, respectively. Again, P_{th} is the upper limit of total transmit power consumption applied to the double-beam optimization problem in (3.21). Consistently with the conclusion in Section 3.5.3, results in the two tables show that the proposed artificial fading scheme can achieve greater reduction of unnecessary coverage area against the single pattern beamforming scheme in Rayleigh fading environment. Meanwhile, the tradeoff between the reduction on the unnecessary coverage and the total power consumption also exists in Rayleigh fading environment.

3.6 Discussion

3.6.1 Node Mobility

In this work, we assume that the direction of the intended receiver is known to the transmitter that is using artificial fading scheme. However, this does not necessarily mean that both the transmitter and the intended receiver must be static. Remember that in the artificial fading scheme, the transmitter is equipped with a smart antenna array. The smart antenna array enables the transmitter to track the Direction of Arrival (DOA) of the signal from the reverse link, and hence, get the direction of the mobile receiver. Direction finding using antenna array is a well studied area and lots of algorithms are available [68, 65, 28, 41]. Since DOA estimation is out of the scope of this work, we simply assume that the transmitter with a smart antenna array can use state of the art DOA

Table 3.4: Unnecessary coverage area of double-beam switching under **multipath Rayleigh fading**. (m^2)

P_{th}(mW)	P_{out}	N_{ant} = 6	N_{ant} = 8	N_{ant} = 10
2	0.1	128	102	70
	0.2	215	168	128
	0.3	303	247	182
	0.4	414	334	256
6	0.1	105	81	58
	0.2	178	145	106
	0.3	259	214	163
	0.4	374	311	236
10	0.1	104	69	39
	0.2	179	127	67
	0.3	262	196	104
	0.4	373	295	163

estimation algorithms to find the direction of a mobile receiver.

3.6.2 Communication Quality for the Intended Receiver

While the target of the proposed artificial fading scheme is communication privacy, one important prerequisite is that the communication quality for the intended receiver should be intact. Although the two patterns for beam-switching are designed to keep the directional gain towards the intended receiver constant, if large alignment error exists, it is possible that the intended receiver will experience periodical phase shift of the received signal. To mitigate this potential issue, one possible way is interleaving. We can shuffle the original data across multiple packets and switch the beam pattern between two packets. In this way, the synchronization and stability of the communication signal for the intended receiver will not be affected by the beam-switching.

Another issue worth mentioning is that in the proposed scheme, the transmitter beamforming is optimized for privacy protection, but it may increase the severity of frequency selective fading. Hence, the intended receiver might not get as good signal quality as when the beamforming patterns are optimized for signal quality enhancement. For instance, the proposed beam-switching scheme may not be helpful in mitigating multipath effect. To mitigate multipath effect and improve the communication quality, a possible solution is to use antenna diversity and/or more powerful equalization techniques at the intended receiver. However, this will increase the hardware cost of the intended receiver for the sake of improved communication quality.

3.6.3 Collaborative Eavesdropping Attack

It is possible for the eavesdroppers in multiple locations to collaboratively exchange and merge their received signal fragments. However, precise synchronization among the eavesdroppers is required to correctly merge the signal fragments, which dramatically increases the cost for eavesdropping. Even collaboration is possible, a simple addition of an extra antenna array to our artificial fading scheme can defeat such collaboration effort. The transmitter can use the additional antenna

array to transmit noise signal using a carefully crafted pattern, which fills the null directions of one beamforming pattern with noise and blurs the timing of beam pattern switching. In this way, it is difficult for eavesdroppers to differentiate and merge their received useful information signals.

3.7 Chapter Summary

The broadcast nature of wireless communication networks makes the communicated confidential information at the risk of being eavesdropped. We propose a physical layer anti-eavesdropping scheme using the novel concept of artificial fading, which is realized by double-beam switching of smart antenna array. Our scheme optimizes the switched beamforming pattern pair, such that the wireless communication links in undesired directions are unusable because of the intentionally produced artificial fading, while the intended transmit direction gets persistent good signal quality. In this way, the unnecessary coverage area is significantly reduced and the secrecy measure is improved. Simulation results show that our artificial fading scheme outperforms single pattern beamforming scheme in reducing unnecessary coverage and provides a controllable tradeoff between the total transmit power consumption and the reduction of unnecessary coverage area.

Chapter 4

Location Privacy Protection Using Antenna Pattern Synthesis

This chapter studies the problem of location privacy protection in WLAN environment, where received signal strength (RSS) at access points (AP) can potentially be obtained by adversaries to obtain the location of a legitimate mobile station. We propose a two-step location privacy protection scheme using a linear smart antenna array on the mobile station. In the first step, the mobile station observes the arrangement of surrounding APs by moving around and estimating the path losses from itself to the APs. Based on the path loss information, in the second step, the mobile station optimizes the radiation pattern of its smart antenna so that its location privacy is protected while its communication quality is not affected. Two strategies are used in the radiation pattern optimization. The first strategy is to limit the number of APs in range of the mobile station to a safe level so that there are not enough measurements from the APs to make an estimation of the mobile station's location. If the first strategy is not possible, the mobile station falls to the second strategy, where its radiation pattern introduces maximum bias to any location estimation attempt so that the mobile station's true location is not revealed. Simulation results show that compared with traditional transmit power control (TPC) scheme, the first strategy significantly increases the probability of inadequate measurements for location computation. Simulation also demonstrates

that the second strategy can significantly degenerate the precision of the positioning system. In many cases, the degenerated location precision is as low as the coverage range of the AP that the mobile station is associated with for communications. This essentially means that the second strategy can invalidate the use of RSS measurement for precise localization.

4.1 Introduction

While wireless localization techniques enable the mobile users to enjoy location based services in pervasively deployed WiFi networks, they also threaten the location privacy of these mobile users. While surfing online with a mobile device, a network user can be physically localized and tracked by malicious parties who get control over the localization system or get access to information that can be used to derive the location of the mobile devcie [67, 79].

The level of threat to location privacy depends on the positioning techniques, which can be grouped into three categories according to who is carrying out the location estimation process. In the first category, the mobile station executes self-localization based on the information provided by the network infrastructure [63]. There is less privacy issue in this scenario as long as the mobile station does not report its location to trustless parties. In the second category, the localization systems need the mobile station's cooperation (e.g. reporting transmit power or RSS readings to the positioning system) for location computation [25]. It is possible for the mobile station to choose not to cooperate with the localization system or provide fuzzy information to the localization system whenever it is unwilling to reveal its location. Hence, the location privacy is under the control of the mobile user. In the third category, called passive localization, a mobile station is localized by either the network provider or a third party that has access to the necessary information [5, 39]. This type of localization schemes analyze the mobile station's signal over the air and can localize the mobile station as long as it emits communication signals. Since they do not require cooperation of the mobile station, it is most challenging to defend the location privacy of a mobile user from these localization systems because emitting signal is inevitable during wireless communications.

Under such circumstances, the mobile station losses control of its location privacy and is in danger of getting its location information exposed to ill-disposed parties. Hence, location privacy of a mobile user is most threatened by passive localization schemes. Existing methods [36] that intent to protect user location privacy from this type of localization systems forces mobile stations to shutdown its communications for long period of time and hope the mobility of the mobile station during the silent period can make it difficult for the localization system to track the mobile station. However, the long interruptions to communications are highly undesirable and a mobile station may not want to constantly move in practice. Hence, we believe that none of the existing location privacy scheme is able to protect mobile users from the third type of localization schemes.

The aim of this work, hence, is to address this challenging open problem of protecting location information of a mobile user from passive localization systems. Specifically, we focus on defending user location privacy from received signal strength (RSS) based localization scheme. Although besides RSS, time of arrival (TOA) and angle of arrival (AOA) are also used by current physical layer localization algorithms, RSS-based localization is most often adopted because it requires no extra hardware support and provides acceptable accuracy in WLAN environment. Because of the popularity of RSS-based localization systems, we only focus on protecting location privacy against them in WLAN.

The main contribution of this work is that it solves the location privacy problem in physical layer through antenna pattern synthesis. To protect location information in physical layer, we use a linear smart antenna array to change the mobile station's radiation pattern from omnidirectional into an optimized radiation pattern. The radiation pattern reduces the number of valid RSS measurements that can be obtained by the localization system and breaks the trilateration principle among the RSS measurements. Without enough measurements, the localization system cannot uniquely localize the mobile station. Even if enough RSS measurements are gathered, the localization result will contain large bias caused by the irregular radiation pattern of the mobile station. At the same time, our radiation pattern synthesize scheme ensures that the mobile station's communications are intact and we do not require the mobile station to move. To our best knowledge, our work is the first application of pattern synthesis for the purpose of protecting location privacy of wireless

mobile users.

This chapter is structured as follows. In Section 4.2, we briefly summarize related works in the area of localization and location privacy. Section 4.3 provides the location privacy threat model, a brief overview of the proposed scheme and the antenna model used in this chapter. The detailed introduction of the proposed scheme is provided from Section 4.4 to Section 4.6. The simulation results are discussed in Section 4.7 and the last section concludes our work.

4.2 Related Work

In this section, we first briefly introduce typical RSS-based localization methods and then provide an overview of current works about location privacy protection.

4.2.1 RSS Localization Techniques

Current RSS localization techniques can be generally grouped into fingerprint based approaches [5, 4, 38] and propagation model based approaches [63, 42, 39]. Fingerprint localization usually consists of an off-line phase and an on-line phase. Before the positioning system can operate, the off-line phase is required to collect RSS measurements at known locations and a database is built up for pattern matching. During the on-line phase, the actual RSS measurements of the target mobile station is compared with the stored database to return a location estimation. Fingerprint of wireless signal highly depends on the specific environment and is not transportable to different places. Consequently, for every different interested area, the off-line phase must be conducted from the very beginning. Additionally, any change of the infrastructure distribution and the physical environment will necessitate an update of the localization system and the collection of new training data. The disadvantage of fingerprint localization is that it requires lots of human work and is time consuming.

In propagation based RSS localization schemes, large scale path loss is related to the distance

between the transmitter and the receiver. Obstacles and noise can also be taken into account in the model. Then given the path loss from the transmitter to the receiver, the distance between them can be estimated and the location of the transmitter can be computed.

4.2.2 Location Privacy Schemes

Four types of location privacy techniques have been proposed to protect location privacy at system level in location-based services (LBS) [22]. These techniques are named "policies", "modification of request", "dummy requests" and "provider change". Policy approaches restrict the precision and conditions under which the location-based service provider (LBSP) can obtain a certain station's location information. Modification of request approaches protect location information by either hiding the user's identifier to the LBSP, or reporting indefinite location information to the LBSP. Dummy requests are designed to confuse the location attacker by generating simulated user requests. Provider change refers to frequently changing the LBSP for a certain service. Recently Meyerowitz and Choudhury [53] developed a new type of camouflage system named "CacheCloak" as a trusted server. It submits intersecting predicted paths of multiple users to the LBSP. Thus the LBSP won't be able to track the path of any individual user. All these existing works discussed so far study how to keep location information unrevealed to LBSP, and some of them depend on a trustable third party server. Thus these methods are not suitable for protecting physical level location privacy in WLAN, where the signal transmitted by the mobile station can reveal its location information.

There are two pioneering works that attempt to protect location privacy from passive localization in physical layer. In [37] Jiang et al. use intelligent transmit power control (TPC) to reduce the APs in range in order to reduce the chance of being localized. While the scheme is simple to implement, its effectiveness is limited when the density of APs in range is high. In [88], a framework of physical layer location privacy scheme with beamforming in AOA localization systems is proposed, where the aim is to reduce the number of possible AOA measurements to thaw any positioning attempt. The authors assume that "signal-to-noise-ratios for successful direction-finding are more

stringent than those required for mere communications". They claim that within a distance range the mobile station is able to communicate with the AP, while the AP cannot estimate the AOA of the mobile station's signal. The problem with this work is that its assumption that communication requires lower SNR than direction finding is questionable. However, we acknowledge that this work inspires us with the idea of using intelligent antenna radiation pattern to protect location information in physical layer.

4.3 Scheme Overview

4.3.1 Threat Model

In this work, we focus on protecting location privacy from potential RSS-based location attacks. Although localization algorithms based on AOA or TOA may have better accuracy, RSS-based localization is more likely to be used by an adversary because it requires no special hardware and, hence, is easy to implement in normal WLAN.

In our threat model, off-the-shelf APs in a legitimate WLAN act as anchors and provide RSS measurements at different known locations. We assume that an adversary can remotely tap into the software systems of these APs and obtain the RSS information. The attacker feeds the RSS information to RSS localization algorithm to localize and track a mobile user.

We do not consider the case that the adversary plants his/her own measurement anchors. It is very expensive, risky and, hence, unlikely for the adversary to physically planting a large number of his/her own private APs to track a mobile user. Directly hacking into the existing WLAN infrastructures is a better and more likely choice for the adversary.

4.3.2 Overview of the Proposed Privacy Protection Scheme

With location privacy concern, the mobile user's goal is to make the localization system unable to correctly localize him/her while maintaining reliable access to the wireless network. Our scheme realizes this goal by equipping the mobile user with a smart antenna and tuning the radiation pattern of the antenna. This scheme is feasible since it has been experimentally proved that attenuation and amplification of the RSS measurements collected by some APs (anchors of the localization system) can significantly degenerate the performance of a RSS-based localization system [15, 7]. The signal attenuation and amplification can be carried out either at the transmitter or at the receiver. These facts make radiation pattern synthesis a good choice to protect location privacy in physical layer. By changing the antenna radiation pattern, a mobile station can reduce the number of APs that can monitor its signal and degenerate the precision of the adversary's localization system while keeping good communication quality with its associated AP. Meanwhile, since radiation pattern synthesis is performed at the transmitter end, it does not hurt the performance of the WLAN to other mobile users.

In our design, the first strategy for the mobile station is to tune the antenna pattern so that the number of APs that can detect the mobile station's signal is minimized. The objective of this strategy is to ensure that not enough RSS measurements can be obtained for a unique location estimation. However, completely preventing the number of RSS measurements to go beyond a safe level is not always possible when there is uncertainty in signal attenuation and the density of APs is high. When a mobile station finds out that it is unlikely to limit the number of APs that can hear itself to a safe level, the mobile station uses the second strategy, which tries to maximize the bias in the location estimation result. The larger the bias is, the less probable that the true location of the mobile station is learned by the adversary. These two strategies constitute our location privacy scheme.

Figure 4.1 illustrates an overview of the whole scheme. The first step of our scheme is silently observing the beacon signals of the surrounding APs and estimating the locations of the APs and the path losses from the mobile station to the APs. Next, based on the estimated AP locations, the

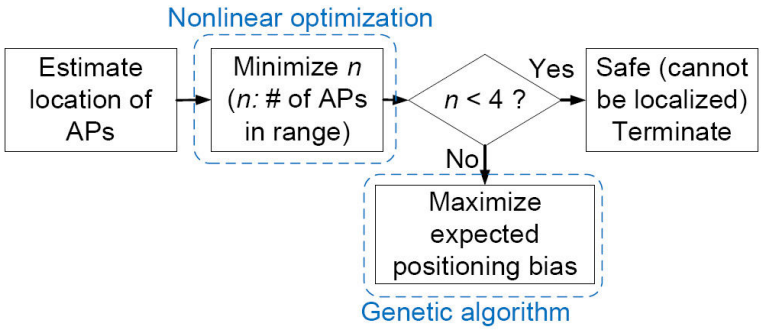


Figure 4.1: Scheme overview.

mobile station checks if it can use the first strategy to limit the number of APs that can hear its signal to be less than 4. This is because for 2-D localization based on RSS, 4 RSS measurements are needed when the transmit power of the mobile station is unknown to the location system. If this is not possible, the mobile station switch to the second strategy. By optimizing the radiation pattern based on the estimated AP locations, the mobile user introduces various attenuation and amplification in the RSS measurements to degenerate the localization performance.

4.3.3 Smart Antenna Model

In our location privacy strategies introduced in the last subsection, either limiting the number of RSS measurements or distorting the RSS measurements requires that the mobile station can control its radiation pattern and transmit power. Hence, how to control the mobile station's radiation pattern and transmit power is the first key problem that need to be addressed. In this chapter, we make use of radiation pattern synthesis over smart antenna to achieve our location privacy scheme. Pattern systhesis enables the mobile station to control the signal strength in different directions by tuning the complex weight vector in the beamforming function of an antenna.

In the remainder of this chapter, we assume that the mobile station is equipped with a linear smart antenna array with N_{ant} isotropic antenna elements uniformly spaced at distance l. This smart antenna model is also called uniform N_{ant}-element linear antenna array. The beamforming function

of this antenna is given by [44] as:

$$G(\theta) = \sum_{i=1}^{N_{ant}} w_i \exp(-j\frac{2\pi}{\lambda}(i-1)l\cos\theta), \tag{4.1}$$

where λ is the signal wavelength, θ represents the direction and $\mathbf{w} = [w_1, w_2, \cdots w_{N_{ant}}]^T$ is the complex weight vector which can be designed to change the radiation pattern.

It is important to note that we choose this N_{ant}-element linear antenna array as an example to illustrate the design of our scheme. Our scheme can also work with antennas with other geometric forms, such like circular arrays, planar arrays, and conformal arrays. Although their beamforming functions differ from equation (5.1), since their radiation patterns are also determined by the complex weight vectors, they can still work with our scheme by simply replacing equation (5.1) with their corresponding beamforming functions.

4.4 Passive Estimation of the Locations of Surrounding APs

In order to determine the optimal radiation pattern, a mobile station needs to know its neighboring APs' locations and the path losses between itself and the APs. However such information is hardly exposed to an ordinary mobile station. In our scheme, we leverage the fact that in WLANs, APs periodically send out beacon signals to announce their existence to mobile stations. Hence, by intelligently measuring APs' beacon signal, we can design a passive estimation method to get APs' location information. This passive scheme has three steps. In the first step, the mobile station passively measures RSS of the beacon signals from APs at several locations. In the second step, the mobile station estimates APs' locations based on the gathered information. In the third step, path losses to the APs are computed. Following is the detailed description of these three steps.

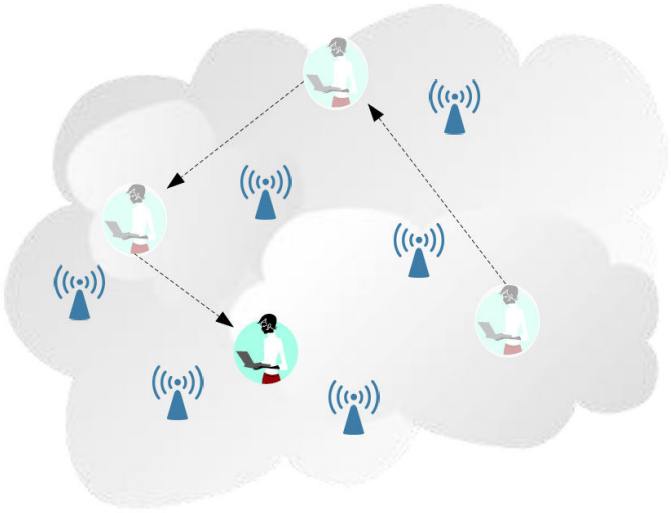


Figure 4.2: Moving around to observe surrounding APs.

4.4.1 Passive RSS Measurement of AP Beacon Signals

Assume that a mobile station has a desired location, called its desired communication spot, where it wants to conduct its communications in the WLAN. To protect its own privacy, before the mobile station starts its wireless communications, it first starts a process called listen-only wardriving [31] as shown by Figure 4.2. In this wardriving process, the mobile station selects 4 different locations, including its desired communication spot, in its neighboring area. Equipped with passive wardriving software, e.g. Kismet [40], and a GPS receiver, the mobile station measures the beacon signal strength of the surrounding APs at the selected locations and record the coordinates of these locations.

In the wardriving process, the APs are differentiated by their MAC addresses and indexed from 1 to K, where K is the total number of APs observed in the wardriving process. The observation at location i is recorded in a format as $\mathbf{O}_i = (o_{xi}, o_{yi}, r_{1i}, r_{2i}, \ldots, r_{Ki})$, where (o_{xi}, o_{yi}) is the coordinate of the observing location and $r_{1i}, r_{2i}, \ldots, r_{Ki}$ are the measured signal strength of the APs' beacon signal at (o_{xi}, o_{yi}).

Note that during the listen-only wardriving process, the mobile device does not communicate with

the WLAN and just listens to the broadcasted beacon signals. Therefore, the mobile station is transparent to the network and cannot be discovered by an adversary. The information collected in this step is used in step two for estimating the coordinates and the transmit power of the APs. The required effort is part of the cost for protecting location privacy. This cost is acceptable especially when the interested area is a place that the mobile user visits a lot.

4.4.2 Estimation of AP Locations

Denote (x_k, y_k) as the location coordinate of AP$_k$ and P_{0k} as the signal power level of AP$_k$ at a small reference distance d_0. With the RSS readings of the APs from the wardriving process, the mobile station is able to estimate (x_k, y_k) and P_{0k} for any AP$_k$ in its neighboring area as follows.

Assuming that the beacon signal of an AP$_k$ has the same strength in all horizontal directions, the beacon signal strength of AP$_k$, the observing locations and the coordinate of AP$_k$ are connected by the following equations according to the log-normal shadowing model [61]:

$$\begin{aligned} r_{k1} &= P_{0k}[(o_{x1} - x_k)^2 + (o_{y1} - y_k)^2]^{-\alpha/2} \\ r_{k2} &= P_{0k}[(o_{x2} - x_k)^2 + (o_{y2} - y_k)^2]^{-\alpha/2} \\ &\cdots \\ r_{kN} &= P_{0k}[(o_{xN} - x_k)^2 + (o_{yN} - y_k)^2]^{-\alpha/2}, \end{aligned} \tag{4.2}$$

where α is the path loss exponent and N is the number of observing locations. By transforming (4.2) we can get the equations below.

$$\begin{aligned} (o_{x1} - x_k)^2 + (o_{y1} - y_k)^2 &= \tfrac{P_{0k}}{r_{k1}}^{2/\alpha} \\ (o_{x2} - x_k)^2 + (o_{y2} - y_k)^2 &= \tfrac{P_{0k}}{r_{k2}}^{2/\alpha} \\ &\cdots \\ (o_{xN} - x_k)^2 + (o_{yN} - y_k)^2 &= \tfrac{P_{0k}}{r_{kN}}^{2/\alpha} \end{aligned} \tag{4.3}$$

Subtracting the last equation from all the other equations, we get an uncorrelated set of equations

as follow:

$$\begin{aligned}
&2x_k(o_{x1}-o_{xN})+2y_k(o_{y1}-o_{yN})+P_{0k}^{\frac{2}{\alpha}}(r_{k1}^{-\frac{2}{\alpha}}-r_{kN}^{-\frac{2}{\alpha}})=o_{x1}^2-o_{xN}^2+o_{y1}^2-o_{yN}^2\\
&2x_k(o_{x2}-o_{xN})+2y_k(o_{y2}-o_{yN})+P_{0k}^{\frac{2}{\alpha}}(r_{k2}^{-\frac{2}{\alpha}}-r_{kN}^{-\frac{2}{\alpha}})=o_{x2}^2-o_{xN}^2+o_{y2}^2-o_{yN}^2\\
&\dots\\
&2x_k(o_{x(N-1)}-o_{xN})+2y_k(o_{y(N-1)}-o_{yN})+P_{0k}^{\frac{2}{\alpha}}(r_{k(N-1)}^{-\frac{2}{\alpha}}-r_{kN}^{-\frac{2}{\alpha}})\\
&\qquad=o_{x(N-1)}^2-o_{xN}^2+o_{y(N-1)}^2-o_{yN}^2.
\end{aligned} \tag{4.4}$$

Rewriting (4.4) into matrix representations, we get

$$\begin{aligned}
&\mathbf{A}_k\beta_k=\mathbf{b}_k\\
&\mathbf{A}_k=\begin{bmatrix}
2(o_{x1}-o_{xN}) & 2\big(o_{y1}-o_{yN}\big) & r_{k1}^{-\frac{2}{\alpha}}-r_{kN}^{-\frac{2}{\alpha}}\\
2(o_{x2}-o_{xN}) & 2\big(o_{y2}-o_{yN}\big) & r_{k2}^{-\frac{2}{\alpha}}-r_{kN}^{-\frac{2}{\alpha}}\\
\cdots & \cdots & \cdots\\
2\big(o_{x(N-1)}-o_{xN}\big) & 2\big(o_{y(N-1)}-o_{yN}\big) & r_{k(N-1)}^{-\frac{2}{\alpha}}-r_{kN}^{-\frac{2}{\alpha}}
\end{bmatrix}\\
&\mathbf{b}_k=\begin{bmatrix}
o_{x1}^2-o_{xN}^2+o_{y1}^2-o_{yN}^2\\
o_{x2}^2-o_{xN}^2+o_{y2}^2-o_{yN}^2\\
\cdots\\
o_{x(N-1)}^2-o_{xN}^2+o_{y(N-1)}^2-o_{yN}^2
\end{bmatrix}\\
&\beta_k=[x_k,y_k,P_{0k}^{\frac{2}{\alpha}}]^T.
\end{aligned} \tag{4.5}$$

Hence, the least square estimation (LSE) of β_k is given by

$$\hat{\beta}_k=[\hat{x}_k,\hat{y}_k,\hat{P}_{0k}^{\frac{2}{\alpha}}]^T=(\mathbf{A}_k^T\mathbf{A})_k^{-1}\mathbf{A}_k^T\mathbf{b}_k. \tag{4.6}$$

It is important to note that $\hat{P}_{0k}$ is not the exact transmit power of AP$_k$. It is the estimated received signal strength at a small reference distance d_0 to AP$_k$.

4.4.3 Estimation of Path Loss to APs

Without loss of generality, suppose the mobile station's desired communication spot is at (o_{x1}, o_{y1}). Based on the estimated AP signal strength level $\hat{P}_{0k}$ from (4.6), the path loss from AP$_k$ to (o_{x1}, o_{y1}) is calculated by

$$\hat{PL}_k(\text{dBm})=\hat{P}_{0k}(\text{dBm})-r_{k1}(\text{dBm}), \tag{4.7}$$

where r_{k1} is the received beacon signal strength of AP$_k$ at (o_{x1}, o_{y1}).

We use equation (4.7) to approximate the path loss from AP$_k$ to the mobile user's location (o_{x1}, o_{y1}) and only far-field path loss is considered.

4.5 Strategy One: Minimizing the Number of RSS Measurements

With the estimated locations of the APs and the path losses between these APs and the mobile station's communication spot (o_{x1}, o_{y1}), we can tune the radiation pattern to limit the number of APs that can hear the mobile station's signal while maintaining the mobile station's communication quality. In the following, we introduce the tuning scheme in two steps. First, the radiation pattern tuning problem is formulated into an optimization problem. Then, this problem is solved to derive the optimal tuning strategy.

4.5.1 Tuning Problem Formulation

To formulate the radiation pattern tuning problem, note that in order to get access to the WLAN, a mobile station has to associate with one of the APs in the WLAN and we denote this AP as AP_c, where $c \in \{1, 2, ...K\}$. For the mobile station to have a stable connection with the WLAN, its signal strength at AP_c must be guaranteed to be larger than the minimum signal strength required by reliable communication, denoted as C_{th}. Hence,

$$P_0|G(\theta_c)|^2(\text{dBm}) \geq \hat{PL}_c(\text{dBm}) + C_{th}(\text{dBm}) + \delta_{\text{dB}}, \tag{4.8}$$

where δ_{dB} is the maximum error of the path loss estimation, θ_c is the direction of radiation from the mobile station to AP_c, and P_0 is the effective isotropic radiated power at reference distance d_0 from the mobile station. The function $G(\cdot)$ is the beamforming function defined in (5.1). The radiation angle θ_c towards AP_c can be computed from the estimated coordinate of APs obtained in (4.6).

While staying connected with AP_c, the mobile station also needs to prevent other APs from detecting its signal. For a particular AP_k, this means that the mobile station needs to guarantee the

following situation:

$$\begin{aligned} &\forall \phi_k \in [\theta_k - \delta_\theta, \theta_k + \delta_\theta], \\ &\quad P_0|G(\phi_k)|^2(\text{dBm}) < \hat{PL}_k(\text{dBm}) + R_{th}(\text{dBm}) - \delta_{\text{dB}}, \end{aligned} \tag{4.9}$$

where R_{th} is the AP receiver sensitivity and δ_θ is the maximum error in the estimation of radiation angle to APs. This error is caused by inaccuracy in AP location estimation.

With the above analysis, the objective of the mobile station, which is preventing too many APs to hear its signal while maintaining stable communications, can be formulated as checking if the following opimtization problem has feasible solutions.

$$\begin{aligned} &\underset{\mathbf{w}}{\text{minimize}}\ \textit{Total Transmit Power} \\ &\text{subject to} \\ &P_0|G(\theta_c)|^2(\text{dBm}) \geq \hat{PL}_c(\text{dBm}) + C_{th}(\text{dBm}) + \delta_{\text{dB}} \\ &y_i = \begin{cases} 1, \text{ if } Z_i \geq R_{th}(\text{dBm}) \\ 0, \text{ otherwise} \end{cases} \\ &Z_i = \max_{\phi_i \in [\theta_i - \delta_\theta, \theta_i + \delta_\theta]} P_0|G(\phi_i)|^2(\text{dBm}) - \hat{PL}_i(\text{dBm}) + \delta_{\text{dB}} \\ &\sum_{i \in \Omega, i \neq c} y_i \leq 2, \end{aligned} \tag{4.10}$$

where Ω is the set of all the APs that the mobile station can sense in its neighboring area. $\mathbf{w}$ is the complex weight vector of the smart antenna in (5.1) and can be tuned to change the radiation pattern. Note that we make the constraint that $\sum_{i \in \Omega, i \neq c} y_i \leq 2$ because we need to make sure that the number of APs that can make RSS measurements is smaller than the number required for successful localization. According to the well known trilateration method, if the transmit power of the mobile station is known to the localization system, and the distance between the mobile user and the APs can be estimated trough path loss model, three RSS measurements are required to uniquely localize the mobile station. However in our case, the localization system has no information about the transmit power of the mobile station. This actually adds one unknown variable to the trilateration localization problem. Consequently the required number of RSS measurements for getting a unique location estimation of the mobile station is 4.

4.5.2 Solving the Tuning Problem

The problem formulated in (4.10) is a mixed-integer nonlinear programming problem and is hard to solve in general. Fortunately, in our situation, it can be easily broken into pure nonlinear programming problems which can be directly solved by existing nonlinear optimization software such like cvx [29] as follows. Since besides AP_c there are $|\Omega| - 1$ APs that may potentially measure the mobile station's signal. To make the number of APs that can take measurements less than 4, we can tolerate at most 2 APs other than AP_c to hear the mobile station's signal, which means at most 2 APs can violate the constraint in (4.9). Hence, we can convert the feasibility check for (4.10) into the feasibility check for multiple subproblems, where the constraint in (4.9) is omitted for 2 APs in each of the subproblem. For example, the subproblem that neglects AP_k and AP_l looks like this:

$$
\begin{aligned}
&\underset{\mathbf{w}}{\text{minimize}}\ \textit{Total Transmit Power} \\
&\text{subject to} \\
&P_0|G(\theta_c)|^2(\text{dBm}) \geq \hat{PL}_c(\text{dBm}) + C_{th}(\text{dBm}) + \delta_{\text{dB}} \\
&\max\nolimits_{\phi_i \in [\theta_i - \delta_\theta, \theta_i + \delta_\theta]} P_0|G(\phi_i)|^2(\text{dBm}) - \hat{PL}_i(\text{dBm}) + \delta_{\text{dB}} < R_{th}(\text{dBm}) \\
&\forall i \in \Omega, i \neq c, k, l.
\end{aligned}
\tag{4.11}
$$

The number of subproblems equals the number of unique combinations of k and l. If any of the subproblem is feasible, we know that the problem in (4.10) is feasible and the solution for that subproblem can be used to tune the radiation pattern. In fact, once we find that for one combination of k and l, the subproblem in (4.11) is feasible, we can stop trying other combinations and terminate the optimization process. As a result, in the worst situation, we need to solve $(|\Omega| - 1)(|\Omega| - 2)/2$ subproblems. In practice $|\Omega|$ is usually not a large number. Hence even solving $(|\Omega| - 1)(|\Omega| - 2)/2$ subproblems is still acceptable.

Finally if the problem in (4.10) is infeasible, the number of RSS measurements gathered by the localization system is enough for unique location estimation. In this case, the mobile station switches to the second strategy which is introduced in the next section.

4.6 Strategy Two: Maximizing Localization Error

In this strategy, a mobile station aims at maximizing the localization error of a RSS localization system when it cannot be sure that it can limit the number of RSS measurements to a safe level (a.k.a. (4.10) has no feasible solution). To understand the design of this strategy, in this section, we will first show how we model the problem of maximizing localization bias; then we solve the problem using Genetic Algorithm (GA).

4.6.1 Problem Model

Since almost all of the current RSS-based localization schemes are based on the assumption that the mobile station is using omnidirectional antenna, pattern synthesis makes the radiation intensity varies a lot in different directions and therefore introduce large bias in their location estimation.

The problem of maximizing localization bias can be modeled as an optimization problem with the absolute location estimation error as the objective function and the antenna's complex weight vector $\mathbf{w}$ as the variables to be optimized. Meanwhile, the restriction that AP_c is well connected still holds. To formulate the objective function, we first simplify the notation in problem formulation, by setting up a coordinate system, where the location of the mobile station is the origin. Next, we look at how location of the mobile station is estimated by a RSS-based localization system. Denoting R_k as the signal strength of the mobile station at AP_k's location, a RSS-based localization system makes a potentially biased estimation of the mobile station's location, denoted as (x', y'), based on the R_k at all APs. Hence, (x', y') is a function of both AP's location (x_k, y_k) and $R_k, k = 1, 2, ..., K$.

$$(x', y') = F(x_1, \cdots, x_K, y_1, \cdots, y_K, R_1, \cdots, R_K) \tag{4.12}$$

To maximize the bias in the above estimation, the mobile station computes the location estimation error of the above localization system using the estimated AP coordinates and the predicted RSS at the APs. Based on the estimation of its path loss to the APs in Section 4.4.3, the mobile station

can estimate its signal strength at AP_k as:

$$\hat{R}_k(\text{dBm}) = P_0|G(\theta_k)|^2(\text{dBm}) - \hat{PL}_k(\text{dBm}). \tag{4.13}$$

In addition, from Section 4.4.2, mobile station can also estimate the coordinate of AP_k as at $(\hat{x}_k, \hat{y}_k)$. Based on these information, the mobile station can make an estimation of (x', y'), which is the RSS-localization system's estimate of its location. Denote $(\hat{x}', \hat{y}')$ as the mobile station's estimate of (x', y'). For the mobile station, the optimization problem of maximizing the bias of a RSS-localization system can be modeled as

$$\begin{aligned}
&\underset{\mathbf{w}}{\text{maximize}} \;\; E[||(\hat{x}', \hat{y}')||] \\
&\text{subject to} \\
&\quad P_0|G(\theta_c)|^2(\text{dBm}) \geq \hat{PL}_c(\text{dBm}) + C_{th}(\text{dBm}) + \delta_{\text{dB}} \\
&\quad (\hat{x}', \hat{y}') = F(\hat{x}_i, \hat{y}_i, \hat{R}_i) \\
&\quad \hat{R}_i(\text{dBm}) = P_0|G(\gamma_i)|^2(\text{dBm}) - \hat{PL}_i(\text{dBm}) \\
&\quad \gamma_i \sim U[\theta_i - \delta_\theta, \theta_i + \delta_\theta] \\
&\quad (\text{i.e. } \gamma_i \text{ is uniformly distributed in } [\theta_i - \delta_\theta, \theta_i + \delta_\theta]) \\
&\quad i = 1, 2, ..., K.
\end{aligned} \tag{4.14}$$

To solve the above optimization problem, the location estimation function $F(\cdot)$ must be known. In the remainder of this chapter, we assume that the localization system uses least square (LS) method since it is a very popular scheme used in many localization systems [94]. Under this method, the function $F(\cdot)$ can be deduced from (4.5).

It is important to note that our scheme is not limited to least square method. If the mobile station knows that another localization algorithm is used by the RSS-based localization system, the mobile station can change function $F(\cdot)$ and optimize its radiation pattern accordingly. Many may argue that the estimation algorithm adopted by the localization system may not be the common least square method (e.g. a fingerprint based estimation algorithm) and the algorithm is not known to the mobile station. In this case, the mobile station has no certain ways to maximize the bias of the location system. Nevertheless, we believe that despite the wrong guess on location estimation

algorithm, the irregular radiation pattern produced by the optimization problem in (4.14) should at least increase the bias for any estimation methods even it cannot maximize it.

4.6.2 Genetic Algorithm (GA) Solution

GA is used to solve the problem in (4.14) since it does not require derivative information of the objective function and it works without limit on the number of variables [32, 92]. The GA procedure in this chapter is similar to its standard form and small modification is made to fit it to our problem.

Chromosome Construction

In our application of pattern synthesis, the complex weight vector $\mathbf{w} = [w_1, w_2, \cdots, w_{N_{ant}}]^T$ is directly used as a chromosome. Each element in $\mathbf{w}$ represents an excitation factor of the corresponding antenna element. Therefore the length of the chromosome is determined by the number of antenna elements N_{ant}.

Initial Population

The number of the chromosomes in the population is denoted by N_{pop}. So the population is actually an $N_{pop} \times N_{ant}$ complex matrix. We initialize the population by randomly generate the real and complex part of the complex gene as a random number within $[0, \frac{1}{N_{ant}}]$.

Natural Selection

Each chromosome in the population is passed to the objective function to calculate corresponding output objective value. Then the chromosomes are sorted according to descending order of their associated objective values. We just keep the best N_{ns} chromosomes and discard the others.

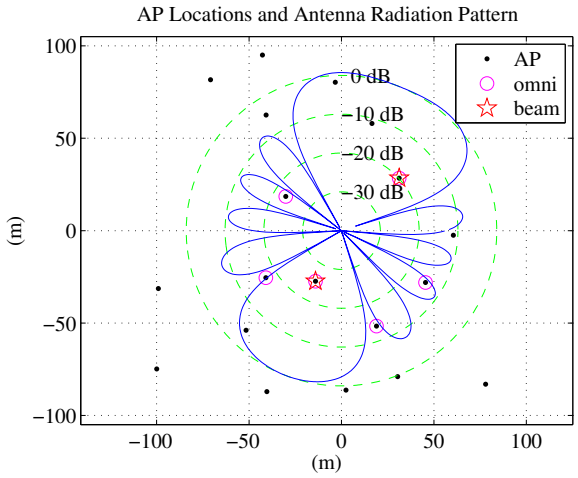
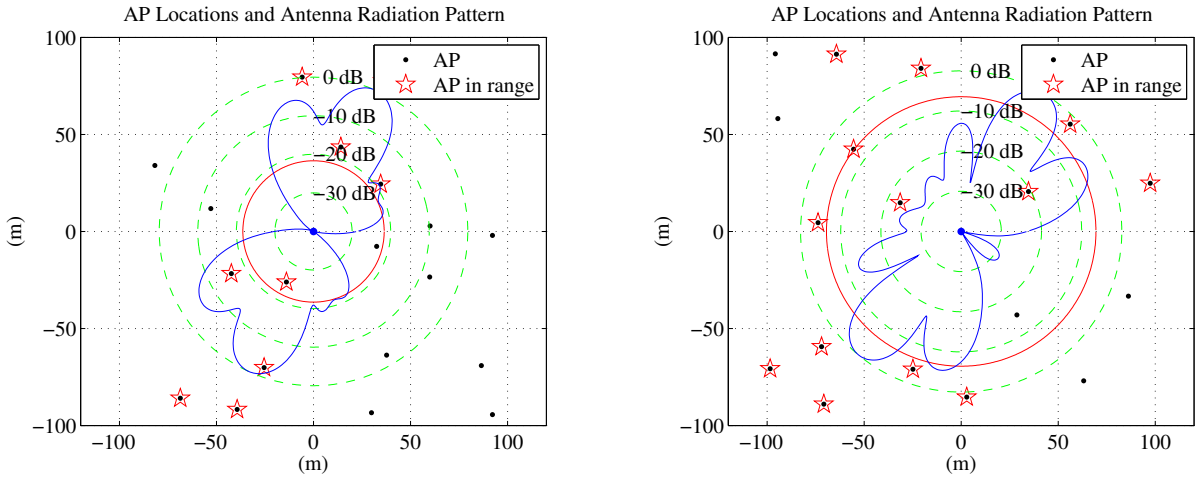


Figure 4.3: An beamforming pattern that limits the number of APs in range to be less than 4. (The radiation pattern of the omnidirectional antenna is the out most green circle.)



(a) (b)

Figure 4.4: Two examples of the optimized beamforming pattern.

Mating

Mate selection is a procedure that two parent chromosomes are picked to produce offspring chromosomes. In our problem, the chromosomes with greater objective value should have higher chance to be selected. We use roulettle wheel selection method [32] and assign higher probability to high ranking chromosomes.

Reproduction

Decimal crossover is used to produce offspring chromosomes. Given the parent chromosomes $\mathbf{w}_f$ and $\mathbf{w}_m$, the child chromosomes are given by:

$$\begin{aligned} \text{child1} &= 0.5\mathbf{w}_f + 0.5\mathbf{w}_m \\ \text{child2} &= 1.5\mathbf{w}_f - 0.5\mathbf{w}_m \\ \text{child3} &= -1.5\mathbf{w}_f + 0.5\mathbf{w}_m. \end{aligned} \tag{4.15}$$

This makes the offspring unbounded by the parent chromosomes while keeps good property of the parent chromosomes.

Mutation

In order to keep the best chromosome in the population, the top ranking chromosome will not be mutated. According to the mutation rate, a group of the genes in the rest chromosomes are randomly selected and their values are reset as a random number within $[0, \frac{1}{N_{ant}}]$. This process is helpful to prevent GA evolution from stagnating at a local optimum.

Terminating Criteria

The evolution process is repeated until a maximum total number of generations is reached. When GA is terminated, the complex weight vector associated with the optimal objective value is adopted

in radiation pattern synthesis. The output optimal objective value is the predicted location estimation bias of the localization system.

Note that due to the possible error in estimating the APs' locations and their angles to the mobile station, difference between the predicted localization estimation bias and the true location estimation bias might exist. However, decision making based on the existing information is the best thing that the mobile user can do.

4.7 Simulation Results

To evaluate the performance of our proposed location privacy scheme, we simulate a WLAN and our privacy protection scheme in Matlab environment. In our simulation, APs are randomly deployed in a 200×200 m^2 2-D space. They are spaced reasonably far away from each other to mimic real network deployment since real WLAN deployment rarely have two APs sit very close to each other to avoid interference and increase efficiency in network coverage.

We first show examples of individual synthesized beamforming patterns of both the first and the second strategy. Then we use Monte Carlo simulation to estimate the success rate of the first strategy and the expected localization bias caused by the second strategy with different combinations of the number of APs and the number of antenna elements.

The setting of the parameters is as follows. The path loss exponent α is set to be 3, $C_{th}(\text{dBm}) = -75$ dBm and $R_{th}(\text{dBm}) = -80$ dBm. Transmit power of the APs are randomly generated in the range of 10 dBm to 20 dBm. For both omnidirectional antenna cases and pattern synthesis cases, shadowing noise variance is 1. For the proposed scheme, $\delta_{\text{dB}} = 5$ dBm and $\delta_\theta = 5^\circ$. Following is the detailed discussion of the simulation results.

4.7.1 Examples of Synthesized Patterns

In the following examples, the linear antenna array consists of 6 isotropic elements and the interval spacing between neighboring antenna elements is half the wavelength.

Strategy One: Limiting AP Measurements to Be Less Than 4

Figure 4.3 illustrates an example of synthesized radiation pattern generated by strategy one of our privacy protection scheme. In this figure, the mobile station is at the origin. When the privacy protection scheme [37] based on power control over omnidirectional antenna is used to protect user privacy, the APs that can hear the mobile station's signal are marked by magenta circles and there are 6 of them. While using the optimized radiation pattern under our strategy one, the APs that can hear the mobile station's signal are marked by red pentagrams and there are only 2 such APs. For both situations, the transmit power is chosen to be the minimum value that satisfies the communication requirement defined by (4.8).

From the above example, it is easy to see that if the mobile station uses omnidirectional antenna, it will be heard by 6 APs and it can be localized. While by using our strategy one of radiation pattern synthesis, the mobile station is able to concentrate the transmit power for communication purpose and limit the power emitted to other directions. Therefore the number of APs that can hear its signal is significantly reduced.

Strategy Two: Maximizing the Location Estimation Bias

When it is inevitable that more than 4 APs can get RSS measurements of its signal, the mobile station optimizes its radiation pattern with GA to bias the location estimation as much as it can. In the GA compuation process, the maximum number of generation is set as 500.

Figure 4.4 illustrates two examples of the optimized radiation pattern overlapping with the AP distribution in the 2-D space. The radius of red circle in the center is the size of estimation error of

LS location estimation algorithm. As we can see from Figure 4.4(a), when the localization error is maximized, our strategy controls the APs that can measure RSS to be on a diagonal that passes the location of the mobile station. This observation is in accordance with the result in [14], which says that collinear deployment of anchors has negative impact on localization performance. In Figure 4.4(b), the directional gain of the smart antenna varies a lot in different direction. Consequently even if the localization system successfully get abundant RSS measurements of the mobile station, those RSS measurements are biased. Directly using these RSS measurements to do localization will cause large estimation error, while refining those measurements are very difficult without knowing the radiation pattern used by the mobile station.

Essentially, we can see that our strategy two degrades the localization performance by not only distorting the RSS measurement but also selectively only letting the APs located collinearly measure RSS.

4.7.2 Statistical Analysis

In this part, we first use Monte Carlo simulation to estimate the success rate of our strategy one, which attempts to limit the number of APs that can hear the mobile station's signal to be below 4. Then, we use Monte Carlo simulation to evaluate the localization bias introduced by our strategy two. We evaluate our scheme under different combinations of the number of APs (N_{ap}) and the number of antenna elements (N_{ant}). For each pair of N_{ap} and N_{ant}, 200 simulation runs are conducted.

Success Rate of the First-priority Strategy

Table 4.1 lists the success rate of the our strategy one. $N_{ant} = 1$ is actually the omnidirectional antenna case and the data in the first row shows the simulated success rate of using transmit power control to limit the number of APs in range to be less than 4. The higher success rate of our pattern synthesis scheme compared with the omnidirectional antenna case indicates that pattern synthesis

Table 4.1: Success rate of strategy one.

N_{ant}	N_{ap} = 10	N_{ap} = 20	N_{ap} = 30
1	0.335	0.355	0.405
4	0.51	0.455	0.595
6	0.575	0.59	0.615
8	0.615	0.61	0.615
10	0.635	0.64	0.7
12	0.705	0.655	0.715

is more powerful to reduce the number of RSS measurements while keeping a mobile station's communication quality intact.

Generally, the success rate tends to increase when N_{ant} increases since smart antenna array with more antenna elements has more flexibility in tuning the radiation pattern. The capability of concentrating the transmit power to desired direction reduces the unnecessary power emission to other directions and keep the mobile station more secure.

We also find that when N_{ap} increases, the success rate of our strategy one also may increase. This is counterintuitive in a sense that higher density of APs should lead to greater chance that the signal from the mobile station to be heard by more APs. However, note that, due to variations in path loss and inherent noise in our AP location estimation, APs in areas that are a little further away than AP_c may still hear the mobile station's signal. We call this as the blurring zone around AP_c and our strategy one has conservatively considered APs in the blurring zone as APs that can measure RSS of the mobile station. According to log-normal shadowing path loss model illustrated by Figure 4.5, the further away that AP_c is from the mobile station, the more flat the curve of signal attenuation is, which results in a larger blurring zone around AP_c. When AP density is high, AP_c usually locates closer to the mobile station, resulting a small blurring zone around AP_c. As the blurring zone is smaller, there is less chance that any AP will happen to be in this blurring zone. Hence, the success rate of strategy one increases.

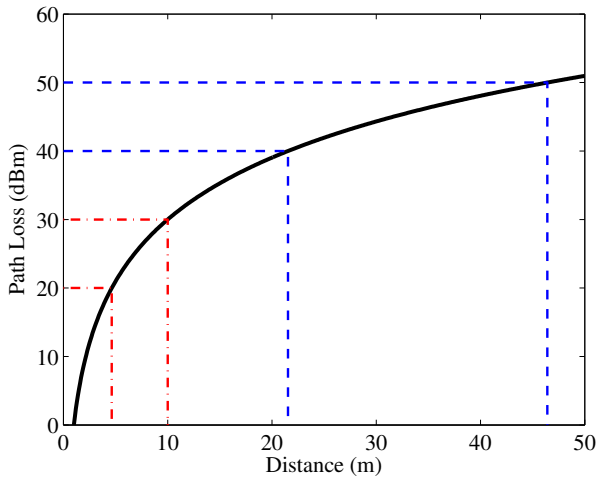


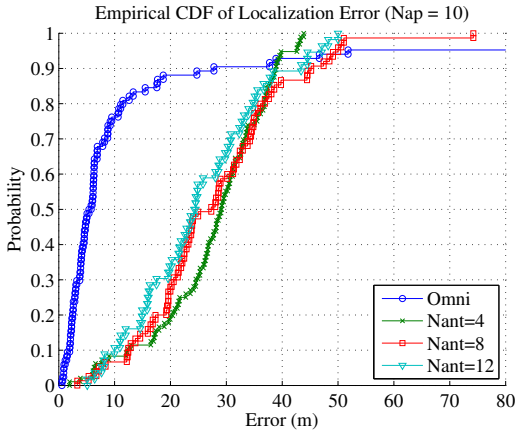
Figure 4.5: Large scale path loss v.s. distance using log-normal shadowing model with $\alpha = 3$.

Localization Bias Introduced by Strategy Two

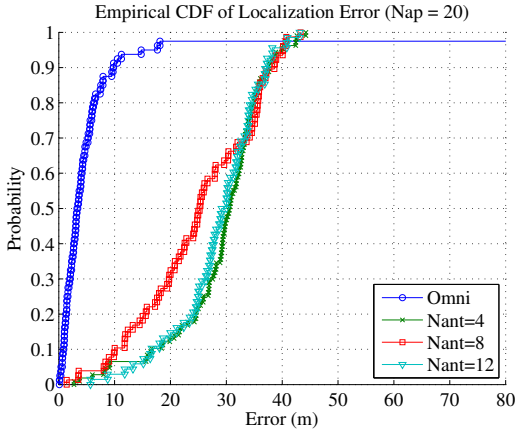
Figure 4.6 shows the cumulative probability distribution (CDF) of the localization bias caused by our strategy two. As we can see from the figure, when omnidirectional radiation pattern is used, the localization bias is around 10 meters and the bias is mainly caused by noise. Comparatively, the CDF curves of our strategy two are more on the right side, indicating significantly larger location estimation bias. Consider that the radius of an AP's coverage area is usually 30 to 50 meters, this estimation bias is fairly large. Thus we can draw the conclusion that our pattern synthesis-based privacy protection scheme can bring large bias to the location estimation result of localization system. However, we do not observe big performance difference among antenna arrays with different number of antenna elements. Hence we conclude that antenna array with different number of antenna elements have similar performance in distorting the localization result.

4.8 Chapter Summary

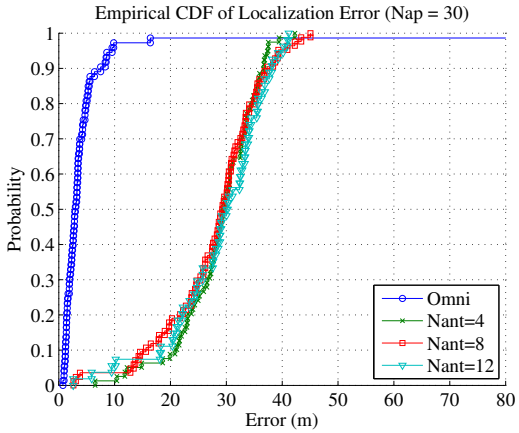
In WLAN environment, a mobile station's location can be revealed by its radiated signal and this poses great threat to the mobile user's location privacy. In this chapter, we proposed a physical layer location privacy protection scheme against RSS-based localization systems using a linear smart antenna array on the mobile station. Our scheme consists of a passive observation step and an antenna pattern synthesis step. In the passive observation step, the mobile station moves around to measure the beacon signal of the neighboring APs and estimate the path losses to the APs. In the pattern synthesis step, two pattern optimization strategies are used to prevent the positioning system from correctly localizing the mobile station while the communication quality is not affected. Simulation results show that our first-priority strategy significantly increases the probability of inadequate RSS measurements and the second strategy substantially degenerates the localization precision.



(a)



(b)



(c)

Figure 4.6: CDF of localization error caused by pattern synthesis.

Chapter 5

Analysis on Beamforming-based Perfect Location Spoofing Attacks

As we know, personal privacy preservation and security assurance at the system level are often conflictive in a sense that privacy preservation tries to conceal personal information, while security assurance needs to obtain as much information as possible to protect the system from potential malicious attacks. Specifically, if the scheme proposed in Chapter 4 is abused and enhanced by malicious parties, it is possible that the attackers can spoof their locations to conceal their crime.

Location spoofing attacks pose serious threats to the location based wireless network mechanisms. In spite of existing schemes for robust localization and location spoofing detection, our study shows that in many circumstances, perfect location spoofing (PLS) can stay undetected even if robust localization algorithms or detection mechanisms are used. In this chapter, we present theoretical analysis on the feasibility of beamforming-based PLS attacks and how it is affected by the geometry of anchor deployment. We formulate PLS as a nonlinear feasibility problem based on smart antenna array pattern synthesis. Due to the intractable nature of this feasibility problem, we solve it using semidefinite relaxation (SDR) in conjunction with a heuristic local search algorithm. Simulation results show the effectiveness of our analytical approach. Based on the experimental results, we show that PLS attack' s feasible region is strongly correlated with localization anchor

deployment. We use this correlation to derive insightful guidelines for defence against such attacks.

5.1 Introduction

Radio localization systems have been integrated into many wireless network solutions. For example, location-based access control (LBAC) determines the users' privileges of accessing critical information by taking the users' physical locations into account [2, 62]. Identity spoofing detection mechanisms use location information to differentiate malicious nodes from legitimate nodes [18]. In the emerging cognitive radio networks, the geo-location database approach mandated by the FCC for dynamic spectrum access uses location of secondary user for spectrum allocation. In these applications, the correctness of the location results provided by the localization systems is critical. Attacks on localization systems can cause errors in location estimation and consequently break these location based mechanisms of wireless networks.

Generally, there are two categories of attacks on localization systems. The first category is location concealing, where the adversary does not have a specific target fake location. The goal of location concealing is simply to distort the measurements of the localization system so that the true location of the adversary cannot be identified. The other category is location spoofing, where an attacker masquerades as being at another target location by falsifying the measurements of the localization system. (An illustration is given by Figure 5.1.) Between the two categories, the latter is more of a threat to the security of wireless networks in the sense that locationally masqueraded attackers can take illegitimate advantage of the network resources and launch further attacks to the network. For instance, in applications of LBAC, if the attacker can masquerade to be at a position where high access privileges are given, he / she may illegitimately access confidential resources. In tracing of adversary in wireless networks, attackers with capability of masquerading locations may plant the crime on innocent wireless nodes and disturb the judgement of the security mechanism. Similarly, the identity attack detection schemes that rely on localization may also fail due to this kind of location spoofing attacks [18, 24, 74]. In this chapter, we focus on investigation of location

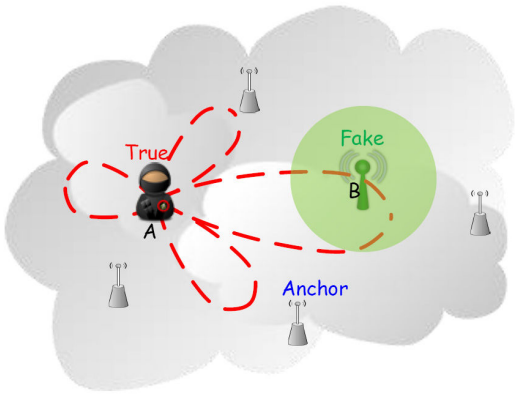


Figure 5.1: A Perfect Location spoofing attack.

spoofing attack to received signal strength (RSS) based localization systems.

The existence of potential location spoofing attacks has been identified for quite a few years. In [17], it is experimentally shown that by attenuating or amplifying the RSS readings at the anchors, the localization system may conclude in false location estimation. Bauer et al. show that attackers with directional antennas [7] have the ability to bias the location estimation to a direction of their choice in addition to introducing significant localization errors. The feasibility of using smart antenna to conceal the real location of the transmitting radio is introduced in [85]. All these works indicate that location spoofing is possible. A few robust localization algorithms have been proposed to countermeasure location spoofing attacks [17, 45, 47], in which statistical analysis methods are used to detect and eliminate some of the biased RSS measurements.

Unfortunately, despite all the existing efforts, we have discovered that robust RSS localization schemes are all limited in their effectiveness no matter what statistical methods they use. In many circumstances, there exist location spoofing attacks that can stay undetected under all of these robust RSS based localization algorithms. We call such attack as "*perfect location spoofing (PLS) attack*". To fully understand the limitations of robust localization algorithms and the level of threat of PLS attacks, in this chapter, we provide a thorough theoretical analysis on the capability of using PLS attacks to evade robust RSS localization algorithms. Our analysis assumes that the attacker uses beamforming to control the directional gains of his radio and hence falsifies the RSS

readings at the anchors. To the best of our knowledge, our analysis is the first to provide answers to the following critical and fundamental questions: *Is it possible for an attacker to launch location spoofing attacks against any robust RSS localization algorithm? Can an attacker launch a PLS attack to a specific location no matter where he/she is? What can be done to reduce the possibility of PLS attacks?*

To answer these questions, we first formulate the PLS problem as a nonlinear feasibility problem based on smart antenna pattern synthesis. Due to the intractable nature of this feasibility problem, we derive close upper and lower bounds of the solution to the feasibility problem through semidefinite relaxation and local search method. Using these upper and lower bounds, we further investigate how the feasibility of PLS is related to anchor deployments and antenna capability. Based on the investigation results, we provide guidelines for localization anchor deployment strategies that can significantly reduce the threat of PLS attacks. To our best knowledge, our work is the first study that presents mathematical formulation and theoretical analysis on the feasibility of PLS attacks, how they are affected by the anchor deployment and how PLS attacks can be solved.

5.2 RSS Based Localization

In this section, we give a brief overview of RSS-based localization systems which are adopted by most commercial applications. In an RSS based localization system, there are multiple signal receivers placed at specific locations which measure the RSS of wireless nodes and report the measurements to the system. These signal receivers are referred as "*anchors*". Localization algorithms are then used to compute location estimates based on anchor measurements. These algorithms fall into two categories: fingerprint based approaches [4, 38] and propagation model based approaches [63, 39]. Fingerprint localization collects RSS measurements of wireless nodes at sample locations and stores these measurements in database in the off-line phase. During the on-line phase, the actual RSS measurements of the target wireless node are compared with the stored database and through pattern matching, a location estimation can be returned. In propaga-

tion model based RSS localization schemes, the distances from the wireless node to the anchors are estimated using large scale path loss model. With these estimated distances, the localization result is obtained geometrically by trilateration.

For both types of approaches, robust data processing algorithms [17, 45, 47] can be used to detect and eliminate some abnormal measurements introduced by location spoofing attacks. However, no matter what robust algorithms are used for these two types of approaches, we will show in the next section that some location spoofing attacks can still be undetectable.

5.3 Attack Model

The location spoofing attack model is illustrated in Figure 5.1, where point "A" is the true location of the attacker and point "B" is the attacker's fake location. Note that no matter which localization algorithm is used in the system, as long as the attacker ensures that the RSS readings at all the anchors are the same as what the RSS readings should be for a wireless node at the fake location, there is no way for any robust localization algorithm to detect the location spoofing attack. We call this type of location spoofing attack as "*perfect location spoofing (PLS)*". Under PLS attack, the location estimations produced by all localization algorithms are the same fake location within a reasonable small error range that are determined by the noise level and the precision of the algorithms.

For conventional omnidirectional radios, realizing PLS attack is not possible because the path loss vector from point "A" to the anchors are different from the path loss vector from point "B". Thus, wireless nodes with omnidirectional antennas at the two points will produce different RSS reading vectors at the anchors. An attacker at point A, however, can use smart antenna's beamforming capability to solve this problem and make the RSS readings at anchors the same as the readings should be when he is at position B. To do this, the attacker first obtains the anchor locations by wardriving [31] (moving around to locate anchors in the neighboring area), spying or other underhand means. Then, the attacker tunes the diverse directional gains produced by beamforming

to compensate the difference between the two path loss vectors from A and B, and hence, falsify the RSS reading vectors at the anchors. To estimate the path loss, the attacker can leverage signal propagation models and field measurement methods. If the falsified RSS reading vector is within the range of typical noised RSS reading vectors produced by a legitimate wireless node at the fake location, we say that a PLS attack is created.

In the remainder of this chapter, we assume that the attacker is equipped with a circular smart antenna array which consists of N_{ant} isotropic elements placed over a circle with radius R. The i^{th} antenna element is located with the phase angle ϕ_i. The beamforming pattern of this circular smart antenna array is expressed as [82]:

$$G(\theta) = \sum_{i=1}^{N_{ant}} w_i \exp[j\frac{2\pi}{\lambda} R\cos(\theta - \phi_i)], \tag{5.1}$$

where λ is the signal wavelength, θ represents the direction and $\mathbf{w} = [w_1, w_2, \cdots, w_{N_{ant}}]^H$ is the complex weight vector which can be tuned to change the radiation pattern.

We choose circular antenna array as an example to illustrate the formulation of our analysis because it can produce flexible asymmetric beamforming patterns and easily deflect a beam through 2π. However, our analysis is not limited to circular antenna array. It is straightforward to plug antenna models with other geometric forms into the analysis by replacing equation (5.1) with their corresponding beamforming functions.

5.4 Problem Overview

To understand how we analyze the conditions that an attacker can launch a PLS attack, let us look at a simple example illustrated in Figure 2, where an attacker at location (x, y) wants to fake his/her location at $(\hat{x}, \hat{y})$. There are K anchors in the neighboring area and their locations are denoted by $(x_k, y_k),\ k = 1, 2, \cdots, K$. Since less than 4 anchors are not enough to uniquely localize even a legitimate node with unknown transmit power, we are only interested in the cases where $K \geq 4$. Suppose the expected path loss from the true location, (x, y), to the i^{th} anchor

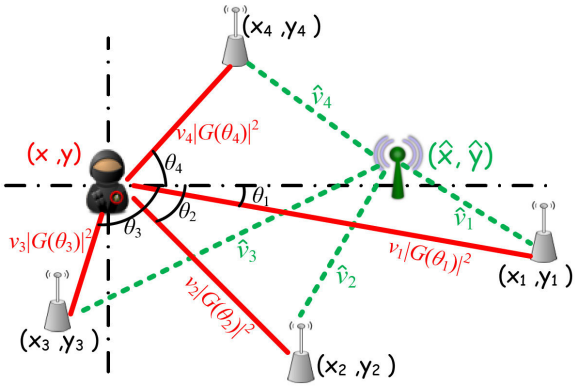


Figure 5.2: Compensating path loss differences using beamforming.

is v_i and $\mathbf{v} = [v_1, v_2, \cdots v_K]^T$. The expected path loss from the fake location, $(\hat{x}, \hat{y})$, to the i^{th} anchor is $\hat{v}_i$ and $\hat{\mathbf{v}} = [\hat{v}_1, \hat{v}_2, \cdots, \hat{v}_K]^T$. Denote the direction angle of the i^{th} anchor with respect to the true location (x, y) as θ_i and $\Theta = [\theta_1, \theta_2, \cdots \theta_K]^T$. To realize a PLS attack, all the anchors' RSS readings of the attacker should be the same as the RSS readings of a legitimate user at the fake location $(\hat{x}, \hat{y})$. Hence, the attacker must tune his/her beamforming pattern defined in (5.1) to satisfy the following constrains,

$$v_k|G(\theta_k)|^2 \approx \hat{v}_k, \forall k = 1, 2, \cdots, K. \tag{5.2}$$

Essentially, (5.2) shows that the requirement of PLS for the attacker is that the beamforming gains in the directions of the anchors must compensate the difference between the path loss vectors from the attacker's true location and from the fake location. If a $\mathbf{w}$ that satisfies all the constraints in (5.2) can be obtained, we conclude that a PLS attack is feasible. Otherwise, it is infeasible to falsify all the RSS readings at the anchors by beamforming and the abnormal RSS readings can potentially be detected by some robust localization algorithms. It is important to note that we use an approximate sign in (5.2) instead of an equal sign. This is because signal path loss usually has random variations. Hence, as long as the attacker's RSS readings are close enough to the desired fake values, a localization system cannot tell whether the discrepancy is caused by attack or natural variations in path loss.

In spite of the straightforward concept of formula (5.2), we will show in Section 5.5 that the formal

mathematical formulation of the PLS feasibility problem is NP-hard in general. In order to solve this problem, we leverage semidefinite relaxation (SDR) technique and a local search algorithm to get approximate answers. Simulation results show that our approximation method can closely approximate the intractable feasibility problem and is effective in analyzing the feasibility of PLS attacks under different situations. The analysis will answer the following questions:

- How is the feasibility of PLS attacks related to the anchor density and the hardware capability of the attacker's smart antenna?
- What kind of anchor deployment is good for guard against location spoofing attacks?
- Given an anchor deployment and a particular fake location, where could the attacker be hiding to launch a PLS attack?

The answers to the above questions provide insightful guidance for deployment of spoof resistant localization system and tracing of location spoofing adversaries.

5.5 Problem Formulation

In this section, we formulate the feasibility of PLS in the form of a non-linear programming problem.

According to the log-distance path loss model, the expected path loss vectors from the attacker's true location (x, y) and his/her target fake location $(\hat{x}, \hat{y})$ to the anchors at locations $(x_k, y_k),\ k = 1, 2, \cdots, K$ can be expressed as the following equations respectively,

$$\begin{aligned} &\mathbf{v} = [v_1, v_2, \cdots v_K]^T, \\ &v_k = PL_0[(x_k - x)^2 + (y_k - y)^2]^{\alpha/2}, \\ &\hat{\mathbf{v}} = [\hat{v}_1, \hat{v}_2, \cdots, \hat{v}_K]^T, \\ &\hat{v}_k = PL_0[(x_k - \hat{x})^2 + (y_k - \hat{y})^2]^{\alpha/2}, \end{aligned} \tag{5.3}$$

where PL_0 is the path loss at the reference distance $d_0 = 1$m and α is the path loss exponent. As illustrated in Figure 5.2, the angle vector $\Theta = [\theta_1, \theta_2, \cdots \theta_K]^T$ is defined by the relationships:

$$\begin{aligned} &\cos\theta_k = \tfrac{x_k - x}{\sqrt{(x_k-x)^2+(y_k-y)^2}}, \\ &\sin\theta_k = \tfrac{y_k - y}{\sqrt{(x_k-x)^2+(y_k-y)^2}}, \\ &k = 1, 2, \cdots, K. \end{aligned} \tag{5.4}$$

From (5.1), the beamforming directional gain in the direction of the k^{th} anchor can be written as

$$|G(\theta_k)|^2 = |\mathbf{w}^H \mathbf{h}_k|^2, \tag{5.5}$$

where

$$\mathbf{h}_k = \begin{bmatrix} \exp[j\frac{2\pi}{\lambda} R\cos(\theta_k - \phi_1)] \\ \exp[j\frac{2\pi}{\lambda} R\cos(\theta_k - \phi_2)] \\ \vdots \\ \exp[j\frac{2\pi}{\lambda} R\cos(\theta_k - \phi_{N_{ant}})] \end{bmatrix}. \tag{5.6}$$

In Section 5.4, we have briefly described the requirement for a PLS using (5.2). We use an approximation sign in formula (5.2) because $v_k|G(\theta_k)|^2$ does not need to be exactly equal to $\hat{v}_k$ for realizing a PLS due to path loss variations in nature environment. Following shadow fading model, the path loss is a Gaussian distributed random variable with a standard deviation in dB. As long as the difference between $v_k|G(\theta_k)|^2$ and $\hat{v}_k$ is within the typical deviation level, a localization system is not able to differentiate the falsified RSS measurements from noised RSS measurements. Thus we use the standard deviation of the Gaussian noise, δ(dB) > 0, as the threshold that defines the closeness requirement for the approximation in (5.2) to hold. Based on this threshold, we convert (5.2) into

$$|10\log_{10}(v_k|G(\theta_k)|^2) - 10\log_{10}(\hat{v}_k)| \leq \delta(\text{dB}). \tag{5.7}$$

For simplicity, note that (5.7) is equivalent to

$$\frac{1}{\delta} \leq \frac{v_k}{\hat{v}_k}|G(\theta_k)|^2 \leq \delta. \tag{5.8}$$

By plugging (5.5) into (5.8), we get

$$\frac{1}{\delta} \leq \frac{v_k}{\hat{v}_k}|\mathbf{w}^H \mathbf{h}_k|^2 \leq \delta. \tag{5.9}$$

Letting

$$\mathbf{f}_k = (\frac{\upsilon_k}{\hat{\upsilon}_k})^{\frac{1}{2}}\mathbf{h_k}, \tag{5.10}$$

(5.9) becomes:

$$\frac{1}{\delta} \leq |\mathbf{w}^H\mathbf{f}_k|^2 \leq \delta. \tag{5.11}$$

The feasibility of PLS now can be modeled as:

$$\begin{aligned} \text{find any} \quad & \mathbf{w}^H \\ \text{s.t.} \quad & |\mathbf{w}^H\mathbf{f}_k|^2 \leq \delta \\ & |\mathbf{w}^H\mathbf{f}_k|^2 \geq \tfrac{1}{\delta} \\ & k = 1, 2, \cdots, K. \end{aligned} \tag{5.12}$$

The formulation in (5.12) is a nonlinear feasibility problem, in which the answer is "yes" or "no". However, this feasibility problem is difficult to answer as we have the following claim.

Claim 1. *The feasibility problem (5.12) is NP-hard.*

Proof. To prove the complexity of problem (5.12), let us consider its complementary problem:

$$\begin{aligned} \max_{\mathbf{w}} \quad & t = \min_k \{|\mathbf{w}^H\mathbf{f}_k|^2\}_{k=1}^K \\ \text{s.t.} \quad & |\mathbf{w}^H\mathbf{f}_k|^2 \leq \delta,\ k = 1, 2, \cdots, K. \end{aligned} \tag{5.13}$$

Given the solution t^* of (5.13), problem (5.12) is feasible if and only if $t^* \geq \frac{1}{\delta}$ and it is infeasible if and only if $t^* < \frac{1}{\delta}$. Conversely, suppose problem (5.12) can be solved in polynomial time. Then for any given value of $\eta \in [0, \delta]$, we can also solve the following problem in polynomial time.

$$\begin{aligned} \text{find} \quad & \mathbf{w}^H \\ \text{s.t.} \quad & |\mathbf{w}^H\mathbf{f}_k|^2 \leq \delta \\ & |\mathbf{w}^H\mathbf{f}_k|^2 \geq \eta \\ & k = 1, 2, \cdots, K. \end{aligned} \tag{5.14}$$

Since the value of η lies in the interval $[0, \delta]$, we can use bisection method to find the turning point η', so that when $\eta > \eta'$, problem (5.14) is infeasible and for $\eta < \eta'$, problem (5.14) is feasible.

This turning point η' is the maximum value of η which makes problem (5.14) feasible, so it is exactly the solution to the max-min problem (5.13). Because bisection method is a polynomial-time algorithm, the reduction from problem (5.13) to problem (5.12) is also polynomial. Thus, problem (5.12) and problem (5.13) are bidirectionally polynomial-time reducible. Hence, if we can show (5.13) is NP-hard, we prove that (5.12) is NP-hard too.

Now consider the case that the solution to (5.13) is obtained when $t^* = |\mathbf{w}^H\mathbf{f}_{k^*}|^2$, and (5.13) becomes:

$$\begin{aligned} \max_{\mathbf{w}} \quad & |\mathbf{w}^H\mathbf{f}_{k^*}|^2 \\ \text{s.t.} \quad & |\mathbf{w}^H\mathbf{f}_k|^2 \leq \delta \\ & |\mathbf{w}^H\mathbf{f}_k|^2 \geq |\mathbf{w}^H\mathbf{f}_{k^*}|^2 \\ & k = 1, 2, \cdots, K. \end{aligned} \tag{5.15}$$

By moving $|\mathbf{w}^H\mathbf{f}_k|^2$ to the other side of the inequality, (5.13) is finally recast as

$$\begin{aligned} \max_{\mathbf{w}} \quad & \mathbf{w}^H(\mathbf{f}_{k^*}\mathbf{f}_{k^*}^H)\mathbf{w} \\ \text{s.t.} \quad & \mathbf{w}^H(\mathbf{f}_k\mathbf{f}_k^H)\mathbf{w} \leq \delta \\ & \mathbf{w}^H(\mathbf{f}_{k^*}\mathbf{f}_{k^*}^H - \mathbf{f}_k\mathbf{f}_k^H)\mathbf{w} \leq 0 \\ & k = 1, 2, \cdots, K. \end{aligned} \tag{5.16}$$

In (5.16), $\mathbf{f}_k\mathbf{f}_k^H$ is a Hermitian positive semi-definite matrix and $\mathbf{w}^H(\mathbf{f}_{k^*}\mathbf{f}_{k^*}^H - \mathbf{f}_k\mathbf{f}_k^H)\mathbf{w}$ is an indefinite matrix. Thus, (5.16) is a non-convex quadratically constrained quadratic programming (QCQP) problem, which is NP-hard in general [50]. Thus, (5.13) is NP-hard in general and so is (5.12). □

5.6 Solving PLS Problem

Since the feasibility problem of PLS defined in (5.12) is, in general, NP-hard, we cannot analyze the properties of PLS by directly solving it. Therefore, in this section, we first provide the derivation of a relaxed problem, the solution to which will provide us an upper bound for the feasibility answers to the PLS problem (meaning if the relaxed problem is infeasible, (5.12) is definitely infeasible). Then we introduce a heuristic algorithm which, in most of the feasible situations of problem

(5.12), can actually find a feasible solution through local search around carefully selected starting points. The local-search-based heuristical algorithm essentially serves as our lower bound on the PLS problem (5.12) (meaning that if local search can find a feasible solution, we know problem (5.12) is definitely feasible). Our experiment in Section 5.7 will show that these two bounds are actually very tight and hence can be used as great approximation tools for analyzing the original PLS problem in (5.12).

5.6.1 Relaxation

To get the relaxed problem, first, we add an objective function to problem (5.12), so that when multiple solutions exist, just the one with minimum objective value is returned. Meanwhile, by letting $\mathbf{Q}_k = \mathbf{f}_k {\mathbf{f}_k}^H$, we reformulate the PLS problem as:

$$\begin{aligned} \min_{\mathbf{w}} \quad & obj = \sum_{k=1}^{K} (\mathbf{w}^H \mathbf{Q}_k \mathbf{w} - 1)^2 \\ \text{s.t.} \quad & \mathbf{w}^H \mathbf{Q}_k \mathbf{w} \leq \delta \\ & \mathbf{w}^H \mathbf{Q}_k \mathbf{w} \geq \tfrac{1}{\delta} \\ & k = 1, 2, \cdots, K. \end{aligned} \tag{5.17}$$

The physical meaning of the objective function in (5.17) is the squared error of the approximation in (5.7) and it achieves zero when $|\mathbf{w}^H \mathbf{f}_k|^2 = \frac{v_k |G(\theta_k)|^2}{\hat{v}_k} = 1,\ \forall k \in \{1, \cdots, K\}$. Physically, a weighting vector $\mathbf{w}$ that solves (5.17) produces a beamforming pattern which is closest to the ideal pattern. Meanwhile, if (5.17) can be solved, then the PLS problem in (5.12) can also be solved. This is because if a solution can be found for (5.17), this solution must satisfy (5.17)'s constraints. Since (5.12) and (5.17) have the same constraints, (5.17)'s solution is a solution to (5.12). If (5.17) does not have a feasible solution, we know that (5.12) also does not have any solution.

Since $\mathbf{w}^H \mathbf{Q}_k \mathbf{w} = \text{trace}(\mathbf{w}^H \mathbf{Q}_k \mathbf{w}) = \text{trace}(\mathbf{w}\mathbf{w}^H \mathbf{Q}_k)$, we can recast (5.17) by assuming $\mathbf{X} =$

$\mathbf{w}\mathbf{w}^H$ and get:

$$\begin{aligned} \min_{\mathbf{w}} \quad & obj = \sum_{k=1}^{K} (\text{trace}(\mathbf{X}\mathbf{Q}_k) - 1)^2 \\ \text{s.t.} \quad & \text{trace}(\mathbf{X}\mathbf{Q}_k) \leq \delta \\ & \text{trace}(\mathbf{X}\mathbf{Q}_k) \geq \tfrac{1}{\delta} \\ & k = 1, 2, \cdots, K \\ & \mathbf{X} \succeq 0 \\ & \text{rank}(\mathbf{X}) = 1. \end{aligned} \tag{5.18}$$

By $\mathbf{X} \succeq 0$, we mean that $\mathbf{X}$ is a Hermitian positive semidefinite matrix.

Note that since problem (5.12) is NP-hard in general, so is problem (5.18). Hence, in the following, we will seek a heuristic solution by analyzing a relaxed version of (5.18). Our relaxation is based on the observation that problem (5.18) is very similar to a semidefinite programming problem except that the last constraint "rank$(\mathbf{X}) = 1$" is non-convex. It is known that a semidefinite programming problem is solvable within polynomial time. Hence, we relax problem (5.18) by ignoring the rank constraint and get the following SDR problem.

$$\begin{aligned} \min_{\mathbf{w}} \quad & \sum_{k=1}^{K} (\text{trace}(\mathbf{X}\mathbf{Q}_k) - 1)^2 \\ \text{s.t.} \quad & \text{trace}(\mathbf{X}\mathbf{Q}_k) \leq \delta \\ & \text{trace}(\mathbf{X}\mathbf{Q}_k) \geq \tfrac{1}{\delta} \\ & k = 1, 2, \cdots, K \\ & \mathbf{X} \succeq 0 \end{aligned} \tag{5.19}$$

The SDR problem can be solved efficiently and its optimal solution provides a lower bound for the objective value in (5.17). If the SDR problem has no solution, we are safe to conclude that (5.12) has no feasible solution. This is because the relaxation makes the feasible region of (5.12), which is the same as the feasible region of (5.17), a subset of the SDR problem's feasible region.

In addition, the SDR problem not only provides us a way to weed out infeasible situations, it also can provide us with clues to search for feasible solutions to the PLS problem. Note that due to the relaxation, the optimal solution $\mathbf{X}_{opt}$ to the SDR problem may violate the "rank$(\mathbf{X}) = 1$"

constraint in (5.18). Since (5.18) and (5.12) essentially have the same constraints, this also means that $\mathbf{X}_{opt}$ is not feasible for problem (5.12) in such a case. However, note that $\mathbf{X}_{opt}$ does have the nice property that it satisfies the other constraints in (5.18) which means that it could be close to the feasible region of the original PLS problem. Thus, there may exist feasible solutions to the PLS problem around $\mathbf{X}_{opt}$. Based on this observation, we propose an effective local search algorithm to search for feasible solution to (5.12).

5.6.2 Heuristic Algorithm

While the solution $\mathbf{X}_{opt}$ of (5.19) gives us one starting point of local search for feasible solution to problem (5.12), this single starting point may not be enough. This is because the feasible space of $\mathbf{X}$ that satisfies the constraints of (5.19) is much larger than the feasible space that satisfies (5.18)'s constraints. (satisfying (5.18)'s constraints means satisfying (5.12)'s constraints). Hence, $\mathbf{X}_{opt}$, which is the optimal solution of (5.19), may locate far from the feasible space of (5.18) so that local search around $\mathbf{X}_{opt}$ cannot find a point that satisfies (5.18)'s constraints. To solve this problem, we essentially need to revise (5.19) to give us more starting points for local search. All these starting points must satisfy all the constraints of (5.19) except the rank constraint.

Based on this idea, we use a heuristic algorithm to approximately solve the PLS problem in (5.12) as follows. Our approach is a combination of a local search algorithm and a feasible region partitioning algorithm. First, starting from $\mathbf{X}_{opt}$, the local search algorithm tries to find a feasible solution to the PLS problem. In case that $\mathbf{X}_{opt}$ is far beyond the feasible region of (5.12) so that local search around $\mathbf{X}_{opt}$ fails, the partitioning algorithm segments the feasible region of (5.19) and generates additional starting points for the local search algorithm. These additional starting points enable local search to span more of the feasible region of the SDR problem (5.19), so that the chance of finding a feasible solution to (5.12) enhances. In the following, we describe the details of our partitioning algorithm and local search process.

Partitioning the feasible region

Algorithm 1 shows the procedure of partitioning the feasible region of the SDR problem. A partitioned SDR sub-problem is given by the following form:

$$\begin{aligned} \min_{\mathbf{w}} \quad & \sum_{k=1}^{K} (\text{trace}(\mathbf{ZQ}_k) - 1)^2 \\ \text{s.t.} \quad & \text{trace}(\mathbf{ZQ}_k) \leq b_k \\ & \text{trace}(\mathbf{ZQ}_k) \geq a_k \\ & k = 1, 2, \cdots, K \\ & \mathbf{Z} \succeq 0. \end{aligned} \tag{5.20}$$

where a_k and b_k represent the new bounds defined by the partitioned feasible region pieces. For each k, $[a_k, b_k]$ is chosen to be either $[r(0), r(1)]$ or $[r(1), r(2)]$, with $r(0) = \frac{1}{\delta}$; $r(1) = (\delta + \frac{1}{\delta})/2$; $r(2) = \delta$. Thus, in total 2^K SDR sub-problems can be established. Note that problem (5.20)'s solution $\mathbf{Z}_{opt}$ is the same as $\mathbf{X}_{opt}$ in the following properties: Both $\mathbf{Z}_{opt}$ and $\mathbf{X}_{opt}$ are Hermitian and semidefinite matrix. Both $\mathbf{Z}_{opt}$ and $\mathbf{X}_{opt}$ satisfy the first two constraints of (5.18) but may violate the (5.18)'s last rank constraint.

This partitioning process is initiated when local search around $\mathbf{X}_{opt}$ cannot find a feasible $\mathbf{w}_l$. The SDR sub-problems are tested one by one. For each SDR sub-problem, after getting the solution $\mathbf{Z}_{opt}$, we use a local search algorithm (described in Section 5.6.2) to search for a feasible $\mathbf{w}_l$ that satisfies all constraints in (5.18). If the current SDR sub-problem is infeasible, or the local search algorithm fails in finding a feasible $\mathbf{w}_l$, the next SDR sub-problem is tested. This process stops when either a feasible $\mathbf{w}_l$ is obtained, or all the 2^K SDR sub-problems have been tested.

Local search

The steps of the local search procedure are illustrated in Algorithm 2. In the local search algorithm, candidate solution vectors, $\mathbf{w}_l$, for (5.12) are randomly generated based on a given starting point $\mathbf{X}$. Note that $\mathbf{X}$ is a Hermitian and semidefinite matrix. Hence, we can use Cholesky decomposition to decompose $\mathbf{X}$ into the product of a lower triangular matrix $\mathbf{V}$ and its conjugate transpose, denoted

Algorithm 1 Partitioning of SDR feasible region.

Input: δ

Output: $\mathbf{w}$

1: $r(0) = \frac{1}{\delta},\ r(1) = \frac{\delta + \frac{1}{\delta}}{2},\ r(2) = \delta$
2: **for** $j = 1 \rightarrow 2^K$ **do**
3: $\mathbf{p} \leftarrow j_{(2)}$; {convert j from decimal to binary and store the binary bits into vector $\mathbf{p}$}
4: $a_k = r([\mathbf{p}]_k), b_k = r([\mathbf{p}]_k + 1),\ k = 1, 2, \cdots, K$;
5: Solve problem (5.20);
6: **if** (5.20) is feasible **then**
7: Call Algorithm 2 with input $\mathbf{Z}_{opt}$ and get $\mathbf{w}$.
8: **if** $\mathbf{w} \neq$ NULL **then**
9: Return $\mathbf{w}$;
10: **end if**
11: **end if**
12: **end for**

as: $\mathbf{V}\mathbf{V}^H = \mathbf{X}$. A candidate vector is created by multiplying $\mathbf{V}$ by a randomly generated vector.

We adopt two effective methods for random vector generation which have been used by [76]. In the first method, we let $\mathbf{w}_l = \mathbf{V}\mathbf{e}_l$, where $\mathbf{e}_l$ is on the unit sphere of the N_{ant}-dimensional space of complex numbers, with each of its element having a phase uniformly distributed on $[0, 2\pi)$. In the second method, we let $\mathbf{w}_l = \mathbf{V}\mathbf{u}_l$, and $\mathbf{u}_l$ has both the real and the imaginary parts of each element following independent standard Gaussian distribution.

Suppose the randomization is repeated N_s times. Each time we put $\mathbf{w}_l$, generated by the two methods, into the PLS problem (5.12) and check if $\mathbf{w}_l$ satisfies all the constraints. After N_s randomization runs, if none of the $\mathbf{w}_l$ satisfies (5.12)'s constraints, we claim that the local search fails.

Algorithm 2 Randomization based local search.

Input: $\mathbf{X},\ \mathbf{Q}_k,\ \delta,\ N_s$

Output: $\mathbf{w}$

Initialize $\mathbf{w} = \text{NULL}$;
Generate $\mathbf{V}$ such that $\mathbf{V}\mathbf{V}^H = \mathbf{X}$;
for $i = 1 \rightarrow N_s$ **do**
  Generate a N_{ant} by 1 vector $\mathbf{e}_l$ on the unit sphere of $\mathbb{C}^{N_{ant}}$;
  Test the feasibility of (5.12) with $\mathbf{w}_l = \mathbf{V}\mathbf{e}_l$;
  if feasible **then**
    Return $\mathbf{w} = \mathbf{w}_l$;
  end if
  Generate a N_{ant} by 1 vector $\mathbf{u}_l$ with
  $Re\{[\mathbf{u}_l]_i\} \sim \mathcal{N}(0,1)$ and $Im\{[\mathbf{u}_l]_i\} \sim \mathcal{N}(0,1)$
  $i = 1, 2, \cdots, N_{ant}$;
  Test the feasibility of (5.12) with $\mathbf{w}_l = \mathbf{V}\mathbf{u}_l$;
  if feasible **then**
    Return $\mathbf{w} = \mathbf{w}_l$;
  end if
end for

Discussions of the heuristic algorithm

At worst, our heuristic algorithm might have to test all the 2^K SDR sub-problems before providing a heuristic solution to the PLS problem (5.12). Nevertheless, according to our simulations, checking all the 2^K SDR sub-problem can be finished within several minutes with $K \leq 10$. Meanwhile, when $K \geq N_{ant}$, in our simulations, the SDR problem in (5.19) is almost always infeasible and the PLS problem (5.12) is answered as infeasible instantly. Hence, the only challenging part for the heuristic algorithm is when N_{ant} is fairly large $(N_{ant} > 10)$, which is unlikely to happen due to the physical limitation on the number of antenna elements of an antenna array in practical antenna

engineering. In addition, although large N_{ant} may theoretically yield feasible solutions for K that is larger than 10, such solutions are usually not usable in practical scenarios. This is because these solutions are very sensitive to the exact fine-tuning of the antenna pattern such that normal fuzziness in the radiation pattern due to reflection and diffraction of the radio signal usually invalidate their feasibility.

Following our SDR based heuristic algorithm, the PLS feasibility problem (5.12) could end up in three different cases. In the first case, the SDR problem in (5.19) is infeasible, which indicates that the PLS problem (5.12) is also infeasible. In the second case, the SDR problem is feasible and a feasible $\mathbf{w}$ to the PLS problem is obtained using our heuristic algorithm. Then it is sufficient that PLS in this case is feasible. In the third case, the SDR problem is feasible, but our heuristic algorithm returns no feasible $\mathbf{w}$ for (5.12). The feasibility of the PLS problem is unknown. Essentially, these three cases show that the feasibility answer to the PLS problem lies in between the feasibility answer to the SDR problem and the feasibility answer of our heuristic solution. Hence, the solution to the SDR problem and our heuristic solution can be seen as an upper bound and a lower bound for the PLS problem in (5.12), respectively. Fortunately, our experiments show that the third case appears very rarely. This essentially means that the feasibility answer to the PLS problem (5.12) is tightly bounded by the feasibility solution of the SDR problem and our heuristic algorithm.

5.7 Simulation Results

In this section, we simulate the SDR relaxed problem and the heuristic algorithm described in Section 5.6 to analyze the feasibility of PLS under different circumstances. Through the analysis, we discuss guidelines for deployment of localization systems and possible solutions to defend against beamforming-based PLS attacks. Our simulation also confirms that our relaxed SDR problem and the local-search heuristic algorithm provide very tight bounds on the PLS problem (5.12). The SDR problems in the simulations are solved using cvx [29] in MATLAB environment on a desktop

with Intel 2.8G Hz CPU and 3Gb memory.

In the simulations, we also add the practical consideration about possible beamforming aiming error. In practice, there might be a small aiming error when the attacker points the beamforming pattern to the anchors. Thus, we require that the beamforming pattern for PLS also satisfies the following additional constraints,

$$\frac{1}{\delta} \leq \frac{v_k}{\hat{v}_k}|G(\theta_k \pm \gamma_\theta)|^2 \leq \delta,\ k = 1, 2, \cdots, K. \tag{5.21}$$

where γ_θ represents a small angle of aiming error. Otherwise, only a small aiming error could fail the location spoofing attack. The following simulation results are obtained by assuming $\gamma_\theta = 1^\circ$.

5.7.1 Fixed Spoofing Distance

First we analyze the feasibility of PLS attacks with fixed true location (x, y) and fake location $(\hat{x}, \hat{y})$ under different anchor deployments. This part of analysis shows the capability of PLS attacks. We randomly generate anchors in a $200\times200m^2$ 2-D space. They are spaced reasonably far enough from each other to mimic real system deployment since a real localization system rarely have two anchors sit very close to each other. The path loss exponent α is set to be $\alpha = 3$. The attacker's true location is (0,0) and the fake location is (30, 40).

PLS Beamforming Pattern

An example of the beamforming pattern of a PLS attack is shown in Figure 5.3. From the figure, we can see how the beamforming pattern compensates the differences between the path loss vector from the true location (x, y) to the anchors and the path loss vector from the fake location $(\hat{x}, \hat{y})$. Towards the directions of anchors which are closer to the fake location than to the true location, the directional gain is comparatively large. On the contrary, for the anchors which are closer to the true location, the directional gain is much smaller. In this way, the overall effect of beamforming together with the natural path loss makes the RSS reading vector at the anchors seems as if they are generated by signal transmitted from the fake location.

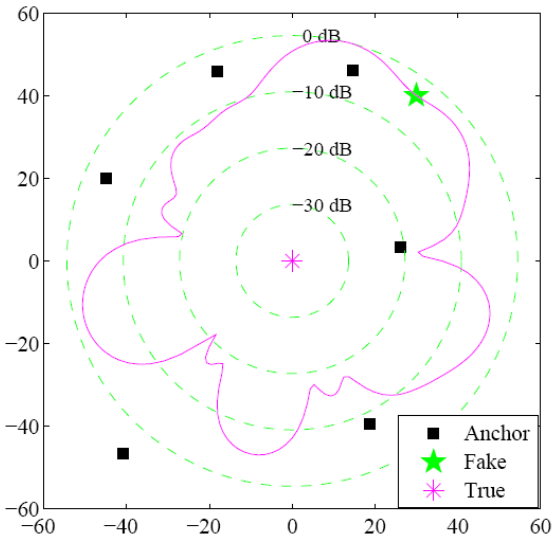


Figure 5.3: A beamforming pattern of PLS.

Success Rate of PLS

We use Monte Carlo simulations to estimate the success rate of PLS with different combinations of the number of antenna elements (N_{ant}) and the number of anchors (K) in the 2-D space. In each simulation run, the locations of the anchors are randomly generated. We also vary the value of the noise threshold δ from 1 dB to 3 dB. For each combination of parameters, totally 200 simulation runs are launched. The number of times where the local-search heuristic algorithm can find feasible solutions (N_{heuri}) and the situations where the relaxed SDR problem has solutions(N_{relax}) are recorded in Table 5.1. Note that the heuristic algorithm provides a lower bound on the original PLS problem at (5.12), while the SDR solutions provide an upper bound. Hence, the number of times that the original PLS problem has feasible solutions lies in between N_{heuri} and N_{relax}.

Three general trends in Table 5.1 can be observed. First, both N_{relax} and N_{heuri} increase when the number of antenna elements N_{ant} increases. The reason is that smart antenna array with more elements has more flexibility in tuning the radiation pattern, and hence is more capable in creating PLS attacks. Mathematically, more antenna elements leads to more tunable $[\mathbf{w}]_i$ and hence larger degree of freedom in the problems. Second, the success rates of the two problems tend to increase

Table 5.1: Number of successful cases out of 200 simulation runs. (N_{heuri}/N_{relax})

δ	K	N_{ant}=6	N_{ant}=8	N_{ant}=10	N_{ant}=12
1dB	4	66/70	142/160	170/181	175/192
	5	4/7	78/97	93/152	106/182
	6	0/0	20/34	43/97	31/162
	7	0/0	0/5	16/64	9/95
	8	0/0	0/0	3/29	1/33
2dB	4	96/96	129/129	171/172	180/181
	5	10/11	105/107	148/148	165/170
	6	0/0	55/56	110/110	134/141
	7	0/0	15/15	81/84	97/107
	8	0/0	1/1	43/50	74/78
3dB	4	80/84	144/145	169/169	186/188
	5	15/16	117/120	148/152	170/176
	6	0/0	60/62	117/120	133/145
	7	0/0	18/20	99/100	100/107
	8	0/0	0/1	44/47	78/86

when the value of the threshold δ increases. This is because greater value of δ means looser bounds and larger feasible region of the PLS problem. Third, both N_{relax} and N_{heuri} decrease when K increases. Mathematically, adding anchors means adding extra constraints to problem (5.12), so that the feasible region decreases.

Another noticeable aspect of Table 5.1 is that the gap between N_{heuri} and N_{relax} is related to the noise threshold δ which indicates the natural variance in path loss. The smaller the δ, the larger the gap. Since the number of times that the PLS problems in (5.12) is feasible falls in between N_{heuri} and N_{relax}, smaller gap between N_{heuri} and N_{relax} indicates better approximate solutions to

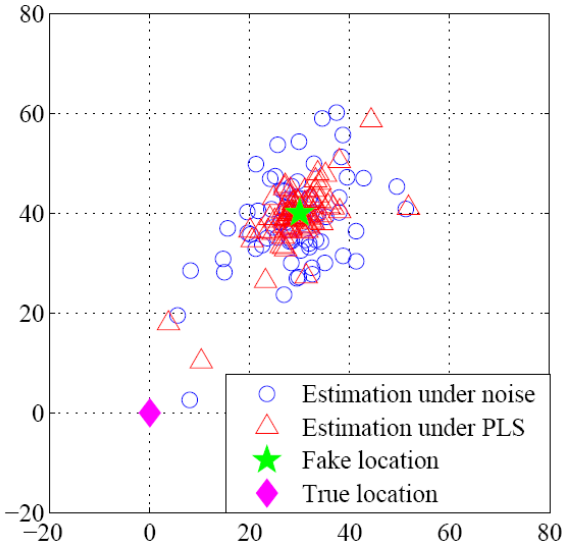


Figure 5.4: Spoofed localization results v.s. noised localization results.

the PLS problem (5.12). Fortunately, in real environment, the natural path loss variance is much larger than 1dB (often in the range of 3-8 dB). Hence, we can expect that the gap between N_{heuri} and N_{relax} is very small in most of the real environments.

Location Estimation under PLS Attacks

Remember that when we formulate the PLS problem, we claim that the RSS readings of the attacker at anchors do not need to be exactly the same as the RSS readings of a legitimate user at the target fake location. As long as the RSS readings of the two situations are close enough, localization systems cannot tell location spoofing from normal variations in path loss. To demonstrate this point, we test least square estimation (LSE) as an example of location estimation algorithm. We compare the location estimates produced by the LSE algorithm under PLS attacks with that under normal path loss variations. For the PLS attacks, we chose the threshold as $\delta = 1$ dB, and the normal path loss variation is modeled as Gaussian noise with variance 1 dB. The output location estimation results for 200 simulation runs are shown in Figure 5.4. We can see that the localization results under PLS attacks are all around the fake location and within the error range of typical

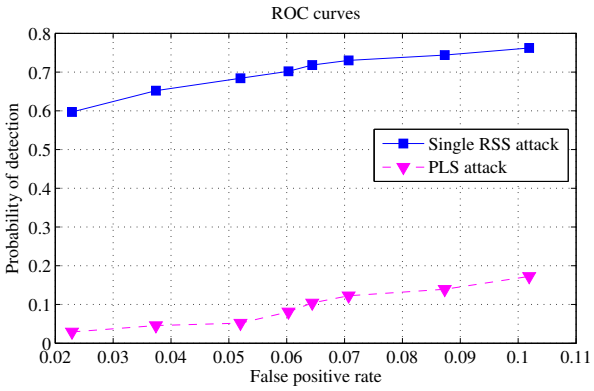


Figure 5.5: ROC curves of attack detection.

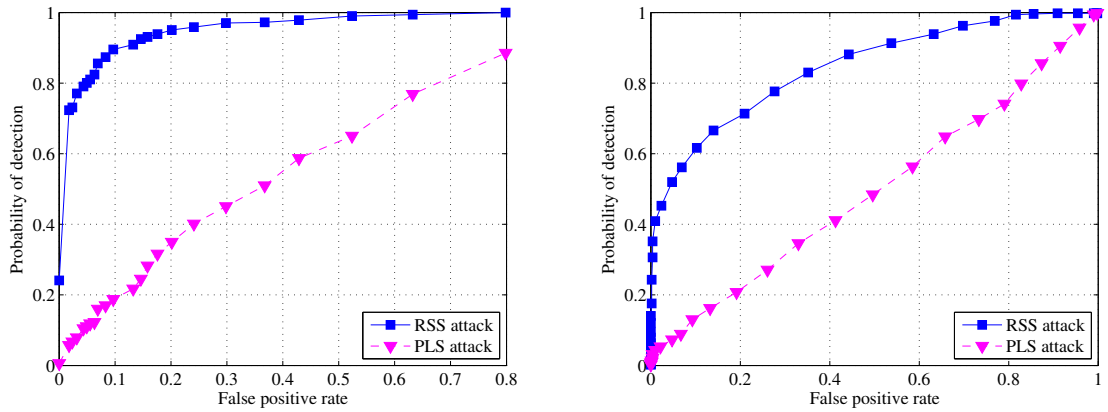
estimation results for legitimate users under normal path loss variations.

5.7.2 Attack Detection under PLS

To get an insight into how PLS attacks are difficult to detect, we evaluated the performance of the attack detection schemes introduced in [17] and [45] under PLS.

First we compare the detection rates under PLS attack and single RSS attack using the location spoofing attack detection algorithm introduced in [17], where the regression residuals of Linear Least Squares (LLS) are utilized to detect RSS attacks. The results after 1000 simulation runs are shown in Figure 5.5 and the settings for PLS attack is the same with Figure 5.4. The single RSS attack is simulated by adding a 30 dB bias to one of the RSS measurements. By comparing the ROC curves, we can see that the detection rates under PLS attacks are much lower and close to the false positive rates, which makes the attack detection algorithm almost invalid.

It might not be surprising that the algorithm in [17] is ineffective for PLS attacks since it is not designed with the consideration of beamforming attacks. Therefore, we further simulate algorithms that are intended to detect beamforming attacks to RSS localization systems. In [45] two schemes are proposed to use statistical and pattern matching techniques to detect location spoofing attacks based on the assumption that in normal conditions, location estimates using RSS and differential



(a) Attack detection with RED.

(b) Attack detection with TRFM.

Figure 5.6: Performance of RED and TRFM degenerates under PLS attacks.

received signal strength (DRSS) are geographically close. The first scheme is called relative error detection (RED). This method uses the norm of the relative error between RSS location estimation and DRSS location estimation as the anomaly measure for the hypothesis testing problem. RED is simple while effective against signal strength attacks. However, the authors observe that it does not perform well under beamforming attacks. Therefore, the authors propose another method which is called topological residual fingerprint matching (TRFM) which uses bilateral dissimilarity of the global topological error signature to detect location spoofing attacks. The residual finger print is a matrix which characterizes the streamlines that connect the critical points (anchors and location estimates). TRFM is shown to be effective for general beamforming attacks, however, we will show that it cannot effectively detect PLS attacks because of the carefully designed beamforming pattern of PLS attacks.

Figure 5.6 shows the ROC curves of attack detection using both RED and TRFM. For RSS attacks, a 30 dB bias is added to one of the RSS readings. As we can see, both RED and TRFM can effectively detect RSS attacks. However, under PLS attacks their false alarm rate is almost the same as the detection rate indicating that PLS attack actually invalidates both schemes. The reason that even TRFM cannot detect PLS attacks is that the carefully designed beamforming pattern coordinates the expected RSS readings at all the anchors within coverage so that the DRSS measurements

are almost the same as the DRSS measurements for signal transmitted from the target fake location, while naive beamforming attacks without such consideration do not hold such property.

To have a better understanding of why RED and TRFM fail for PLS attacks, we present the visualization of the topological residual fingerprints for normal shadow noise and PLS attack situations in Figure 5.7. For both cases, the transmitter is at the origin of the coordinates. The target fake location for PLS attack is $(30, 40)$. Figure 5.7(a) and 5.7(b) show the topological residual fingerprints for RSS and DRSS localization with normal shadow noise and Figure 5.7(c) and 5.7(d) are corresponding to the situations under PLS attacks. The level curves represent different levels of the LSE error function and the streamlines are instantaneously tangent to the negative gradient of the error function [45]. These streamlines start from the anchors and converge to the estimated transmitter positions marked by red dot for RSS estimation and green pentagon for DRSS estimation respectively. The idea of RED is to detect location spoofing attacks using the geometrical distance between the RSS estimation and the DRSS estimation. However, as shown in Figure 5.7, with a successful PLS attack, the RSS and the DRSS location estimates are as close as it is for the normal noise situation. Thus RED is not able to differentiate them. Differently, TRFM takes into account the global feature of the error function and assumes that location spoofing attacks will cause topological dissimilarity between the streamlines of RSS and DRSS localization. Unfortunately, we can observe that the streamlines in Figure 5.7(c) and 5.7(d) actually have very similar topology. By comparing the topological similarity of the streamlines in Figure 5.7, we are not able to differentiate the PLS attack case and the shadow noise situation. This explains that PLS attacks are undetectable with RED and TRFM.

5.7.3 Fixed Anchor Deployment

In this part, we investigate how the feasibility of PLS is affected by the anchor deployment and the relative position of the attacker's true location with respect to the anchors. In the simulations, the fake location $(\hat{x}, \hat{y})$ and the anchor locations are all fixed. We vary the true location (x, y) along a quare grid in the whole simulated 2-D space to identify the feasible locations where the attacker

can launch PLS attacks.

A group of simulation results are shown in Figure 5.8. The parameters used in the simulations are $N_{ant} = 10,\ \delta = 2$ dB, $K = \{5, 6, 7, 8\}$. In Figure 5.8, the asterisk represents a true location (x, y) of the attacker where our heuristic algorithm has found feasible solutions to the PLS problem in (5.12). In other words, at the locations marked by asterisks, the attacker is able to successfully spoof his/her location to the fake location (shown as green pentagram in the center of the figure) using our heuristic algorithm. The blue diamonds represent true locations where the SDR problems are feasible. All the other locations on the grid without marks are locations where PLS is impossible. In the figure, most off the locations where SDR problems are feasible are also marked by asterisks (sign of feasible PLS problem). This implies that the answers to the PLS problem (5.12) are tightly bounded by solutions to the SDR problem and the solutions to our heuristic algorithm.

Anchor Density

By comparing the four graphs in Figure 5.8, we find that when the anchor density increases, the attacker has less choices of locations to launch a successful PLS attack. This indicates that higher density of anchor deployment is effective in lowering the success rate of PLS attacks in the 2-D geometric space.

Geometry of Anchor Deployment

We also observe that most of the asterisks are within an area which is bounded by the nearest surrounding anchors around the fake location. Meanwhile, if we pay attention to the blank space among the asterisks, we can find that it is almost always in the extending directions of a segment connecting a pair of anchors. This phenomenon is most obvious in Figure 5.8(b), however, it actually happens to all of the four graphs, as very few asterisk or diamond marks exist in the extending directions of the line segments joining a pair of anchors. We want to briefly raise this interesting observation here. Detailed analysis of this observation and how it can be helpful for

attack resistant anchor deployment will be presented in the next section.

Based on the above observations, we conclude that generally anchor deployment with higher density not only lowers the success rate of PLS attacks, but also limits the possible hiding locations of an attacker to be close to the fake location. In other words, the attacker's feasible spoofing distance is smaller, and hence, the capability of location spoofing attacks is weakened.

5.8 Guard Against Location Spoofing Attacks

This section presents guidelines for spoof resistant anchor deployment based on the simulation results. Generally, increasing the anchor density is good for guard against location spoofing attacks. However, uniformly increasing the anchor density could be expensive or unnecessary. It will be more efficient to design the anchor deployment according to the practical security requirements and specific characteristics of the application environment.

5.8.1 Preventing Attacks from Unsecured Region

It is common that the security level of subregions of a large area can differ a lot due to the geometry of natural or manmade barriers. Usually regions with open or easy access are more likely to be the hideout of attackers such like a public parking lot close to the secured building. In this part, we provide method for eliminating potential PLS attacks within such unsecured regions based on previous observations from the simulation results. As mentioned in Section 5.7.3, locations collinear with a pair of anchors but not in between the anchors are usually not feasible hiding positions for an attacker to launch successful PLS attack. Here we use mathematical analysis to explain why it happens and how we can take advantage of this property to guard against PLS attacks from a particular region.

Assume the attack's true location is (x, y). Two anchors located at (x_a, y_a) and (x_b, y_b) are in the same relative direction with respect to (x, y) as shown in Figure 5.9. The direction of the two

anchors satisfies

$$\begin{aligned} &\theta_a = \theta_b, \\ &\cos\theta_k = \frac{x_k - x}{\sqrt{(x_k-x)^2+(y_k-y)^2}}, \\ &\sin\theta_k = \frac{y_k - y}{\sqrt{(x_k-x)^2+(y_k-y)^2}}, \\ &k \in \{a, b\}. \end{aligned} \tag{5.22}$$

The target fake location is noted as $(\hat{x}, \hat{y})$. Based on (5.3) and (5.8), we can get the PLS requirements defined merely for these two anchors.

$$\frac{1}{\delta} \leq \frac{v_a}{\hat{v}_a}|G(\theta_a)|^2 \leq \delta \tag{5.23}$$

$$\frac{1}{\delta} \leq \frac{v_b}{\hat{v}_b}|G(\theta_b)|^2 \leq \delta \tag{5.24}$$

Since $\theta_a = \theta_b$, by dividing (5.23) with $\frac{v_b}{\hat{v}_b}|G(\theta_b)|^2$, we can get the following relationship.

$$\frac{1}{\delta^2} \leq \frac{v_a \cdot \hat{v}_b}{v_b \cdot \hat{v}_a} \leq \delta^2 \tag{5.25}$$

As the attacker's true location and the two anchors' location are already known, the distances from the attack to the two anchors are actually a constant given by

$$C = \frac{[(x_a - x)^2 + (y_a - y)^2]^{1/2}}{[(x_b - x)^2 + (y_b - y)^2]^{1/2}}. \tag{5.26}$$

Based on (5.3), (5.25) and (5.26), we can deduce that

$$\frac{1}{\delta^{2/\alpha} \cdot C} \leq \frac{[(x_b - \hat{x})^2 + (y_b - \hat{y})^2]^{1/2}}{[(x_a - \hat{x})^2 + (y_a - \hat{y})^2]^{1/2}} \leq \frac{\delta^{2/\alpha}}{C}. \tag{5.27}$$

(5.27) is a necessary but not sufficient condition for a feasible PLS attack. This condition is wholly determined by the relative geometry of the attacker's true location relative to the two anchors and is irrelevant to the directional gain of the attacker's antenna. Hence the attacker cannot use different directional gain of beamforming to satisfy this constraint. Figure 5.10 demonstrates the feasible region defined by (5.27), with $\delta = 3$ dB. The anchors are at $(0, 0)$ and $(100, 0)$. The attack's true location varies in the four subfigures in Figure 5.10 from $(-100, 0)$ to $(-25, 0)$. The green region represents the potential fake locations that could satisfy condition (5.27). This region is bounded by two circles which are corresponding to the upper and lower limits in (5.27).

Figure 5.10 shows that the constraint (5.27) significantly limits the potential fake locations for PLS attacks no matter what smart antenna is used by the attacker and how it's beamforming pattern is designed. Meanwhile, as the attacker's true location gets closer to the two anchors, the feasible region of condition (5.27) is shrinking dramatically and further limited to be close to the attacker's true location. Remember that the current feasible region is obtained by only considering the two anchors that are shown in the figures. Thus, when we take into account all the other anchors within the coverage area of the attacker's radio, the final feasible region of possible fake locations will be much more smaller due to the additional constraints, which also means for a random fake location, the possibility of successful PLS attack will be significantly lower. Hence we draw the conclusion that locations collinear with a pair of anchors on one side of it tend to be infeasible for launching PLS attacks.

Examples of how the relative geometry of anchor deployment affects the chances of PLS attack in a particular region are given by Figure 5.11. There are 4 anchors in Figure 5.11(a) and 5 anchors in Figure 5.11(b) and the target fake location is at the origin of the coordinates. The asterisks represent locations where the attacker is able to successfully spoof to the fake location. A and B are two square regions with the same size. However, in both cases, region A has a much lower chance of having PLS attacks inside compared with region B, because region A is roughly covered by the pairwise connecting lines of the anchors. Therefore, to make sure that adversaries in an open access region cannot spoof to be in the guarded crucial region, anchors should be placed in a way that makes the unsecured region covered by the lines passing through the anchor pairs.

5.8.2 Guarding Critical Location

Another possible case is that some special locations have high privileges and it is necessary to make sure attackers cannot spoof to these positions. According to the simulation results shown in Figure 5.8 and Figure 5.11, with a high density of nearby anchors around the target fake location, PLS attack is feasible only if the attackers are physically inside the region bounded by the surrounding anchors, which is actually very close to the target fake location. Therefore, it is desirable

to put more anchors around crucial areas where it is highly dangerous if an attacker can fake to be inside this area.

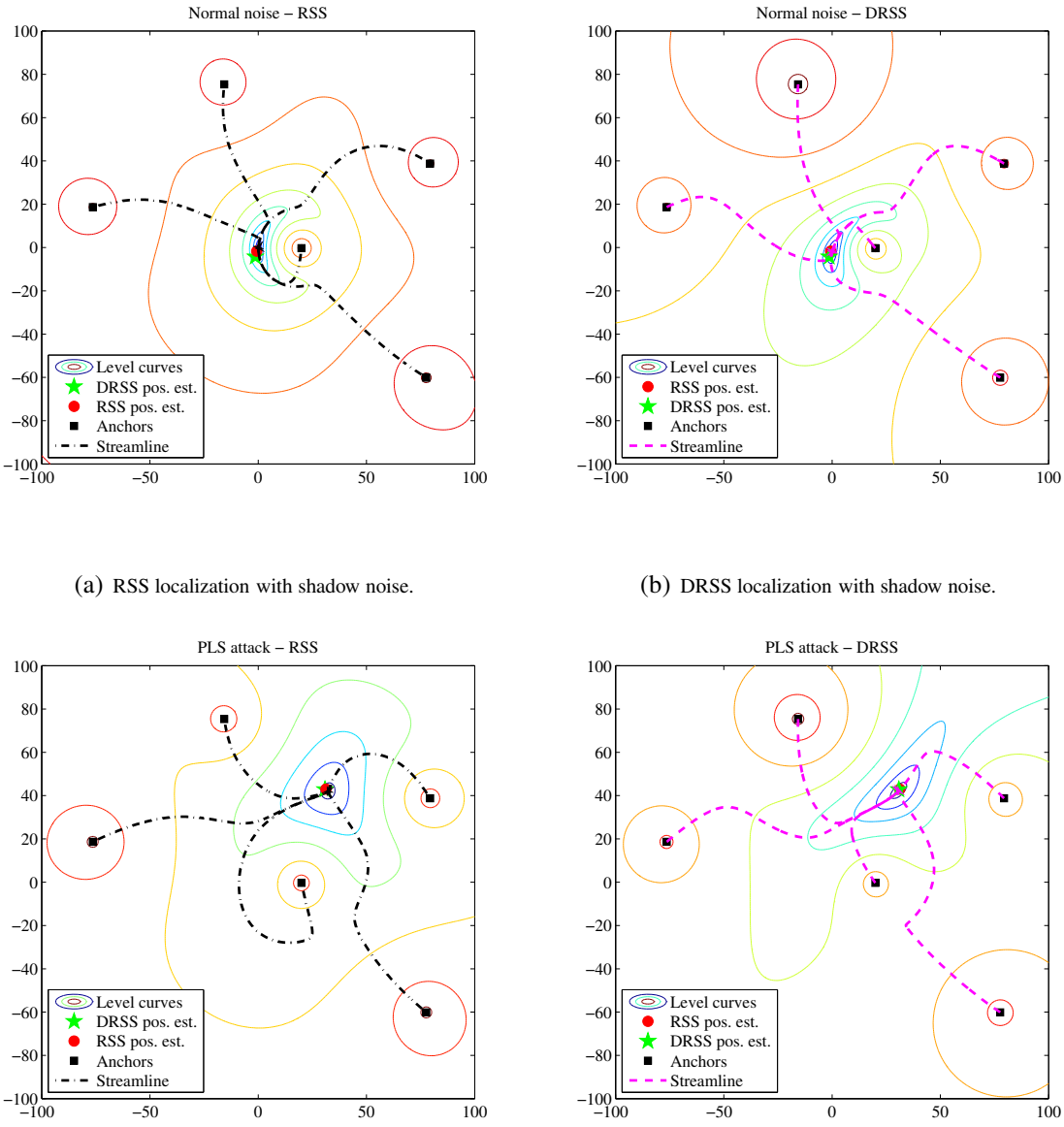
5.8.3 Mobile Anchor

Another way to tackle PLS attack to RSS localization systems is to use mobile anchors. The mobility of anchors makes it extremely difficult for the attacker to locate the anchors. Hence, the attacker will not be able to figure out a desired beamforming pattern to launch PLS attack.

In sum, our analysis can be used to find the weakness of a given anchor deployment and effectively improve it to prevent PLS attacks. Furthermore, our analysis also can be used to trace location spoofing attackers. When a PLS attack is discovered by means outside of localization systems, our analysis could help to narrow down the possible hiding locations of the attacker since PLS can only happen in certain areas.

5.9 Chapter Summary

In this chapter, we analyzed the feasibility of PLS attacks using beamforming and investigated its relationship with the anchor deployment of localization systems. We utilized SDR technique and a heuristic local search algorithm to efficiently solve the PLS feasibility problem which is NP-hard in general. Simulation results show that our approach provides great approximation to the PLS feasibility problem. Meanwhile, it is indicated that higher anchor density generally performs better in resisting PLS attacks and the geometry of anchor deployment also plays an important role for reginal defense against PLS attacks. Based on the analysis and simulation results, we provide insightful guidance for spoofing resistant anchor deployment.



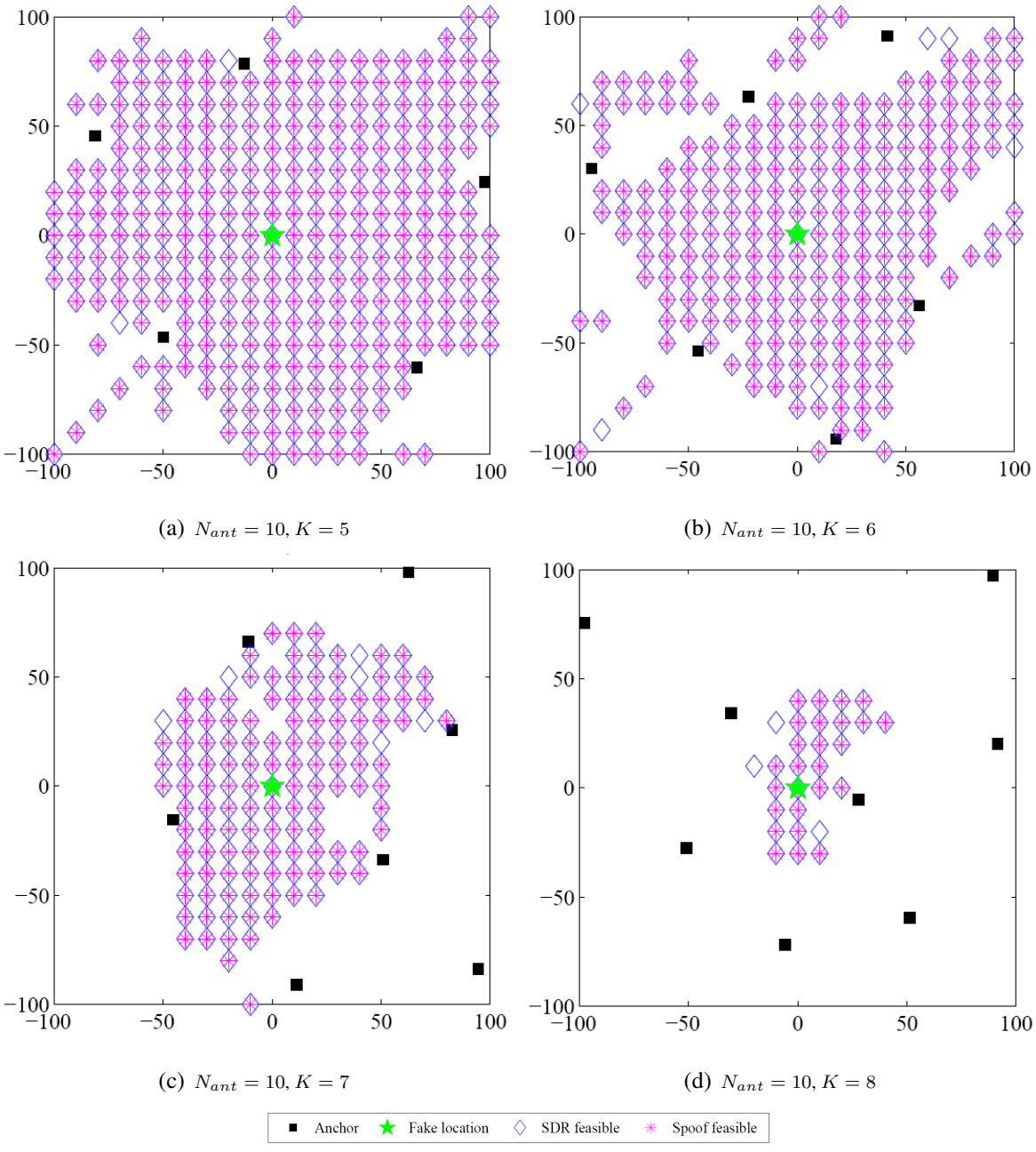
(a) RSS localization with shadow noise.

(b) DRSS localization with shadow noise.

(c) RSS localization under PLS attack.

(d) DRSS localization under PLS attack.

Figure 5.7: Visualization of topological residual fingerprints with transmitter located at the origin.



(a) $N_{ant} = 10, K = 5$

(b) $N_{ant} = 10, K = 6$

(c) $N_{ant} = 10, K = 7$

(d) $N_{ant} = 10, K = 8$

Figure 5.8: Geometrical statistic of location spoofing feasibility with random generated anchors.

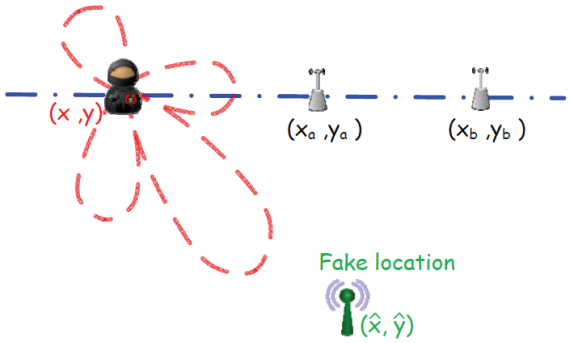


Figure 5.9: Attacker's location is collinear with two anchors.

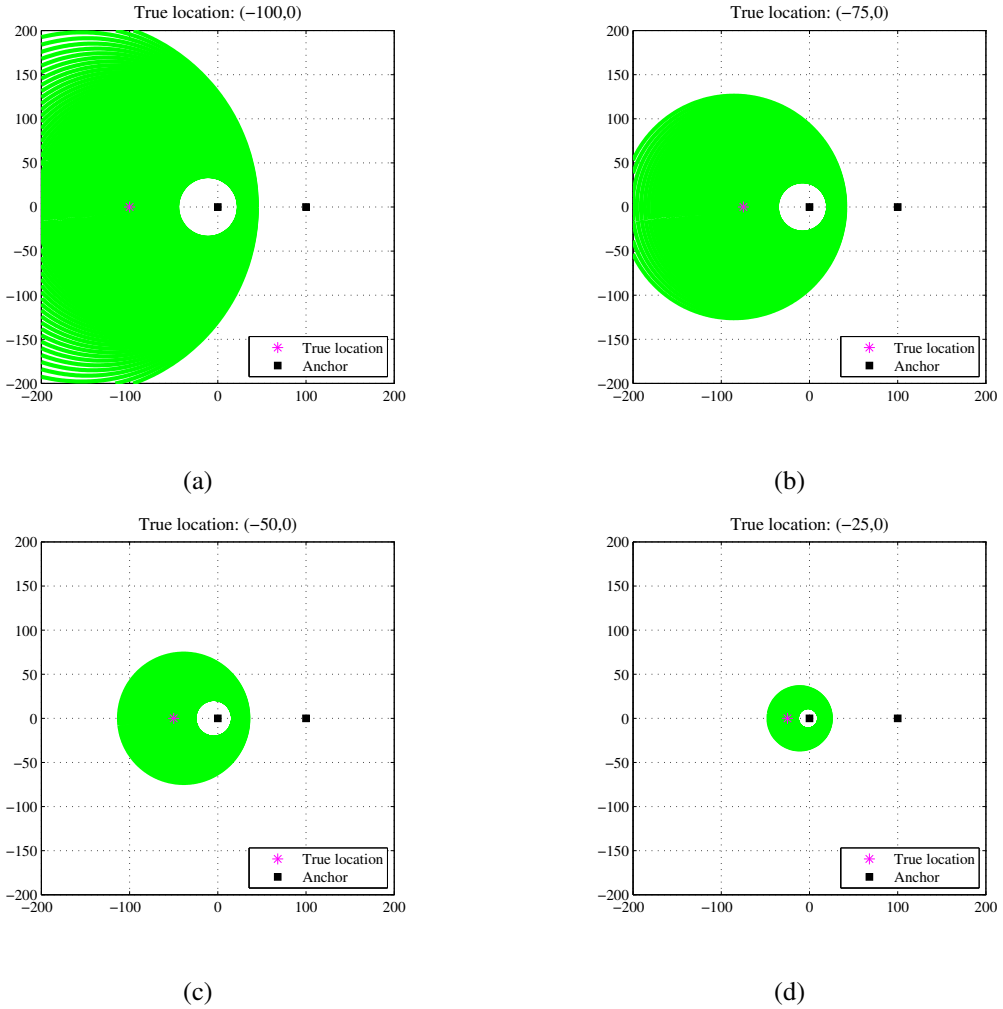


Figure 5.10: Feasible region with two anchors in the same direction ($\delta = 3$ dB).

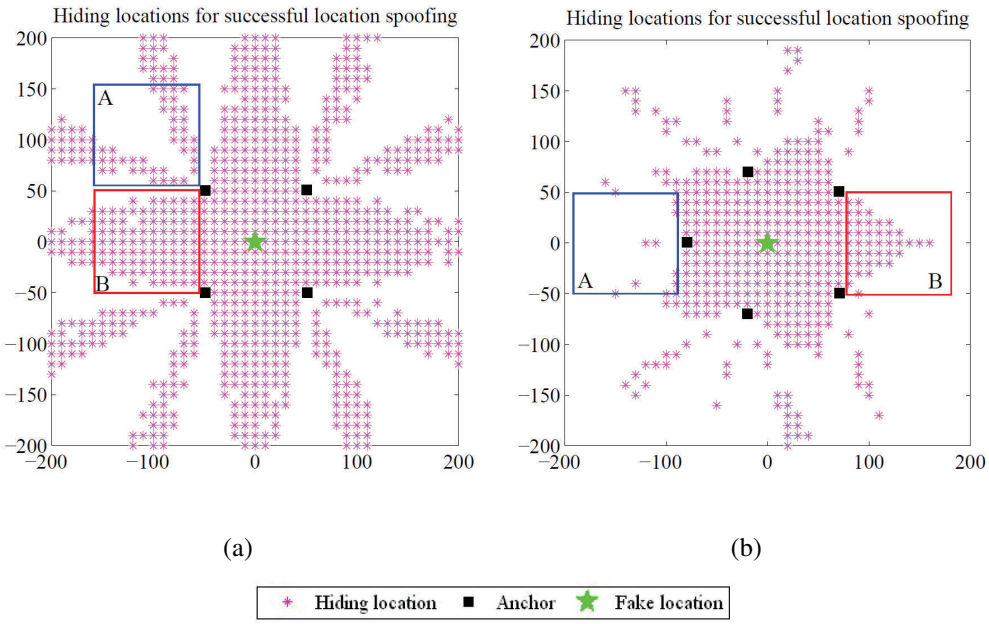


Figure 5.11: Geometrical statistic of location spoofing feasibility.

Chapter 6

Conclusions

In this dissertation, security and privacy issues in the wireless network physical layer are studied. In particular, we address the problems of anti-eavesdropping and location privacy protection using the smart antenna technique.

For the topic of communication privacy, a novel artificial fading scheme is proposed in Chapter 3. Although smart antennas are known for their capability of concentrating transmit power to a target direction, and this property has already been used to reduce the unnecessary coverage area for anti-eavesdropping purpose, our study shows that by using double-beam switching of the smart antenna array and optimizing the switched beam patterns, we can achieve even more deduction of the unnecessary coverage area. The method for generating artificial fading is that we optimize a pair of beamforming patterns, such that they both provide good signal quality to the intended receiver, while their overlap apart from the intended direction is minimized. The transmitter switches between the two optimized patterns at a high frequency to produce severe signal fading in undesired directions. Simulation results show the effectiveness of the proposed artificial fading scheme in reducing the unnecessary coverage, and we observe a tradeoff between the total transmit power consumption and the reduction of the unnecessary coverage area.

From the perspective of location privacy protection, we present a two-step location privacy preser-

vation scheme in Chapter 4. We assume that the attacker is using RSS based localization system to pinpoint wireless users, and APs are used to collect RSS measurements of the users' signals. The first step of the scheme is to passively estimate the locations of nearby APs through a war-driving process. In the second step, based on the estimated AP locations, two pattern optimization strategies are used to prevent the positioning system from correctly localizing the mobile user, and at the same time, keep the communication quality of the wireless user intact. The first strategy is to minimize the number of APs that can hear the signal of the mobile user, so that the adversary does not have enough RSS measurements to get a unique location estimation result. The second strategy is to use the genetic algorithm to maximize the bias to the positioning system. Simulation results show that our strategies can significantly lower the chance of being localized and substantially degenerate the location estimation precision.

Chapter 5 investigates the feasibility of beamforming-based PLS attacks and provides guidelines for corresponding defense strategies. This problem is closely related to the location privacy problem in Chapter 4, but from a completely different point of view. The fundamental difference is that for PLS attacks, the attacker targets at a specific fake location, and if the attack successes, it can fool the location based security mechanism and enable other potential threats. We formulate the problem of PLS attack as a nonlinear programming problem. Because of its NP-hardness, we solve this feasibility problem using the SDR technique together with a heuristic local search algorithm. Simulation results validate the effectiveness of our approach and provide clues to possible countermeasures. We show that the geometry of the anchor deployment has a big impact on the spacial distribution of potential PLS attacks. Schemes for improving anchor deployment to prevent PLS attacks are discussed.

Chapter 7

Bibliography

[1] Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Std 802.11-2007*.

[2] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati. Supporting location-based conditions in access control policies. In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, ASIACCS, 2006.

[3] M. Azizyan, I. Constandache, and R. Roy Choudhury. Surroundsense: mobile phone localization via ambience fingerprinting. In *Proceedings of the 15th annual international conference on Mobile computing and networking*, MobiCom '09, pages 261–272, New York, NY, USA, 2009. ACM.

[4] P. Bahl and V. N. Padmanabhan. Enhancements to the radar user location and tracking system. Technical report, Microsoft Research, 2000.

[5] P. Bahl and V. N. Padmanabhan. Radar: an in-building rf-based user location and tracking system. In *Proceedings of IEEE INFOCOM*, 2000.

[6] P. Bao and M. Liang. A security localization method based on threshold and vote for wireless sensor networks. *Procedia Engineering*, 15(0):2783–2787, 2011.

[7] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker. The directional attack on wireless localization: how to spoof your location with a tin can. In *Proceedings of IEEE GLOBECOM*, 2009.

[8] K. Bauer, D. Mccoy, B. Greenstein, D. Grunwald, and D. Sicker. Physical layer attacks on unlinkability in wireless lans. In *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies*, PETS '09, 2009.

[9] S. Bellofiore, C. Balanis, J. Foutz, and A. Spanias. Smart-antenna systems for mobile communication networks. part 1. overview and antenna design. *IEEE Antennas and Propagation Magazine*, 44(3):145–154, Jun 2002.

[10] S. Bellofiore, J. Foutz, R. Govindarajula, I. Bahceci, C. Balanis, A. Spanias, J. Capone, and T. Duman. Smart antenna system analysis, integration and performance for mobile ad-hoc networks (MANETs). *IEEE Transactions on Antennas and Propagation*, 50(5):571–581, May 2002.

[11] N. Bulusu, J. Heidemann, and D. Estrin. Gps-less low-cost outdoor localization for very small devices. *IEEE Personal Communications*, 7(5):28–34, Oct 2000.

[12] J. Carey and D. Grunwald. Enhancing WLAN security with smart antennas: a physical layer response for information assurance. In *Proceedings of IEEE Vehicular Technology Conference*, 2004.

[13] D. Chasaki, Q. Wu, and T. Wolf. Attacks on network infrastructure. In *Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, 2011.

[14] Y. Chen, J.-A. Francisco, W. Trappe, and R. Martin. A practical approach to landmark deployment for indoor localization. In *Proceedings of IEEE SECON*, volume 1, pages 365–373, 2006.

[15] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. P. Martin. The robustness of localization algorithms to signal strength attacks: a comparative study. In *Proc. Intl Conf. Distributed Computing in Sensor Systems (DCOSS)*, 2006.

[16] Y. Chen, D. Lymberopoulos, J. Liu, and B. Priyantha. Fm-based indoor localization. In *Proceedings of the 10th international conference on Mobile systems, applications, and services*, MobiSys '12, pages 169–182, New York, NY, USA, 2012. ACM.

[17] Y. Chen, W. Trappe, and R. P. Martin. Attack detection in wireless localization. In *Proceedings of IEEE INFOCOM*, 2007.

[18] Y. Chen, W. Trappe, and R. P. Martin. Detecting and localizing wireless spoofing attacks. In *Proceedings of IEEE SECON*, 2007.

[19] X. Cheng, A. Thaeler, G. Xue, and D. Chen. Tps: A time-based positioning scheme for outdoor wireless sensor networks. In *Proceedings of IEEE INFOCOM*, volume 4, pages 2685–2696, 2004.

[20] I. Constandache, X. Bao, M. Azizyan, and R. R. Choudhury. Did you see bob?: human localization using mobile phones. In *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, MobiCom '10, pages 149–160, New York, NY, USA, 2010. ACM.

[21] I. Constandache, R. R. Choudhury, and I. Rhee. Towards mobile phone localization without war-driving. In *Proceedings of IEEE INFOCOM*, 2010.

[22] M. Decker. Location privacy-an overview. In *Proceedings of the 2008 7th International Conference on Mobile Business (ICMB)*, pages 221–230, 2008.

[23] S.-H. Fang, C.-C. Chuang, and C. Wang. Attack-resistant wireless localization using an inclusive disjunction model. *IEEE Transactions on Communications*, 60(5):1209–1214, may 2012.

[24] D. B. Faria and D. R. Cheriton. Detecting identity-based attacks in wireless networks using singalprints. In *Proceedings of ACM Workshop on Wireless Security (WiSe)*, 2006.

[25] C. Feng, W. Au, S. Valaee, and Z. Tan. Compressive sensing based positioning using rss of wlan access points. In *Proceedings of IEEE INFOCOM*, 2010.

[26] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, 2008.

[27] S. A. Golden and S. S. Bateman. Sensor measurements for wi-fi location with emphasis on time-of-arrival ranging. *IEEE Transactions on Mobile Computing*, 6(10):1185–1198, Oct. 2007.

[28] R. Goossens and H. Rogier. A hybrid UCA-RARE/Root-MUSIC approach for 2-D direction of arrival estimation in uniform circular arrays in the presence of mutual coupling. *IEEE Transactions on Antennas and Propagation*, 55(3):841–849, Mar. 2007.

[29] M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 1.21. `http://cvxr.com/cvx`, Apr. 2011.

[30] F. Gross. *Smart Antennas for Wireless Communications: With MATLAB*. McGraw-Hill, 2005.

[31] D. Han, D. G. Andersen, M. Kaminsky, K. Papagiannaki, and S. Seshan. Access point localization using local signal strength gradient. In *Proceedings of Passive & Active Measurement (PAM)*, Seoul, South Korea, Apr. 2009.

[32] R. L. Haupt and D. H. Werner. *Genetic Algorithms in Electromagnetics*. A John Wiley & Sons, Inc., 2007.

[33] J. Hayes. Policy-based authentication and authorization: secure access to the network infrastructure. In *Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC)*, 2000.

[34] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher. Range-free localization schemes for large scale sensor networks. In *Proceedings of the 9th annual international conference on Mobile computing and networking*, MobiCom '03, pages 81–95, 2003.

[35] L. Hu and D. Evans. Using Directional Antennas to Prevent Wormhole Attacks. In *Network and Distributed System Security Symposium Conference Proceedings (NDSS)*, 2004.

[36] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Enhancing wireless location privacy using silent period. In *Proceedings of IEEE WCNC*, volume 2, pages 1187–1192, 2005.

[37] T. Jiang, H. J. Wang, and Y.-C. Hu. Preserving location privacy in wireless lans. In *Proceedings of ACM MOBISYS*, 2007.

[38] K. Kaemarungsi and P. Krishnamurthy. Modeling of indoor positioning systems based on location fingerprinting. In *Proceedings of IEEE INFOCOM*, 2004.

[39] S. Kim, H. Jeon, and J. Ma. Robust localization with unknown transmission power for cognitive radio. In *Proceedings of IEEE MILCOM*, 2007.

[40] kismet. *http://www.kismetwireless.net/index.shtml*.

[41] Y. H. Ko, Y. J. Kim, H. I. Yoo, W. Y. Yang, and Y. S. Cho. 2-D DoA estimation with cell searching for a mobile relay station with uniform circular array. *IEEE Transactions on Communications*, 58(10):2805–2809, Oct. 2010.

[42] A. M. Ladd, K. E. Bekris, A. Rudys, G. Marceau, L. E. Kavraki, and D. S. Wallach. Robotics-based location sensing using wireless ethernet. In *Proceedings of ACM MOBICOM*, 2002.

[43] S. Lakshmanan, C. Tsao, and R. Sivakumar. Aegis: Physical space security for wireless networks with smart antennas. *IEEE/ACM Transactions on Networking*, 18(4):1105–1118, 2010.

[44] H. Lebret and S. Boyd. Antenna array pattern synthesis via convex optimization. *IEEE Transactions on Signal Processing*, 45(3):526–532, Mar. 1997.

[45] J. H. Lee and R. Buehrer. Location spoofing attack detection in wireless networks. In *Proceedings of IEEE GLOBECOM*, 2010.

[46] X. Li, M. Chen, and E. Ratazzi. Array-transmission based physical-layer security techniques for wireless sensor networks. In *Proceedings of IEEE Int. Conf. on Mechatronics and Automation*, 2005.

[47] X. Li, Y. Chen, J. Yang, and X. Zheng. Designing localization algorithms robust to signal strength attacks. In *Proceedings of IEEE INFOCOM*, 2011.

[48] X. Li, J. Hwu, and E. P. Ratazzi. Using antenna array redundancy and channel diversity for secure wireless transmissions. *Journal of Communications*, 2(3):24–32, 2007.

[49] H. Liu, Y. Gan, J. Yang, S. Sidhom, Y. Wang, Y. Chen, and F. Ye. Push the limit of wifi based localization for smartphones. In *Proceedings of the 18th annual international conference on Mobile computing and networking*, Mobicom '12, pages 305–316, New York, NY, USA, 2012. ACM.

[50] Z. Luo, W. Ma, A. So, Y. Ye, and S. Zhang. Semidefinite relaxation of quadratic optimization problems. *IEEE Signal Processing Magazine*, 27(3):20–34, may 2010.

[51] R. Mailloux. *Phased array antenna handbook*. Artech House, 2005.

[52] J. G. Manweiler, P. Jain, and R. Roy Choudhury. Satellites in our pockets: an object positioning system using smartphones. In *Proceedings of the 10th international conference on Mobile systems, applications, and services*, MobiSys '12, pages 211–224, New York, NY, USA, 2012. ACM.

[53] J. Meyerowitz and R. Roy Choudhury. Hiding stars with fireworks: location privacy through camouflage. In *Proceedings of ACM MOBICOM*, 2009.

[54] Q. Mi, J. A. Stankovic, and R. Stoleru. Secure walking gps: a secure localization and key distribution scheme for wireless sensor networks. In *Proceedings of the third ACM conference on Wireless network security*, WiSec '10, pages 163–168, New York, NY, USA, 2010. ACM.

[55] A. Mukherjee, S. A. Fakoorian, J. Huang, and A. L. Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *http://arxiv.org/abs/1011.3754*, 2010.

[56] D. Niculescu and B. Nath. Ad hoc positioning system (APS) using AOA. In *Proceedings of IEEE INFOCOM*, 2003.

[57] S. Oh, T. Vu, M. Gruteser, and S. Banerjee. Phantom: Physical layer cooperation for location privacy protection. In *IEEE INFOCOM*, 2012.

[58] Plasma Antennas Limited. Selectable Multibeam Antennas, Jul 2011.

[59] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location-support system. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 32–43, 2000.

[60] J. Proakis. *Digital Communications*. McGraw-Hill, 4th edition edition, 2001.

[61] T. S. Rappaport. *Wireless Communications: Principles & Practice*. Prentice Hall, 2002.

[62] I. Ray and M. Kumar. Towards a location-based mandatory access control model. *Computers & Security*, 25(1):36–44, 2006.

[63] M. Robinson and I. Psaromiligkos. Received signal strength based location estimation of a wireless lan client. In *Proceedings of IEEE WCNC*, 2005.

[64] P. Rong and M. Sichitiu. Angle of arrival localization for wireless sensor networks. In *Proceedings of 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (SECON)*, 2006.

[65] R. Roy and T. Kailath. Esprit-estimation of signal parameters via rotational invariance techniques. *IEEE Trans. on Acoustics Speech and Signal Processing,*, 37(7):984–995, Jul. 1989.

[66] A. A. Sani, L. Zhong, and A. Sabharwal. Directional antenna diversity for mobile devices: Characterizations and solutions. In *Proceedings of ACM MOBICOM*, 2010.

[67] B. Schilit, J. Hong, and M. Gruteser. Wireless location privacy protection. *Computer*, 36:135–137, 2003.

[68] R. Schmidt. Multiple emitter location and signal parameter estimation. *IEEE Transactions on Antennas and Propagation*, 34(3):276–280, mar 1986.

[69] S. Sen, R. R. Choudhury, and S. Nelakuditi. Spinloc: spin once to know your location. In *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*, HotMobile '12, New York, NY, USA, 2012. ACM.

[70] S. Sen, B. Radunovic, R. Choudhury, and T. Minka. Spot localization using phy layer information. In *Proceedings of ACM MOBISYS*, 2012.

[71] S. Sen, B. Radunovic, R. Roy Choudhury, and T. Minka. Precise indoor localization using phy information. In *Proceedings of the 9th international conference on Mobile systems, applications, and services*, MobiSys '11, pages 413–414, New York, NY, USA, 2011. ACM.

[72] Y. Shang, W. Ruml, Y. Zhang, and M. Fromherz. Localization from connectivity in sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 15(11):961–974, Nov. 2004.

[73] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz. Localization from mere connectivity. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '03, 2003.

[74] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell. Detecting 802.11 MAC layer spoofing using received signal strength. In *Proceedings of IEEE INFOCOM*, 2008.

[75] D.-S. Shiu, G. Foschini, M. Gans, and J. Kahn. Fading correlation and its effect on the capacity of multielement antenna systems. *IEEE Transactions on Communications*, 48(3):502–513, Mar. 2000.

[76] N. Sidiropoulos, T. Davidson, and Z.-Q. Luo. Transmit beamforming for physical-layer multicasting. *IEEE Transactions on Signal Processing*, 54(6):2239–2251, June 2006.

[77] H. Steyskal. Wide-band nulling performance versus number of pattern constraints for an array antenna. *IEEE Transactions on Antennas and Propagation*, 31(1):159–163, 1983.

[78] M. Strasser, C. Pöpper, and S. Čapkun. Efficient uncoordinated fhss anti-jamming communication. In *Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing*, MobiHoc '09, pages 207–218, New York, NY, USA, 2009. ACM.

[79] C. Tang and D. O. Wu. Mobile privacy in wireless networks-revisited. *IEEE Transactions on Wireless Communications*, 7(3):1035–1042, Mar. 2008.

[80] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun. On the requirements for successful gps spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security (CCS)*, pages 75–86, 2011.

[81] G. Tsoulos. Smart antennas for mobile communication systems: benefits and challenges. *Electronics Communication Engineering Journal*, 11(2):84–94, Apr. 1999.

[82] R. Vescovo. Pattern synthesis with null constraints for circular arrays of equally spaced isotropic elements. In *IEE Proceedings of Microwaves, Antennas and Propagation*, volume 143, pages 103–106, 1996.

[83] H. Wang, S. Sen, A. Elgohary, M. Farid, M. Youssef, and R. R. Choudhury. No need to wardrive: unsupervised indoor localization. In *Proceedings of the 10th international conference on Mobile systems, applications, and services*, MobiSys '12, pages 197–210, New York, NY, USA, 2012. ACM.

[84] T. Wang and Y. Yang. Analysis on beamforming-based perfect location spoofing attacks. *submitted to IEEE Transactions on Mobile Computing*.

[85] T. Wang and Y. Yang. Location privacy protection from RSS localization system using antenna pattern synthesis. In *Proceedings of IEEE INFOCOM*, pages 2408–2416, 2011.

[86] T. Wang and Y. Yang. Enhancing wireless communication privacy with artificial fading. In *Proceedings of IEEE 9th International Conference on Mobile Adhoc and Sensor Systems (MASS)*, pages 173–181, 2012.

[87] T. Wang and Y. Yang. Analysis on perfect location spoofing attacks using beamforming. In *Proceedings of IEEE INFOCOM*, 2013.

[88] F. L. Wong, M. Lin, S. Nagaraja, I. Wassell, and F. Stajano. Evaluation framework of location privacy of wireless mobile systems with arbitrary beam pattern. In *Proceedings of Fifth Annual Conference on Communication Networks and Services Research (CNSR)*, 2007.

[89] B. Wu, J. Chen, J. Wu, and M. Cardei. A survey of attacks and countermeasures in mobile ad hoc networks. *Wireless network security*, pages 103–135, 2007.

[90] K. Xing, S. S. R. Srinivasan, M. J. M. Rivera, J. Li, and X. Cheng. Attacks and countermeasures in sensor networks: A survey. *Network security*, pages 251–272, 2010.

[91] J. Xiong and K. Jamieson. Secureangle: Improving wireless security using angle-of-arrival signatures. In *ACM HotNets Workshop*, 2010.

[92] K.-K. Yan and Y. Lu. Sidelobe reduction in array-pattern synthesis using genetic algorithm. *IEEE Transactions on Antennas and Propagation*, 45:1117–1122, 1997.

[93] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: challenges and solutions. *IEEE Wireless Communications*, 11(1):38–47, Feb. 2004.

[94] J. Yang and Y. Chen. Indoor localization using improved RSS-based lateration methods. In *Proceedings of IEEE GLOBECOM*, 2009.

[95] H. Yu, L. Zhong, A. Sabharwal, and D. Kao. Beamforming on mobile devices: A first study. In *Proceedings of ACM MOBICOM*, 2011.

[96] B. Zhang, J. Teng, J. Zhu, X. Li, D. Xuan, and Y. F. Zheng. EV-Loc: integrating electronic and visual signals for accurate localization. In *Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '12, pages 25–34, 2012.

[97] X. Zhou and M. McKay. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Trans. on Vehicular Technology*, 59(8):3831–3842, 2010.