Physical Layer Security for Wireless Position Location in the Presence of Location Spoofing

Jeong Heon Lee

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
Electrical Engineering

R. Michael Buehrer, Chair
Jeffrey H. Reed
Y. Thomas Hou
Yaling Yang
Michael R. Taaffe

March 4, 2011
Blacksburg, Virginia

Keywords: Location Estimation, Location Security, Secure Positioning, Attack Detection

Physical Layer Security for Wireless Position Location in the Presence of Location Spoofing

Jeong Heon Lee

(ABSTRACT)

While significant research effort has been dedicated to wireless position location over the past decades, most location security aspects have been overlooked. Recently, with the proliferation of diverse wireless devices and the desire to determine their position, there is an increasing concern about the security of location information which can be spoofed or disrupted by adversaries or unreliable signal sources. This dissertation addresses the problem of securing a radio location system against location spoofing, specifically the characterization, analysis, detection, and localization of location spoofing attacks by focusing on fundamental location estimation issues.

The objective of this dissertation is four-fold. First, it provides an overview of fundamental security issues for position location, particularly associated with range-based localization. Of particular interest are security risks and vulnerabilities in location estimation, types of localization attacks, and their impact. The second objective is to characterize the effects of signal strength and beamforming attacks on range estimates and the resulting position estimate. The characterization can be generalized to a variety of location spoofing attacks and provides insight into the anomalous behavior of range and location estimators when under attack. Through this effort we can also identify effective attacks that are of particular interest to attack detection and localization. The third objective is to develop an effective technique for attack detection which requires neither prior environmental nor statistical knowledge. This is accomplished by exploiting the bilateral behavior of a hybrid framework using two received signal strength (RSS) based location estimators. We show that the resulting approach is effective at detecting attacks with the detection rate increasing with the severity of the induced location error. The last objective of this dissertation is to develop a localization method resilient to attacks and other adverse effects.

Since the detection and localization approach relies solely on RSS measurements in order to be applicable to a wide range of wireless systems and scenarios, this dissertation focuses on RSS-based position location. Nevertheless, many of the basic concepts and results can be applied to any range-based positioning system.

Dedication

This work is dedicated to my parents and my wife.

Acknowledgments

This work would not have been possible without support of my mentors, family, colleagues, and friends. First and foremost, I am deeply grateful to my advisor, Dr. Michael Buehrer, who has been an excellent mentor, teacher and person. I thank him for his support, guidance, understanding, and commitment. Throughout the entire course of my Ph.D. program, I have always been motivated and inspired by his invaluable advice, insights, and great personality. It has been, simply, a true privilege to be his student. I also thank other members of my doctoral committee, Drs. Jeffrey Reed, Thomas Hou, Yaling Yang, and Michael Taaffe.

I extend my gratitude to my colleagues at the Mobile and Portable Radio Research Group (MPRG), Virginia Tech. They made my life at school more enjoyable and less stressful. Especially, I thank my current and former cube mates, Mahmud Harun, Chang Li, Sho Sho Chen and Arjun Bhupathi raju, with whom I shared laughs and happy moments. I am grateful to MPRG Korean fellows, Kyou Woong Kim, Kye Hun Lee, Kyung Kyun Bae, Hae Soo Kim, Jong Han Kim, Jang Hoon Oh, and Bum Suk Choi. I also thank Swaroop Venkatesh, Harpreet Singh Dhillon, Tao Jia, Chris Phelps, Haris Volos, Rekha Menon, Jihad Ibrahim, Youping Zhao, Natalia Rivera, Justin Kelly, Jesse Reed, Matthew Roney, Ambuj Agrawal, Hunter DeJarnette, Benton Thompson, Corey Cooke, Javier Schloemann, and Yeashfi Hasan. I also thank my (senior) friends at VT including Jeong Ki Kim, Chee Woo Lee, Jae Hyuck Kim, and Joo Hong Lee.

I would like to particularly thank my parents and my wife for believing in me, and their constant support and encouragement.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Position Location in Wireless Networks

Recent advances in radio and networking technologies have enabled the proliferation of wireless networks with increasing connectivity. People can now experience convenient, affordable (even free) high-speed access to wireless networks in private, enterprise and public places. Further, the demand for greater radio coverage continues to grow. According to a recent survey conducted by Devicescape [1], 84 percent of Wi-Fi users desire citywide Wi-Fi, and 91 percent expect Wi-Fi on the road (*e.g.*, hotel, airport, bus terminal, cafe, etc.). In addition, it has been reported that the wireless penetration rate is approaching 100 percent in the U.S. and experts anticipate that we will reach 300 percent penetration in the near future [2]. Meanwhile, new wireless technologies such as wireless sensor networks (WSNs) and cognitive radio networks (CRNs) are being developed for a range of emerging wireless applications including security-related applications [3, 4]. It is widely envisioned in the industry that wireless will be infused into all manners of consumer/industrial electronics such as household gadgets and medical devices [5, 6].

In this wireless era, one of the fundamental problems is to determine the unknown location of a mobile client or device in the network. Location information about tetherless devices is valuable due to its crucial role in data collection, reliable communications, resource management, emergency services/maintenance, and other important functions of wireless systems. Further, the increasing popularity of location-based applications and services has increased the interest in wireless position location. In cellular networks and wireless local area networks (WLANs), position information is valuable not only to fulfill the wireless Enhanced 911 (E-911) mandate for locating wireless 911 callers, but also to meet the increasing demand for navigation/tracking and location-based services (LBSs) [7–9]. In ad-hoc wireless technologies such as WSNs and CRNs, the task of localizing sensors or radios with unknown position is important for the operation and configuration of the network. The operational

Table 1.1: A List of Radio Location Systems Developed

Signal Parameter	Examples of Radio Location Systems
RSS	RADAR [15], QRSS [16], SpotOn [17], Nibble [18]
TOA	GPS [19], A-GPS [20], UWB PAL [21], many UWB/CDMA systems [22–24]
TDOA	LORAN [25], AHLoS [26], Cricket [27], standard cellular positioning systems including E-OTD (for GSM/GPRS), U-TDOA (for GSM/4G), A-FLT (for cdmaOne/CDMA2000) and OTDOA (for WCDMA) [28]
AOA	APS [29], SDP [30], nonstandard cellular positioning systems using an (adaptive) array antenna [22, 31, 32]

scenarios include data collection, surveillance and inventory tracking among many others. Also, the knowledge of node position can be useful for routing, interference avoidance and other basic functions [10]. This significance has stimulated research into a variety of localization techniques based on either received signal strength (RSS), differential RSS (DRSS), time-of-arrival (TOA), time-difference-of-arrival (TDOA), angle-of-arrival (AOA), or their hybrids [7, 11–14]. A list of well-known location systems is provided in Table 1.1. Most of the existing studies in location estimation focus on *location accuracy* presuming *reliable* and *cooperative* signal sources.

1.1.1 Problem of Location Estimation

The problem of position location based on signal measurements can be described as a series of three major phases: (a) signal observation, (b) extraction of position-related signal parameters and (c) estimation of location coordinates. Specifically, upon arrival of a signal, one or more signal parameters or features–among which are signal power for RSS/DRSS, arrival time for TOA/TDOA and direction of arrival for AOA–are extracted depending upon the type of location system as exemplified in Table 1.1. The parameters are then used to estimate the target position by exploiting prior (statistical) knowledge of the observed data. Since a location estimator is subject to various environmental and systematic errors during any localization phase, it is vital to understand the source of these errors to develop a robust location system (see Chapter 2).

Let us consider a typical source localization problem as follows. Suppose that given m anchor nodes with known coordinates $\boldsymbol{x_i} = [x_i, y_i]^T$, their RSS measurements are translated into the distances $\{\hat{d}_i\}_{i=1}^m$ to the signal source (or mobile) using a large-scale signal propagation model. Then, denoting the unknown target position as $\boldsymbol{\theta} = [x, y]^T$ we can formulate a basic

mathematical problem for position location, referred to as *lateration*, as

$$\begin{aligned} \hat{d}_i^2 &= \|\boldsymbol{\theta} - \boldsymbol{x_i}\|^2 \\ &= (x - x_i)^2 + (y - y_i)^2, \quad i = 1, \ldots, m. \end{aligned} \tag{1.1}$$

By solving this set of nonlinear equations ($m \geq 3$), the position (x, y) can be determined. The solution can be interpreted geometrically, thus giving another (more intuitive) perspective of the problem (see Chapter 3). This 2-dimensional (2-D) single source localization problem, which is assumed in this work, can readily be extended to three-dimensional (3-D) and to multiple sources by incorporating necessary node coordinates into the problem.

In position location, there are two primary factors that pose a challenge in solving the location problem: (a) sources of error and (b) the optimality of a solution. Specifically, due to noise and other error sources, additional anchor measurements are valuable for better location accuracy. However, there exists no unique solution that satisfies with equality the resulting overdetermined system. Also, the problem formulation as in Eq. (1.1) does not fully exploit all the available data and statistical information. Thus, it is often preferred to find an optimal or practical location estimator by solving the problem

$$\text{Minimize} \quad \phi(\boldsymbol{\theta}) \tag{1.2}$$

$$\text{subject to} \quad g_i(\boldsymbol{\theta}) \leq 0, \quad i = 1, \ldots, l_g \tag{1.3}$$

$$h_j(\boldsymbol{\theta}) = 0, \quad j = 1, \ldots, l_h \tag{1.4}$$

where $\boldsymbol{\theta}$ may include "nuisance" parameters in addition to the parameters (x, y) of interest. $\phi(\boldsymbol{\theta})$ is a linear or nonlinear objective function incorporating our (statistical) knowledge of the observations, a signal/system model and error statistics (if known *a priori*). The constraints $g_i(\boldsymbol{\theta})$ and $h_j(\boldsymbol{\theta})$ are optional, but should be exploited if possible to reduce a feasible region and avoid excessive location errors. For instance, knowledge of non-line-of-sight (NLOS) measurements or radio coverage can be used to impose the constraints. The objective in solving the problem given in Eq. (1.2) is to find the optimal solution $\boldsymbol{\theta}^*$–that is the best location estimate–such that $\phi(\boldsymbol{\theta}^*) \leq \phi(\boldsymbol{\theta})$ for each feasible point $\boldsymbol{\theta}$. In Chapter 3, we discuss various estimators which are widely used for location estimation.

There has been a great deal of attention paid to the achievable accuracy of a location estimator, particularly using the Cramer Lower Rao Bound (CRLB) which provides the lower bound on the covariance of an unbiased estimator, which is usually employed as a benchmark in many studies. We will discuss further the theoretical bound on the performance of a location estimator in Chapter 3.

1.2 Wireless Location Security

1.2.1 What is Wireless Location Security?

Location security is now of greater concern than ever, as location information is increasingly used as a key element in the operation of wireless applications/services related to personal, business and national security. Analogous to information security [33], we use the term "location security" to mean **protecting location information and systems from *location security risks* in order to ensure *quality of location security services***. The location security risks include *unauthorized access, use, disclosure, modification, disruption* and *destruction*, whereas the quality of location security services (QoLSs) correspond to *availability, reliability, integrity*, and *confidentiality*. We note that confidentiality is more related to privacy issues concerning spatio-temporal location information of legitimate clients. On the other hand, location spoofing is more concerned with the availability, reliability and integrity of location information of an attacker or a legitimate client. We discuss this classification further in Chapter 4, where attack strategies are classified according to three primary attack types and potential location security risks. Further, location spoofing attacks against RSS-based location estimators are characterized in Chapter 5.

1.2.2 Security Concerns for Location Systems

Although a great deal of attention has been directed at the problem of wireless localization, most location security aspects have been overlooked. In fact, location security was not a major concern previously because early location systems were designed specifically for military applications, such as radar systems and the military version of the Global Positioning System (GPS), which are physically protected or securely encrypted. On the other hand, civilian location systems are highly vulnerable to security risks due to their principles of openness and wide public availability.

As wireless penetrates into every corner of our lives, location security is of greater concern than ever, noting that location information/systems are now used for critical aspects of many applications and services. As an example, GPS is used for numerous applications including vehicle navigation, synchronization of national power grids with power stations, financial transaction time stamps, air traffic control and criminal tracking. Recently, researchers have warned that civilian GPS systems can be "spoofed" (or sabotaged) by adversaries, and the cost and effort of spoofing are rapidly decreasing [34, 35]. Also, it has been revealed that current public wireless positioning systems are vulnerable to location spoofing and location data manipulation attacks [36]. However, most popular location algorithms (which require some degree of cooperation from a signal source) are not capable of locating the spoofer for attacker traceback [37, 38]. Even the secure positioning techniques that have been proposed are not effective under practical attack scenarios.

1.2.3 Relationship to Network Security

Location security and wireless network security are interrelated. In wired network systems, the network can only be accessed by plugging an Ethernet cable into an LAN port at the *fixed* and *known* position. This means that the network can be secured from unauthorized access physically as, for example, the port is monitored/disabled by the simple network management protocol (SNMP) [39] and the room/building is protected by security guards and physical security keys. Although the physical security measures can be bypassed, in general, the attacker can be traced back when malicious attempts are detected [37, 38]. On the other hand, wireless networks are known to be much more vulnerable to network security threats. In particular, mobility (which typically requires mobility support at the Internet Protocol (IP) layer unlike wired networking) and notoriously unpredictable radio propagation environments pose considerable challenges in tracing and pinpointing an attack's origin. Further, the characteristics of radio propagation vary considerably from environment to environment [40], thus making it difficult to precisely control a wireless network coverage area.

Therefore, an attractive tactic for attackers or hackers would be driving around some town and accessing "free" or weakly secured private/enterprise networks using a high-gain antenna while sitting in the car to"sniff" someone's data packets or launch an attack on remote critical infrastructure such as financial, transportation, and energy services. The effort and time can be substantially reduced if they consider publicly accessible wireless access points (APs). To make themselves geographically anonymous, the attacker could exploit the vulnerability in a location system by disguising its own signal features used for localization. More inexpensive but effective software/hardware tools are available than ever before which empower the adversary to be more pseudonymous and location anonymous.

Although location security in wireless networks is technically challenging, if ensured, secure location information can be used to leverage network security measures and access control, thus complementing long-term secret keys such as passwords and private keys [41]. For example, the network can prevent unauthorized access beyond some specified service area or "virtual port." When unauthorized network access beyond this secured spot is detected, the network can track down the attacker to enforce accountability. Further, it is possible to greatly reduce critical security threats related to sybil attacks [42] and unauthorized or rogue APs/jammers [43, 44] by detecting their positions. Another important benefit of location security is to ensure the security for WSNs or CRNs (including embedded wireless systems), where the location information of nodes is crucial for their operations [3, 6]. On account of the effects of cooperative localization in this type of ad hoc multihop network, a fraction of the nodes under attack (*e.g.*, by removing or compromising nodes) could cause location error propagation through their own network or interference with legacy systems.

1.2.4 Relationship to Reliable Positioning

Another notable aspect of location security is its close relationship to *location reliability*. If some location algorithm or solution is robust to location attacks, as described later in this work, it will be robust to other environmental and systematic biases or errors. The natural biases can also limit the performance of location algorithms substantially. In fact, as detailed in Chapter 5, from an estimator's perspective, there is the fundamental similarity between malicious attacks and natural yet systematic biases. As an example, biased range estimates due to an attack could look like those naturally biased by NLOS propagation or systematic error (*e.g.*, due to node malfunctioning or system/software glitches) with respect to the resulting location error. It is worth noting that natural range biases can deliberately be introduced by adversaries by, for example, removing a direct signal or line-of-sight (LOS) path using a directional antenna or taking advantage of nearby obstacles. Also, inadvertent yet abnormal estimator behaviors can lead to anomalous position estimates or excessive location error. Thus, securing position location against spoofing attacks will contribute to reliable positioning in many applications where malicious attacks are not of concern. Also, dealing with attacks is similar to handling the issues with large position errors (*e.g.*, characterization, detection and localization).

1.3 Problem Statement

In this dissertation we are mainly concerned with location spoofing attacks launched by a wireless node (the mobile) to falsify (degrade) its own position estimate $\hat{\boldsymbol{\theta}} = [\hat{x}, \hat{y}]^T$. To describe the problem of location spoofing, consider a basic location problem where the mobile position (x, y) is determined using a set of m range estimates $\{d_i\}_{i=1}^m$ as in Eq. (1.1). The range estimates can be obtained based either on RSS measurements $\{P_i\}_{i=1}^m$ at the anchors using the maximum likelihood (ML) estimator of distance d_i:

$$\hat{d}_i = d_0 \cdot 10^{\frac{P_0 \text{ (dBm)} - P_i \text{ (dBm)}}{10 n_p}} \tag{1.5}$$

where n_p is the path loss exponent and P_0 (a function of mobile transmit power P_t) which is the signal power observed at a close-in distance d_0 or on TOA measurements $\{t_i\}_{i=1}^m$ through the equation

$$\hat{d}_i = (t_i - t_{tx})c \tag{1.6}$$

where t_i, t_{tx} and c are the receive time at the ith anchor, transmit time at the mobile and the speed of light, respectively. That is, $t_i - t_{tx}$ is the time of flight between the mobile and the ith anchor. In the absence of noise or multipath fading, the position estimate will be the same as the true position as illustrated in Fig. 1.1a. While the mobile is supposed to transmit a signal at a known power level P_t for RSS or at a known time t_{tx} (the transmitter

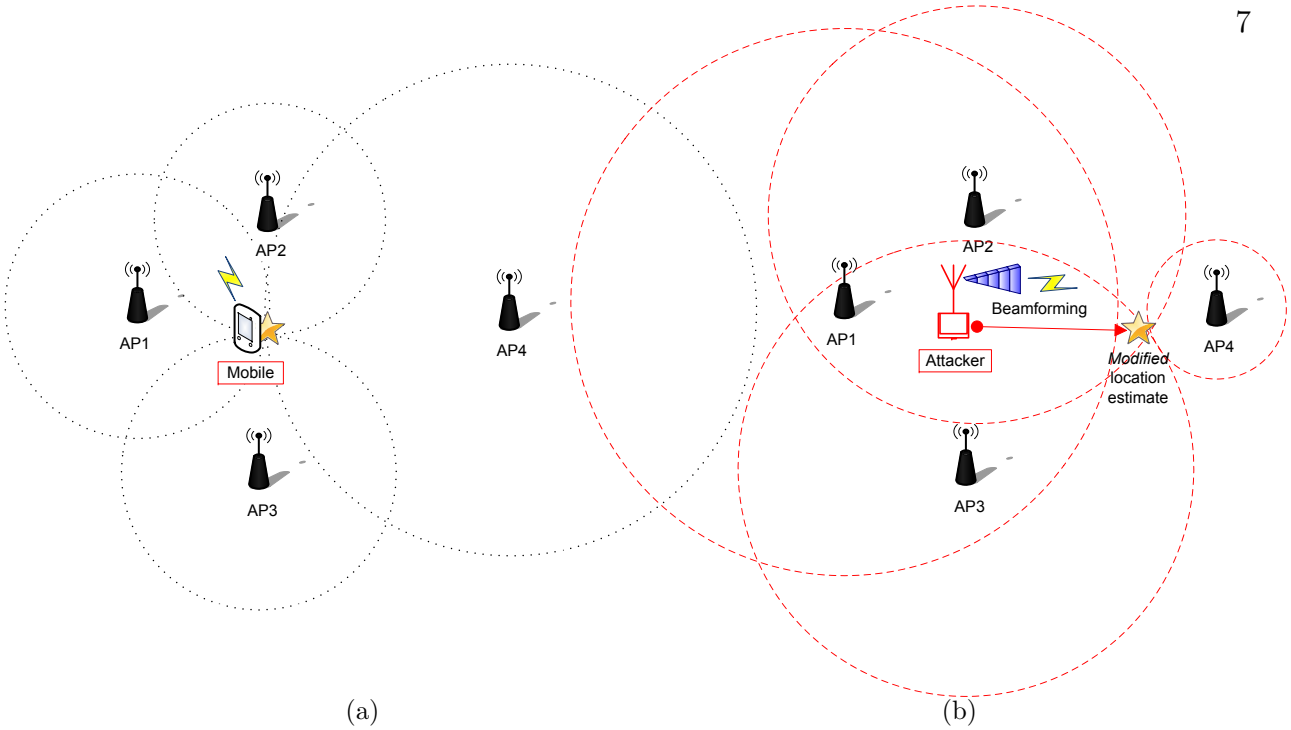


Figure 1.1: An example scenario of a location spoofing attack (noiseless case). (a) No attack. (b) Under beamforming attack. The shaded entity indicates the one in charge of signal measurements, while the entity whose name is in a box indicates the signal source. The dotted circles centered at each anchor position and the star represent range estimates and the resulting (falsified) position estimate, respectively.

parameter values may be informed to the anchors afterward), an attacker can falsify P_t or t_{tx} (which is under attacker's control) to disguise its distance to the anchors and the resulting position estimate. This simple attack situation is illustrated in Fig. 1.1. As noted, the major security concern arises due to the passive dependency of location algorithms on the mobile which is potentially malicious. However, even if we remove the dependency, for example, using other types of location systems (*e.g.*, DRSS and TDOA), there still exist security risks specific to the system. More details on the security issues with more practical scenarios will be discussed in Chapters 4 and 5.

This work investigates the assessment, detection and localization of location spoofing attacks by focusing on fundamental location estimation problems. In particular, we develop an approach based solely on RSS measurements which thus can be applied to nearly any wireless system without requiring additional radio resources or hardware. Further, in many security scenarios, RSS will only be available information in order to detect and track wireless attackers or jammers which are obviously not communicative. Despite our emphasis on RSS-based location estimation and its security issues, many of the basic concepts and results can be applied to any range-based position location network, not just RSS-based systems.

In summary, the main problems that we address in this dissertation are as follows:

- Exploring the fundamentals of range-based position location, specifically RSS-based location estimation;
- Characterizing location spoofing attacks and the resulting impact on a location estimator;
- Assessing the quality of a node's location estimate under attack to measure the associated security risk;
- Detection of both signal strength and beamforming attacks;
- Mitigating the anomalous behavior pf a location estimator and reducing the error in both attack-prone and attack-free conditions;
- Position location resilient to location spoofing attacks as well as reliable location estimation.

The efforts of this work will contribute toward the security of a location system while ensuring the availability, integrity and reliability of location information.

1.4 Related Work

Recent research activities concerning location spoofing attacks have primarily been derived from two increasing concerns: (a) *attack position spoofing* and (b) *anchor signal spoofing*. The two types of attacks are classified according to whether the target location information to be falsified or disrupted is the attacker's own position (*i.e.*, attack position spoofing) or the victim's position (*i.e.*, anchor signal spoofing). Despite our focus on attack position spoofing in this work, most of our discussion and results can also be applied to anchor signal spoofing due to the fundamental similarity between the two attack types. We will look further into the major types of location attacks and present a survey of recent work on each attack type in Chapter 4.

Due to current research interest and greater vulnerability, most of the prior studies on attack position spoofing focus on infrastructure-based networks (*e.g.*, WLANs), whereas most of the efforts to defend against anchor signal spoofing consider (large-scale) ad-hoc sensor network applications. The former attack case typically deals with the detection and localization of attacks using a pre-established *reliable* radio map [15] or RSS database [45, 46]. Their major drawbacks include limited application/attack scenarios and costly offline training procedures which need to be repeated regularly to reflect the time-varying nature of wireless environments. Further, in practice it would be challenging to construct a reliable, accurate radio map due to unpredictable wireless channels, user behavior and interference.

On the other hand, the goal of the work against anchor signal spoofing is usually the location discovery of sensors through the system-level protocol design or algorithmic approach (*e.g.*,

location verification using distance bounding [47–49], voting-based schemes [50, 51] or deployment knowledge [52]). The success of the approach will depend upon system/hardware requirements, assumptions and/or application scenarios. Among these are a directional antenna in each anchor, sufficient radio resources, the absence of jamming/interference, a majority of benign observations and common control channels.

To protect position location networks from location spoofing attacks, researchers have proposed techniques for detecting or positioning location attacks. Among the techniques are either a range-based approach using statistical methods (*e.g.*, linear least squares (LS) [45], least median squares (LMS) [53], minimum mean square estimation (MMSE) [51]) and location verification algorithms [47, 49, 51], or a range-free approach [48, 50, 54]. The previous studies (which typically require pre-established infrastructure or prior statistical knowledge) increases the resiliency to attacks at the expense of overall location accuracy in the absence of an attack and/or high computational and hardware complexity. As a result, this tradeoff limits the applicability of the approach. Further, adversaries could take advantage of the prior information used by the approach. The details of the previous work can be found in Chapter 4.

1.5 Original Contributions and Outline of Dissertation

To the best of our knowledge, this dissertation includes the most comprehensive treatment and several new aspects in regard to securing position location against location spoofing while focusing on fundamental location estimation issues. Due to our general approach to the problem, specifically the assessment, detection and localization of attacks, our discussion and concepts are not limited to a specific set of applications or requirements unlike previous studies. The approach neither relies on the cooperation of the mobile nor requires any prior statistical or environmental knowledge such as pre-established infrastructure, offline training or error statistics. To make the approach flexible and applicable to various scenarios and systems, we only use signal strength (SS) observations which can readily be acquired in (nearly) every wireless system without any system modifications. This SS-based framework can be integrated into another type of location system as a hybrid approach for better location accuracy. Further, since location attacks are manifested as modifications to the observed RSS values, we characterize the effects of location attacks on range and location estimation. Despite our focus on source localization using RSS measurements, this work can be extended to self-positioning involving unreliable/malicious anchors, jammers or rogue APs as well as other measurement types.

The outline of this dissertation and the main original contributions highlighted in each chapter are as follows:

In Chapter 2, we first discuss the optimality criterion or risk measure which is used in this work to evaluate the performance and security risk of location estimators and techniques.

Then, primary factors in designing a radio location system are presented. We also describe major sources of location error and how to mitigate them to understand their impact on range and location estimation in comparison to location attacks. Chapter 2 also presents the realistic adversary and radio propagation models employed in this study.

Original Contributions in Chapter 2:

- Establishment of a practical simulation environment where realistic adversary and spatially correlated shadowing models are developed.

In Chapter 3, we present the fundamentals of RSS-based position location, specifically major techniques (*i.e.*, range-based, RF fingerprinting, proximity-based), geometric interpretations and location estimators (*i.e.*, CRLB, ML estimator, LS estimators). Then, RSS- and DRSS-based localization methods are evaluated in correlated shadow fading conditions and their performance results are compared. In addition, Chapter 3 compares numerical optimization algorithms for location estimation and presents an initial solution selection algorithm for DRSS-based localization.

Original Contributions in Chapter 3:

- Comprehensive overview of RSS-based position location from various aspects including major localization techniques, estimators and optimization algorithms [55];
- Development of a DRSS-based positioning approach and its comparison with RSS-based positioning in the presence of spatially correlated shadow fading;
- Development of an initial solution selection algorithm for DRSS-based location estimation.

In Chapter 4, we discuss security issues for position location, specifically major types of location attacks and security risks in RSS-based positioning, along with a survey of recent work on each attack type. Then, we investigate the impact of location spoofing attacks on location accuracy with several examples. When examining the impact of location spoofing attacks, Chapter 4 compares two typical location estimators; one assuming prior knowledge of path loss rate and the other estimating the nuisance channel parameter jointly with the position parameters of interest. The chapter also shows the impact of incorrect knowledge of the path loss rate and the form of bias on range estimators.

Original Contributions in Chapter 4:

- Examination of location attacks and their categorization into: (a) attack position spoofing, (b) anchor signal spoofing and (c) location disclosure [56];
- Investigation of the effects of location spoofing attacks against two typical location estimation strategies;
- Showing the significant impact of incorrect estimation of path loss rate on estimator performance, particularly from a security perspective.

Chapter 5 provides a characterization and analysis of location spoofing attacks. More specifically, we characterize attacks according to the form of bias to the individual range estimators and subsequently the position estimator. Then, the behavior of a location estimator under attack is analyzed from several key estimation aspects, namely knowledge of nuisance parameters, heavy-tail issues and the bias-variance tradeoff. Further, we investigate how the bias-variance characteristics impact the performance of a location estimator and the theoretical limits to the estimator accuracy.

Original Contributions in Chapter 5:

- Mathematical characterization of location spoofing attacks in both range and location estimation which are generalized into two types of estimator bias (*i.e.*, uniform or selective; positive or negative);
- Characterization of the behavior of a location estimator from fundamental aspects of location estimation: (a) knowledge of nuisance parameters, (b) heavy-tailed behavior and (c) the bias-variance tradeoff;
- Analysis of the bias-variance tradeoffs of a location estimator and the related theoretical limits to the estimator's accuracy from the perspective of general location estimation.

Chapter 6 deals with the problem of attack detection. In this chapter, we first introduce a novel approach termed bilateral dissimilarity detection (BDD) which exploits the bilateral dissimilarity based on two SS-based estimators. Then, we present two methods for BDD; one is a statistical method using point error signatures and the other is a pattern matching scheme using topological error signatures. Also, this chapter describes the adverse effect of node geometry on attack detection and how to improve the geometric adversity.

Original Contributions in Chapter 6:

- Development of an approach to attack detection by exploiting the bilateral dissimilarity of RSS- and DRSS-based location estimators. This approach can assess the anomalous behavior of a location estimator due to an attack without the aid of prior statistical or environmental information;
- Development of two techniques for attack detection based on point or topological error signatures which require neither prior statistical nor environmental knowledge;
- Identification of the adverse effect of node geometry on attack detection and how to reduce the geometric impact and thus improve the detection performance.

The objective of Chapter 7 is to localize a mobile device which may be attempting to falsify or disrupt its position information. To achieve this goal, we develop an attack-resilient location estimator, termed the penalized Joint LS estimator, based on our understanding of the major security risks in RSS-based location estimation. Specifically, we developed the joint optimization approach with a penalty function which is employed to exploit additional information about radio range constraints. As a result, the impact of anomalous location estimates with large error on location accuracy is significantly reduced. The resiliency of the estimator is further enhanced by correcting residual anomalous errors once they are detected. This chapter also presents a metric for assessing the security risk of a node's location estimate with respect to location error.

Original Contributions in Chapter 7:

- Development of a unified framework which includes the substantial reduction of large location error, and the discovery and correction of residual anomalous errors. This framework requires neither any prior statistical and environmental knowledge nor pre-installed infrastructure and system protocols;
- Development of a penalized joint LS estimator which is resilient to location attacks;
- A framework for measuring the security risk of a mobile's location estimate with respect to location error;
- Development of a novel algorithm for iteratively correcting excessively large errors due to an attack or other systematic bias.

Chapter 2

Background

In this chapter we first introduce the optimality criterion for location estimators–that is the mean square error–which can measure the goodness or risk of location estimates. This risk measure will be used to examine the impact of location attacks on location accuracy and analyze the behavior of an estimator in the presence of attacks. Then, major factors in location system design are introduced in order to discuss important issues that need to be taken into consideration in the design of a location system. Also, we describe primary sources of location error and the corresponding mitigation techniques to understand their impact on location estimation in comparison with location spoofing attacks. Specifically, the error sources are multipath fading, NLOS propagation, shadow fading, systematic bias and the geometry of nodes. Because many of the results in this dissertation are based on computer simulation, we develop practical adversary and simulation models which are used for the study of two important issues: the impact of spatial correlation in shadow fading and the impact of location spoofing attacks. Effective attacks found from the simulation study are then applied in order to evaluate the performance of attack detection and localization techniques developed in this work.

2.1 Optimality Criterion and Risk Measure

Location estimation is a classical estimation problem in which the parameters $\boldsymbol{\theta}$ of interest are deterministic but unknown. A location algorithm solves the problem by determining $\boldsymbol{\theta}$ based on a set of signal observations $\{v_1, v_2, \ldots, v_m\}$ which are subject to environmental/systematic biases and various errors. Therefore, one of the primary goals of a location system designer is to search for an optimum location estimator $\hat{\boldsymbol{\theta}}^*$ given system constraints and application requirements. To this end we need to adopt some optimality criterion for the estimator which can also be used for a goodness measure of its localization performance.

In signal processing, the most widely used (and important) criterion is the *mean square error*

(MSE), defined as

$$\mathrm{MSE}(\hat{\boldsymbol{\theta}}) = E\left\{\|\hat{\boldsymbol{\theta}} - \boldsymbol{\theta}\|^2\right\}, \tag{2.1}$$

which is the average squared norm error of the estimator that is equal to the sum of the average squared deviation of each estimator from its true parameter value. Despite the use of notation $\boldsymbol{\theta}$ as a collection of the unknown parameters, when evaluating the performance of location estimators or techniques, we will only incorporate the position parameters (not the nuisance parameters) in $\boldsymbol{\theta}$ which are of our particular interest, unless indicated otherwise. As noted, the MSE is a direct measure of location estimation error or estimator performance. Many studies on position location employ several other goodness measures such as mean, median ($50th$ percentile) and other percentile values. However, one should be cautious about using them alone since they do not take into account important aspects of location error such as bias and heavy-tail issues described later in this dissertation.

In statistical decision making, the MSE is a risk function of a statistical decision based on the quadratic loss function [57]. It can measure a (Bayes) risk or mean loss of an estimator's decision on the location estimates. Location security system designers wish to minimize this risk quantity while adversaries typically attempt to maximize it by employing one or more effective attack strategies. Therefore, we explore the effect of location spoofing attacks on location estimators in terms of the square root of MSE or *root mean square error* (RMSE). We use the RMSE throughout this work since it has the same unit as the position coordinates being estimated (*i.e.*, *meter*).

2.2 Factors in Location System Design

As listed in Table 1.1, there have been a variety of radio location systems or techniques developed by incorporating specific design aspects for a target application. Specifically, we take into account many factors leading to the tradeoffs between localization performance and system complexity. Some factors are system constraints while others are desired performance requirements for a specific application.

2.2.1 Environment

One of the primary design factors is the environment, *i.e.*, where the system will be deployed. Since this is typically a design requirement which limits the system performance, we need to explore other design factors carefully to ensure that the system will operate reliably in the environment. For position location, the environment is typically classified as either indoor, urban or other. For both indoor and outdoor environments, one of the important decisions is whether or not to use the existing infrastructure such as APs, Wi-Fi hot spots, and cellular

phone systems. When considering the outdoor environment, we need to choose whether to use GPS due to its high location accuracy, convenience and ubiquity. Although the price and size of GPS receivers continue to drop, the constraints still limit its use for many consumer electronics and wireless devices. We also note that a high percentage of wireless devices or phones are used in indoor and urban areas, where severe multipath fading impedes many location techniques including GPS.

2.2.2 Signal Parameter Measured

Taking into account the environment, accuracy requirements, and system constraints, we must choose which position-related signal parameter (*i.e.*, RSS, DRSS, TOA, TDOA, or AOA) will be used for location estimation. This decision has a considerable impact on achievable location accuracy, hardware requirements, and system complexity. Due to this significant role, it is common to classify location systems according to a signal parameter used by the system as done in Table 1.1. Localization methods based on AOA, TOA, and TDOA including their hybrid approaches can generally provide fine ranging resolution, but require relatively high computational power and/or complex hardware to retain bearing for AOA or high-precision timing and synchronization for TOA and TDOA. On the other hand, RSS-based positioning typically provides location estimates of lower accuracy, but is a cost-effective solution without the aid of additional hardware. The more attractive aspects of using RSS measurements for localization are discussed in Chapter 3.

2.2.3 System Structure (Measurement Entity)

In implementing a radio location network, a system designer needs to choose one of three possible system structures, either network-based positioning, client-based (or client-assisted) positioning, or collaborative positioning. In network-based positioning systems (*e.g.*, AOA-based systems, U-TDOA, RF fingerprinting), the network measures signals from a mobile client via APs or base stations (BSs) and computes the mobile's position with/without the client's cooperation. On the other hand, in client-based or -assisted positioning networks (*e.g.*, E-OTD, OTDOA, A-FLT, A-GPS), a mobile client measures signals broadcast by each anchor, and then calculates its own position (*i.e.*, client-based positioning) or forwards the measurement data to the network (or central solver) for a position calculation (*i.e.*, client-assisted positioning). On the contrary, a system designer may consider a cooperative localization approach particularly for multihop ad-hoc networks. In this approach, unlocalized neighboring sensors communicate with each other and use peer-to-peer measurements to form a location map of the network [12, 13, 58]. This approach has attracted growing attention in recent years due to the increasing popularity of WSNs.

2.2.4 Other Design Factors

Other factors taken into consideration include the target's mobility/speed, the number of unlocalized nodes, the number of anchor nodes, the network architecture, location security/privacy issues, and government policies.

2.3 Sources of Location Error and Mitigation

Localization performance is fundamentally limited by various estimation biases and errors. However, signal or RSS measurements are so unpredictable that it is important to understand their sources of error in order to design a robust location system with a desired accuracy. Further, in location security, the natural errors impede the detection and localization of location attacks. We thus discuss major sources of error as well as key techniques developed to mitigate the errors.

2.3.1 Multipath Fading and NLOS Propagation

Multipath fading is the major concern in wireless environments since it degrades the reliability and accuracy of a location system considerably. This error source which, causes frequency-selective fading, is random and unpredictable by nature [40]. It varies with node geometry, mobile position, and the surrounding environment. The effects of multipath fading are of great concern for many envisioned location applications which aim for operation in indoor and urban areas, where an LOS path is typically blocked and substantial scattering exists.

With respect to the NLOS issue, a great deal of research has been devoted to mitigating NLOS bias effects in location estimation [59].

The primary observation concerning NLOS signals exploited in many studies is that NLOS-corrupted measurements are positively biased so that a constrained optimization problem as in Eq. (1.2) can be formed. Also, researchers have proposed algorithms which selectively remove or scale NLOS measurements by examining the LS residual error of an estimator for TOA [60], TDOA [61], and AOA [62]. Recently, ultra-wideband (UWB)-based ranging techniques have been of considerable interest as a promising indoor location solution [21, 23, 24].

2.3.2 Shadow Fading

Assuming multipath fading is averaged out or diminished, a received signal power envelope fluctuates slowly over distance (refer to Eq. (3.1)). Then, the dominant error source is

large-scale shadow fading. As discussed in Chapter 3, shadow fading values at different locations are spatially correlated [63, 64]. In the study of cellular phone systems, a primary effort to mitigate this effect on link quality is made through macro diversity. However, few effective techniques have been shown for position location. If some measurements are *known* to be reliable, the LS residuals of the other measurements can be exploited to selectively mitigate their effects. Note that RSS-based range or location estimators are biased over typical wireless channels.

2.3.3 Systematic Bias or Error

In practice, radio location systems usually encounter systematic errors mainly due to imperfect receiver measurements, radio miscalibration, and hardware/software accuracy. While most location studies ignore this type of error because of its unpredictable and complex nature, it can be detrimental to location estimation. Systematic errors often bias location estimators, thereby making the mean of the estimator different from the true value. When the errors are constant to mobile target position or static over time for stationary targets, they cannot be eliminated by repeating measurements or averaging over a number of observations. Nevertheless, recent advancements in radio and digital signal processing technologies have considerably reduced their impact. Also, some techniques such as clock offset correction and hybrid localization methods have been proposed to tackle this issue. If channel/noise states are time-varying, a recursive Bayesian approach such as Kalman filters and particle filters can be employed [65, 66].

2.3.4 Geometric Node Configuration

The geometry of nodes or anchors relative to the mobile is a crucial factor that impacts the localization performance. This error source has been studied particularly for the GPS system in early location research, and is often termed the geometric dilution of precision (GDOP) [19, 67]. To minimize the adverse impact of node geometry, a location system designer can increase node density or seek optimal anchor positions [68–70]. It is important to note that such a geometric solution has recently become more attractive as wireless connectivity has been rapidly increasing, along with a growing interest in WSNs/CRNs.

2.4 Adversary and Simulation Models

This dissertation deals with many complex problems where nonlinear complexities hinder analytical or theoretical analysis. Thus, in this section we develop practical adversary and simulation models upon which numerical analysis and simulation results are based. Here,

our goal is to establish a practical simulation environment that replicates real-world radio/channel conditions. Special attention is given to constructing a realistic shadow fading model with spatial correlation, and network scenarios with mobile devices of practical radio/antenna types. By accomplishing this task we can test various types of attacks to understand their behavior, effectiveness, and potential impact. We will use the models throughout the work unless otherwise mentioned.

2.4.1 Adversary and Network Models

In this work we desire to simulate general network scenarios while reflecting key features of location estimators under attack. The specific network configuration assumed here employs short-range (approximately 15 m) unknown/unlocalized mobile target(s) and 100 nodes with known coordinates among which only a small fraction of nodes are *hearable* anchors as seen in Fig. 2.1. Other unhearable anchors are not involved in localization process. The nodes are randomly placed in a two-dimensional area of size 100×100 m^2 (σ_S = 5 dB, the spatial correlation distance of shadowing D_c = 10 m, receiver sensitivity S_{rx} = −75 dBm, n_p = 4) as shown in Fig. 2.1. The feasible solution region is set to be *unconstrained* due to the unpredictable nature of radio propagation and the attacker's unknown position.

The mobile targets are considered as legitimate network clients or attackers employing either an omni-directional antenna or a directional (smart) antenna. Specifically, the adversaries falsify either SS features (*i.e.*, a signal strength or SS attack), an antenna beam pattern (*i.e.*, a beamforming or BF attack) or their combination (*i.e.*, SS+BF attack). As detailed in Chapter 4, the mobile position can be falsified by misinforming the network of transmitter parameter values (*e.g.*, P_t, G_t) or amplifying/attenuating the transmitted power with the aid of hardware or environmental effects. The degree of such a falsification is termed the *SS attack level*.

Example 2.3 – Modeling a Beamforming Attack

In many applications, it is necessary to electrically steer an antenna main beam in a desired direction. This adaptive BF or smart antenna technique can be employed by an adversary to cause very large location errors–namely, a BF attack. One of the simplest yet commonly used antenna types is a *uniform circular array* (UCA) due to the capability of steering a main beam at any azimuth angle with little change in either the beamwidth or the sidelobe level [71, 72]. The array factor (AF) for a UCA–that is the radiation pattern assuming an isotropic point source for each element–is equal to

$$AF(\Theta, \Phi) = \sum_{n=1}^{N_a} I_n \exp(j\varpi_n) \tag{2.2}$$

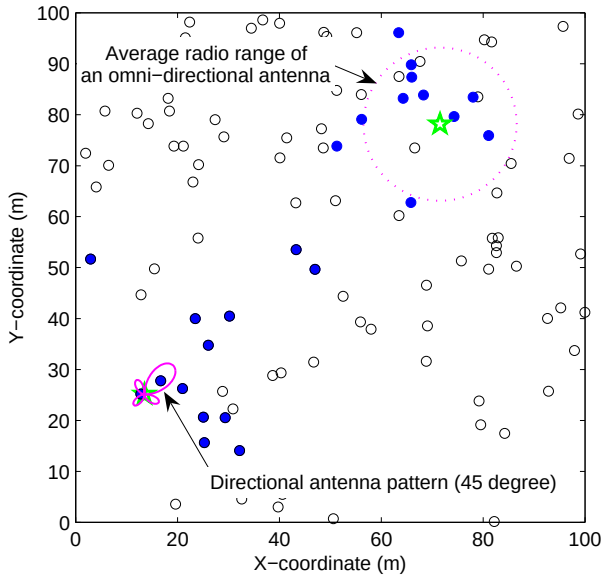


Figure 2.1: An example network scenario with 100 randomly placed nodes in an area of 100×100 m^2. Two attacker models are employed using either an omni-directional antenna (right top corner) or a directional antenna (left bottom corner) ($P_t = 0$ dBm, $S_{rx} = -75$ dBm, $n_p = 4$, $\sigma_S = 6$ dB, "○": inactive anchors (*i.e.*, not used for localization), "●": active (*i.e.*, hearable) anchors, "☆": mobile's true position).

where Θ and Φ are the radiation direction on the x–y plane and along the z-axis, respectively. N_a is the number of array elements and $\varpi_n = \frac{2\pi}{\lambda} d_a \sin\Phi \cos(\Theta - \Theta_n) + a_n$. Here, λ and d_a are the signal wavelength and the radius of the circular array, while I_n and a_n are the excitation amplitude and phase of the nth element, respectively. $\Theta_n = \frac{2\pi n}{N}$ is the angular position of the nth element on the x–y plane. Concerning the development of an adversary model, it is of our interest to:

(a) Find an equation for a_n to direct the mainbeam to a desired direction (Θ_0, Φ_0) given $I_n = 1$.

(b) Assuming a 2-dimensional location problem (*i.e.*, $\Phi = 90°$), examine the antenna pattern and AF azimuthally through 360°.

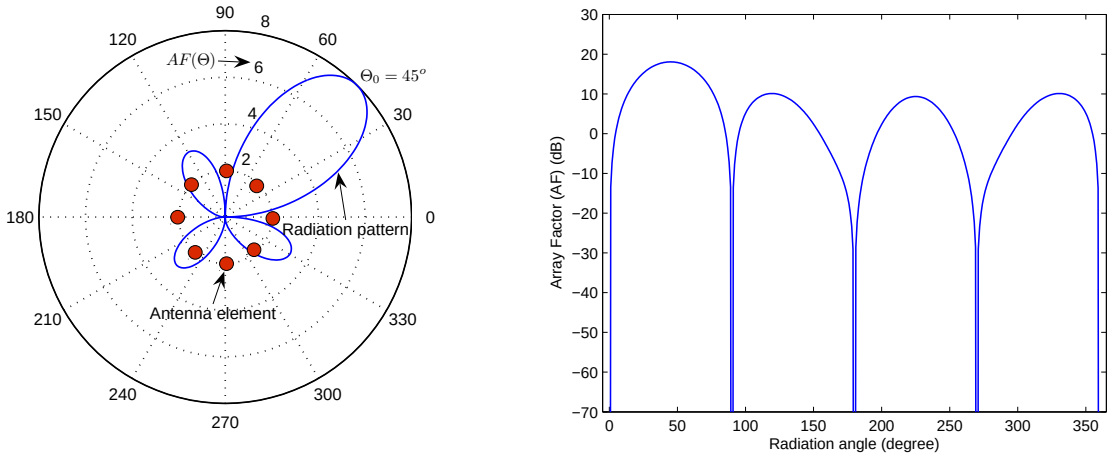
(c) Examine how an adversary can reduce the main beamwidth, and the advantages and disadvantages of having narrower/wider beamwidth from an attacker perspective.

Solution

(a) In order to direct the peak of the main beam in a desired direction (Θ_0, Φ_0), the phase of the nth element needs to be

$$a_n = -\frac{2\pi}{\lambda} d_a \sin\Phi_0 \cos(\Theta_0 - \Theta_n) \tag{2.3}$$

and $I_n = 1$ so that the maximum of AF occurs for $\varpi = 0$.



(a) (b)

Figure 2.2: (a) Directional antenna pattern of an eight-element uniform circular array and (b) the corresponding array factor (AF) at each radiation direction.

(b) Using the above antenna equations, a beamforming pattern can be examined. As an example, we plot the beam pattern using an eight-element UCA with $N_a = 8$, $\Theta_0 = 45°$, $\Phi = 90°$ and the corresponding AF at each azimuth angle in Fig. 2.2. In the rest of this dissertation we use a random beam direction $\Theta_0 \in [0, 2\pi]$ to launch a BF attack.

(c) As N_a increases, the main lobe narrows. Consequently, the attacker can reduce the number of "hearable anchors" within the main beam, making itself less visible to the location system. A smaller number of anchors (*i.e.*, smaller RSS data size) generally leads to a degradation of the location accuracy. However, more sidelobes appear with increasing N_a, although the peaks decrease. Thus, more anchors "behind" the attacker may observe the signal for better node geometry. Further, such a geometric improvement will enhance the performance of attack detection and localization as well as the reliability of location estimation. This geometric issue will be investigated further in Chapter 6.

2.4.2 Spatial Correlation of Shadow Fading

As described in Chapter 3, it is typically observed that shadow fading effects at different receiver locations are spatially correlated. Thus, it is important to take into account the spatial correlation when analyzing the performance of location estimators and the impact of location attacks. We now present a mathematical model that characterizes the spatial correlation of shadow fading.

A correlated shadow fading vector $\boldsymbol{X}_\sigma = [X_{\sigma_1}, \cdots, X_{\sigma_m}]^T$ can be generated by the following procedure. First, we obtain an $m \times m$ covariance matrix $\boldsymbol{K}$ where the ij-element is computed

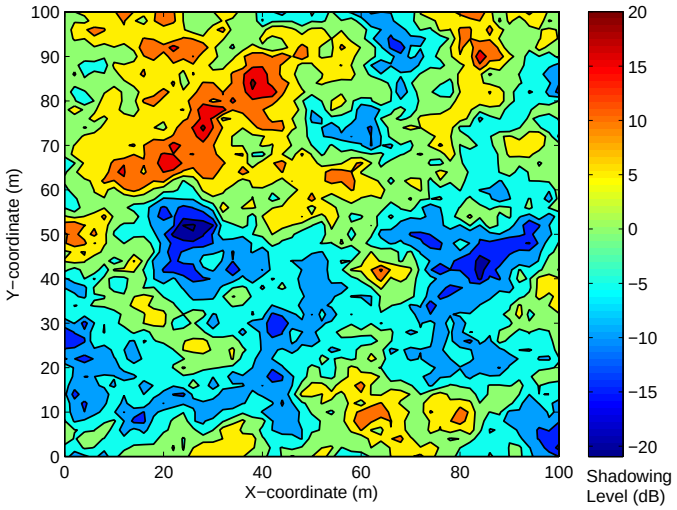


Figure 2.3: A "shadowing map" with spatial correlation generated using Eq. (2.4) with $D_c = 10\ m$ and $\sigma_S = 6$ dB.

as

$$K_{ij}(d_{ij}) = \sigma_S^2 \exp\left(-\frac{d_{ij}}{D_c}\ln 2\right) = \begin{cases} \sigma_S^2, & \text{if } d_{ij} = 0 \\ 0, & \text{if } d_{ij} = +\infty \end{cases} \tag{2.4}$$

where D_c is termed the correlation distance. The above equation indicates that the spatial correlation between any two locations separated by a distance d_{ij} exponentially decays with a constant correlation distance D_c. Previous empirical studies have shown that this location-dependent shadowing model reflects well the real wireless environment [73,74]. The symmetric and nonnegative definite matrix $\boldsymbol{K}$ is then decomposed into $\boldsymbol{K} = \boldsymbol{L}\boldsymbol{L}^T$ by means of Cholesky factorization [75] which can be used to create $\boldsymbol{X}_\sigma = \boldsymbol{L}\boldsymbol{w}$. Here $\boldsymbol{w} = [w_1, \cdots, w_m]^T$ is a vector of m zero-mean, unit-variance, uncorrelated random variables. The resulting "shadowing map" generated by one simulation instance is shown in Fig. 2.3.

In position network simulations with large data sizes (*e.g.*, large-scale WSNs), the above procedure via a matrix operation with Eq. (2.4) may be too computationally intensive and require memory too much. An alternative means for approximating the effect of correlated shadowing is to use a distance-independent covariance matrix (assuming $\rho_{S_{ij}} = \rho_{S_{ji}}$)

$$K_{ij} = \begin{cases} \sigma_S^2 & \text{if } i = j \\ \rho_{S_{ij}}\sigma_S^2 & \text{if } i \neq j \end{cases} \tag{2.5}$$

instead of Eq. (2.4). Note in this model that as the correlation ρ_S increases, the overall shadowing variance of ΔX_σ in the DRSS case (refer to Eq. (3.8)) tends to decrease. (This relationship can be seen from Eq. (3.13).) According to our simulation results, the average performance of both RSS- and DRSS-based location estimators with Eq. (2.5) closely

approximates that with Eq. (2.4). Nevertheless, we employ a more sophisticated spatial correlation model given in Eq. (2.4) in this dissertation except in Chapter 3 where the average estimator performance is of particular concern.

Chapter 3

Fundamentals of Received Signal Strength Based Position Location

3.1 Introduction

In this dissertation, our approach to detecting and locating a malicious node which is attempting to falsify its position is developed based on using received signal strength or RSS measurements. Thus, it is important to understand the fundamentals of RSS-based position location and the associated estimation issues. To this end, this chapter addresses the fundamental aspects of location estimation based on RSS measurements. The problem of RSS-based location estimation can be mathematically formulated as one introduced in Chapter 1, where the measurements are signal strength (SS) or power levels of the mobile device–emitting RF energy–observed at a set of anchor nodes.

Localization techniques using RSS measurements are classified mainly into (a) range-based positioning, (b) RF fingerprinting and (c) proximity-based positioning (see Section 3.2). While we introduce all three techniques in this chapter, we focus our attention on the method of range-based positioning (see Sections 3.3–3.5) which will be used for attack detection and adversary localization later in this dissertation. Specifically, we discuss their geometric interpretations, solutions, achievable location accuracy, and optimal/practical estimators. Then, we show via simulation results the effect of spatially correlated shadow fading, the number of anchor nodes, and path loss rate.

3.1.1 Why is RSS Attractive for Localization?

The task of location estimation has attracted a great deal of attention from academia, industry and the military for over 60 years. In the early years, most research activities were driven by the military demand for target detection and tracking (*e.g.*, radar and sonar). The most

stringent requirement of military applications is the accuracy of location estimation, while the system cost and complexity are typically not a major concern. On the other hand, the aforementioned civilian location applications which have led to many recent location studies from academia and industry are very concerned about the cost, complexity and feasibility of a location system. For many practical location applications, the goal of a location system designer is to minimize the system requirements despite reasonable degradation in location accuracy. To this end, an RSS-based approach is an attractive candidate for position location in wireless networks.

It should be noted that in the early years, location applications employed only a small number of sophisticated receivers or sensor/antenna arrays, typically as few as two or three, particularly for long-distance positioning. Consequently, it was typically preferred to use TDOA/TOA or AOA measurements over RSS to achieve high location accuracy [76–78]. However, the recent proliferation of wireless devices and networks has enabled a larger number of observation points which are thus relatively close to the mobile target. Further, new wireless applications and services for which the RSS approach is suitable have been developed, particularly in indoor and urban non-line-of-sight (NLOS) environments. In these scenarios, an RSS-based approach is a viable, cost-effective solution which can be applied to a broad range of applications, while providing comparable location accuracy.

Despite lower location accuracy with a small number of nodes in general, RSS-based localization is a simple, low-complexity method which can be integrated into another type of location system as a hybrid approach. Particularly, RSS values are readily available in (nearly) every wireless system without additional hardware or system modifications. In fact, RSS information is required by many wireless standards and specifications for the purpose of basic radio functions such as clear channel assessment, link quality estimation, handover, and resource management. Further, it may be the only ranging information available, for example, in severe multipath environments or for surveillance/security applications.

3.2 Techniques Using RSS for Position Location

We next describe the major RSS-based localization approaches: (a) range-based positioning, (b) RF fingerprinting and (c) proximity-based positioning.

3.2.1 Range-Based Positioning

The signal power or RSS observed over wireless channels changes in a random and unpredictable manner, and thus can only be characterized statistically. Therefore, a statistical model for RSS is employed to estimate a transmitter-receiver distance or "range" d_i which is then used to infer location coordinates via lateration as described in Section 3.3. On the other hand, noting that this method is sub-optimal we can also incorporate the model

directly into an optimization framework as in Section 3.4.

Statistical Model for RSS

In the wireless transmission media, a signal transmitted by a mobile device travels along a number of different paths of varying lengths, referred to as *multipath*. This radio propagation causes signal distortions and fades which are attributed to reflection, scattering, diffraction, and/or refraction from buildings, trees, furniture and other obstructions in the environment [40]. The overall loss in signal strength is typically characterized as a product of three factors; namely, local mean propagation loss, long-term or slow fading, and short-term or fast fading. The first two factors are considered large-scale (*i.e.*, 10's or 100's of meters) effects, whereas short-term fading is a small-scale (*i.e.*, $< 1\ m$) effect.

Let us consider a location system where m anchor nodes estimate their distances d_i to the mobile of interest using the observed signal strength $\{P_i\}_{i=1}^{m}$. The received power or RSS (dBm) at a transmitter-receiver distance d_i for the ith anchor is characterized as

$$P(d_i) = P_t - \underbrace{\left(\overline{PL}(d_i) + \mathcal{M}_{F_i} + X_{\sigma_i}\right)}_{\text{Total propagation loss on the } i\text{th link}} \tag{3.1}$$

where P_t (dBm) is the mobile's transmit power and $\overline{PL}(d_i)$ (dB) is the local mean propagation or path loss as a function of distance d_i. The small-scale fading $\mathcal{M}_F$ (dB) generally varies abruptly (as much as 30 or 40 dB) over a distance of only a fraction of a wavelength. On the other hand, X_σ (dB) is the slow-term fading due to shadowing effects. Thus, by relating the received power $P(d_i)$ to a path loss model for $\overline{PL}(d_i)$ we can estimate d_i.

The path loss (PL) is typically modeled as a function of $PL(d_0)$ (dB) measured at a close-in reference distance d_0 ($< d_i$) or predicted by an empirical model (*e.g.*, Eq. (3.7) with $d_i = d_0$). As many measurement campaigns [40, 63] and analytical results [79] have shown, the relationship between path loss and distance can be captured in a log-distance equation

$$PL(d_i)\ (\text{dB}) = \overline{PL}(d_0) + 10 n_p \log_{10}\left(\frac{d_i}{d_0}\right) + X_{\sigma_i} \tag{3.2}$$

where n_p is termed the path loss exponent or gradient, indicating that the transmitted signal power P_t decays with d^{n_p} on average. The value of n_p typically ranges from two (in the free space or clear LOS channels) to five, which tends to increase with more NLOS paths [40]. Assuming that the effect of small scaling fading is reduced by averaging it out over a range of frequencies, space or some time period, location estimation using Eq. (3.2) is mainly subject to large-scale shadow fading $X_\sigma \sim \mathcal{N}(0, \sigma_S^2)$; it is empirically modeled as a log-normal random variable with zero mean and variance σ_S^2 (σ_S in dB). This environment-dependent variability is one of the most influential yet unavoidable factors in RSS-based localization. Hence, the received power P at d_i is also log-normally distributed with mean $\bar{P}$ as

$$P(d_i)\ (\text{dBm}) \sim \mathcal{N}\big(\bar{P}(d_i), \sigma_S^2\big) \tag{3.3}$$

where the ensemble mean received power

$$\bar{P}(d_i)\ (\text{dBm}) = P(d_0)\ (\text{dBm}) - 10n_p(\log_{10} d_i - \log_{10} d_0). \tag{3.4}$$

Equivalently, the modified observation v_i at anchor i is defined as

$$\begin{aligned} v_i\ (\text{dB}) &= P(d_0) - P(d_i) \\ &= L(d_i) + X_{\sigma_i} \end{aligned} \tag{3.5}$$

where $L(d_i) = 10n_p(\log_{10} d_i - \log_{10} d_0)$. Noting that d_i is a function of the unknown target position (x, y), we will use the notation $L_i(\boldsymbol{\theta})$ interchangeably depending on the context. Due to the log-normal shadowing term, the observation v_i is also log-normally distributed with mean $L_i(\boldsymbol{\theta})$ and the probability of density function (PDF)

$$f_V(v_i; \boldsymbol{\theta}) = \frac{1}{\sqrt{2\pi}\sigma_S} \exp\left(\frac{-(v_i - L_i(\boldsymbol{\theta}))^2}{2\sigma_S^2}\right). \tag{3.6}$$

Basics of Differential RSS

The received signal power $P(d_0)$ at d_0 in Eq. (3.5) is a function of two types of parameters– that is transceiver and environmental parameters–as reflected in the Friis free space equation [40]

$$P(d_0) = P_t \frac{G_t \mathcal{L}_t^{-1} G_r \mathcal{L}_r^{-1} \lambda^2}{(4\pi)^2 d_0^2} \tag{3.7}$$

where G_t and $\mathcal{L}_t$ (or G_r and $\mathcal{L}_r$) denote antenna gain and system loss factors of a transmitter (or a receiver), respectively. λ is the wavelength of the transmitted signal. In this unobstructed LOS channel model, the signal power decays according to the inverse-square law (*i.e.*, $n_p = 2$). To minimize location error, we should know or estimate the system parameters as precisely as possible, thus requiring offline calibrations. However, in many practical situations, this manual effort may be too costly or infeasible. Even if the environmental parameters can be accurately determined or known *a priori*, the transmitter parameter values may not be readily available at the anchors, or could be erroneously reported or even falsified. In most studies, the values are assumed to be perfectly known *a priori*. This assumption is made by relying on some form of cooperation from reliable signal sources (*e.g.*, via a *predefined* beacon/pilot signal) and an accurate radio calibration of the transmitter. This passive dependency raises security concerns for location systems subject to various attacks as presented later in this dissertation.

One means of eliminating or reducing the need for knowledge of the system parameters is to change the observation to *differential* RSS or DRSS

$$\begin{aligned} v_{ij}\ (\text{dB}) &= v_j - v_i \\ &= L(d_i, d_j) + \Delta \mathrm{X}_{\sigma_{ij}} \end{aligned} \tag{3.8}$$

where

$$L(d_i, d_j) = 10n_p(\log_{10} d_j - \log_{10} d_i) \tag{3.9}$$

and $L(d_i, d_j)$ (or $L_{ij}(\boldsymbol{\theta})$) is a differential log-distance path loss model with $i, j \in \{1, \ldots, m\}$, $i < j$. As a general rule of notation in this work, the subscripts fall in this range, unless indicated otherwise. It can be noticed that all or most of the transmitter uncertainties in $P(d_0)$ are removed. Also, note that RSS measurements at m anchor nodes yield an un-ordered set of M distinct DRSS measurements and corresponding path loss equations where

$$M = \binom{m}{2} = \frac{m(m-1)}{2} = \underbrace{m-1}_{\text{basic}} + \underbrace{\frac{(m-1)(m-2)}{2}}_{\text{redundant}} \tag{3.10}$$

in which an ij-pair and a ji-pair are counted only once. This means that the whole set of size M can be determined by a linear combination of the $m-1$ basic (or non-redundant) measurements. The geometric interpretation of these equations for localization is presented in Section 3.3.

Example 3.1 – Statistical Features for DRSS

Based on the fact that shadow fading X_σ and the RSS observation can be modeled as log-normal, we can find the joint PDF of two shadowing components X_{σ_i} and X_{σ_j} at anchor positions i and j. Because $P(d_i)$ is a Gaussian random variable (conditioned on the distance d_i), the random variables $P(d_i)$ and $P(d_j)$ from the same signal source are jointly Gaussian in the log domain. Specifically, the two random variables X_{σ_i} and X_{σ_j} can be related by a bivariate Gaussian distribution so that the joint probability density of X_{σ_i} and X_{σ_j} is

$$f_{X_{\sigma_i}, X_{\sigma_j}}(\eta_i, \eta_j) = \frac{1}{2\pi\sigma_S^2\sqrt{1-\rho_{S_{ij}}^2}} \exp\left\{\frac{-\left(\eta_i^2 - 2\rho_{S_{ij}}\eta_i\eta_j + \eta_j^2\right)}{2\sigma_S^2(1-\rho_{S_{ij}}^2)}\right\} \tag{3.11}$$

where $\rho_{S_{ij}}$ is the correlation coefficient reflecting the degree of spatial correlation between the shadow fading components at any two locations i, j. The PDF for $\Delta X_{\sigma_{ij}}$ which represents the difference of the correlated Gaussian random variables can be derived using Eq. (3.11) as

$$\begin{aligned} f_{\Delta X_\sigma}(\Delta\eta_{ij}) = {} & \frac{1}{2\pi\sigma_S^2\sqrt{1-\rho_{S_{ij}}^2}} \\ & \cdot \int_{-\infty}^{+\infty} \exp \frac{-\left(\eta_i^2 - 2\rho_{S_{ij}}\eta_i(\eta_i - \Delta\eta_{ij}) + (\eta_i - \Delta\eta_{ij})^2\right)}{2\sigma_S^2(1-\rho_{S_{ij}}^2)} d\eta_i \end{aligned} \tag{3.12}$$

so that

$$f_{\Delta X_\sigma}(\Delta\eta_{ij}) = \frac{1}{2\sigma_S\sqrt{\pi(1-\rho_{S_{ij}})}} \exp\Big(\frac{-\Delta\eta_{ij}^2}{4\sigma_S^2(1-\rho_{S_{ij}})}\Big). \tag{3.13}$$

It is clear that ΔX_σ is Gaussian with zero mean and variance $\hat{\sigma}_S^2 = 2(1-\rho_{S_{ij}})\sigma_S^2$. The variance $\hat{\sigma}_S^2$ can also be derived as $\hat{\sigma}_S^2 = 2\sigma_S^2 - 2\mathrm{C}(X_{\sigma_i}, X_{\sigma_j})$ where the covariance $\mathrm{C}(X_{\sigma_i}, X_{\sigma_j}) = \rho_{S_{ij}}\sigma_S^2$. From Eqs. (3.8) and (3.13), we can see that the observation v_{ij} is log-normally distributed with mean L_{ij} and variance $\hat{\sigma}_S^2 = 2(1-\rho_{S_{ij}})\sigma_S^2$. Thus, its PDF is

$$f_V(v_{ij};\boldsymbol{\theta}) = \frac{1}{2\sigma_S\sqrt{\pi(1-\rho_{S_{ij}})}} \exp\Big(\frac{-(v_{ij}-L_{ij}(\boldsymbol{\theta})^2}{4\sigma_S^2(1-\rho_{S_{ij}})}\Big). \tag{3.14}$$

which depends on the spatial correlation $\rho_{S_{ij}}$ of shadow fading components over different links.

Although most existing studies in RSS-based localization simply assume that shadowing noise components at two locations are independent (*i.e.*, $\rho_S = 0$), in reality the spatial correlation of shadow fading is often substantial due to similar terrain or obstacles on the signal propagation paths between the source and anchor nodes. It has been found in previous empirical studies that a typical value for the correlation coefficient ranges from 0.2 to 0.8 in indoor [63] and outdoor [64] channels, and as the angle and distance between a pair of reference locations decreases, the correlation tends to increase. Therefore, for simulation studies, it is important to take the correlation into account for accurate analysis of signal strength-based location estimation [80]. In this work, we employ the model for the spatial correlation introduced in Chapter 2.4.2.

3.2.2 RF Fingerprinting

We have discussed earlier that multipath fading degrades the performance of a location system significantly. Especially in indoor and urban environments where many recent location applications are targeted, the effect of fading is often so severe that other positioning techniques based on TOA/TDOA and AOA encounter difficulties. Also, range-based positioning using RSS will experience higher shadowing variance under greater multipath fading.

In the multipath location problem, we can exploit the high variability of multipath signals to relate each position $\boldsymbol{z_j} = [x_j, y_j]^T$ to its unique signal signature $\mathcal{F}_j$ which is referred to as an *RF "fingerprint"* [15]. The more the signal strength varies over different locations, the more selective fingerprints can be collected, thus leading to better location accuracy. The simplest form of the signal signature $\mathcal{F}_j$ is a vector of RSS readings at each anchor position, thereby avoiding sophisticated hardware. When each receiver can provide its measured multipath delay profile, the fingerprinting resolution can be improved. However, since the acquisition

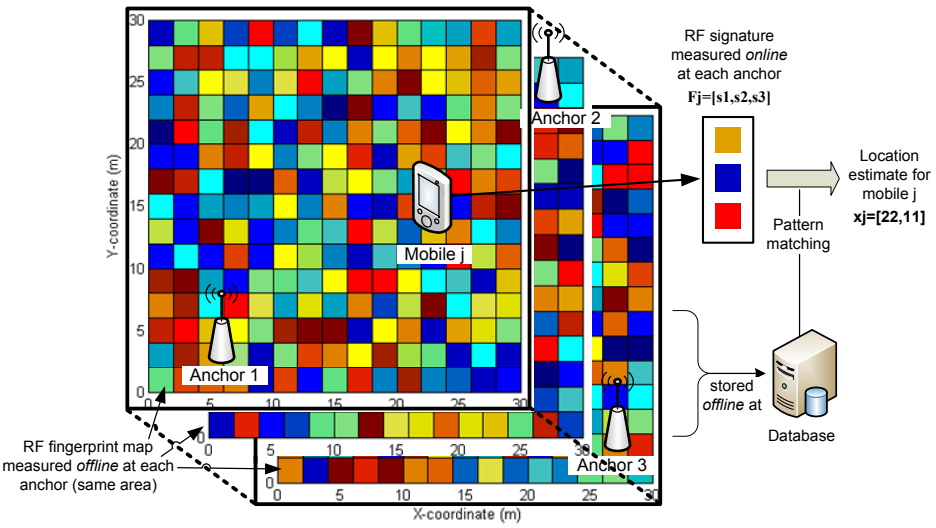


Figure 3.1: An illustration of RF fingerprinting for locating a mobile device.

of the multipath profile usually requires wide signal bandwidth and sophisticated hardware, it may be too costly unless the existing infrastructure provides that capability.

As illustrated in Fig. 3.1, the process of RF fingerprinting can be divided into the following two primary phases as similarly implemented in [15].

1. *Offline training phase*–For each of N positions $\{\boldsymbol{z}_j\}_{j=1}^{N}$ (on a grid) in the area of interest, signal measurements are taken at m observation (or receiver) points to produce the associated RF fingerprints $\{\mathcal{F}_j\}_{j=1}^{N}$, where $\mathcal{F}_j = [s_{j1}, \ldots, s_{jm}]^T$. The observed data s_j can be an RSS value, a multipath delay profile, and/or orientation of the operator's body. Then, the fingerprints are collected to construct a "radio map" which is stored in a database prior to the localization process.

2. *Online localization phase*–Upon arrival of a signal, the signal signature of interest $\bar{\mathcal{F}}_i = [\bar{s}_{i1}, \ldots, \bar{s}_{im}]^T$ for mobile i is extracted and compared to the radio map using one or more pattern matching techniques (*e.g.*, k-nearest neighbors, naive Bayes classifiers). Then, the mobile position is estimated as $\hat{\boldsymbol{z}}_{\boldsymbol{i}} = [\hat{x}_i, \hat{y}_i]^T$ by selecting the best match or interpolating among the best matches on the radio map.

Despite attractive aspects of RF fingerprinting, there are practical issues that hinder widespread adoption of the approach. In particular, the construction of accurate RF fingerprints or a radio map requires considerable offline effort and cost due to offline measurements, manual calibration, thorough site planning, and more. Also, since wireless channels and networks are inherently time-varying, the radio map needs to be updated regularly (*e.g.*, when large furniture or a wall is removed). Therefore, the success of this RSS approach will depend on

how one addresses unpredictable wireless environments, interference, user behaviors (*e.g.*, antenna/body orientation), costly hardware and other practical issues.

3.2.3 Proximity-Based Positioning

In distributed ad-hoc wireless applications such as WSNs, a majority of sensors with unknown position try to localize themselves through cooperation–what is sometimes referred to as *relative positioning* [12, 81]. Their absolute positions are then found with the aid of a small number of reference nodes with *global* coordinate knowledge. Relative position location can be accomplished using range-based techniques. However, in large-scale networks, iterative optimization algorithms generally create challenging issues of computational inefficiency, non-guaranteed global optimality and convergence to construct a global map of node locations. Also, for some WSN applications, just coarse-grain sensor locations are sufficient.

In such location scenarios, range-free localization techniques based on *proximity* or *connectivity* information are attractive. By "connectivity" we mean whether or not unlocalized sensors/nodes are within communications range (or radio range) with others in the network. The principle of this approach is that the relative positions of (neighboring) nodes in the network are found according to the proximity constraints. As a descriptive example, a pair of unlocalized sensor position vectors "push" each other to be outside the radio range when the sensors are not connected. On the other hand, when connected, the position vectors "pull" each other to be within the radio range, but this effort may be restricted by other neighbors which do the same to them. When RSS readings are available, this simple proximity information can be enhanced by taking into account approximate distances (or ranges) among the nodes. This principle can be implemented by various means among which we choose a dimensionality reduction approach below to demonstrate the proximity-based concept. Other approaches are described with references in [13].

Dimensionality Reduction Using Geographical Proximity

In recent years, the problem of *dimensionality reduction* has arisen in various fields of research dealing with large amounts of high-dimensional data including psychology, computer vision, artificial intelligence, and cognitive sciences [82, 83]. The popularity is a consequence of the growing awareness that the underlying structure of relations among the observed data can be revealed and their similarity (or proximity geometrically) can be observed through the concept of dimensionality reduction. Specifically, in this process, the fundamental information of high dimensional data can be embedded and visualized as a set of points in a low-dimensional space. For example, a number of images of a person's face depicting different appearance variations such as illuminations and poses are explored and then visualized as a set of 2-D or 3-D dimensional vectors in a Euclidean space, where axes are associated with observed modes of variability [82].

Recently, many attempts have been made to develop efficient algorithms that discover a geometric embedding structure of input data, while integrating classical algorithmic features of dimensionality reduction such as guaranteed global optimality and convergence. Unlike traditional parametric approaches such as LS and maximum likelihood (ML) estimation through which unknown parameters of some data model are optimized iteratively, they estimate the parameters based on the functional dependence of the observed data on distance measures. The type of dependence, whether linear or nonlinear, classifies dimensionality reduction algorithms. Multidimensional Scaling (MDS) and Principal Component Analysis (PCA) are classical linear dimensionality reduction algorithms [84], whereas Isomap [82], Locally Linear Embedding (LLE) [83], Hessian-based Locally Linear Embedding (HLLE) [85] and Laplacian Eigenmap (LE) [86] are those developed for nonlinear dimensionality reduction.

Among many types of MDS methods, classical MDS is the simplest one for quantitative data (*i.e.*, RSS measurements or proximity data), using one similarity matrix, and the proximity between the data is treated as a Euclidean distance [87, 88]. The key of the algorithm is to find interpoint Euclidean distances d_{ij} between a pair of data points $\boldsymbol{z}_i = [x_{i1}, \ldots, x_{i\mathcal{D}}]^T$ and $\boldsymbol{z}_j = [x_{j1}, \ldots, x_{j\mathcal{D}}]^T$. These distances are then related to the proximity measures p_{ij} of the data of size n and dimension $\mathcal{D}$. To reveal the *linear* relationship, a linear transformation is applied to relate d_{ij} to p_{ij} such that $d_{ij} = \alpha + \beta p_{ij}$ where p_{ij} are elements of an $n \times n$ proximity matrix $\mathbf{P}$. It can be shown that the matrix $\mathbf{P}$ is double centered so that the elements of $\mathbf{P}$ satisfy the relation [88]

$$-\frac{1}{2}\left(p_{ij}^2 - \frac{1}{n}\sum_{i=1}^{n} p_{ij}^2 - \frac{1}{n}\sum_{j=1}^{n} p_{ij}^2 + \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^2\right) = \sum_{k=1}^{\mathcal{D}} x_{ik}x_{jk}. \tag{3.15}$$

Using singular value decomposition (SVD), the double centered matrix on the left side, say $\mathbf{G}$, can be found as $\mathbf{G} = \mathbf{L}\Sigma\mathbf{L}^T$ so that we have a coordinate matrix $\mathbf{X} = \mathbf{L}\Sigma^{1/2}$. By computing the first $\mathfrak{d}$ largest eigenvalues and associated eigenvectors we can determine the coordinates of the sensors in the space of lower dimension $\mathfrak{d}$ ($\mathfrak{d} < \mathcal{D}$) (*e.g.*, $\mathfrak{d} = 2$ in 2-D localization).

Despite some good features of the MDS algorithm such as the closed-form solution, global optimality and convergence, the assumed linear relationship between the proximity measure p_{ij} and the Euclidean distance d_{ij} should hold for reconstructing the original geometric map. However, when exploiting useful proximity-related information such as the degree of proximity using a nonlinear path loss model in Eq. (3.2) or spatial correlation of the data [89], the linearity assumption may be an oversimplification. Also, the classical MDS technique needs global knowledge of the network, thus hindering its adoption in many application scenarios. To address this issue, nonlinear manifold algorithms can be employed for dimensionality reduction.

The main idea behind manifold algorithms is that despite the nonlinearity of the intrinsic embedding structure of the data in a high dimensional space, a local neighborhood region (where K points are grouped) is approximately linear. Thus, inter-point Euclidean distances or weights in the small region can be used to represent the data while preserving the original

nonlinear manifold. Isomap is similar to classical MDS except for the first stage that finds the geodesic shortest path for a pair of all non-neighboring nodes. Most manifold algorithms try to find the eigenvectors associated with the $\mathfrak{d}+1$ largest eigenvalues from the $\mathfrak{d}$-dimensional embedding coordinates. A detailed description of the algorithms can be found in in [82–86].

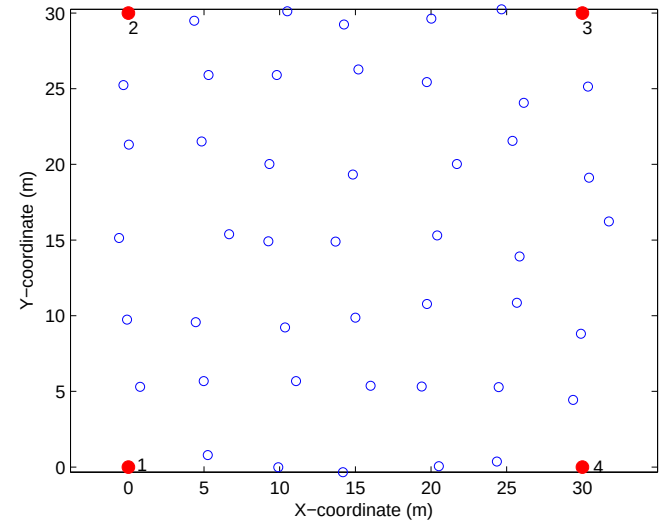
Note that these relative positioning algorithms produce the embedded relative map of sensor coordinates. To obtain a global (or absolute) map of sensor coordinates, we need to exploit knowledge of the anchors' positions (if known) to transform the relative map into the global map via a geometric transformation including translation, rotation, scaling and/or reflection as similarly done in Eq. (3.24).

Example 3.2 – Simulating Dimensionality Reduction Algorithms

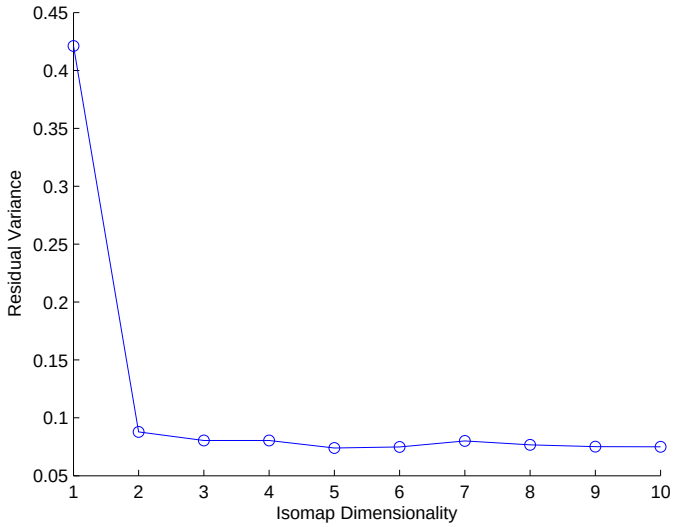
We now use dimensionality reduction algorithms implemented in Maltab for sensor localization. Download the Matlab toolbox of the algorithms, named `toolbox_dimreduc`, available in [90]. Consider a simple 2-D location scenario as shown in Fig. 3.2a, where 45 unlocalized sensors (denoted by blue hollow circles) are deployed on a $30m \times 30m$ grid with placement error $e_p \sim \mathcal{N}(0, 0.5^2)$ over the channel with $\sigma_S = 5$ dB and $n_p = 3$. Four anchor nodes (denoted by filled red circles), one at each corner, are located at known coordinates. Generate RSS data using Eqs. (3.3) and (3.4) so that each algorithm takes as input Euclidean distances between the data. (a) Find the intrinsic dimensionality of the data. (b) Construct the 2-D embedding for each algorithm and reconstruct the original location map. Compare the results with MDS and other nonlinear dimensionality reduction algorithms.

(a) In general, the original dimension embedded in the data can be found by examining major principal components and the eigenvalues which correspond to the variance explained by the principal components. For example, as shown in Fig. 3.2b, the intrinsic dimensionality can be determined using Isomap by seeking the "knee" point on the curve from which the variance begins to exhibit little change over dimensionality after dropping abruptly.

(b) In Fig. 3.3, we show 2-D embeddings (left column) and reconstructed location maps (right column) using classical MDS (Figs. 3.3a and 3.3b) and Isomap with different neighborhood sizes ($K = 5, 10$) (Figs. 3.3c–3.3f). From the embedded relative map of sensor coordinates (which is the output of the algorithm), the knowledge of the anchors' coordinates is used to transform the relative map into the global map. From the simulation results, we can see that the nonlinear algorithm, Isomap, reconstructs the original location map better than classical MDS. However, not all the nonlinear algorithms perform as desired.



(a)



(b)

Figure 3.2: (a) Grid node placement with 4 anchors (at each corner) and 45 unlocalized sensors placed erroneously. (b) A typical residual variance curve to measure the embedded original dimension ($\mathfrak{d} = 2$, $\sigma_S = 5$ dB, $n_p = 3$).

.

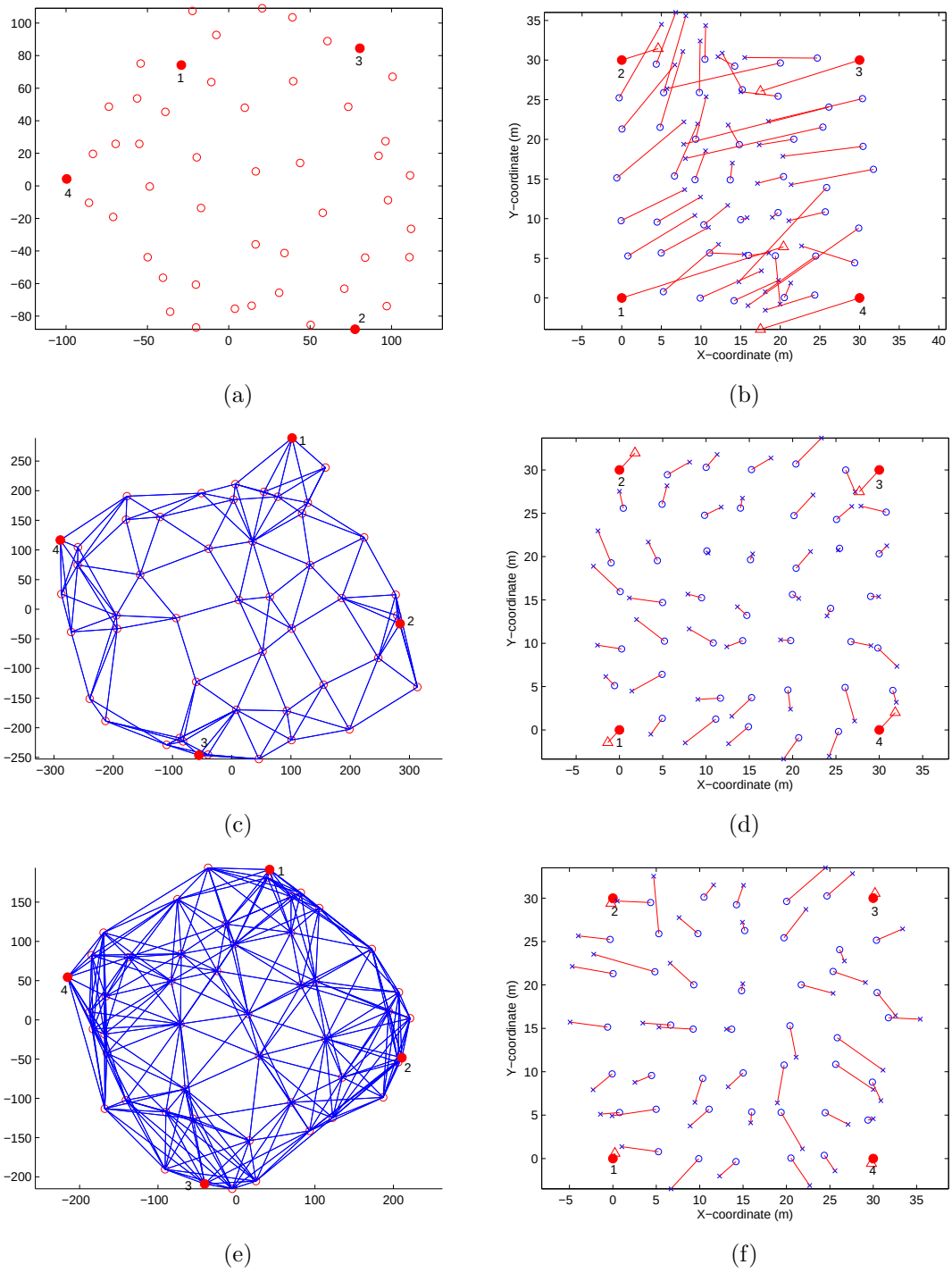


Figure 3.3: (a,b) MDS: 2-D embedding (left) and reconstructed map of sensor coordinates (right). (c,d) Isomap: 2-D embedding (left) and reconstructed map (right) using a neighborhood graph with $K = 5$. (e,f) Isomap: 2-D embedding (left) and reconstructed map (right) with $K = 10$. The unfilled circles and crosses indicate true and estimated positions, respectively.

3.3 Geometric Interpretations of SS-Based Positioning

The problem of wireless localization is to find the unknown mobile position which is equivalent to a point in the 2-D or 3-D Cartesian coordinate system. Thus, it is natural to represent the point in a geometric form so that the problem can be described using basic geometric equations. The geometric interpretation not only sheds light on the problem, but also facilitates development of new location algorithms and theories. This section provides geometric interpretations of range-based positioning using SS measurements (*i.e.*, RSS or DRSS) along with the mathematical representations of RSS/DRSS lateration. We show that although the two approaches exhibit the same geometric shape (*i.e.*, circular), the geometry and redundancy of the circles are different.

3.3.1 RSS-Based Lateration

We have described that the mobile position can be determined using a set of m range estimates. In RSS-based positioning, the range estimates can be represented by m circles with radii $\{\hat{d}_i\}_{i=1}^m$ in the 2-D space (or spheres in the 3-D space) centered at each anchor position $\{\boldsymbol{x_i}\}_{i=1}^m$ as described by Eq. (1.1). The circumference of the circle defines an uncertainty of mobile position (x, y). This means that, in a noiseless case, the position can be found at the common intersection point of m circles as illustrated in Fig. 3.4. Due to the nonlinearity of the equations, it is necessary for 2-D source localization to have $m \geq 3$ to avoid an ambiguous solution. Even when this condition is satisfied, in practice, there exists no unique intersection point due to various sources of error (including shadow fading) which perturb the circles or range estimates. Thus, it is usually better to have $m > 3$.

Example 3.3 – Linear Solution of RSS Trilateration

Consider a range-based location network of three anchor nodes with known coordinates $\boldsymbol{x_i} = [x_i, y_i]$. Based on RSS measurements subject to noise, suppose that each anchor i estimates its distance d_i to some mobile device. Then, we can estimate the mobile position (x, y) by solving the system of three nonlinear equations in Eq. (1.1) (*i.e.*, $m = 3$) in a geometric approach. Assuming the circles all intersect each other, as described in Fig. 3.4 we can connect two intersection points for each pair of circles to generate a line of position on which the mobile is supposed to lie. In a noiseless case, the mobile will lie on the common intersection point of the lines or circles.

We now write a mathematical equation that represents such a geometric line of position. A line of position that passes through two intersection points of a pair of circles i, j can be obtained by taking the difference of an RSS circle i from another RSS circle j for $i < j$ as

$$(x_j - x_i)x + (y_j - y_i)y = \frac{1}{2}\left\{\|\boldsymbol{x_j}\|^2 - \|\boldsymbol{x_i}\|^2 - (\hat{d}_j^2 - \hat{d}_i^2)\right\}, \quad i < j \tag{3.16}$$

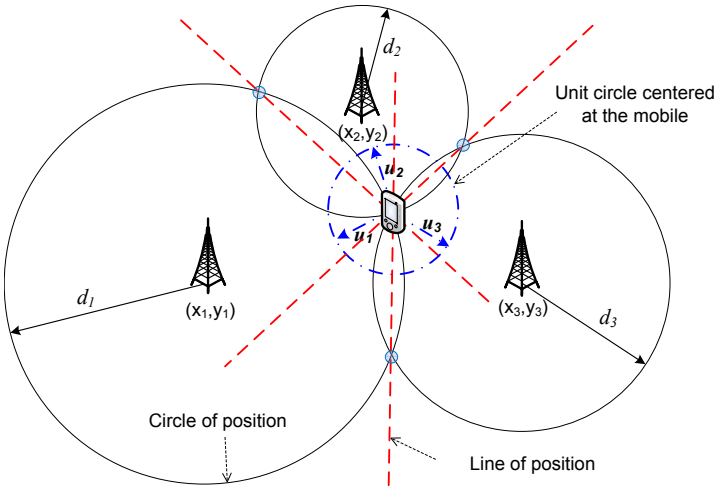


Figure 3.4: Trilateration using RSS range measurements $\{\hat{d}_i\}_{i=1}^{m}$ ($m = 3$) in a noiseless scenario (*i.e.*, $\hat{d}_i = d_i$). $\boldsymbol{u}_i$ is the unit vector in the direction of ith anchor.

or

$$y = -\left(\frac{x_j - x_i}{y_j - y_i}\right)x + \frac{\|\boldsymbol{x_j}\|^2 - \|\boldsymbol{x_i}\|^2 - (\hat{d}_j^2 - \hat{d}_i^2)}{2(y_j - y_i)}, \quad i < j. \tag{3.17}$$

For m circles (or anchors), we can only use $m-1$ *basic* (or non-redundant) lines to form an original system of linear equations. For trilateration (*i.e.*, $m = 3$), two basic lines of position are used to produce the linear system $\boldsymbol{Ax} = \boldsymbol{b}$, where

$$\boldsymbol{A} = \begin{bmatrix} x_2 - x_1 & y_2 - y_1 \\ x_3 - x_1 & y_3 - y_1 \end{bmatrix}, \ \boldsymbol{b} = \frac{1}{2}\begin{bmatrix} \|\boldsymbol{x_2}\|^2 - \|\boldsymbol{x_1}\|^2 - (\hat{d}_2^2 - \hat{d}_1^2) \\ \|\boldsymbol{x_3}\|^2 - \|\boldsymbol{x_1}\|^2 - (\hat{d}_3^2 - \hat{d}_1^2) \end{bmatrix}. \tag{3.18}$$

Then, the mobile position (x, y) can be estimated as $\boldsymbol{x} = \boldsymbol{A}^{-1}\boldsymbol{b}$.

Using Eq. (3.5), it is not difficult to obtain a range estimator as

$$\hat{d}_i = d_0 \cdot 10^{\frac{v_i}{10n_p}} \tag{3.19}$$

which is indeed an ML estimator for the distance d_i due to the log-normality of shadow fading or v_i.

By substituting the given parameter values into Eq. (4.6), we have the distance estimates as $\{\hat{d}_i\}_{i=1}^{3} = \{36.34, 13.13, 31.77\}$ meters. The mobile position is then estimated as

$$\boldsymbol{x} = \boldsymbol{A}^{-1}\boldsymbol{b} = \begin{bmatrix} 30 & 50 \\ 50 & 10 \end{bmatrix}^{-1}\begin{bmatrix} 2274.10 \\ 1455.63 \end{bmatrix} = \begin{bmatrix} 22.75 \\ 31.84 \end{bmatrix}. \tag{3.20}$$

In this example with the true mobile position $(x, y) = (26, 42)$, the location error is 10.67 m. We can improve the location accuracy by (a) exploiting additional anchor measurements to increase the robustness to shadow fading (*e.g.*, via an LS estimator) and (b) incorporating the underlying statistical model in Eq. (3.5) directly into an optimization framework in the form of Eq. (1.2) (see Example 3.4). Before discussing such a more effective (or optimal) approach in the next section, we now explore geometric aspects of DRSS-based positioning.

3.3.2 DRSS-Based Lateration

Recall that DRSS and TDOA data are generated in the same manner (*i.e.*, differences in RSS or TOA data which both define a circle centered at each anchor). While TDOA defines a hyperbolic curve of position, the geometric interpretation of DRSS position is circular, as we will show.

Geometry of Relative DRSS Positioning

Suppose that the relative distance $D_{ij} = \|\boldsymbol{x_i} - \boldsymbol{x_j}\|$ of a pair of anchors or sensors i, j is known *a priori*. Here $\{\boldsymbol{x_i}\}_{i=1}^m$ denotes the ith *absolute* coordinate vector $\boldsymbol{x_i} = [x_i, y_i]^T$ which may be unknown. Next, the middle of the link connecting the pair is translated to the origin of the local coordinate system (X, Y) for the pair. Thus, the two nodes are located at $(-\frac{D_{ij}}{2}, 0)$ and $(\frac{D_{ij}}{2}, 0)$ on the local x-axis, respectively. In detecting a signal from some unknown mobile, the local coordinate system produces a geometric function of $L_{ij}(\boldsymbol{\theta})$ using Eq. (3.9) as

$$\begin{aligned} L_{ij}(\boldsymbol{\theta}) &= 5n_p \left[\log_{10}\left((X - \tfrac{D_{ij}}{2})^2 + Y^2 \right) - \log_{10}\left((X + \tfrac{D_{ij}}{2})^2 + Y^2 \right) \right] \\ &= 5n_p \log_{10}\left(1 - \frac{2D_{ij}X}{(X + \frac{D_{ij}}{2})^2 + Y^2} \right). \end{aligned} \tag{3.21}$$

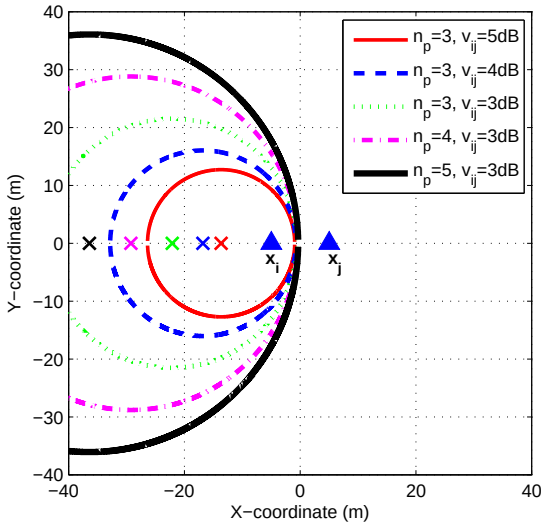
Then, a local y-coordinate of the source location is estimated as

$$Y = \pm\sqrt{\frac{2D_{ij}X}{1 - h_{ij}} - \left(X + \frac{D_{ij}}{2} \right)^2} \tag{3.22}$$

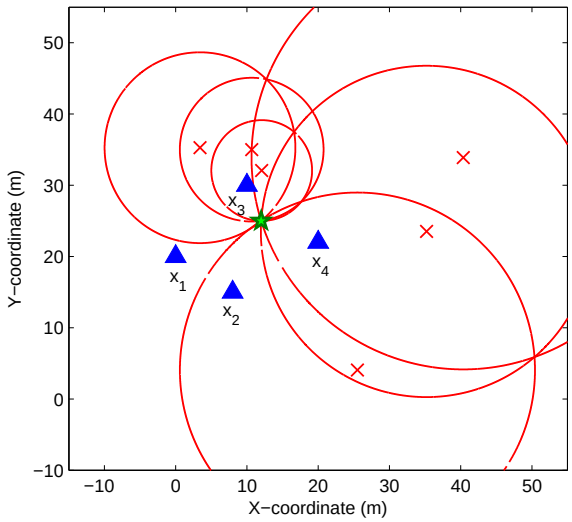
where $h_{ij} = 10^{v_{ij}/5n_p}$. Thus, a pair of nodes form a *local* DRSS circle

$$\left(X + \frac{D_{ij}}{2}\left(\frac{h_{ij} + 1}{h_{ij} - 1} \right) \right)^2 + Y^2 = \frac{h_{ij} D_{ij}^2}{(h_{ij} - 1)^2} \tag{3.23}$$

on which a target node is assumed to (or will in a noiseless case) be located. As noticed in Fig. 3.5a ($D_{ij} = 10$ m), the focus of the circle (marked as "×") is located at $\left(-\frac{D_{ij}}{2}\left(\frac{h_{ij}+1}{h_{ij}-1} \right), 0 \right)$



(a)



(b)

Figure 3.5: (a) Local and (b) global geometric interpretations of DRSS-based positioning in a noiseless case. The source, anchor and the center of each DRSS circle are indicated by "★", "▲" and "×", respectively.

on the x-axis in the local coordinate system. Clearly, the geometry (focus and radius) of the circles is different from that in RSS/TOA-based lateration shown in Fig. 3.4, where the centers of the circles are located at the node/anchor positions. It is also noted that the circles are impacted by the path loss gradient n_p and observation v_{ij} as well as the relative distance D_{ij}. As shown in Fig. 3.5a, the circle grows as either v_{ij} decreases or n_p increases. This is because, for fixed n_p and decreasing v_{ij} (*i.e.*, DRSS $P(d_i, d_j)$ in Eq. (3.8) is decreasing), the source is further from the ith node *relative to* the distance to the jth node. On the other hand, for fixed v_{ij} and smaller n_p, h_{ij} becomes larger for the same DRSS value so that the pattern is reversed. Note that unlike RSS/TOA-based lateration, where each measurement results in a circle, a pair of sensor/anchor measurements correspond to a single circle.

With three or more distinct local circles ($m \geq 4$), the target position can be estimated. It can be noticed from Eq. (3.23) that the observed v_{ij} and relative distance D_{ij} are the only information necessary for relative positioning. Such a framework for relative positioning is particularly useful for developing a distributed location algorithm without requiring prior knowledge of absolute anchor positions [91, 92]. Further, as discussed earlier, the use of DRSS does not necessitate any cooperation from the signal source to obtain transmitter-related parameter values. Consequently, scarce wireless resources such as bandwidth and energy can be saved.

Geometry of Absolute DRSS Positioning

Although simply knowing the relative location will suffice for some scenarios such as WSNs/CRNs, global knowledge of the source position is essential in many location applications. To this end, we can transform local geometric systems $\boldsymbol{X} = [X, Y]^T$ in Eq. (3.23) built by pairs of neighboring nodes into a global geometric system $\boldsymbol{x} = [x, y]^T$ via a linear transformation. This is a linear mapping in the form of $\boldsymbol{x_s} = \mathbf{T}^{(k)}\boldsymbol{X_s}$, $k = 1, \ldots, M$, where, in the problem of single source location[1],

$$\boldsymbol{x_s} = \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix}_{3\times 1}, \quad \mathbf{T}^{(k)} = \begin{pmatrix} c & -s & t_{13} \\ s & c & t_{23} \\ 0 & 0 & 1 \end{pmatrix}_{3\times 3}, \quad \boldsymbol{X_s} = \begin{pmatrix} \boldsymbol{X} \\ 1 \end{pmatrix}_{3\times 1}. \tag{3.24}$$

Here, the rotation elements c and s are $\cos(\varphi_{ij})$ and $\sin(\varphi_{ij})$ where $\varphi_{ij} = \arctan\left(\frac{y_j - y_i}{x_j - x_i}\right)$ is the angle of the vector pointing from the ith anchor to the jth anchor relative to the x-axis measured counterclockwise. The translation elements $t_{13} = \frac{1}{2}(x_i + x_j)$ and $t_{23} = \frac{1}{2}(y_i + y_j)$ denote the x and y coordinates of the center of the link connecting an ij-pair of anchors, respectively. If v_{ij} is negative, the circles are reflected.

Also, a set of *global* or absolute DRSS circles centered at $\boldsymbol{c_{d_k}} = [x_{d_k}, y_{d_k}]^T$ can be obtained

[1]For multiple source localization, a unique solution usually cannot be found so that an optimization scheme (*e.g.*, least squares) needs to be employed.

directly using a system of nonlinear equations ($M > m \geq 4$)

$$(x - x_{d_k})^2 + (y - y_{d_k})^2 = r_{d_k}^2, \quad k = 1, 2, \ldots, M \tag{3.25}$$

where

$$x_{d_k} = \frac{h_{ij}x_i - x_j}{h_{ij} - 1}, \; y_{d_k} = \frac{h_{ij}y_i - y_j}{h_{ij} - 1}, \; r_{d_k} = \frac{\sqrt{h_{ij}} \cdot D_{ij}}{|h_{ij} - 1|} \tag{3.26}$$

and $|\cdot|$ denotes the absolute value. In Fig. 3.5b, using different $M = \binom{5}{2} = 10$ pairs of nodes, ten global circles are formed which all intersect at the source position (x, y). Unlike the local circle in Eq. (3.23), the center of the global circle is a function of absolute node coordinates. Note that both the circle's radius and focus will be affected by shadow fading unlike in other range-based circular positioning methods (*i.e.*, RSS, TOA).

Let us now look into the geometric implication of the DRSS redundancy discussed in Section 3.2.1. In the simple noiseless example with three anchors ($m = 3$), we discussed earlier that two basic and one redundant measurements exist. Accordingly, using Eq. (3.25) we can create three distinct geometric circles, yet only the two associated with the basic measurements are independent. This is reflected by the fact that the circle associated with the redundant measurement intersects both of the other circles at the same two points at which the two independent circles meet. Thus, we need a fourth anchor in order to have an unambiguous solution. Despite the need for an additional independent measurement as compared with other circular positioning methods, in the presence of noise the redundant DRSS measurements increase robustness against noise as demonstrated in Section 3.5.

Linear Solution of DRSS Location

As was similarly done for the RSS case, a geometric solution of DRSS positioning can be obtained from the difference of a DRSS circle k and the other circles l for $k < l$. Then, we have

$$(x_{d_l} - x_{d_k})x + (y_{d_l} - y_{d_k})y = \frac{1}{2}\left\{\|\boldsymbol{c_{d_l}}\|^2 - \|\boldsymbol{c_{d_k}}\|^2 - (r_{d_l}^2 - r_{d_k}^2)\right\}, \; k < l \tag{3.27}$$

which leads us to estimate the DRSS solution $\boldsymbol{x} = \boldsymbol{A}^{-1}\boldsymbol{b}$ ($m = 4$), where

$$\boldsymbol{A} = \begin{bmatrix} x_{d_2} - x_{d_1} & y_{d_2} - y_{d_1} \\ x_{d_3} - x_{d_1} & y_{d_3} - y_{d_1} \end{bmatrix}, \; \boldsymbol{b} = \frac{1}{2}\begin{bmatrix} \|\boldsymbol{c_{d_2}}\|^2 - \|\boldsymbol{c_{d_1}}\|^2 - (r_{d_2}^2 - r_{d_1}^2) \\ \|\boldsymbol{c_{d_3}}\|^2 - \|\boldsymbol{c_{d_1}}\|^2 - (r_{d_3}^2 - r_{d_1}^2) \end{bmatrix}.$$

When additional DRSS measurements are available, the overdetermined system can be solved by an LS estimator as presented in the following section.

3.4 Location Estimators

We now discuss two fundamental issues in location estimation: (a) determining achievable location accuracy and (b) searching for optimal and practical estimators.

3.4.1 Cramer-Rao Lower Bound

We have discussed in Section 2.3 that a location system is subject to various errors which may not be predictable or measured individually. Therefore, in designing a location system, one of the most important tasks is to determine the achievable location accuracy of the system. The theoretical limit on an *unbiased* location estimator can be measured by the Cramer Rao Lower Bound (CRLB). The CRLB, as the name indicates, is a lower bound on the covariance of an unbiased location estimator $\hat{\boldsymbol{\theta}}$ which must satisfy

$$\mathrm{C}(\hat{\boldsymbol{\theta}}) - \mathrm{F}^{-1}(\boldsymbol{\theta}) \geq \mathbf{0}. \tag{3.28}$$

Here $\mathrm{F}(\boldsymbol{\theta}) = -E[\nabla_{\boldsymbol{\theta}}(\nabla_{\boldsymbol{\theta}} \ln f_V(\boldsymbol{v};\boldsymbol{\theta}))^T]$ is the Fisher information matrix (FIM) [57] given by

$$[\mathrm{F}(\boldsymbol{\theta})]_{kl} = -E\left[\frac{\partial^2 \ln f_V(\boldsymbol{v};\boldsymbol{\theta})}{\partial\theta_k \partial\theta_l}\right] \tag{3.29}$$

where $f_V(\boldsymbol{v};\boldsymbol{\theta})$ is the joint PDF of the observation vector $\boldsymbol{v}$. If some estimator is unbiased and attains the CRLB, it must be the minimum variance unbiased (MVU) estimator whose covariance matrix is $\mathrm{F}^{-1}(\boldsymbol{\theta})$ of dimension $\mathfrak{d} \times \mathfrak{d}$ for $\mathfrak{d}$-dimensional $\boldsymbol{\theta}$ [57].

We now develop the CRLB for an RSS location estimator. For mathematical simplicity, let us assume that the elements of the observation vector $\boldsymbol{v}$ in Eq. (3.5) are independent and identically distributed[2]. Then, using Eq. (3.6) we have the *log-likelihood function* $\ln f_V(\boldsymbol{v};\boldsymbol{\theta})$ in Eq. (3.29) as

$$\ell(\boldsymbol{\theta}) = -\frac{1}{2\sigma_S^2}\sum_{i=1}^{m}\left(v_i - L_i(\boldsymbol{\theta})\right)^2. \tag{3.30}$$

By substituting Eq. (3.30) into Eq. (3.29), we can derive the FIM for RSS-based location estimation as

$$[\mathrm{F}(\boldsymbol{\theta})]_{kl} = \begin{cases} \frac{1}{\sigma_S^2}\sum_{i=1}^{m}\left(\frac{\partial L_i(\boldsymbol{\theta})}{\partial\theta_k}\right)^2, & k = l \\ \frac{1}{\sigma_S^2}\sum_{i=1}^{m}\left(\frac{\partial L_i(\boldsymbol{\theta})}{\partial\theta_k}\frac{\partial L_i(\boldsymbol{\theta})}{\partial\theta_l}\right), & k \neq l \end{cases} \tag{3.31}$$

[2]In practice, the observations $\boldsymbol{v}$ at different anchors are spatially correlated as discussed in Section 3.2.1. In this case, the FIM will include a correlation factor since the joint PDF $f_V(\boldsymbol{v};\boldsymbol{\theta})$ is a function of a non-diagonal covariance matrix for the shadow fading term.

where the gradient of $L_i(\boldsymbol{\theta})$ is derived in Section 3.4.3 (see Eq. (6.5)). The FIM and CRLB for DRSS-based location estimation can be derived in a similar manner by considering spatial correlation.

Since the CRLB assumes unbiasedness, it can measure the achievable location accuracy in terms of the MSE. Specifically, from Eq. (3.28), the MSE of any *unbiased* estimator is lower bounded as

$$\begin{aligned} \mathrm{MSE}(\hat{\boldsymbol{\theta}}) &= \mathrm{Tr}\left(\mathrm{C}(\hat{\boldsymbol{\theta}})\right) \\ &\geq [\mathrm{F}^{-1}(\boldsymbol{\theta})]_{11} + [\mathrm{F}^{-1}(\boldsymbol{\theta})]_{22} \\ &= \frac{\mathrm{F}_{11} + \mathrm{F}_{22}}{\mathrm{F}_{11}\mathrm{F}_{22} - \mathrm{F}_{12}^2}. \end{aligned} \tag{3.32}$$

In the above derivation, the key assumption was the *unbiasedness* of the estimator. However, many practical estimators including ML/LS estimators and many "optimal" estimators are biased. In this case, the CRLB will not provide a lower bound on location accuracy [93]. For biased estimators, the uniform CRLB can be used as the lower bound on the MSE instead [94].

3.4.2 Maximum Likelihood Estimator

In signal processing, it is customary to seek an unbiased estimator first, and then find the one that exhibits the least variability–that is the MVU estimator [57]. However, many practical issues in location estimation not only challenge us to find the MVU estimator, but also make it sub-optimal in terms of the MSE (compare Eqs. (2.1) and (3.32)). Specifically, since in practice we often encounter small data sizes (*e.g.*, a small number of anchor nodes) and/or correlated location errors, many practical estimators are inefficient and biased. Although an MVU estimator exists, it may be outperformed by biased estimators [93–95]. In the rest of the section, we describe three popular approaches to obtain practical estimators which are biased in many cases.

Given a set of data and an underlying statistical model, perhaps the most popular approach to parameter estimation is based on the *maximum likelihood* principle. This approach is attractive due to the fact that ML estimators can be found even for complex estimation problems, and are efficient and unbiased *asymptotically* (*i.e.*, for large data sizes) [57]. The ML estimator $\hat{\boldsymbol{\theta}}_{\mathrm{ML}}$ is defined as one that maximizes the likelihood function or, equivalently, the log-likelihood function $\ell(\boldsymbol{\theta})$. Thus, the ML location estimator using RSS measurements can be found by solving $\partial\ell(\boldsymbol{\theta})/\partial\boldsymbol{\theta} = \mathbf{0}$, where $\ell(\boldsymbol{\theta})$ is from Eq. (3.30). The solution is the maximizer of $\ell(\boldsymbol{\theta})$. Since this maximization problem is nonlinear and nonconvex, we need either to employ an iterative algorithm to find the globally optimal solution or to linearize the equation to have a closed-form approximate solution. This is the same procedure used to solve the problem of nonlinear LS estimation as presented next.

3.4.3 Nonlinear Least Squares Estimator

The ML estimator can be derived only if the statistical properties of the observed data are known. Even when a statistical distribution of the data is known, we still need to know or estimate the underlying statistical parameters of the distribution. Specifically, for RSS-based location estimation using the statistical model given in Section 3.2.1, RSS measurements are jointly Gaussian, but are not independent with unknown covariances. In particular, when the spatial correlation factor of shadow fading (which cannot be measured at every position in the feasible region) is involved, the corresponding covariance matrix is non-diagonal with unknown parameters.

The *least squares* approach is widely used in practice due to its applicability to various location problems without resorting to statistical assumptions about the observed data. Its ease of implementation due to the special structure of the estimator also makes it attractive. Specifically, regardless of the complexity of the problem we can easily form an LS location estimation problem. For example, in DRSS-based localization we can incorporate the redundant DRSS data in an LS framework without knowledge of the statistical properties of the correlated shadowing. Note that it is difficult to exploit the redundancy using many well-known statistical methods. Particularly, a covariance matrix of all the measurements is typically nonpositive definite or singular due to the data collinearity [96]. Also, as noticed by comparing Eqs. (3.30) and (3.40), an LS estimator is indeed an ML estimator when the residuals $r_i = v_i - L_i(\boldsymbol{\theta})$ are jointly normally distributed; $\boldsymbol{r} \sim \mathcal{N}(\mathbf{0}, \sigma_S^2 \boldsymbol{I})$.

Despite the attractive aspects of the LS approach, it has some limitations. One of the most notable issues is its non-robustness to data *outliers*. Hence, the LS location problem should be constrained in the form of Eq. (1.2). The constraints can be set by exploiting the inherent characteristics of environmental and system constraints associated with network connectivity (or radio range), spatial correlation, node geometry, *etc.*

Since an LS-RSS optimization framework can be handily derived from its DRSS counterparts, let us first consider the LS-DRSS formulation. Given the DRSS observations v_{ij} in Eq. (3.8), an LS-DRSS location estimator determines a parameter vector $\boldsymbol{\theta} = [x, y, n_p]^T$ of source coordinates and path loss gradient n_p, possibly subject to some constraints $[l_{\boldsymbol{\theta}}, u_{\boldsymbol{\theta}}]$ on $\boldsymbol{\theta}$ as

$$\hat{\boldsymbol{\theta}}_D = \arg\min_{\boldsymbol{\theta}} \left\{ \phi_D(\boldsymbol{\theta}) = \frac{1}{2} \sum_{\substack{i,j \in \{1,\ldots,m\} \\ i<j}} r_{ij}^2(\boldsymbol{\theta}) \right\} \qquad (3.33)$$
$$\text{subject to: } l_{\boldsymbol{\theta}} \le \boldsymbol{\theta} \le u_{\boldsymbol{\theta}}$$

where the residual $r_{ij}(\boldsymbol{\theta}) = v_{ij} - L_{ij}(\boldsymbol{\theta})$, and $L_{ij}(\boldsymbol{\theta})$ is the path loss model for DRSS given in Eq. (3.9). With a residual vector $\boldsymbol{r}_D = [r_{12}, \ldots, r_{1m}, r_{23}, \ldots, r_{(m-1)m}]^T$, we have $\phi_D(\boldsymbol{\theta}) = \frac{1}{2}\|\boldsymbol{r}_D(\boldsymbol{\theta})\|^2$. The subscript D or R indicates the DRSS or RSS location estimator (DLE or RLE), while omitting the subscript for the equations common to both RLE and DLE. The

first derivative of ϕ_D with respect to $\boldsymbol{\theta}$–that is the gradient vector field–is

$$\begin{aligned}\nabla\phi_D(\boldsymbol{\theta}) &= \sum_{i=1}^{m-1}\sum_{j=i+1}^{m} r_{ij}(\boldsymbol{\theta})\nabla r_{ij}(\boldsymbol{\theta}) \\ &= -\boldsymbol{J}_D(\boldsymbol{\theta})^T\boldsymbol{r}_D(\boldsymbol{\theta})\end{aligned} \tag{3.34}$$

where $\boldsymbol{J}_D$ is the $M \times 3$ Jacobian matrix of the vector $\boldsymbol{L}_D(\boldsymbol{\theta})$:

$$\boldsymbol{J}_D(\boldsymbol{\theta}) = \left[\frac{\partial L_{ij}(\boldsymbol{\theta})}{\partial\theta_k}\right]_{\substack{i,j\in\{1,\ldots,m\},\ i<j \\ k=1,2,3}}. \tag{3.35}$$

The ij-th row vector $\boldsymbol{J}_{ij}$ for DLE is found to be

$$\boldsymbol{J}_{D,ij} = -\frac{10n_p}{\ln 10}\left[z_{ij,x}, z_{ij,y}, -\frac{1}{n_p}\ln\left(\frac{d_j}{d_i}\right)\right]_{\substack{i,j\in\{1,\ldots,m\}, \\ i<j}} \tag{3.36}$$

in which, geometrically, $z_{ij,x}$ and $z_{ij,y}$ are x- and y-elements of the *difference* vector $\boldsymbol{z}_{ij} = z_{ij,x}\boldsymbol{e}_x + z_{ij,y}\boldsymbol{e}_y$, given by

$$z_{ij,x} = \frac{u_{j,x}}{d_j} - \frac{u_{i,x}}{d_i} \text{ and } z_{ij,y} = \frac{u_{j,y}}{d_j} - \frac{u_{i,y}}{d_i} \tag{3.37}$$

where

$$u_{i,x} = \frac{x_i - x}{d_i},\ u_{j,x} = \frac{x_j - x}{d_j}, \tag{3.38}$$

$$u_{i,y} = \frac{y_i - y}{d_i},\ u_{j,y} = \frac{y_j - y}{d_j}. \tag{3.39}$$

The basis vectors $\mathbf{e}_x$ and $\mathbf{e}_y$ are unit vectors in the direction of x- and y-axes, respectively. $u_{i,x}$ and $u_{i,y}$ are x- and y-elements of the unit position vector $\boldsymbol{u}_i$ of the ith anchor with respect to the target position, as expressed by $\boldsymbol{u}_i = u_{i,x}\boldsymbol{e}_x + u_{i,y}\boldsymbol{e}_y$. This geometric unit vector represents the direction from the source to each anchor node as illustrated in Fig. 3.4. It should be noted that the difference vector $\boldsymbol{z}_{ij}$ is formed by a pair of the ith and jth unit position vectors *inversely* scaled by their respective position vector lengths d_i and d_j, respectively, unlike the TDOA case [67].

We now turn to the LS-RSS formulation. Given the simplified RSS observations $\{v_j\}_{j=1}^m$ in Eq. (3.5), the problem of LS-RSS optimizatiom can be formed as

$$\begin{aligned}\hat{\boldsymbol{\theta}}_R = \arg\min_{\boldsymbol{\theta}} &\left\{\phi_R(\boldsymbol{\theta}) = \frac{1}{2}\sum_{j=1}^{m} r_j^2(\boldsymbol{\theta})\right\} \\ &\text{subject to: } l_{\boldsymbol{\theta}} \le \boldsymbol{\theta} \le u_{\boldsymbol{\theta}}\end{aligned} \tag{3.40}$$

where the residual $r_j(\boldsymbol{\theta}) = v_j - L_j(\boldsymbol{\theta})$, and $L_j(\boldsymbol{\theta})$ is the path loss model for RSS given in Eq. (3.5). By denoting the residual vector $\boldsymbol{r}$ for RLE as $\boldsymbol{r}_R = [r_1, \ldots, r_m]^T$, we have $\phi_R(\boldsymbol{\theta}) = \frac{1}{2}\|\boldsymbol{r}_R(\boldsymbol{\theta})\|^2$. By setting $i = 0$ in Eqs. (3.34)–(3.38), where the terms associated with i are thus removed, we can obtain the RSS counterparts. This modification replaces the vector $\boldsymbol{J}_{ij}$ in Eq. (6.7) by $\boldsymbol{J}_j$ for RLE as

$$\boldsymbol{J}_{R,j} = -\frac{10n_p}{\ln 10}\left[\frac{u_{j,x}}{d_j^2},\ \frac{u_{j,y}}{d_j^2}, -\frac{\ln d_j}{n_p}\right]_{j=1,\ldots,m} \tag{3.41}$$

which forms the $m \times 3$ Jacobian matrix $\boldsymbol{J}_R$ of the log-distance vector $\boldsymbol{L}_R(\boldsymbol{\theta})$ for RLE. Thus, we can obtain the gradient vector field $\nabla\phi_R(\boldsymbol{\theta})$ for RLE as

$$\nabla\phi_R(\boldsymbol{\theta}) = -\boldsymbol{J}_R(\boldsymbol{\theta})^T\boldsymbol{r}_R(\boldsymbol{\theta}). \tag{3.42}$$

Example 3.4 – Improving Location Accuracy in Example 3.3

Repeat Example 3.3(c) by estimating the mobile position $\boldsymbol{\theta} = [x, y]^T$ using the above LS-RSS framework in Eq. (3.40) (assuming $n_p = 3$ known *a priori*). In this case, the distance estimates are not needed, yet a numerical optimization algorithm is necessary to deal with the nonconvex objective function. Using one of the algorithms implemented by the Matlab optimization toolbox function `lsqnonlin`, the solution (*i.e.*, minimizer) is found to be $\hat{\boldsymbol{\theta}} = [27.07, 36.03]^T$. The previous location error of 10.67 m is then reduced to 6.07 m which will be further improved with more RSS measurements.

3.4.4 Linear Least Squares Estimator

The LS objective or merit function $\phi(\boldsymbol{\theta})$ formulated in Eq. (3.33) or (3.40) is inherently nonlinear and nonconvex (*i.e.*, multimodal) with respect to the unknown parameters $\boldsymbol{\theta}$. Consequently, there exists no closed-form solution, and thus it is imperative to solve the problem numerically; a numerical algorithm tries to find an optimal solution iteratively, starting from some initial guess. Due to the unknown curvature and complexities of the objective function, not only can the number of required iterations be large, but the algorithm may also converge to a local minimum.

In the case where the computational complexity and convergence rate are of concern, one may seek to find a closed-form solution through the *linear LS approach*, converted from the original nonlinear LS function ϕ. There are two popular methods for the conversion. The first method is to linearize the original LS function directly to form a system of linear LS equations. In general, the LS equations are a function of either a statistical RSS/DRSS model considered here or a simpler distance/range model in Eq. (1.1). Second, as discussed in Section 3.3, a geometric system of nonlinear equations of position (*i.e.*, circles) can be linearized to form a system of linear LS equations as in Eq. (3.17) or (3.27).

Let us first look into the first linearization method to obtain a closed-form approximate solution. In order to apply the linear LS approach by modifying $\phi(\boldsymbol{\theta})$ directly, we first need to linearize the path loss model $\boldsymbol{L}(\boldsymbol{\theta})$ at some point $\bar{\boldsymbol{\theta}}$ so that

$$\boldsymbol{L}(\boldsymbol{\theta}) \approx \boldsymbol{L}(\bar{\boldsymbol{\theta}}) + \boldsymbol{J}(\bar{\boldsymbol{\theta}})(\boldsymbol{\theta} - \bar{\boldsymbol{\theta}}). \tag{3.43}$$

Then, we can solve the normal equations $\boldsymbol{J}^T\boldsymbol{J}\bar{\boldsymbol{h}} = \boldsymbol{J}^T\boldsymbol{r}$, where the step size $\bar{\boldsymbol{h}} = \hat{\boldsymbol{\theta}} - \bar{\boldsymbol{\theta}}$, to obtain the linear LS solution [57, 75]

$$\hat{\boldsymbol{\theta}} = \bar{\boldsymbol{\theta}} + \left(\boldsymbol{J}(\boldsymbol{\theta})^T\boldsymbol{J}(\boldsymbol{\theta})\right)^{-1}\boldsymbol{J}(\boldsymbol{\theta})^T\boldsymbol{r}(\boldsymbol{\theta})\Big|_{\boldsymbol{\theta}=\bar{\boldsymbol{\theta}}}. \tag{3.44}$$

As noted, this linear LS solution is very simple and computationally attractive. Nevertheless, if the evaluated point $\bar{\boldsymbol{\theta}}$ is far from the global minimum, the first-order approximation does not accurately represent the actual function, and no further improvement can be made. Note that this solution is equivalent to the first iterate of a Gauss-Newton method with a starting point $\boldsymbol{\theta_0} = \bar{\boldsymbol{\theta}}$. Thus, the appropriate determination of the linearization point $\bar{\boldsymbol{\theta}}$ is crucial to have the desired performance of the linear LS estimator.

An alternative linear LS approach is to exploit the geometric relationship between the range estimates described in Section 3.3. Specifically, we formulate a linear LS framework with the residual $\boldsymbol{r} = \boldsymbol{b} - \mathbf{A}\boldsymbol{\theta}$ such that

$$\hat{\boldsymbol{\theta}} = \arg\min_{\theta} \frac{1}{2}\left(\boldsymbol{b} - \mathbf{A}\boldsymbol{\theta}\right)^T\left(\boldsymbol{b} - \mathbf{A}\boldsymbol{\theta}\right). \tag{3.45}$$

For the RSS case ($m \geq 3$), from Eq. (3.17) we have

$$\mathbf{A} = \begin{bmatrix} x_{12} & x_{13} & \cdots & x_{1m} \\ y_{12} & y_{13} & \cdots & y_{1m} \end{bmatrix}^T_{2\times(m-1)}, \quad \boldsymbol{b} = \left[b_{12}\ b_{13}\ \cdots\ b_{1m}\right]^T_{1\times(m-1)}$$

where $x_{ij} = x_j - x_i$, $y_{ij} = y_j - y_i$, and $b_{ij} = \frac{1}{2}\left\{\|\boldsymbol{x_j}\|^2 - \|\boldsymbol{x_i}\|^2 - (\hat{d}_j^2 - \hat{d}_i^2)\right\}$. Similarly, for the DRSS case ($m \geq 4$), from Eq. (3.27) we have

$$\mathbf{A} = \begin{bmatrix} x_{d_{12}} & x_{d_{13}} & \cdots & x_{d_{1M}} & x_{d_{23}} & \cdots & x_{d_{(M-1)M}} \\ y_{d_{12}} & y_{d_{13}} & \cdots & y_{d_{1M}} & y_{d_{23}} & \cdots & y_{d_{(M-1)M}} \end{bmatrix}^T_{2\times {}_M\mathrm{C}_2}$$

$$\boldsymbol{b} = \left[b_{12}\ b_{13}\ \cdots\ b_{1M}\ b_{23}\ \cdots\ b_{(M-1)M}\right]^T_{1\times {}_M\mathrm{C}_2}$$

where $x_{d_{ij}} = x_{d_j} - x_{d_i}$, $y_{d_{ij}} = y_{d_j} - y_{d_i}$, and $b_{ij} = \frac{1}{2}\left\{\|\boldsymbol{c_{d_j}}\|^2 - \|\boldsymbol{c_{d_i}}\|^2 - (r_{d_j}^2 - r_{d_i}^2)\right\}$.

It is then straightforward to find a linear LS estimator using the closed-form LS solution [57, 75]

$$\hat{\boldsymbol{\theta}} = \left(\mathbf{A}^T\mathbf{A}\right)^{-1}\mathbf{A}^T\boldsymbol{b}. \tag{3.46}$$

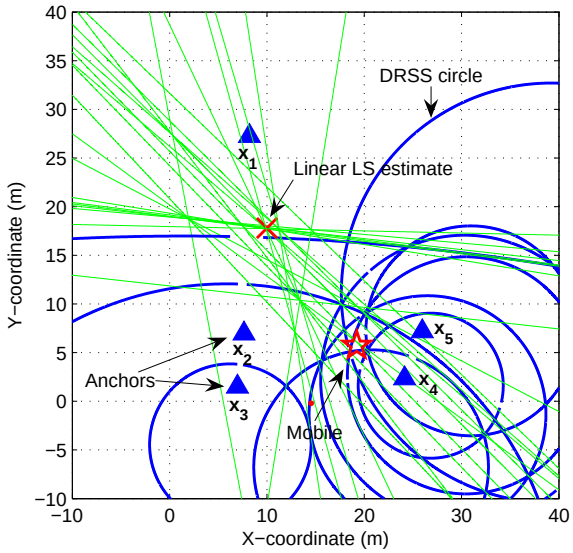


Figure 3.6: A geometric linear LS approach which linearizes a system of nonlinear geometric DRSS equations (*i.e.*, circles).

We note that in the DRSS case, the size of $\mathbf{A}$ increases rapidly with additional measurements. The matrix inversion operation is usually not a problem with a small or medium-scale network. However, for large-scale networks, the linear LS approach may be erroneous and computationally challenging due to computational and ill-conditioning issues [75].

Since the second linear LS approach does not require an initial solution in the non-iterative procedure, for RSS-based positioning, it generally performs better than the first linearization method if we have no knowledge of a good linearization point. This can be inferred from Fig. 3.4, since shadow fading only perturbs the circles' circumferences. However, in the case of DRSS, the shadowing noise affects both the circumferences and centers of DRSS circles, which will result in further degradation of the estimate as can be seen in Fig. 3.6. This also implies that DRSS positioning is more sensitive to the geometry of anchors or nodes than its RSS counterpart. Note that in both localization cases, a linear LS approach is also not robust to data outliers.

3.5 Performance Evaluation

3.5.1 Simulation Settings

In this section, the performance of range-based location techniques based on RSS/DRSS measurements (*i.e.*, RLE/DLE) is evaluated using the nonlinear LS approach presented in

Section 3.4.3. For simplicity, we only estimate the position parameters given prior knowledge[3] of n_p (*i.e.*, $\boldsymbol{\theta} = [x, y]^T$). Regarding the geometry of nodes, $m+1$ anchor and unknown source locations are randomly placed in a 30×30 m^2 area for every simulation iteration to reflect the effect of node geometry [67]. The results are parameterized by several primary factors affecting location estimation–specifically, the number of anchor nodes, spatial correlation of shadowing, shadowing variance, and path loss gradient. To evaluate the impact of spatial correlation of shadow fading, we adopt the model in Eq. (2.5) for generation of a correlated shadowing map. Despite the simpler form of Eq. (2.5) as compared to Eq. (2.4), in general, the average performances of estimators using Eqs. (2.4) and (2.5) were found to be similar according to our simulation study. Here, the location accuracy is shown in terms of the RMSE (meters).

Numerical Optimization Algorithm Considered

There have been many iterative algorithms proposed specifically for nonlinear LS optimization, exploiting the special structure of ϕ to enhance efficiency. We tested various methods including steepest descent, Gauss-Newton, Levenberg-Marquardt (LM) and trust region (TR), and found that the method of trust region using a subspace technique and preconditioned conjugate gradients [75,97] performs best in terms of location accuracy and robustness to random initial solutions. It effectively tackles scenarios where LM may not work properly such as negative curvature and poor scaling. This approach finds the local minimizer in the constrained "trust region" whose size at the kth iteration Δ_k is adjusted according to its performance during the previous iteration. The TR quadratic subproblem is

$$\boldsymbol{\theta}_{k+1} = \min_{\boldsymbol{\theta}_{k+1} \leftarrow \boldsymbol{h}_k} \left\{ \boldsymbol{r}(\boldsymbol{\theta}_k)^T \boldsymbol{J}(\boldsymbol{\theta}_k) \boldsymbol{h}_k + \frac{1}{2} \boldsymbol{h}_k^T \boldsymbol{J}(\boldsymbol{\theta}_k)^T \boldsymbol{J}(\boldsymbol{\theta}_k) \boldsymbol{h}_k : \right. \tag{3.47}$$
$$\left. \|D_k \boldsymbol{h}_k\| \le \Delta_k, \boldsymbol{h}_k \in \text{span}[\boldsymbol{J}^T \boldsymbol{r}, \left(\boldsymbol{J}^T \boldsymbol{J} + \gamma I\right)^{-1} \boldsymbol{J}^T \boldsymbol{r}] \right\}$$

where γ is chosen so as to ensure that $\boldsymbol{J}^T \boldsymbol{J} + \gamma I$ is positive definite, and D_k is the diagonal scaling matrix. This algorithm is implemented by the Matlab optimization toolbox function `lsqnonlin`. All the results presented next are obtained by this approach. Since a single start for the optimization can bias the comparison due to the multimodal LS error functions, we evaluate the functions multiple times using random starting points and then select the minimizer.

[3]When n_p is jointly estimated, the estimator performances are comparable to those presented here. The value may be determined during an offline training phase.

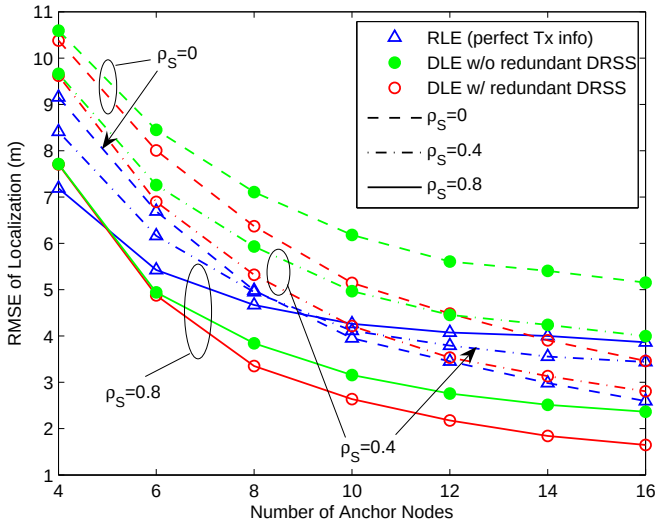


Figure 3.7: RMS location errors of RLE and DLE versus the number of anchor nodes m (σ_S = 5 dB and n_p = 3).

3.5.2 Results and Analysis

Impact of Number of Anchor Nodes and Spatial Correlation

In Fig. 3.7, the performance of RLE and DLE with respect to the number of anchor nodes is presented for σ_S = 5 dB and n_p = 3. The results are parameterized by the shadowing correlation to demonstrate its impact. Note that an ideal assumption was made for RLE in that perfect information about the radio/propagation parameters in Eq. (3.5) was available (*i.e.*, $P(d_0)$ was known perfectly).

We summarize the performance of the two techniques as follows. First, higher correlation actually improves the accuracy of RLE when the number of anchors is small ($m < 9$), but deteriorates its performance when the number is increased beyond $m = 9$. When the number of anchors is small (*i.e.*, small data size), the RLE is biased, and the correlation tends to help location estimation. On the other hand, as more anchors are added (*i.e.*, more RSS measurements), RLE becomes unbiased and approaches the CRLB asymptotically. In this case, it is observed that the error increases with higher correlation values. The second key observation is that the performance of DLE with higher correlation is always better for different numbers of anchors. When the correlation is high, in general, DLE outperforms RLE. Note that other range-based positioning techniques, by contrast, perform worse in highly correlated shadowing environments such as indoor/urban wireless networks. Third, incorporating the redundant DRSS measurements is beneficial for localization. Specifically, a performance advantage can be found with more anchors for both DLE and RLE, but the rate of improvement with additional anchors is higher for DLE due to the redundancy.

Thus, when the network size m is large, DLE becomes comparable to RLE even with lower correlation. In other words, the larger the number of anchors involved, the larger the rate of increase in DRSS redundancy as noted in Eq. (3.10). As a result, its susceptibility to fading and measurement noise can be mitigated, as similarly found for TDOA [98].

Impact of Correlated Shadow Fading

In Fig. 3.8, the impact of log-normal shadow fading on RLE and DLE is shown by varying σ_S. Due to the two-sided localization behavior of RLE observed above, two cases of $m = 6$ and $m = 14$ are considered in Figs. 3.8a and 3.8b, respectively. From the results, similar observations can be made. Specifically, for $m = 6$, the correlation improves the performance of both RLE and DLE, but the improvement rate of DLE is higher. When the correlation is low ($\rho_S < 0.4$), RLE outperforms DLE whereas higher correlation makes DLE superior to RLE. On the other hand, for $m = 14$, the correlation degrades the performance of RLE, whereas the accuracy of DLE is noticeably improved. We also see that the redundant DRSS information improves the performance of DLE.

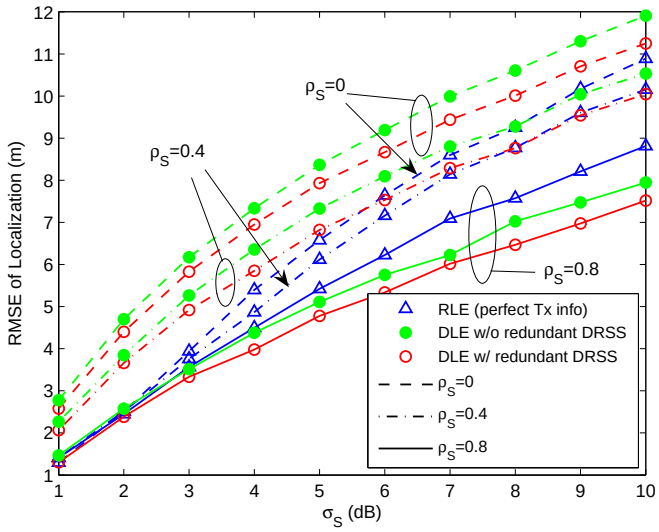
Impact of Path Loss and Spatial Correlation

We now examine the effect of path loss gradient n_p which indicates the rate of path loss over distance. In addition to the above study of shadow fading, this investigation is especially valuable as more location applications have considered indoor and urban environments. For instance, one of the greatest concerns for the wireless E-911 mandate is the unavailability or large error of the emergency caller's location information in indoor areas.

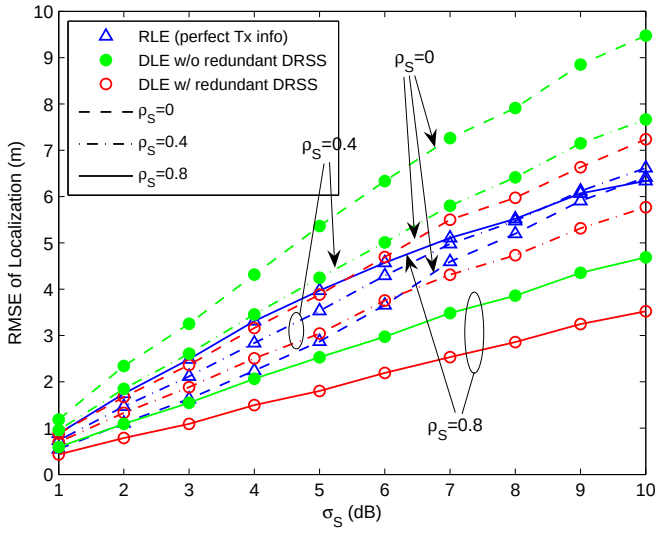
One may expect that larger values of n_p (*i.e.*, higher rates of signal power loss over distance) would degrade the performance of location estimators. However, a larger path loss rate tends to improve the RSS-based estimator performance because given some RSS uncertainty, the size of the corresponding uncertainty domain of a distance d becomes smaller with larger path loss rates. This can be readily observed on the scatter plot of RSS (or path loss) as a function of the distance d [40]. This conjecture is confirmed by Fig. 3.9, where the performances of both RLE and DLE improve with higher values of n_p. From the figure, the effects of the correlation and DRSS redundancy over a range of n_p values can be found to be very similar to those observed previously. Since the number of anchors is small ($m = 6$), RLE generally outperforms DLE except for high correlation values

3.6 Conclusion

In this chapter we have presented the fundamental aspects of RSS-based position location (*esp.*, lateration techniques). Our emphasis was placed on two range-based approaches using



(a)



(b)

Figure 3.8: RMS location errors of RLE and DLE versus std. dev. of shadow fading σ_S ($n_p = 3$) for (a) $m = 6$ and (b) $m = 14$.

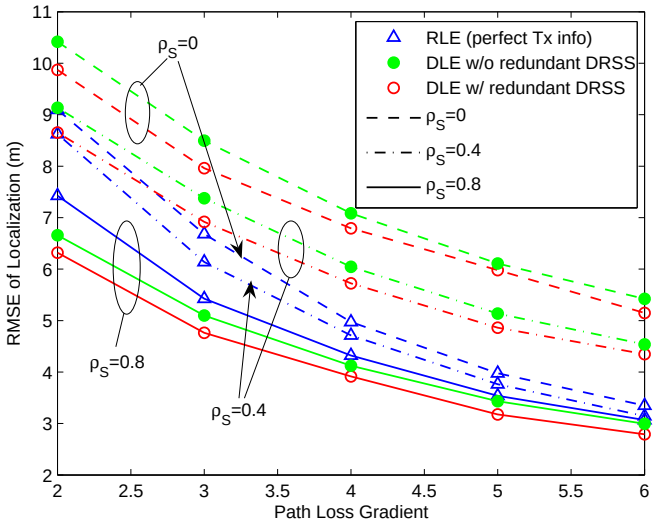


Figure 3.9: RMSE of RLE and DLE versus path loss gradient n_p (σ_S = 5 dB and m = 6).

RSS and DRSS measurements, while we also introduced other major RSS-based techniques, namely RF fingerprinting and connectivity- or proximity-based localization. Our goal in this chapter was to present an overview of RSS position location, its possibilities and limitations from both theoretical and practical perspectives. To accomplish this goal, we have covered the basics of RSS/DRSS-based positioning, location error sources, geometric interpretations, and theoretical and practical issues associated with location estimation.

We also provided the results and analyses of a simulation study on RSS and DRSS location estimation. The results were presented and compared with respect to four major factors affecting the performance of location estimators, namely the number of anchor nodes, the variance and spatial correlation of shadow fading, and path loss rate. We observed that the beneficial factors in improving location accuracy for both RSS and DRSS location estimators are additional anchor nodes, higher path loss rate, and smaller variance of shadow fading. On the other hand, under realistic correlated shadowing conditions, the two estimators exhibit different localization behaviors, depending upon the degree of the spatial correlation.

3.7 Appendix 3A: Numerical Algorithms for Location Estimation

In this section, we present numerical algorithms considered for both RSS and DRSS-based positioning. All the results on the estimation performance of RLE and DLE in this rest of the chapter are produced by solving the LS location problem in Eq. (3.33) or (3.40) using the same numerical methods discussed here. The fact that the merit function $\phi(\boldsymbol{\theta})$ is inherently

multimodal (*i.e.*, nonlinear and nonconvex) results in no closed-form solution for the global minimizer $\hat{\boldsymbol{\theta}}$. Typically, the closed-form approximate solution is obtained using a linear LS (LLS) method by which $\boldsymbol{L}(\boldsymbol{\theta})$ is linearized at some point $\bar{\boldsymbol{\theta}}$ such that

$$\boldsymbol{L}(\boldsymbol{\theta}) \approx \boldsymbol{L}(\bar{\boldsymbol{\theta}}) + \boldsymbol{J}(\bar{\boldsymbol{\theta}})(\boldsymbol{\theta} - \bar{\boldsymbol{\theta}}). \tag{3.48}$$

Then, we can solve the normal equations $\boldsymbol{J}^T\boldsymbol{J}\bar{\boldsymbol{h}} = \boldsymbol{J}^T\boldsymbol{r}$, where the step size $\bar{\boldsymbol{h}} = \hat{\boldsymbol{\theta}} - \bar{\boldsymbol{\theta}}$, to obtain the LLS solution [57, 75]

$$\text{LLS:} \qquad \hat{\boldsymbol{\theta}} = \bar{\boldsymbol{\theta}} + \left(\boldsymbol{J}(\boldsymbol{\theta})^T\boldsymbol{J}(\boldsymbol{\theta})\right)^{-1}\boldsymbol{J}(\boldsymbol{\theta})^T\boldsymbol{r}(\boldsymbol{\theta})\Big|_{\boldsymbol{\theta}=\bar{\boldsymbol{\theta}}}. \tag{3.49}$$

If the evaluated point $\bar{\boldsymbol{\theta}}$ is far from the global minimum, the first-order approximation does not accurately represent the actual function, and no further improvement can be made. In fact, this estimator is equivalent to the first iterate of a Gauss-Newton method with a starting point $\boldsymbol{\theta_0} = \bar{\boldsymbol{\theta}}$ (see Eq. (3.51)). As discussed earlier, an alternative LLS approach is to exploit a geometric relationship between the range estimates demonstrated in Section 3.3. Since such an LLS approach does not require an initial solution in the non-iterative procedure, we consider this approach as one of the initial solution selection algorithms used for nonlinear LS (NLS) iterative methods presented next.

There have been many iterative algorithms proposed specifically for NLS optimization, exploiting the special structure of ϕ to enhance both efficiency and optimality. Among them, Levenberg-Marquardt (L-M) and trust region (TR) methods are widely regarded as the most robust and efficient NLS algorithms [97, 99, 100]. These techniques can be viewed (indirectly) as a hybrid between robust steepest descent (SD) and fast Gauss-Newton (G-N) methods. When far from the solution, the approach takes an SD direction $\boldsymbol{J_k}^T\boldsymbol{r_k}$ such that the kth iterate of $\boldsymbol{\theta}$ in SD is expressed as

$$\text{SD:} \qquad \boldsymbol{\theta_{k+1}} = \boldsymbol{\theta_k} + \lambda_k\boldsymbol{J}(\boldsymbol{\theta_k})^T\boldsymbol{r}(\boldsymbol{\theta_k}), \tag{3.50}$$

where λ_k is the kth line search step size to be determined exactly or inexactly [99]. On the other hand, the approach converges fast in the neighborhood of the solution via the method of G-N by solving the normal equations $\boldsymbol{J_k}^T\boldsymbol{J_k}\boldsymbol{h_k} = \boldsymbol{J_k}^T\boldsymbol{r_k}$ where the increment $\boldsymbol{h_k} = \boldsymbol{\theta_{k+1}} - \boldsymbol{\theta_k}$ is found such that GN produces

$$\text{GN:} \qquad \boldsymbol{\theta_{k+1}} = \boldsymbol{\theta_k} + \left(\boldsymbol{J}(\boldsymbol{\theta_k})^T\boldsymbol{J}(\boldsymbol{\theta_k})\right)^{-1}\boldsymbol{J}(\boldsymbol{\theta_k})^T\boldsymbol{r}(\boldsymbol{\theta_k}). \tag{3.51}$$

As noted, an approximate Hessian of $\boldsymbol{J}^T\boldsymbol{J}$ is used for NLS instead of computing the actual Hessian to reduce computation. Combining the algorithms for L-M, we have

$$\text{LM:} \quad \boldsymbol{\theta_k} = \boldsymbol{\theta_k} + \left(\boldsymbol{J}(\boldsymbol{\theta_k})^T\boldsymbol{J}(\boldsymbol{\theta_k}) + \mathbf{D_k}\right)^{-1}\boldsymbol{J}(\boldsymbol{\theta_k})^T\boldsymbol{r}(\boldsymbol{\theta_k}), \tag{3.52}$$

where $\mathbf{D_k}$ is the diagonal scaling matrix. The method of TR resembles this L-M approach but uses a concept of the "trust" region within which the quadratic approximation at a given point $\boldsymbol{\theta_k}$ represents the original function. The local minimizer is found in this constrained region, and the size of the region at the kth iteration Δ_k is adjusted according to its performance during the previous iteration. Hence, the selection of Δ_k is important in the TR quadratic subproblem

$$\text{TR: } \boldsymbol{\theta_{k+1}} = \min_{\boldsymbol{\theta_{k+1}} \leftarrow \boldsymbol{h_k}} \left\{ \boldsymbol{r}(\boldsymbol{\theta_k})^T \boldsymbol{J}(\boldsymbol{\theta_k}) \boldsymbol{h_k} + \frac{1}{2} \boldsymbol{h_k}^T \boldsymbol{J}(\boldsymbol{\theta_k})^T \boldsymbol{J}(\boldsymbol{\theta_k}) \boldsymbol{h_k} : \|\mathbf{D_k} \boldsymbol{h_k}\| \leq \Delta_k \right\}. \tag{3.53}$$

There have been many classes of proposed TR algorithms which effectively tackle scenarios where L-M may not work properly such as negative curvature and poor scaling. In this work we employ a subspace technique along with the method of preconditioned conjugate gradients (PCG) [75, 97, 100, 101] that we found to be robust and efficient for localization problems. In the method of TR, the two-dimensional subspace is spanned by the SD direction $\boldsymbol{J}^T \boldsymbol{r}$ and approximate G-N direction $\left(\boldsymbol{J}^T \boldsymbol{J}\right)^{-1} \boldsymbol{J}^T \boldsymbol{r}$ solved by PCG. When the algorithm meets negative curvature in that its Hessian is indefinite (corresponding to a saddle point), the PCG outputs an approximate direction of the negative curvature by solving $\boldsymbol{h}^T \boldsymbol{J}^T \boldsymbol{J} \boldsymbol{h} < 0$ instead. This procedure can be embedded in Eq. (3.53) with an additional constraint, either $\boldsymbol{h_k} \in \text{span}\left\{ \boldsymbol{J}^T \boldsymbol{r}, \left(\boldsymbol{J}^T \boldsymbol{J} + \gamma I\right)^{-1} \boldsymbol{J}^T \boldsymbol{r} \right\}$ on the region of negative curvature or $\boldsymbol{h_k} \in \text{span}\left\{ \boldsymbol{J}^T \boldsymbol{r}, \left(\boldsymbol{J}^T \boldsymbol{J}\right)^{-1} \boldsymbol{J}^T \boldsymbol{r} \right\}$ otherwise. Here, γ is appropriately chosen to ensure that $\boldsymbol{J}^T \boldsymbol{J} + \gamma I$ is positive definite while reducing the quadratic model [97, 100]. It is worth noting that this subproblem in two variables is computationally inexpensive, thus showing its potential for large-scale location problems. In addition, the naturally constrained form in Eq. (3.53) enables an easy extension to constrained optimization [102]. For instance, to mitigate non-line-of-sight (NLOS) error mitigation one would formulate a constrained DRSS/RSS or DRSS/TOA hybrid nonlinear program with the objective function subject to NLOS RSS or TOA range estimates as studied in [103] for a linear program.

3.8 Appendix 3B: Algorithms for Initial Solution Selection in DRSS-Based Localization

In most iterative algorithms for multimodal function optimization including those introduced above, the choice of a starting point significantly impacts the optimization characteristics such as global optimality, convergence rate and computational efficiency [99]. When the starting point is chosen close to the optimum, a very simple algorithm can work effectively. For example, Newton-type methods can be well defined and readily converge to the solution. On the other hand, in a region far from the optimal point, even sophisticated algorithms may fail to find the global solution, ending up in a local optimum. Therefore, the best initial

solution selection algorithm would be one which can efficiently find a starting point as close as possible to the global optimum. In the following, we first present two methods for initial solution selection, termed Random Selection (RAND) and LLS Solution (LLSS), and then propose a novel, scalable algorithm which we call Minimum Vertex of Tangential Rectangle (MVTR).

- *Algorithm 1: RAND*

As its name indicates, RAND takes a random starting point in the feasible search region $\mathscr{F}$ which may be used for situations where there is a lack of information about the objective function. The whole optimization process usually needs to be repeated multiple times with a wide range of initial values in order to find the global optimum.

- *Algorithm 2: LLSS*

As detailed in Section 3.4.4, we can seek the mobile position (x, y) without resort to an initial solution via a geometric approach by examining a set of observed DRSS circles $(x - x_{d_k})^2 + (y - y_{d_k})^2 = r_{d_k}^2$, $k = 1, 2, \ldots, M$, formed from Eq. (3.25). Specifically, we linearize the nonlinear system geometrically, similar to [104] for TOA, observing that the solution can be interpreted in noiseless cases (see Fig. 3.5b) as the intersection of straight lines connecting the two intersecting points where each pair of circles meet. These lines can be obtained by differencing the nonlinear equations to form a linear system of ${}_M\mathrm{C}_2 = \binom{M}{2}$ distinct lines, $x_{d_{kl}} x + y_{d_{kl}} y = b_{kl}$, where $x_{d_{kl}} \triangleq x_{d_k} - x_{d_l}$, $y_{d_{kl}} \triangleq y_{d_k} - y_{d_l}$, and $b_{kl} \triangleq \frac{1}{2}\left(\|c_{d_k}\|_2^2 - \|c_{d_l}\|_2^2 - (r_{d_k}^2 - r_{d_l}^2)\right)$; $k, l \in \{1, 2, \ldots, M\}$, $k < l$. In actual wireless conditions where the observables are corrupted by shadow fading, the circles are perturbed so that the intersecting lines are shifted accordingly.

- *Algorithm 3: MVTR*

Next, we present an efficient initial solution selection algorithm particularly designed for DLE. This algorithm is developed to address the question: how shall we reduce the number of potential initial search points needed to find the global minimum, and distribute them over the search region $\mathscr{F}$ effectively? In RAND, random points chosen from a large set of necessary search points S_0 independent of the objective function significantly reduce the reliability of the approach. Thus, one may consider a grid-based search algorithm to reduce the size of the set where one minimizing the objective function over $\mathscr{F}$ serves as the best starting point. This underscores the importance of the size of S_0 and its distribution over the search region. The complexity of this type of brute-force search is generally impacted by the size of the search space, but not the number of anchor/sensor nodes involved. On the other hand, LSSS is not affected by the size of the region but is dependent on the number of nodes as pointed out earlier. Further, while LSSS exploits the geometric features of DLE

to find a better initial solution, the intersecting lines do not meet near the solution in many cases as shown in Fig. 3.10. This phenomenon is more severe in DLE because the foci of the circles do not reside at each node and, moreover, are perturbed by noise unlike other circular positioning techniques.

Based on the above observations we devise MVTR as a cross between the grid-based search and LLSS. MVTR includes only up to four candidate points in S_0, whereas their distribution on the grid called the *tangential rectangle* is determined by observing the geometry of the circles as demonstrated in Fig. 3.10. This indicates that MVTR is directly impacted by *neither* the size of the search region *nor* the number of nodes. The MVTR algorithm is provided in Algorithm 3.1.

Algorithm 3.1 Minimum Vertex of Tangential Rectangle

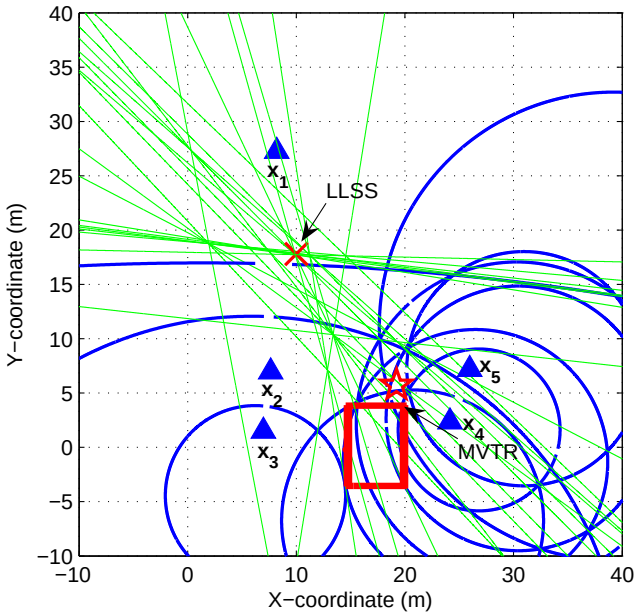
Given a DRSS observation vector $\boldsymbol{v}$ from m anchor nodes;
$M \leftarrow \binom{m}{2}$;
Compute $\{\boldsymbol{x}_{d_k}\}_{k=1}^{M}$, $\{\boldsymbol{y}_{d_k}\}_{k=1}^{M}$, and $\{\boldsymbol{r}_{d_k}\}_{k=1}^{M}$ from Eq. (3.25);
for $k \leftarrow 1$ **to** M
    $l_k \leftarrow x_{d_k} - r_{d_k}$; $r_k \leftarrow x_{d_k} + r_{d_k}$;
    $b_k \leftarrow y_{d_k} - r_{d_k}$; $t_k \leftarrow y_{d_k} + r_{d_k}$;
end for
$A \leftarrow \{\max(\boldsymbol{l}), \min(\boldsymbol{r})\}$; $B \leftarrow \{\max(\boldsymbol{b}), \min(\boldsymbol{t})\}$;
$V_{lb} \leftarrow (\min(A), \min(B))$; $V_{rb} \leftarrow (\max(A), \min(B))$;
$V_{rt} \leftarrow (\max(A), \max(B))$; $V_{lt} \leftarrow (\min(A), \max(B))$;
Construct $S_0 \leftarrow \{V_{lb}, V_{rb}, V_{rt}, V_{lt}\}$;
Find MVTR $\boldsymbol{\theta}_0 \leftarrow \arg\min_{\boldsymbol{\theta}} \phi(\boldsymbol{\theta}) : \boldsymbol{\theta} \in S_0 \cap \mathscr{F}$;

(Note: the symbol "←" indicates the assignment)

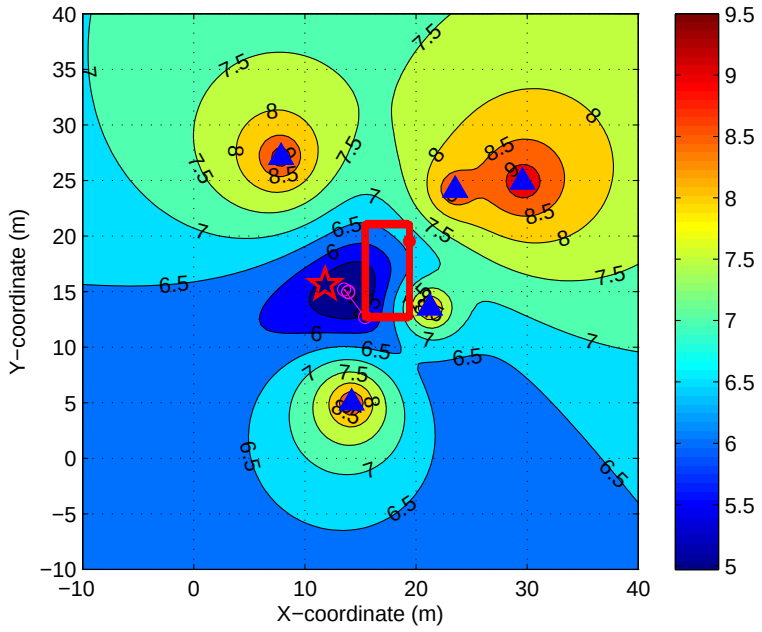
As observed from Fig. 3.10, the shape and position of the tangential rectangle is affected by the node geometry as well as the shadowing variability. We have observed from a number of simulations that the MVTR is located in or very close to a near-convex region surrounding the solution, as the geometry of the rectangle changes with different shadowing values and node geometry. In the near-convex region, the numerical algorithms enjoy local quadratic convergence. As we see in the next section, this is the dominant factor in the performance.

3.9 Appendix 3C: Comparing Optimization Algorithms for Location Estimation

We now examine the performance of the three practical numerical methods (*i.e.*, SD, LM, and TR) with each of the initial solution selection algorithms (RAND, LLSS, and MVTR) to determine the best DLE optimization scheme. Here, the location accuracy is shown in terms



(a)



(b)

Figure 3.10: Geometric view of initial solution selection algorithms ($m = 5, \sigma_S = 5$ dB, $n_p = 3$). (a) LSSS from linear intersecting lines and MVTR on the tangential rectangle. (b) Contour plot of the NLS objective function ϕ in logarithmic scale showing its search path starting from MVTR. The source and anchor locations are indicated by "★" and "▲", respectively.

of the root mean squared error (RMSE) in a $30m \times 30m$ area. The comparison results are parameterized by several primary factors affecting the location estimation, including shadowing variance, spatial correlation and node density. Note that the effect of node geometry on localization is taken into account here by randomly selecting $m+1$ anchor and source locations in every iteration of the simulation.

The goal of the next evaluation is to compare different combinations of the numerical methods and the initial solution algorithms, thereby finding the best optimization choice for DLE. As before, the shadow fading variance and the number of anchors are parameterized under different correlated shadowing conditions. The former parameter gives insight into how reliably each algorithm performs under different radio conditions, whereas the latter shows the effectiveness of the algorithm for different numbers of anchors available for localization.

Fig. 3.11 illustrates the RMS location error of SD when integrated with different initial solution selection algorithms (RAND, LLSS, and MVTR). We employ a quadratic-fit line search without any additional safeguards here since it is known to converge fast under benign assumptions such as pseudoconvexity [99]. This simple gradient method with the exact line search may generally be disregarded for NLS optimization in practice but is chosen here in order to determine if the produced starting point is near the global optimum. Using RAND, as expected the performance is very bad no matter what shadowing conditions and regardless of the number of anchors considered. Notice that no improvement is achieved with lower shadowing variance or higher node density. However, when MVTR is used, the performance is dramatically improved and better localization performance is seen with smaller shadowing variance and/or higher node density which is consistent with our intuition. The localization accuracy of SD-LLSS is seen to fall in between that of SD-RAND and SD-MVTR.

Next, the location accuracy of LM is evaluated in the same way as SD, and shown in Fig. 3.12. Under all conditions, LM is considerably superior to SD when integrated with RAND and LLSS, whereas only little improvement (approximately 0.5 meters) is observed in the case of MVTR. The main reason for the improvements with RAND and LLSS is the way that LM evaluates the objective function ϕ and determines the scaling matrix $\mathbf{D_k}$ in Eq. (3.52). Nevertheless, LM may not perform reliably if $\boldsymbol{J}(\boldsymbol{\theta}_k)^T\boldsymbol{J}(\boldsymbol{\theta}_k) + \mathbf{D_k}$ is negative definite or, equivalently, has negative eigenvalues. This situation can often be found in the region far from the global optimum.

Lastly, the performance of TR is presented in Fig. 3.13. In comparison to SD and LM, significant improvements are observed for RAND and LLSS via TR. More noticeably, the RMSE results among TR-RAND/LLSS/MVTR show little difference when six anchor nodes are involved. This implies the best robustness of TR over SD and LM with respect to the choice of initial solutions. However, the RMSE gap between TR-MVTR and TR-RAND/LLSS increases with the number of anchors. Interestingly, with MVTR the localization accuracies of LM and TR (similar to SD) are nearly indistinguishable. This result can be explained by the fact that if $\boldsymbol{J}(\boldsymbol{\theta}_k)^T\boldsymbol{J}(\boldsymbol{\theta}_k) + \mathbf{D_k}$ is positive definite, LM can be viewed as a type of TR [99]. From this, we can infer the effectiveness of the MVTR algorithm, which selects an initial

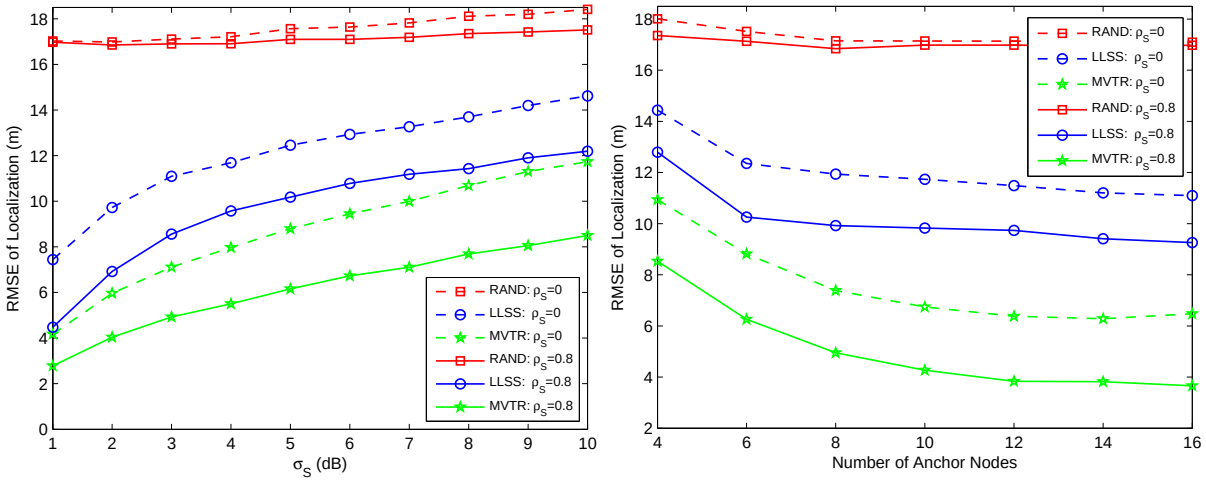


Figure 3.11: RMS localization error of SD with different initial solution algorithms versus (a) std. of shadow fading σ_S ($m = 6, n_p = 3$) and (b) the number of anchor nodes m ($\sigma_S = 5$ dB, $n_p = 3$). The results include RMSE with $\rho_S = 0$ and 0.8, while RMSE with other correlation values can be inferred in between.

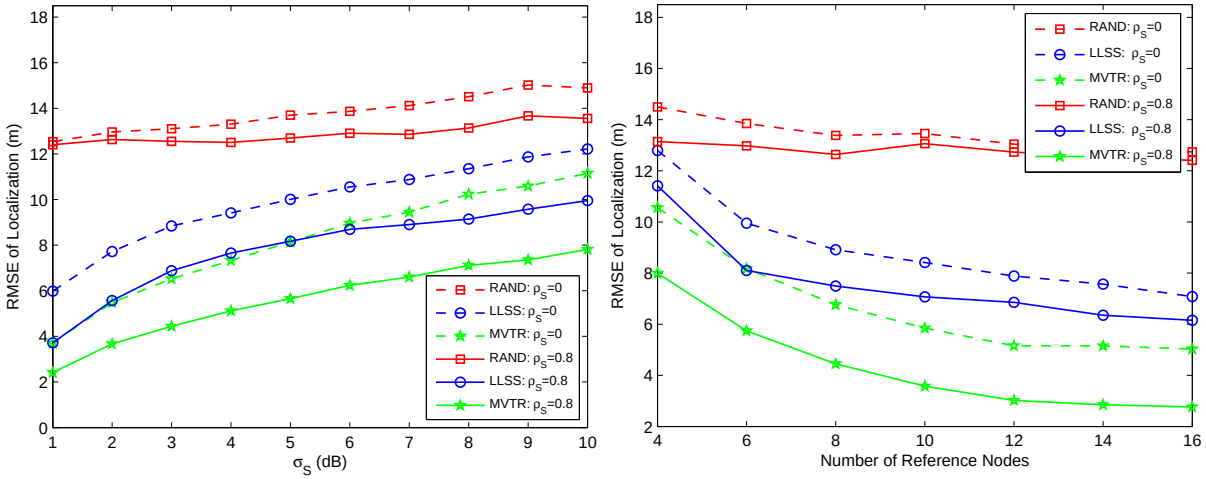
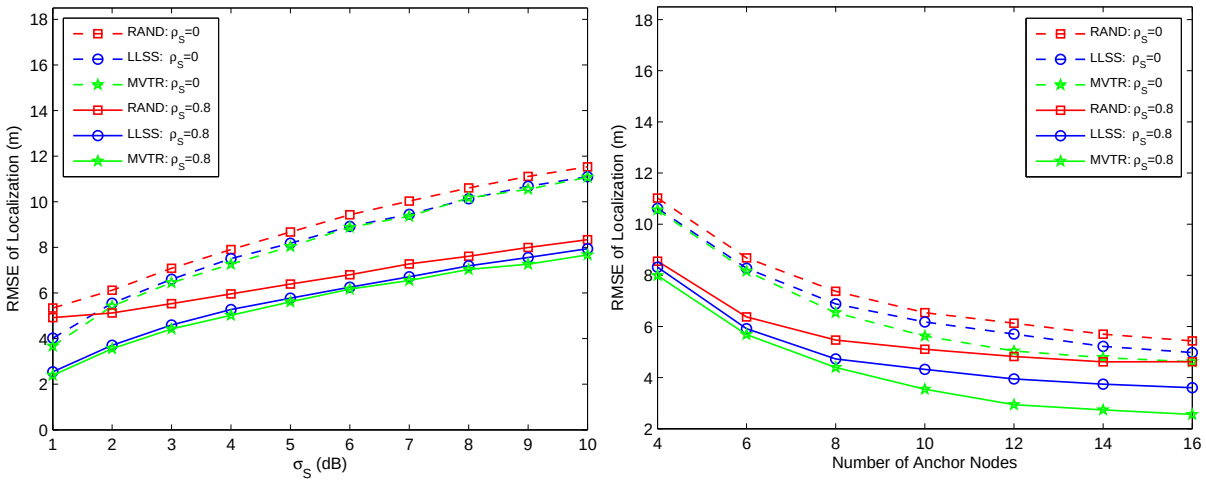


Figure 3.12: RMS localization error of LM with different initial solution algorithms versus (a) std. of shadow fading σ_S ($m = 6, n_p = 3$) and (b) the number of anchor nodes m ($\sigma_S = 5$ dB, $n_p = 3$). The results include RMSE with $\rho_S = 0$ and 0.8, while RMSE with other correlation values can be inferred in between.



(a) (b)

Figure 3.13: RMS localization error of TR with different initial solution algorithms versus (a) std. of shadow fading σ_S ($m = 6, n_p = 3$) and (b) the number of anchor nodes m ($\sigma_S = 5$ dB, $n_p = 3$). The results include RMSE with $\rho_S = 0$ and 0.8, while RMSE with other correlation values can be inferred in between.

solution very close to or in the near-convex region of the global minimizer. In the case where the sub-meter location accuracy is needed, one may consider a multi-start option with up to four candidates (*i.e.*, corner points of the tangential rectangle), and find the minimizer[4].

Comparing all the results in Figs. 3.11-3.13, we summarize our findings in the following.

- Without regard to numerical algorithms employed, better localization performance is achieved through MVTR. Specifically, examining RMSE we find that MVTR $\ll$ LLSS $<$ RAND.
- Without regard to the initial solution algorithms, better localization performance is achieved with TR. Specifically, after examining RMSE, TR $\leq$ LM $<$ SD.
- MVTR is so effective that the three DLE algorithms all show good and comparable localization performance when it is used.
- While TR is much more robust to the choice of an initial solution than LM, they both yield nearly the same (best) localization performance if integrated with MVTR.

[4]Some improvement ($\lesssim 1$ meter) was observed under good localization conditions (*i.e.*, large m or small σ_S) in this arbitrary node placement setup.

Chapter 4

Security Issues for Wireless Position Location

4.1 Introduction

In most wireless location systems, particularly range-based positioning networks, security risks arise from their passive dependency on signal sources which transmit (or broadcast) using position-related signal parameters. The signal sources are either mobile targets for network-based positioning or beacons with known coordinates (*i.e.*, anchor nodes such as access points or base stations) for client-based positioning. After measuring one or more signal features (such as received power level, the time of arrival or the angle of arrival), a location estimator relates the feature(s) to the position-related signal parameters assumed *a priori* to determine position coordinates (x, y). The signal parameters typically used for location estimation are the transmit power or signal strength P_t, antenna gain G_t and system loss factor S_t for RSS/DRSS, the signal departure time and clock offsets for TOA/TDOA, and the antenna gain/type/direction for AOA. The signal sources are believed to be legitimate, thus conforming to system protocols and informing the network or mobile of *correct* information about the signal parameter values. As described in Chapter 1.3, adversaries take advantage of this passive reliance to launch a location attack.

In Chapter 3 we discussed the fundamental aspects of wireless position location based on RSS measurements from a general estimation perspective, assuming *reliable* signal sources. Specifically, the major source of location error was the signal distortion due to shadow fading. In addition to the environmental effect, a location estimator is subject to systematic bias, especially due to location spoofing attacks. In this chapter, therefore, we begin with two fundamental approaches to RSS-based location estimation by investigating their security risks in Section 4.2. Then, in Section 4.3 we introduce primary types of location attacks–namely, attack position spoofing, anchor signal spoofing and location disclosure–and discuss their

similarities and differences. This chapter also surveys recent efforts toward the security of location information and systems, specifically against the three attack types. The classification of attacks along with a survey on the related work will facilitate understanding various issues with respect to location security and identifying strong aspects of this dissertation compared to previous studies. With this basic understanding, we examine the impact of location spoofing attacks on two typical estimation strategies with particular emphasis on attack position spoofing in Section 4.5. In the next chapter, we continue our discussion on the attack effects by characterizing location spoofing attacks mathematically with a detailed analysis of the results.

Due to the reliance of this work on RSS-based position location, our discussion in this chapter will concentrate on the security issues associated with range-based localization using RSS measurements. However, it should be noted that many of the fundamental concepts and results can be applied to any range-based positioning system.

4.2 Revisiting SS-Based Localization: Security Risks

In this section we discuss the security risks in RSS-based position location by revisiting two fundamental approaches to location estimation using RSS measurements.

4.2.1 Received Signal Strength Based Positioning

Consider a two-dimensional location system using RSS measurements $\{P_i\}_{i=1}^m$ at m anchor nodes to estimate mobile target coordinates $\boldsymbol{\theta} = [x, y]^T$. We assume the use of a lateration-based system which estimates distances from the anchors to the target using an assumed relationship between large scale power loss and distance. More specifically, given the ith anchor position at $\boldsymbol{x}_i = [x_i, y_i]^T$, its distance (or range) $d_i = \|\boldsymbol{\theta} - \boldsymbol{x}_i\|$ to the mobile is estimated by assuming that the observed signal power is a log-normal random variable with standard deviation σ_S and whose mean (in the log domain) depends on the distance d_i:

$$P(d_i; \boldsymbol{\Psi}_i) \text{ (dBm)} \sim \mathcal{N}\big(\bar{P}(d_i; \boldsymbol{\Psi}_i), \sigma_S^2\big), \tag{4.1}$$

with

$$\bar{P}(d_i; \boldsymbol{\Psi}_i) \text{ (dBm)} = P(d_0; \boldsymbol{\Psi}_i) \text{ (dBm)} - 10 n_p \log_{10}\left(\frac{d_i}{d_0}\right) \tag{4.2}$$

where n_p is the path loss gradient, and $P(d_0; \boldsymbol{\Psi}_i)$ is the signal power observed at a close-in distance d_0 or predicted using the Friis equation [40]. The semicolon ";" is used here to indicate the dependence of the RSS on prior uncertainties or nuisance parameters $\boldsymbol{\Psi}_i = (n_p, \boldsymbol{\psi}_i)$,

that are a combination of environmental and system parameters n_p and $\boldsymbol{\psi}_i = (P_t, S_t, G_{t_i})$, respectively. P_t, S_t and G_{t_i} are the transmit power, system loss factor and transmitter antenna gain seen by the ith anchor, respectively.

Most of the previous studies in localization assume that $\boldsymbol{\Psi}_i$ is exactly known *a priori* or determined later using the cooperation of the mobile via a *predefined* control channel or system protocol. Then, $P(d_0; \boldsymbol{\Psi}_i)$ can be simplified to a known constant $P(d_0)$, and the observed RSS, v_i is related to the unknown position through the range d_i:

$$v_i = P(d_0)\ (\text{dBm}) - 10n_p(\log_{10} d_i - \log_{10} d_0) + X_{\sigma_i}, \qquad i = 1, \ldots, m, \tag{4.3}$$

where the unknown random variable X_σ represents the log-normal shadow fading and thus the major uncertainty in the observation; $X_\sigma \sim \mathcal{N}(0, \sigma_S^2)$. The observable is thus related to the unknown target position by fitting it to $L_i(\boldsymbol{\theta}) = P(d_0)\ (\text{dBm}) - 10n_p \{\log_{10}(\|\boldsymbol{\theta} - \boldsymbol{x}_i\|) - \log_{10} d_0\}$. More specifically, we estimate $\boldsymbol{\theta}$ by minimizing the error function $\|\boldsymbol{v} - \boldsymbol{L}(\boldsymbol{\theta})\|_2^2$. To elaborate slightly on the shadowing assumed, as discussed earlier we need to take into account the spatial correlation of shadowing fading components at different receiver locations.

It should be noted that the prior knowledge of $\boldsymbol{\Psi}_i$ is an oversimplification for most practical scenarios. In particular, the availability of the path loss exponent n_p is not always realistic. Thus, in this work we will assume that n_p is a nuisance parameter to be estimated along with position. Of more importance in this work is the impact of the reference value $P(d_0)$ since this depends on the behavior of the target. More specifically, $P(d_0)$ is either a measured value for a specifc power level or is calculated using the Friis transmission formula:

$$P(d_0)\ (\text{dBm}) = P_t\ (\text{dBm}) + G_t\ (\text{dB}) - S_t\ (\text{dB}) - 20\log_{10}\left(\frac{4\pi d_0}{\lambda}\right) \tag{4.4}$$

where λ is the signal wavelength. In other words, we rely on the target to use (or provide) reliable values for P_t, G_t and S_t. By purposely modifying these values (relative to the values assumed or communicated to the location system) the target can dramatically impact an estimate of range (and thus position) which is based on the received signal power values.

4.2.2 DRSS-Based Positioning

From a security perspective, the passive dependency on the source-dependent parameters $\boldsymbol{\psi}_i$ in $P(d_0; \boldsymbol{\Psi}_i)$ makes the location system vulnerable to location attacks as mentioned above. To remove some of this reliance, one may use the difference in RSS levels at different anchors or DRSS [14]. In this case, the required knowledge of the transmitter parameter values can be significantly relaxed. Specifically, we change the observation from RSS to *differential*

RSS:

$$v_{ij} \triangleq v_j - v_i \tag{4.5a}$$
$$= P(d_0)\ (\text{dBm}) - 10n_p \log_{10} d_j - P(d_0)\ (\text{dBm}) + 10n_p \log_{10} d_i + X_{\sigma_j} - X_{\sigma_i} \tag{4.5b}$$
$$= 10n_p(\log_{10} d_i - \log_{10} d_j) + \Delta \mathrm{X}_{\sigma_{ij}}, \tag{4.5c}$$

where $\Delta \mathrm{X}_{\sigma_{ij}} = X_{\sigma_j} - X_{\sigma_i};\ i, j \in \{1, \ldots, m\},\ i < j$ and we have assumed that the system parameters for the two links are the same. This is valid for transmit power, system loss and path loss exponent. However, in some cases, the antenna gain will not be the same on the two links, especially with some types of attacks as we will see. Specifically, the difference in the transmitter antenna gains $\Delta G_{t_{ij}} = G_{t_i} - G_{t_j}$, seen by anchors i, j, is close to zero for a target with an omni-directional antenna (*i.e.*, $G_{t_i} = G_{t_j}, \forall i, j$) but can be significant when the target is equipped with a directional antenna (*i.e.*, $G_{t_i} \neq G_{t_j}, \exists i \neq j$). However, the other transmitter uncertainties in $P(d_0; \boldsymbol{\Psi_i})$ are removed. Notice that m RSS observables yield an un-ordered set of $M = \binom{m}{2}$ distinct DRSS observables and differential model equations $L_{ij}(\boldsymbol{\theta}) = 10n_p \{\log_{10}(\|\boldsymbol{\theta} - \boldsymbol{x}_i\|) - \log_{10}(\|\boldsymbol{\theta} - \boldsymbol{x}_j\|)\}$.

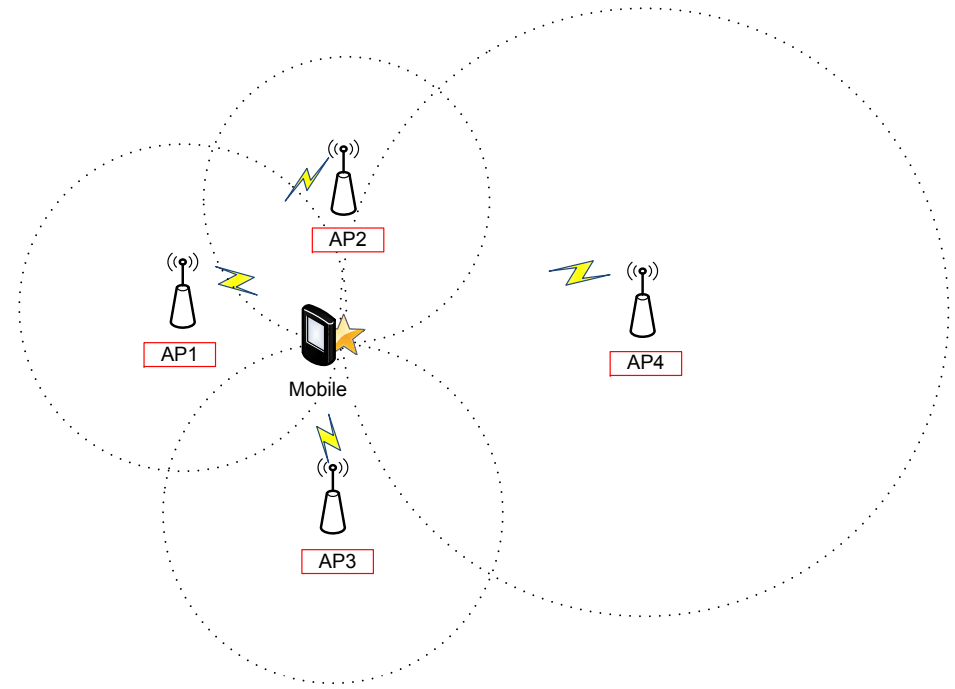
4.3 Types of Position Location Attacks

The design of a secure radio location system requires an understanding of the different types of potential threats and attack strategies which may take advantage of highly unpredictable wireless environments. Location spoofing attacks can primarily be classified according to two basic approaches to designing a radio location network: (a) *network-based positioning* (*e.g.*, GSM cellular networks) and (b) *client-based positioning* (*e.g.*, GPS and some CDMA cellular networks). As described in Fig. 4.1, this classification depends on which entity (either the network or the client) is in charge of signal measurements (and the location calculation in many cases) [7, 11].

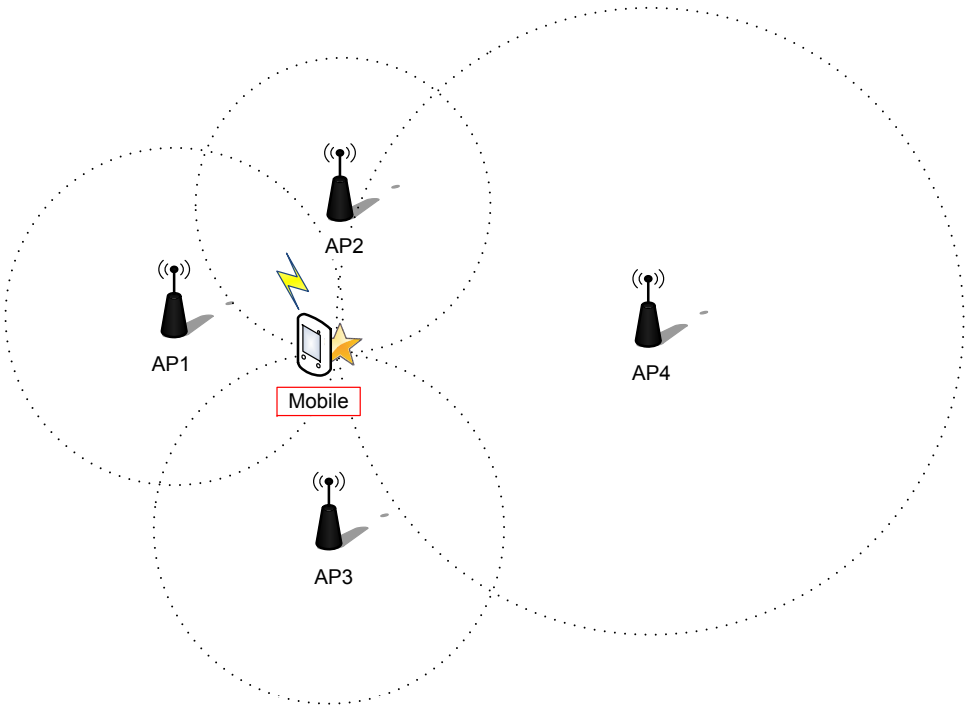
Consequently, as illustrated in Fig. 4.2, there can be two primary attack types or goals for adversaries, depending upon whose location information (either the attacker's or the client's) an attacker attempts to falsify: *attack position spoofing* and *anchor signal spoofing*. The emphasis of this section is upon major security risks due to these two attack types– specifically, modification and disruption/destruction of location information/system, while giving a brief overview of an increasing privacy issue associated with *location disclosure*. In discussing each attack type we provide a summary of recent work and efforts on location security in Section 4.4.

4.3.1 Attack Position Spoofing

In network-based positioning systems, the position (x, y) of a mobile client is typically estimated based on one or more of the mobile's signal features measured at a set of m anchor



(a)



(b)

Figure 4.1: Primary types of range-based position location networks (noiseless cases). (a) Client-based positioning. (b) Network-based positioning. The shaded entity indicates the one in charge of signal measurements, while the entity whose name is in a box indicates the signal source. The dotted circles centered at each anchor position and the star represent range estimates and the resulting position estimate, respectively.

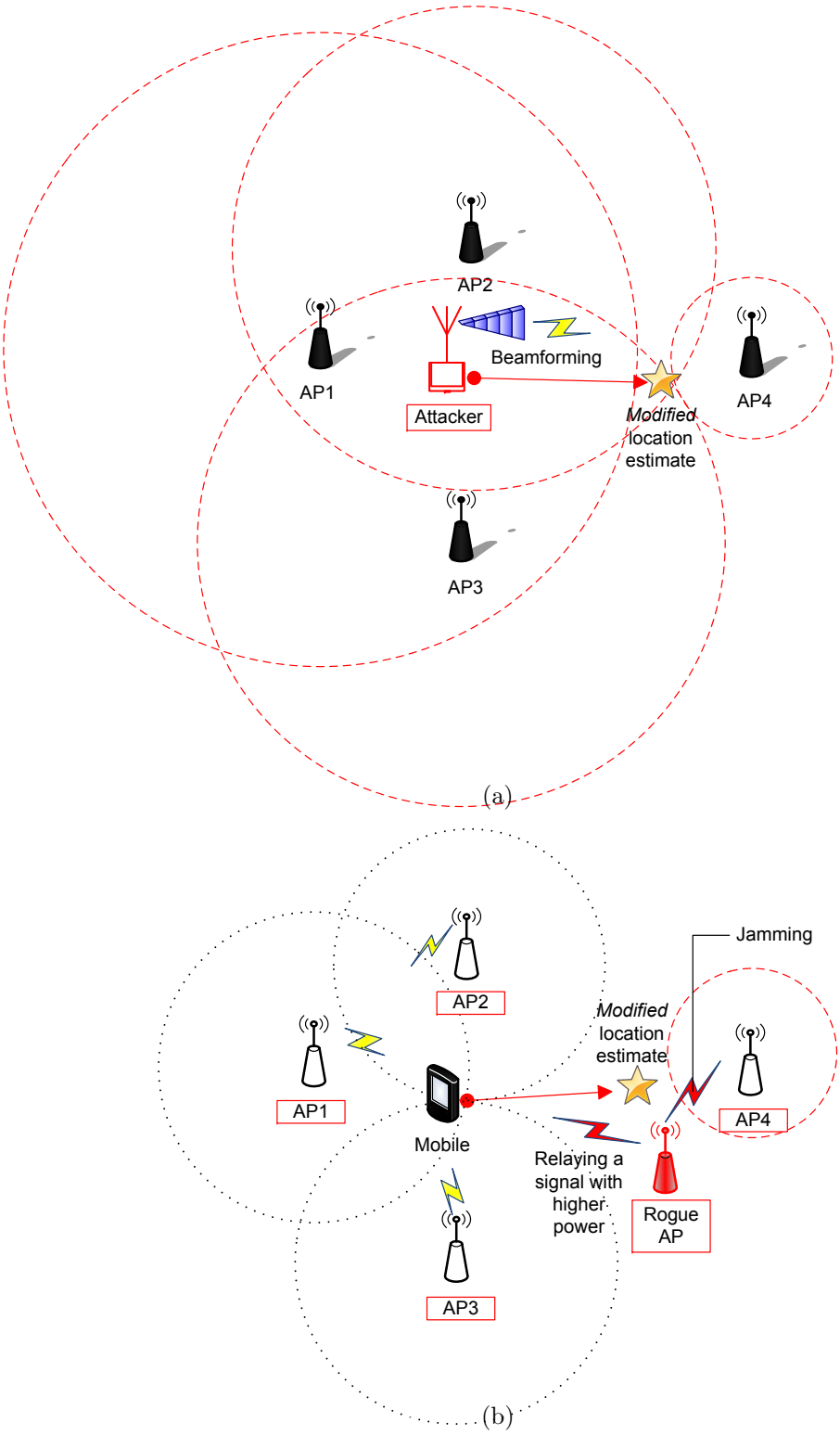


Figure 4.2: Primary types of location spoofing attacks (noiseless cases). (a) Attack position spoofing. (b) Anchor signal spoofing. The shaded entity indicates the one in charge of signal measurements, while the entity whose name is in a box indicates the signal source. The dotted circles centered at each anchor position and the star represent range estimates and the resulting (falsified) position estimate, respectively.

nodes or landmarks with known coordinates $\{\boldsymbol{x}_i\}_{i=1}^{m}$. An attacker against this passive system can spoof or disrupt its own location information by falsifying one or more of the signal parameters, thus hindering the network from correctly locating its attack position. The wireless network security issues raised earlier are associated with this category or attack position spoofing.

Modification of Attack Position

An attacker attempts to modify its position as it appears somewhere else (*e.g.*, inside a corporate building as opposed to off-site) by falsifying its signal parameter(s) as illustrated in Fig. 4.2a. If the attacker's identity is hidden, its position could be disguised as much as it desires. Also, a stationary attacker could make it appear as if it is traveling in a planned direction.

The attacker may employ a smart antenna technique to modify its attack position [32, 71]. To launch this adaptive beamforming (BF) attack, it needs to be equipped with an antenna array or other directional antenna. Due to the recent development of radio technologies such as software-defined radio (SDR) [32, 105], this type of attack is becoming more feasible.

Disruption of Attack Position

The signal parameters or features of an attacker can be (continuously) varied to disrupt a location algorithm. As a result, the algorithm would be misled significantly, or have a computation/convergence error without producing a reliable output. A simple yet effective strategy would be varying transmit power levels or packet departure times while pretending to follow the system's protocol. This attack strategy may be considered equivalent to the modification attack, but is differentiated here for a more detailed understanding. Specifically, the primary aim of the disruption attack is to simply confuse a target location system. On other hand, the modification attack strategy intends to misrepresent the attacker's position by some desired degree or to specific position. Launching this intelligent attack requires more sophisticated algorithms and/or hardware, and would be harder to detect.

It should be noted that attackers will likely exploit the uncertainties of the fading channel and target location as well as its mobility factor. In particular, a BF attacker can intentionally generate multipath error by removing an LOS propagation path or varying its main beam direction. Also, attackers can take advantage of the impact of node geometry in location estimation. For example, a novice attacker who lacks sophisticated knowledge/hardware may attempt to spoof a location system by sitting at a bad localization spot such as near the wall or in the corner of a room/building, hoping the system will experience a large estimation error.

Example 4.1 – Impact of Attack Position Spoofing

Consider an RSS-based location estimator using a set of range estimates $\{\hat{d}_i\}_{i=1}^m$ based on RSS measurements $\{P_i\}_{i=1}^m$ (dBm) at m anchor nodes. As detailed earlier, the estimates $\hat{d}_i$ can be determined by a statistical model known as a log-distance path loss model $PL(d_i)$. Then, the maximum likelihood estimator of the distance d_i can be shown to be

$$\hat{d}_i = d_0 \cdot 10^{\frac{P_0 \text{ (dBm)} - P_i \text{ (dBm)}}{10 n_p}} \tag{4.6}$$

where n_p is the path loss gradient (or exponent), and $P_0 = P_t + G_t + S_t - PL(d_0)$ which is the signal power observed at a close-in reference distance d_0. Consider three anchors located at $\{\boldsymbol{x_i}\}_{i=1}^3 = \{[0,0]^T, [5,20]^T, [10,5]^T\}$ meters in a noiseless scenario, where $n_p = 2$ and path loss $PL(d_0) = 30$ dB at $d_0 = 1$ m. According to system protocols, a mobile target is supposed to use the assumed values of signal parameters as $P_t = 10$ dBm, $G_t = 0$ dB, and $S_t = -3$ dB.

(a) In the absence of attack, estimate the distance d_i to each anchor which measures the target signal power as $\{P_i\}_{i=1}^3 = \{-42.91, -45.38, -34.14\}$ dBm.

(b) Repeat when the true (yet unknown) $P_t = -10$ dBm (*i.e.*, SS attenuation attack) for APS given $\{P_i\}_{i=1}^3 = \{-62.91, -65.38, -54.14\}$ dBm.

(c) Repeat when the true $P_t = 30$ dBm (*i.e.*, SS amplification attack) for APS given $\{P_i\}_{i=1}^3 = \{-22.91, -25.38, -14.14\}$ dBm.

(d) Which type of SS attack adds a positive (or negative) bias to a range estimator?

Solution

(a) Using (4.6), the distance d_i to each anchor is estimated as $\{\hat{d}_i\}_{i=1}^3 = \{9.90, 13.15, 3.61\}$ meters which should be equal to the true range in the absence of any error source.

(b) Due to the SS attenuation attack, the distance d_i to each anchor is falsified so that $\{\hat{d}_i\}_{i=1}^3 = \{98.97, 131.52, 36.06\}$ meters.

(c) Due to the SS amplification attack, the distance d_i to each anchor is falsified so that $\{\hat{d}_i\}_{i=1}^3 = \{0.99, 1.32, 0.36\}$ meters.

(d) By comparing the above results, we can see that SS attenuation and amplification attacks add positive and negative biases to range estimates, respectively.

From this example, we see that location spoofing attacks can be characterized according to the form of bias (*i.e.*, either positive or negative bias) to a range or location estimator. The further details will be presented in the next chapter, where location spoofing attacks are mathematically characterized.

4.3.2 Anchor Signal Spoofing

In the case of client-based positioning, adversaries exploit the reliance of a mobile client on the anchors' signal features observed at the mobile to determine its own position. An

adversarial (or compromised) network anchor attempts to falsify its beacon signal to be used by self-positioning victim clients, or to directly degrade/jam eligible anchor signals. In the former case, the attacker typically pretends to be a legitimate anchor after infiltrating the network, and causes a victim to be synchronized to the malicious anchor (*e.g.*, rogue access points [43, 44]). The GPS/WLAN spoofing issue discussed earlier is in this category. This attack type is a critical issue particularly for collaborative WSNs/CRNs, where the resulting location error propagates throughout the network.

Modification of Legitimate Position

Spoofing the position of a legitimate network client is of increasingly serious concern as more mobile applications are dependent on the mobile's position. As an example scenario, mobile clients can be convinced that they are moving in the right direction while actually traveling towards a hazardous area. One possible attack scheme is to compromise authorized anchors or jam and relay signals of legitimate anchors as illustrated in Fig. 4.2b. To modify the victim's position, techniques similar to those used for attack position spoofing can be applied. Another simple approach is manually moving anchors or localized sensors to other places so that location estimates become falsified even with correct information about location parameters.

Disruption of Legitimate Position

This attack is similar to the modification attack but instead of modifying location information, an adversary simply disrupts the mobile's location estimation procedure. As discussed in the case of attack position spoofing, this attack can be launched in a simpler manner in terms of software/hardware complexity. Besides the use of malicious anchors, the disruption can occur either directly at the mobile client (*e.g.*, jamming) or at those legitimate anchors associated with the victim (*e.g.*, by compromising or moving).

Another critical attack scenario is where an adversary attempts to disrupt/destroy the whole location system such as the system's location database (*e.g.*, access point location data [36], RSS radio map [15]). Thus, the location system may malfunction, be out of service or continuously produce excessive location errors. As a consequence, the associated location applications/services (*e.g.*, healthcare service, home/enterprise surveillance system) become unreliable or may be out of service.

Example 4.2 – Impact of Anchor Signal Spoofing

Repeat Example 4.1 while switching the role of signal measurements between the mobile to be localized and the anchor nodes in order to examine the impact of anchor signal spoofing attacks. This means that we consider a mobile-based positioning network, where the mobile

client under attack takes RSS measurements on beacon signals from m anchors. In this attack case, one or more of the anchors are adversarial (may have been compromised).

What are the similarities and differences between the effects of the two types of location spoofing attacks (*i.e.*, attack position spoofing and anchor signal spoofing)?

Solution

In the absence of an attack and other external factors, the range estimates (and thus location estimates) should be the same as in Example 4.1. The major difference is that the range estimators are biased selectively by the associated anchors or attackers. Note that this selective attack for anchor signal spoofing is fundamentally similar to an attack position spoofing strategy through antenna beamforming. The beamforming attack (*i.e.*, $G_{t_i} \neq G_{t_j},\ \exists i \neq j$) biases the individual range estimators selectively as detailed later in this chapter.

This example implies that the characterization of location spoofing attacks should be based on the type of bias caused to the individual range estimators (*i.e.*, either uniformly or selectively). The details of the mathematical characterization will be presented in the next chapter.

4.3.3 Location Disclosure

The security aspect of this attack type is fundamentally different from the above attack types which directly impact the attacker's or victim's position information. Specifically, this attack type is more concerned with privacy issues regarding spatio-temporal location information of legitimate clients. When this attack is successful, the disclosed location information of the victim can be abused by malicious entities for blackmail, kidnapping, interference, or other assaults on the victim's privacy.

The need and level of location privacy are differently perceived by each individual. Thus, noting that the protection of location confidentiality usually leads to the degradation of system performance such as data throughput and latency, one should be careful to balance the system performance, location confidentiality and location availability, depending upon the client's needs.

4.4 Recent Work on Location Security

We described above that location attacks can be classified primarily into three types: (a) attack position spoofing, (b) anchor signal spoofing and (c) location disclosure. Accordingly, we can categorize related studies according to the three attack types, although the first two types of attacks are launched in a similar manner to spoof the position of an attacker or victim. Because of current research interests and the more vulnerable attack scenarios, most

of the previous research efforts regarding attack position spoofing and location privacy focus on (small/medium-scale) infrastructure-based networks (*e.g.*, WLANs and cellular networks), whereas the security issues concerning anchor signal spoofing have typically been tackled for (large-scale) wireless sensor or ad-hoc networks.

4.4.1 Attack Position Spoofing

There has recently been an increasing number of research activities involving the detection and localization of a location attacker. Chen et al. [45, 106] propose a statistical approach using a linear LS (LLS) estimator for attack detection and localization. More specifically, by examining the residual error between the observed RSS and a stored database of RSS data (*i.e.*, radio frequency (RF) fingerprints or a radio map [15]), they form a statistical hypothesis testing problem. The test statistic is the resulting residual error, assuming *a priori* knowledge of error statistics.

The construction of an accurate RSS database or RF fingerprints usually requires considerable effort and cost due to offline measurements, manual calibration, thorough site planning, and more. Since the wireless environment changes over time (*e.g.*, AP relocation/addition and varying surroundings) as do the statistical properties, it is necessary to continuously re-measure the time-varying environment. Further, in practice it may be challenging to build a reliable location database or RF fingerprints due to notorious fading effects, mobility, random antenna orientation and diverse device/radio types among many other factors. Even if this approach based on pre-established information or signal features detects location attacks, it may be difficult to localize the attacker accurately, particularly BF attackers.

4.4.2 Anchor Signal Spoofing

Most of the studies on defending a location system from ASS are focused on WSNs. In securing WSNs, the primary objective is to correctly discover legitimate sensor locations in the presence of an attack. Li et al. [53] and Liu et al. [51] similarly propose range-based, robust statistical methods to achieve robustness against spoofing beacons using the LMS and MMSE, respectively. The former secure system also builds upon the pre-established signal strength database [15]. The latter scheme makes a decision based on a "consistency check" among multiple beacon signals and "majority voting," assuming that a majority of beacon signals are benign (*i.e.*, attack-free and have a small noise variance). Thus, the success of the approaches will depend on the system constraints, assumptions and/or reliable offline training.

Lazos et al. [48, 50, 54] propose several range-free sensor location discovery algorithms called SerLoc, HiRoc and ROPE. These methods all adopt a conceptual sectored antenna (*i.e.*, deterministic cone-shape beam without side/back lobes) at every anchor node to actively/securely

discover the overlapping region where sensors are located. They initially proposed SerLoc whose location resolution is improved by HiRoc at the expense of higher computational complexity and communication overhead. They both assume no jamming attacks. ROPE integrates HiRLoc and SPINE [49] which uses verifiable multilateration and distance bounding algorithms [107] while solving the issues of jamming for HiRLoc and the need for many nodes with SPINE. However, it still requires nanosecond processing and time measurements (as does SPINE) as well as a directional antenna at every node. When real directional antennas (exhibiting an irregular antenna pattern) are employed over spatially correlated radio environments, the performance will likely be degraded considerably.

Sastry et al. [47] propose a secure in-region verification algorithm that verifies location claims made by sensors. Specifically, insecure, unlocalized sensors, called "provers," verify their location claims through secure beacon nodes called "verifiers." They argue that 80-90 % of legitimate location claims by stationary verifiers can be correctly verified. While it can be used for security access control, its use is generally limited due to algorithm constraints and assumptions. This disadvantage is also faced by the proximity-based algorithm proposed by Ray et al. for emergency WSNs [108]. This approach employs majority voting and an identifying code, thereby requiring high computational complexity and high storage overhead.

As noted, many previous studies in this category are only applicable to WSN applications because of their assumptions (*e.g.*, high node density and less location accuracy).

4.4.3 Location Disclosure

The concern about this security threat is increasing due to the increasing use of private location information for LBSs, location-based social networking and many other promising applications. Accordingly, many of the current research efforts concerning location security are devoted to location privacy provisions. Due to the nature of the problem, many studies focus on system-level (*e.g.*, link/network/message/policy-based) solutions rather than on location estimation issues.

Jiang et al. [109] propose methods at the link level. Specifically, location privacy can be protected by changing user's pseudonyms (*e.g.*, MAC and IP addresses) or by controlling a MAC silent period and transmit power at the expense of lower data throughput and higher system complexity. They measure the achieved location privacy using information entropy. Gedik et al. [110] develop a scalable architecture for ensuring the location privacy based on a personalized k-anonymity model, as similarly found in [111]. Specifically, they achieve location privacy through a message perturbation engine for which several variations of spatio-temporal cloaking algorithms [111] are developed. Contrary to anonymity-based methods, others propose system-level approaches such as privacy policy based methods [112].

4.5 Impact of Location Spoofing Attacks

In the rest of the dissertation we place our emphasis on major issues related to the falsification of a node's own position, which is usually associated with a location attacker (*i.e.*, attack position spoofing). Nevertheless, many of our discussions, results and solutions can also be applied to anchor signal spoofing cases. Further, a secure location system resilient to attack position spoofing can be adopted to prevent anchor signal spoofing by detecting/locating malicious anchors, GPS spoofers or jammers which emit RF energy regardless of the attack type. In Chapter 7, we will see that the source of anchor signal spoofing can be located without any cooperation from the malicious node.

With respect to a location disclosure attack, this chapter will provide insight into how to ensure location privacy of a legitimate client at the physical or link level. This is due to the inherent similarity between the two security problems, as the major issue of this chapter is to reveal the attacker's location information–that is equivalent to the act of location disclosure–at the physical layer. Note that despite the effort of protecting private location information at the system level (*e.g.*, encrypting signal transmissions), an adversary can still potentially locate the victim by observing its RSS.

In the effort to develop an approach to the detection or localization of location spoofing attacks, it is important to understand the potential security risks and vulnerabilities of a location estimator under attack. In particular, we must examine the impact of different types of attacks on location accuracy, and discover the primary type(s) of harmful threats. This study will enable us to develop effective techniques for attack detection and localization and evaluate their performance.

Before looking into practical localization scenarios, it is worthwhile to examine a simple noiseless case so as to estimate the direct impact of attacks on a location estimator. The following simple example using a linear LS estimator and three anchor nodes will give insight into the effect of location attacks in practice.

Example 4.3 – The Effect of Location Spoofing Attacks (Noiseless Case)

Repeat Example 4.1 focusing on the location estimator instead of individual range estimates. As detailed in Chapter 3, the mobile position $\boldsymbol{\theta} = [x, y]^T$ can be estimated via trilateration as $\hat{\boldsymbol{\theta}} = \boldsymbol{A}^{-1}\boldsymbol{b}$ where

$$\boldsymbol{A} = \begin{bmatrix} x_2 - x_1 & y_2 - y_1 \\ x_3 - x_1 & y_3 - y_1 \end{bmatrix}, \ \boldsymbol{b} = \frac{1}{2}\begin{bmatrix} \|\boldsymbol{x_2}\|^2 - \|\boldsymbol{x_1}\|^2 - (\hat{d}_2^2 - \hat{d}_1^2) \\ \|\boldsymbol{x_3}\|^2 - \|\boldsymbol{x_1}\|^2 - (\hat{d}_3^2 - \hat{d}_1^2) \end{bmatrix}. \tag{4.7}$$

Repeat questions (a)–(c) in Example 4.1 (where *true* $P_t = 10$ dBm) to determine the location estimate $\hat{\boldsymbol{\theta}}$ and then answer the question (d).

Solution

(a) Using (4.7), the target position (x, y) is determined as $\hat{\boldsymbol{\theta}} = [7, 7]^T$ which is the same as the true target position since neither attack nor noise was considered.

(b) In the presence of the SS attenuation attack with an *assumed* $P_t = -10$ dBm, the location estimate is falsified as $\hat{\boldsymbol{\theta}} = [593.67, -325.38]^T$.

(c) When the SS amplification attack with *assumed* $P_t = 30$ dBm is considered, the location estimate is falsified as $\hat{\boldsymbol{\theta}} = [1.13, 10.32]^T$.

(d) By comparing the above results, we can see that SS attenuation attacks are significantly more detrimental than SS amplification attacks. In Example 4.1, we observed that positive range bias is induced by SS attenuation attacks. Is this statement true in general under practical localization scenarios? In the following, we seek the answer to this important question.

With a basic understanding of the impact of location attacks in Example 4.3, we now turn our attention to practical localization scenarios. Since translating the effect of an attack or range bias into location error is mathematically intractable for nonlinear LS estimation, we rely here on simulation using realistic shadow fading and simulation models presented in Chapter 2.

4.5.1 Attack Regions and Scenarios for Analysis

Before going further, let us describe how we categorize location spoofing attacks or scenarios against RSS-based estimators in order to reveal the harmful characteristics of attacks. More specifically, the security of location information will be discussed in terms of the RMSE or location error under four primary attack scenarios: (a) no attack, (b) SS attack, (c) BF attack, and (d) BF attacks coupled with SS attacks (*i.e.*, SS+BF attacks). Special attention is given to the estimator error behavior subject to SS or SS+BF attacks with a range of SS attack levels in dB. The magnitude of the dB value indicates the falsified SS level $\sum_{k=1}^{2} |\Delta\psi_{i,k}|$ (dB) of $\boldsymbol{\Psi}_i$ in Eq. (4.1) along with "+" or "−" indicating either a positively biased or negatively biased attack, respectively. Here, $\Delta\psi_{i,k} = \psi_{i,k} - \hat{\psi}_{i,k}$ (dB) is defined as a fallacious change or error in the *a priori* known (or assumed) value $\hat{\psi}_{i,k}$ for the kth element of $\boldsymbol{\psi}_i$. Hence, $\hat{\boldsymbol{\psi}}_i$ includes the *assumed* transmit power, transmitter system loss and antenna gain on the ith link. The *zero* SS attack level (*i.e.*, $\sum_{k=1}^{2} |\Delta\psi_{i,k}| = 0$ dB) is equivalent to the absence of any SS attack, though a BF attack can be present (*i.e.*, $\Delta\psi_{i,3} \neq 0$ dB). For simulation analysis we employ the adversary and simulation models given in Section 2.4 with the true $P_t = 0$ dBm for SS attacks and varying $\{G_{t,i}\}_{i=1}^{m}$ for BF attacks.

To demonstrate the effectiveness of SS attacks, BF attacks, and their combinations we define a pair of *attack regions* as shown in Fig. 4.3: (a) *negative* SS attack region and (b) *positive* SS attack region. Attacks in the negative SS attack region add a negative bias to the range estimators $\hat{d}_i$, which are equivalent to SS *amplification* attacks in RSS-based location estimation. On the other hand, attacks in the positive SS attack region introduce a positive

bias to the true range, which are equivalent to SS *attenuation* attacks. As observed in Example 4.3 and we will see soon, this classification enables us to differentiate effective and ineffective location attacks.

Further, through this generalization according to estimator bias we can incorporate various kinds of location attacks or systematic biases leading to anomalous behavior of a location estimator. For instance, most well-known environmental biases, including NLOS propagation and signal power attenuation due to LOS blockage and obstructions between the transmitter and receiver, fall in the positive SS attack region. On the other hand, negative biases can be caused by systematic errors induced by, for instance, miscalibration of RF components and over-estimated path loss rate. Therefore, as future work, our study in this dissertation can be extended to the problem of reliable/robust position location subject to various types of natural, environmental and intentional biases.

4.5.2 With Prior Knowledge of Path Loss Rate

In many location studies, it is typical to assume that the path loss (PL) rate or n_p is known *a priori*. We now examine the effect of location attacks on this type of location estimator referred to as Known-PL. Then, the impact on a more practical estimator, referred to as Joint-PL, which does not rely on this prior knowledge is given and compared with Known-PL. Note that Known-PL estimates position parameters only, given a known path loss model, whereas Joint-PL estimates the nuisance parameter n_p of the PL model and the position parameters jointly. However, neither of the estimators has knowledge of the spatial correlation nor the variance of shadow fading.

In Fig. 4.3, the RMSE performance of Known-PL is presented in the presence of different types of attacks. The estimator operates in a channel with $n_p = 4$ (known) and $\sigma_S = 2,\ 5,$ or 8 dB. We summarize key results in the following, while providing the detailed analysis in the next chapter.

- *Attack Region*–The effects of location attacks are very different depending upon which SS attack region that the attack resides. Regardless of the attack type, in the positive SS attack region, the RMS location error increases at a high rate with an increase in the positive SS attack level (in dB). On the other hand, in the negative SS attack region, the increasing rate of the RMSE is much slower with an increase in the magnitude of the negative SS attack level;

- *Attack Type*–One may expect that SS+BF attacks are more effective than SS attacks alone for the same SS attack level. This intuition is found to be correct in the negative SS attack region, where the RMSE difference is approximately 5 m. However, for SS attack levels greater than 10 dB, the effectiveness of SS attacks alone is greater by approximately 4 m;

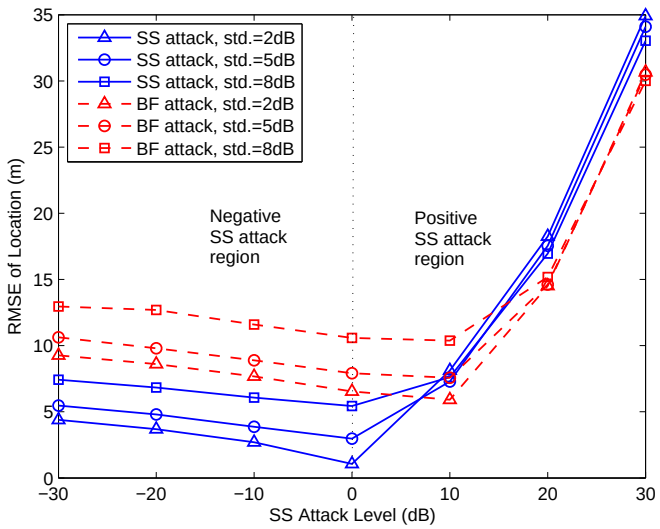


Figure 4.3: Impact of signal strength (SS) and beamforming (BF) attacks on an RSS-based location estimator with known path loss rate (*i.e.*, Known-PL).

- *Minimum MSE*–As intuitively expected, the minimum MSE (MMSE)[1] occurs in the absence of any location attack (*i.e.*, SS attack with the SS attack level of 0 dB). However, the MMSE for the SS+BF attack case is observed when the SS attack level is 10 dB regardless of the shadowing variance σ_S^2. In other words, the SS attack *negates* the adverse effect of the BF attack until the SS attack level is greater than 10 dB;
- *Shadow Fading*–As intuitively expected, the performance of the estimator is worse with higher shadowing variance in the negative SS attack region. However, with SS attack levels greater than 10 dB for SS attacks and 20 dB for SS+BF attacks, the estimator performance is dominated by an attack-induced bias rather than the environmental variability.

4.5.3 Impact of Incorrect Path Loss Estimation

In the above simulation with Known-PL, we have assumed that the parameter value of the path loss gradient n_p is known *a priori*. However, this assumption is an oversimplification in many practical localization scenarios. In practice, it requires costly off-line measurements and manual effort to estimate the exact value of n_p which varies with environment. Although this channel parameter value is in the small range, typically from 2 to 5 [40], a small error in its estimation has a considerable impact on location accuracy due to its representation for the path loss rate over log distances.

[1]From a location estimator standpoint, this MMSE point is optimal in order to minimize the impact of an attack.

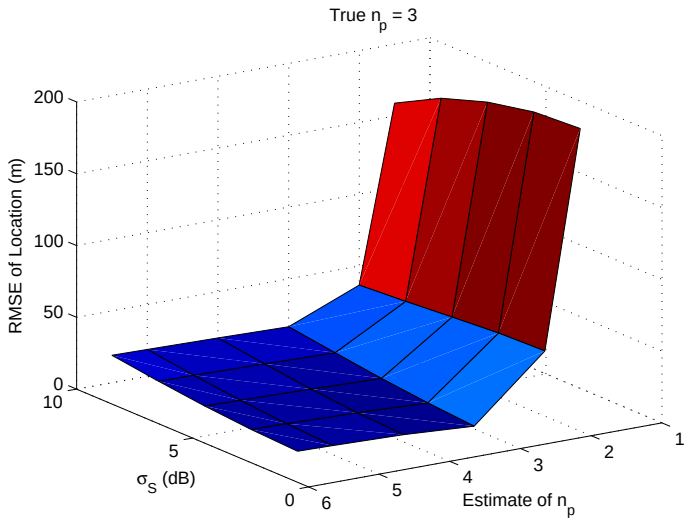


Figure 4.4: Impact of the incorrect estimation of path loss gradient n_p.

In Fig. 4.4, the RMSE of an RSS estimator which operates in a channel with $n_p = 3$ and various σ_S levels is shown for a range of n_p estimates. It can be clearly seen that underestimation is much more destructive than overestimation for the RSS approach. We also note that its impact is much more significant than the adverse effect of shadow fading. This result suggests that if accurate estimation of n_p is not feasible, it is a good strategy to bias an estimator of n_p so that its value is overestimated.

Note the similarity between Figs. 4.3 and 4.4. Estimates of n_p lower than its true value are equivalent to adding *positive* bias to range measurements as in the positive SS attack region. Thus, there is a security concern involving the estimation of n_p. More specifically, an adversary may exploit the adverse effect of the incorrect estimate of n_p. For example, attackers take advantage of the fact that channel conditions vary (unpredictably) over a short period of time in public sites (*e.g.*, airports, coffee shops, *etc.*) or for mobile users. Also, we may encounter situations where the estimate of n_p is erroneous (possibly due to attacks) or unknown *a priori* (in most practical cases). In particular, we note that one useful anchor signal spoofing strategy will be to deliver falsified information about n_p to self-positioning nodes that rely on the channel information from anchors (refer to Section 4.3.2).

4.5.4 Joint Parameter Estimation

As discussed in Chapter 4.2, the prior knowledge of nuisance parameters $\mathbf{\Psi}_i$ in a radio propagation model is not always realistic. Particularly, it is often costly or infeasible to obtain the path loss gradient n_p prior to the process of location estimation. Even if the procedures for offline system training are available for the estimation of the channel parameter value,

there is always the possibility that the estimation could be erroneous or falsified. Also, since the wireless channel is time-varying by nature, the path loss rate n_p also needs to be updated regularly. In the next chapter we will investigate the issues regarding nuisance parameters in detail from both estimation and security perspectives.

Here we present a summary of our key simulation results with Joint-PL as shown in Fig. 4.5. To compare the attack effects on Known-PL and Joint-PL, the results in the both cases are plotted together in Fig. 4.5 and compared in the following. Note that we assume perfect knowledge of n_p for Known-PL. The detailed analysis will be given along with the characterization of location attacks in the next chapter.

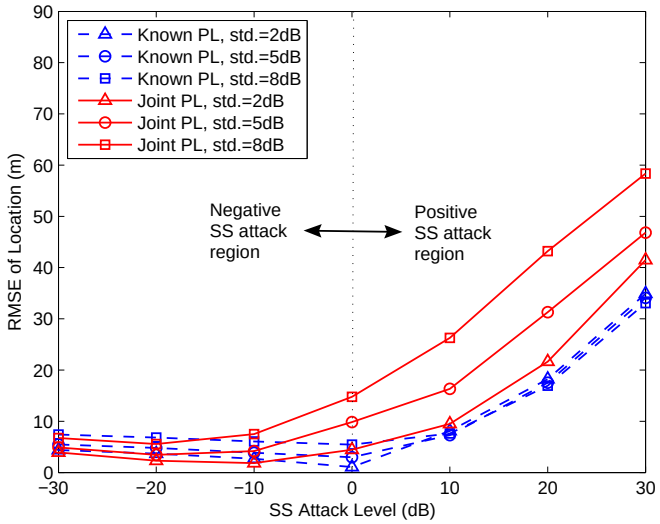
- *Attack Region*–As observed previously, the effects of location attacks are very different depending upon the form of bias to the estimators due to the attack. For both of the estimators, location error increases rapidly with an increase in the positive SS attack level. Particularly, Joint-PL is more susceptible to higher positive SS attacks, noting that the RMSE increases almost exponentially with the positive SS attack level. On the other hand, negative attacks are not effective or useless from an attacker perspective. Even more, Joint-PL tends to *benefit* from negative SS attacks. This result will be explained through nuisance parameters and heavy-tailed error in the next chapter;

- *Estimation Strategy*–Comparing the two estimators, while Known-PL outperforms Joint-PL in the positive SS attack region, it is interesting to note that Joint PL exhibits somewhat better RMSE performance in most part of the negative SS attack region. This result will also described through nuisance parameters and heavy-tailed error in the next chapter;

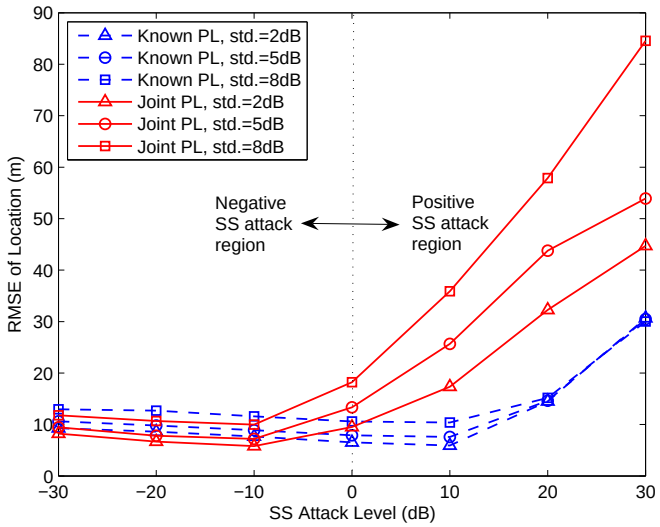
- *Attack Type*–While BF attacks alone do not introduce significant location error (simpler SS attacks with large SS attack levels would be more effective), the BF attacks coupled with SS attacks (*i.e.*, SS+BF attacks) can be very detrimental. This is because SS+BF attacks can lead to a high positive bias while frequently introducing abnormal RSS observations referred to as position outliers or anomalies. The location estimate anomalies will lead to the heavy-tailed error. This result will be further examined through the heavy-tailed error and the bias-variance tradeoff in the next chapter;

- *Minimum MSE*–It is also interesting to note that the MMSE is observed at *non-zero* SS attack levels. Specifically, the MMSE for Joint-PL can be found at the SS attack levels of −20 dB and −10 dB in the presence of SS attacks alone and SS+BF attacks, respectively. On the other hand, the MMSE for Known-PL can be observed when the SS attack level is 10 dB with BF attacks. Without the BF attack, its MMSE is found when there exists no attack. This result will be described through the bias-variance tradeoff in the next chapter;

- *Shadow Fading*–The impact of location spoofing attacks becomes higher for Joint-PL in the worse shadowing environment, especially in the positive SS attack region. However,



(a)



(b)

Figure 4.5: Impact of (a) signal strength (SS) attacks and (b) beamforming (BF) attacks coupled with SS attacks on an RSS-based estimator which jointly estimates position coordinates (x, y) and the nuisance parameter n_p (*i.e.*, Joint-PL) as well as Known-PL (copied from Fig. 4.3).

Known-PL is not very sensitive to the variability of shadowing, particularly when the positive SS attack level dominates the shadowing noise. In other words, when the path loss gradient n_p needs to be estimated jointly, positive SS attacks are more effective in more cluttered wireless environments (*e.g.*, indoor and urban environments). This issue will be further discussed through the heavy-tailed error in the next chapter;

Let us next look into the impact of attacks on Joint-PL from a different viewpoint. Specifically, we plot the simulated cumulative distribution function (CDF) of the location error in Fig. 4.6. It can be seen that the effects of an SS attack vary depending upon which form of bias is added to the range measurements. The impact of an attack which induces a *positive* bias is significant and detrimental, whereas the effect of an attack which induces a *negative* bias is insignificant. This result agrees with the above observation in Fig. 4.5 and can be attributed to two basic effects as detailed in the next chapter. First, a negative[2] bias (reducing the range estimate) reduces the feasible region of the problem while a positive bias increases the feasible region. More specifically, the solution is constrained to be inside the set of anchors by negative SS attacks (*i.e.*, decreasing range circles from a geometric viewpoint), whereas attacks which induce a positive bias increase the region farther away from the true position. Secondly, negative SS attacks can actually improve the estimator's accuracy by negating the natural positive bias due to shadow fading. This can be seen by examining the tails of the CDF in the attack-free case as compared to negative SS attacks. Specifically, the tails are heavier (*i.e.*, more likely to give large error) in the attack-free case.

The impact of BF attacks are also shown in Figure 4.6. As observed earlier, such attacks have larger impact than negative-bias SS attacks or even moderate positive-bias SS attacks (< 10 dB). They are not as effective, however, as large positive-bias SS attacks. The effectiveness of a BF attack can be improved by coupling BF attacks with positive-bias SS attacks (*i.e.*, positive SS+BF attacks) as shown in the figure. Thus, the most effective attacks are those which induce a uniform positive range bias or a selective range bias. For attack detection and adversary localization, therefore, particular emphasis should be placed on positive-bias SS and SS+BF attacks.

4.6 Conclusion

In order to understand the potential security risks in location estimation, we have classified location attacks according to three primary attack types–specifically, attack position spoofing, anchor signal spoofing, and location disclosure–and discussed the associated security risks. The effects of the location spoofing attacks were compared using examples. Then, due to our focus on network-based position location for attack detection and localization, we further explored the impact of attack position spoofing–simply called location (spoofing)

[2]It should be remembered that a negative bias is induced by *increasing* either the transmit power or antenna gain, while a positive bias is induced by *decreasing* either of the transmitter parameters.

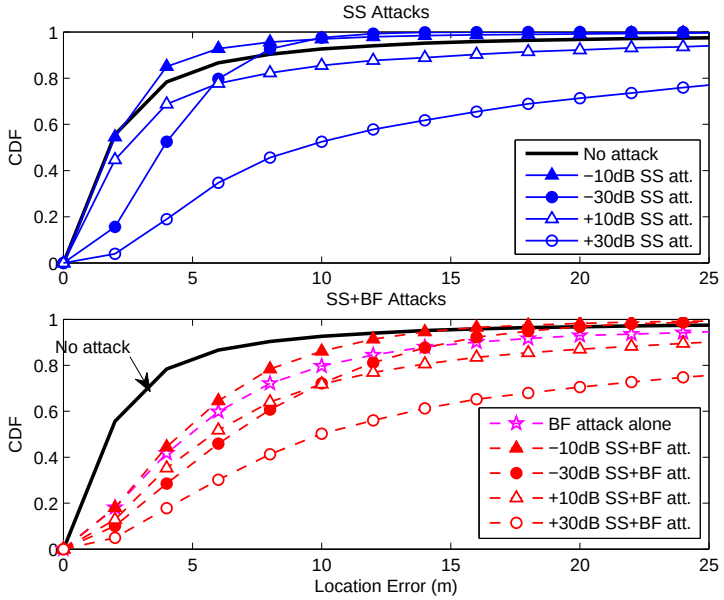


Figure 4.6: Cumulative distribution functions (CDFs) of location error under SS attacks (top) and BF or SS+BF attacks (bottom) using Joint-PL.

attacks in the rest of the dissertation. Specifically, we investigated the effects of various position spoofing strategies (*i.e.*, SS, BF and SS+BF attacks) on two typical estimators, one assuming prior knowledge of path loss rate n_p and the other estimating the nuisance parameter n_p jointly with the position parameters of interest. We showed via simulation results the similarities and differences of attacks on the two estimators. By categorizing location attacks depending on the form of the bias to a location estimator or the individual range estimators (*i.e.*, positive or negative; uniform or selective), we found that positive-bias attacks are more detrimental to location estimators. We will analyze the attack effects in more detail in the following chapter.

Chapter 5

Characterization and Analysis of Location Spoofing Attacks

5.1 Introduction

When dealing with systematic error in signal processing, it is useful to characterize the source of error and its effect on the system or estimator behavior. In location estimation, as described earlier, a location spoofing attack can be regarded as a source of systematic error which is usually associated with a bias in the process of range/position estimation. If the bias effect can be characterized, the impact of location attacks can be understood better, thus facilitating the design of a secure location system.

In the previous chapter we explored via simulation the effects of location attacks in terms of the RMS error of a location estimator under attack. We next examine the impact of attacks on range and location estimation based on RSS measurements. More specifically, the main purpose of this chapter is to analyze the behavior and security issues of location estimators in the presence of attacks observed in Chapter 4. The analysis will give insight into how to address the problem of attack detection and localization in the rest of this dissertation. The main contributions of this chapter are thus as follows:

- In Section 5.2 we characterize the impact of location spoofing attacks in an analytic form to understand their fundamental characteristics. Specifically, it is shown that location attacks are represented mathematically as a *scaling factor* which biases individual range estimates and thus the location estimate. Depending on whether the scaling factor biases the range estimates uniformly or selectively, attacks are categorized as either uniform attacks or selective attacks, which are realized through signal strength (SS) falsification and beamforming (BF), respectively, in RSS-based systems. Since the bias can be either positive or negative, attacks are further classified into positive-bias and negative-bias attacks. The characterization along with the results in

Chapter 4 will indicate on which types of attack we should place an emphasis in attack detection and localization (as considered in Chapters 6 and 7);

- Section 5.3 discusses one of the three important issues related to two typical location estimators, one with prior knowledge of path loss rate n_p (*i.e.*, Known-PL) and the other estimating the channel parameter jointly with the position parameters (x, y) (*i.e.*, Joint-PL). Specifically, we describe reasons for the better performance of Known-PL than Joint-PL which is supposed to perform better in correlated, biased estimation conditions based on the previous theoretical analysis [57, 113, 114]. We argue that the main reason for the better performance is the practical issue known as the heavy-tailed behavior of an estimator, which becomes worse with more effective attacks. Then, we show that the "potential performance" of Joint-PL (better than Known-PL) can be achieved *if* the anomalous behavior is addressed (as accomplished in Chapter 7);

- The heavy-tail issue in location estimation is further investigated in Section 5.4. It is shown that more effective attacks introduce more severe heavy-tailed behavior by causing location estimates with more excessive error. We illustrate that even if the anomalous errors occur only occasionally, their impact on location accuracy is detrimental in the MSE sense. This investigation also emphasizes the significance of dealing with the heavy-tailed behavior for secure position location (as studied in Chapter 7);

- In Section 5.5 we explain why the minimum MSE (MMSE) (*i.e.*, best location accuracy) was found at *non-zero* SS attack levels in Chapter 4 (see Fig. 4.5). Also, in Chapter 4, the value of the MMSE was observed at different attack levels for different estimators and attack cases. Noting that location attacks induce a systematic bias to the estimates, we demonstrate that the bias-variance tradeoff issue is the primary reason. This chapter also presents the bias-variance characteristics of a location estimator and the related theoretical limits to the estimator's accuracy from the perspective of general location estimation.

5.2 Characterization of Location Spoofing Attacks

In this work we are concerned with range-based localization which relies on RSS observations to estimate range and subsequently position. Location spoofing attacks are thus manifested as modifications to the observed RSS value. Thus, we wish to characterize location attacks with respect to their impact on range and location estimation. From the perspective of a location estimator, it can be shown that an attack is fundamentally equivalent to a scaling factor $\mathcal{S}_i$ that deceptively scales or biases the estimator of the ith range d_i. We will examine the estimator bias in the absence and presence of an attack in the following.

5.2.1 Natural Bias

Before characterizing the effect of attacks, we must first examine any natural biases in the range estimation process. Even when no attack is present, range-based location estimators using RSS measurements are inherently biased in two respects. First, most practical estimators in signal processing are biased with small data sets. Specifically, ML and LS estimators are known to be *asymptotically* efficient, and hence *asymptotically* unbiased [57]. With finite data records and nonlinear models as in most practical localization scenarios, they are usually *biased* and *inefficient*. Second, it can be shown that the range (and thus location) estimator using RSS is inherently biased in the presence of log-normal shadowing. It should be noted that, however, the natural bias is typically small compared to the bias induced by effective attacks as demonstrated in Chapter 6.

As described in Chapter 4, the received power level P_i ($\equiv P(d_i;\mathbf{\Psi}_i)$) at a specific distance $\{d_i\}_{i=1}^m$ follows the log-normal distribution

$$f_P(P_i;d_i) = \frac{10/P_i}{\sqrt{2\pi}\sigma_S \ln 10} \exp\left\{-\frac{\left(\ln P_i - \ln \bar{P}_i\right)^2}{2\left(\sigma_S \frac{\ln 10}{10}\right)^2}\right\} \tag{5.1}$$

assuming the absence of any attack, *i.e.*, $\sum_{k=1}^{3}|\Delta\psi_{i,k}|$ (dB) = 0 in Eq. (4.1). When dealing with radio parameters it is common to use decibel values. However, it is often simpler to use linear values for derivations. Thus, only when using notations in decibel (dB) we explicitly state it. Otherwise, linear values are assumed. After substituting the average received power $\bar{P}_i = P_0\left(\frac{d_0}{d_i}\right)^{n_p}$ ($P_0 \equiv P(d_0;\mathbf{\Psi}_i)$) into Eq. (5.1), we have

$$f_P(P_i;d_i) = \frac{10/P_i}{\sqrt{2\pi}\sigma_S \ln 10} \exp\left\{-\frac{1}{2}\left(\frac{10n_p}{\sigma_S \ln 10}\right)^2 \left(\ln\left[\left(\frac{P_i}{P_0}\right)^{\frac{1}{n_p}} \frac{d_i}{d_0}\right]\right)^2\right\}. \tag{5.2}$$

The corresponding log-likelihood function $\ell(d_i)$–that is the logarithm of the PDF as a function of the unknown parameter d_i–given the value of n_p (which can be treated as a nuisance parameter for the derivation) is

$$\ell(d_i) = \ln f_P(P_i;d_i), \qquad i = 1,\ldots,m \tag{5.3a}$$

$$= \ln\left(\frac{10/P_i}{\sqrt{2\pi}\sigma_S \ln 10}\right) - \frac{1}{2}\left(\frac{10n_p}{\sigma_S \ln 10}\right)^2 \left(\ln\left[\left(\frac{P_i}{P_0}\right)^{\frac{1}{n_p}} \frac{d_i}{d_0}\right]\right)^2. \tag{5.3b}$$

And, the first derivative of $\ell(d_i)$ with respect to d_i is

$$\frac{\partial \ln f_P(P_i;d_i)}{\partial d_i} = -\left(\frac{10n_p}{\sigma_S \ln 10}\right)^2 \ln\left[\left(\frac{P_i}{P_0}\right)^{\frac{1}{n_p}} \frac{d_i}{d_0}\right] \frac{1}{d_i}. \tag{5.4}$$

which is set to zero to obtain the ML estimator of d_i:

$$\hat{d}_i^{(\mathrm{ML})} = d_0 \left(\frac{P(d_0; \mathbf{\Psi}_i)}{P(d_i; \mathbf{\Psi}_i)} \right)_{i=1,\ldots,m}^{\frac{1}{n_p}} \tag{5.5}$$

where $P(d_0; \mathbf{\Psi}_i)$ and $P(d_i; \mathbf{\Psi}_i)$ are the observed RSS values P_0 and P_i, respectively, which depend on the radio parameters in $\mathbf{\Psi}_i$. When an attack is not present and the uncertainty in $\mathbf{\Psi}_i$ does not exist, $P(d_0; \mathbf{\Psi}_i)$ and $P(d_i; \mathbf{\Psi}_i)$ can be simplified to known constants $P(d_0)$ and $P(d_i)$, respectively. However, due to log-normal fading, it can be shown that the ML estimator $\hat{d}_i^{(\mathrm{ML})}$ is naturally biased:

$$\mathrm{E}\left[\hat{d}_i^{(\mathrm{ML})}\right] = \mathrm{E}\left[d_0 P(d_0)^{\frac{1}{n_p}} P(d_i)^{-\frac{1}{n_p}} \right] \tag{5.6}$$

$$= d_0 P(d_0)^{\frac{1}{n_p}} \exp\left\{ \ln\left[\frac{d_i}{d_0} P(d_0)^{-\frac{1}{n_p}} \right] + \frac{1}{2}\left(\frac{\sigma_S \ln 10}{10 n_p} \right)^2 \right\} \tag{5.7}$$

$$= d_i \exp\left\{ \frac{1}{2}\left(\frac{\sigma_S \ln 10}{10 n_p} \right)^2 \right\} \tag{5.8}$$

$$= \mathcal{B} \cdot d_i, \qquad i = 1, \ldots, m, \tag{5.9}$$

where $\mathcal{B}$ is a scaling factor due to log-normal shadowing:

$$\mathcal{B} = \exp\left\{ \frac{1}{2}\left(\frac{\sigma_S \ln 10}{10 n_p} \right)^2 \right\}. \tag{5.10}$$

Thus, we have a natural bias of $(\mathcal{B} - 1)\, d_i$ which is *positive* in typical wireless channels as $\mathcal{B}$ ranges from 1.02 to 1.94 for $n_p \in [2, 5]$ and $\sigma_S \in [4, 10]$ (dB) [40].

5.2.2 Adversary Model

Next, suppose that there exists a location attack (*i.e.*, falsification of the transmitter parameters $\boldsymbol{\psi}_i$). In this work we are concerned with attacks which impact the RSS seen at a particular anchor node. Let $P^*(d_i; \mathbf{\Psi}_i)$ denote the received power level at the ith anchor influenced by an attack, *i.e.*, $\sum_{k=1}^{3} |\Delta\psi_{i,k}|$ (dB) > 0, while the received power in the absence of an attack is denoted by $P(d_i)$. Recall that $\Delta\psi_{i,k}$ denotes the fallacious modification level of the kth transmit parameter of $\boldsymbol{\psi}_i$ in Eq. (4.1) by the attack such that $\Delta\psi_{i,k} = \psi_{i,k} - \hat{\psi}_{i,k}$ (dB) where $\hat{\psi}_{i,k}$ is the *assumed value* of $\psi_{i,k}$.

In the presence of an attack, the log-normal random variable $P(d_i)$ in Eq. (4.1) is modified as

$$P^*(d_i; \mathbf{\Psi}_i) \text{ (dBm)} \sim \mathcal{N}\left(\bar{P}(d_i) + \sum_{k=1}^{3} \Delta\psi_{i,k},\ \sigma_S^2 \right), \tag{5.11}$$

where $\sum_{k=1}^{3} \Delta\psi_{i,k}$ (dB) is the sum of fallacious changes in the transmit parameters (*i.e.*, transmit power, system loss and transmit antenna gain) seen by the ith anchor. This falsification modifies (or biases) the estimator $\hat{d}_i^{(\mathrm{ML})}$ of the true range d_i in Eq. (5.5), thus resulting in a modified ML (MML) estimator $\hat{d}_i^{(\mathrm{MML})}$. Positive (or negative) values of $\Delta\psi_{i,k}$ (dB) induce negative (or positive) bias on the range estimate so that the modified range assumed by the estimator appears to be smaller (or larger) than its actual range.

To derive the bias of an attack-corrupted (or modified) range estimator $\hat{d}_i^{(\mathrm{MML})}$, we first obtain the mean of $\hat{d}_i^{(\mathrm{MML})}$ by replacing $P(d_i)$ in Eq. (5.5) with one falsified by an attack $P^*(d_i;\boldsymbol{\Psi}_i)$ through Eq. (5.11) as

$$\mathrm{E}\left[\hat{d}_i^{(\mathrm{MML})}\right] = \mathrm{E}\left[d_0 P(d_0)^{\frac{1}{n_p}} P^*(d_i;\boldsymbol{\Psi}_i)^{-\frac{1}{n_p}}\right] \tag{5.12}$$

$$= d_0 P(d_0)^{\frac{1}{n_p}} \exp\left\{\ln\left[\frac{d_i P(d_0)^{-\frac{1}{n_p}}}{d_0 \prod_k \Delta\psi_{i,k}^{\frac{1}{n_p}}}\right] + \frac{1}{2}\left(\frac{\sigma_S \ln 10}{10 n_p}\right)^2\right\} \tag{5.13}$$

$$= \frac{d_i}{\prod_k \Delta\psi_{i,k}^{\frac{1}{n_p}}} \exp\left\{\frac{1}{2}\left(\frac{\sigma_S \ln 10}{10 n_p}\right)^2\right\} \tag{5.14}$$

$$= \frac{\mathrm{E}\left[\hat{d}_i^{(\mathrm{ML})}\right]}{\mathcal{C}_i} \tag{5.15}$$

$$= \mathcal{S}_i \cdot d_i, \qquad i = 1, \ldots, m, \tag{5.16}$$

where $\Delta\psi_{i,k} = 10^{\frac{(\psi_{i,k} - \hat{\psi}_{i,k})\ (\mathrm{dB})}{10}}$ and the attack factor $\mathcal{C}_i$

$$\mathcal{C}_i = 10^{\frac{\sum_k \Delta\psi_{i,k}\ (\mathrm{dB})}{10 n_p}}. \tag{5.17}$$

The link-dependent scale factor $\mathcal{S}_i$ (> 0) is a function of both the natural scaling $\mathcal{B}$ and the scaling due to the attack $\mathcal{C}_i$:

$$\mathcal{S}_i = \frac{\mathcal{B}}{\mathcal{C}_i}, \quad i = 1, \ldots, m. \tag{5.18}$$

Then, the bias of the MML estimator of range d_i is given by

$$b(d_i, \mathcal{S}_i) = (\mathcal{S}_i - 1) d_i. \tag{5.19}$$

The values of $\mathcal{B}$ and $\mathcal{C}_i$ which represent natural and unnatural effects, respectively, contribute to the range bias $b(d_i, \mathcal{S}_i)$ in opposite ways. Further, while the natural bias $\mathcal{B}$ is inherently limited and uncontrollable, the unnatural bias $\mathcal{C}_i$ can be varied through $\Delta\boldsymbol{\psi}_i$ to the extent

possible. As mentioned, $\mathcal{B}$ ranges from 1.02 to 1.94 in typical wireless environments [40], indicating that a range estimator is *positively* biased by 2 ~ 94 % even in the absence of an attack. When an attack is present, this naturally biased estimator is *rescaled* by the attack. More specifically, when the sum of the fallacious changes in the position-related parameters, *i.e.*, $\sum_{k=1}^{3}\Delta\psi_{i,k}$ (dB), is −30, −10, 10, and 30 dB (assuming $n_p = 4$), $\mathcal{C}_i = 0.18,\ 0.56,\ 1.78$, and 5.62, respectively. The former two values of $\sum_{k=1}^{3}\Delta\psi_{i,k}$ are related to power amplification attacks, whereas the latter two values correspond to power attenuation. Note that the values of $\mathcal{B}$ and $\mathcal{C}$ impact the range bias in opposite ways; Specifically, $\mathcal{B} > 1$ *increases* the bias of a range estimator (*i.e.*, positive-bias natural sources), whereas $\mathcal{C} > 1$ *decreases* it (*i.e.*, negative-bias attacks). This result is a mathematical interpretation of our previous description that SS amplification and attenuation attacks lead to reduced and increased range estimates than assumed (or believed) by an estimator.

Finally, to assess the effect of the attack on the resulting position estimates we rewrite an RSS-based location estimator $\hat{\boldsymbol{\theta}}_R$ as a function of $\hat{d}^{(\mathrm{ML})}$ (*i.e.*, without attack) and the attack factor $\mathcal{C}$. This can be done by substituting the residuals $\boldsymbol{r}(\boldsymbol{\theta}) = \boldsymbol{v} - \boldsymbol{L}(\boldsymbol{\theta})$ (under attack) where

$$
\begin{aligned}
r_i(\boldsymbol{\theta}) &= v_i - L_i(\boldsymbol{\theta}) && (5.20)\\
&= P^*(d_i;\boldsymbol{\Psi}_i)\ (\mathrm{dBm}) - P(d_0)\ (\mathrm{dBm}) + 10n_p\log_{10}\left[\frac{d_i(\boldsymbol{\theta})}{d_0}\right] && (5.21)\\
&= 10\log_{10}\prod_k \Delta\psi_{i,k} - 10\log_{10}\left[\frac{P(d_0)}{P(d_i)}\right]\left(\frac{d_0}{d_i(\boldsymbol{\theta})}\right)^{n_p} && (5.22)\\
&= 10\log_{10}\left[\left(\frac{d_i(\boldsymbol{\theta})}{\hat{d}_i^{(\mathrm{ML})}}\right)^{n_p}\prod_k \Delta\psi_{i,k}\right]_{i=1,\ldots,m} && (5.23)
\end{aligned}
$$

into the LS merit function

$$
\phi(\boldsymbol{\theta}) = \frac{1}{2}\|\boldsymbol{r}(\boldsymbol{\theta})\|_2^2 \tag{5.24}
$$

which needs to be minimized to obtain the position estimate

$$
\hat{\boldsymbol{\theta}}_R = \arg\min_{\boldsymbol{\theta}}\left\{50n_p^2\sum_{i=1}^{m}\left[\log_{10}\left(\frac{\mathcal{C}_i\cdot d_i(\boldsymbol{\theta})}{\hat{d}_i^{(\mathrm{ML})}}\right)\right]^2\right\}. \tag{5.25}
$$

From this equation, it is clear that an RSS location estimator is a function of naturally biased $\hat{d}_i^{(\mathrm{ML})}$ and the attack factor $\mathcal{C}_i$ which modifies $\hat{d}_i^{(\mathrm{ML})}$. Another important result which can be noticed from Eq. (5.23) is that the residuals $\boldsymbol{r}$ or their norm $\|\boldsymbol{r}\|_2^2 = \|\boldsymbol{v} - \boldsymbol{L}(\boldsymbol{\theta})\|_2^2$ cannot be used as a reliable measure for attack detection, even if the range or location estimator is accurate and robust to natural sources of error (*i.e.*, $var\left[d_i(\boldsymbol{\theta})\right]$ is small and $\frac{\hat{d}_i^{(\mathrm{ML})}}{\mathrm{E}(d_i(\boldsymbol{\theta}))} \approx 1$). This is because when the residual is increased (or decreased) by $\mathcal{C}_i$ (which characterizes the

effect of an attack), it can also be decreased (or increased) by the estimated ranges $d_i(\hat{\boldsymbol{\theta}})$. Additional analysis (particularly a mathematical proof) will be done as future work. We will look further into Eqs. (5.23) and (5.25) in Section 5.5 when discussing the bias-variance tradeoff.

From Eqs. (5.12)–(5.19), we can characterize the effects of location attacks in two respects:

1. A location attack modifies (or scales) ranging parameters $\boldsymbol{\psi}_i$ so as to add either a *negative* or *positive* bias to the range estimate for d_i. In other words, if the attacker increases power or antenna gain ($\Delta\psi_i > 1$), the range estimate is reduced (negative bias), whereas if the attacker decreases power or antenna gain ($\Delta\psi_i < 1$) the range estimate is increased (positive bias);

2. Range estimators over different links $\{\hat{d}_i\}_{i=1}^{m}$ are either *uniformly* biased; $\mathcal{S}_i = \mathcal{S}_j,\ \forall i, j$, or *selectively* biased; $\mathcal{S}_i \neq \mathcal{S}_j,\ \exists i \neq j$.

Accordingly, location attacks can be characterized as either a *uniform attack* (UA) or a *selective attack* (SA). Note that uniform attacks can be further classified according to the form of the range bias induced (*i.e.*, negative or positive). Using this classification, falsifying P_t (an SS attack) corresponds to a UA since all range estimates will be biased either positively or negatively while modifying the antenna pattern will generally be an SA since some ranges will be biased negatively and others positively. More specifically, a target which transmits at a higher power level than it claims (or is allowed) will create $\Delta\boldsymbol{\psi}_i > 1$ for $\forall i$, which will negatively bias all range measurements. Thus, increasing transmit power results in a negative UA. On the other hand, a node which transmits at a lower power will cause uniformly positive range biases which is termed a positive UA. A target which uses a beamforming or smart antenna technique [32, 71] (BF attack) is clearly using an SA since the induced bias will depend on the direction to the particular anchor. Combining transmit power modifications with beamforming (SS+BF attack) would also lead to SAs. Although we have developed this approach with RSS-based positioning in mind, range-based positioning which utilizes time-of-arrival could also be classified in the same manner.

When equipped with a directional antenna, an attacker can launch a BF or SS+BF attack. Without loss of generality, we consider BF attacks using an uniform circular array (UCA) [72] of radius with the array factor (AF) given as

$$AF(\Theta, \Phi) = \sum_{n=1}^{N_a} I_n \exp(j\varpi_n) \tag{5.26}$$

where Θ and Φ are the radiation direction on the x–y plane and along the z-axis, respectively. N_a is the number of array elements, $\varpi_n = \frac{2\pi}{\lambda} d_a \sin\Phi \cos(\Theta - \Theta_n) + a_n$, and d_a is the radius of the circular array. And, $\Theta_n = \frac{2\pi n}{N}$ is the angular position of the nth element on the x–y plane. Here I_n and a_n are the excitation amplitude and phase (relative to the array center)

of the nth element, respectively. In order to direct the peak of the main beam in a desired direction (Θ_0, Φ_0), the excitement phase of the nth element is selected to be

$$a_n = -\frac{2\pi}{\lambda} d_a \sin\Phi_0 \cos(\Theta_0 - \Theta_n) \tag{5.27}$$

so that the maximum of AF occurs for $\varpi = 0$ ($I_n = 1$). As a consequence, the spatial directivity through BF techniques biases range estimates selectively. In a 2-dimensional location problem, the angle Φ along the z-axis is set to $\Phi = 90°$.

We next explore the behavior of a location estimator in the presence of an attack while further looking into the results obtained in Chapter 4. In particular, the estimator behavior is analyzed in three respects: (a) prior knowledge of nuisance parameters, (b) heavy-tailed error and (c) the bias-variance tradeoff. This effort will help us better understand the effect of a location attack and develop an effective approach to the detection and localization of attacks.

5.3 Prior Knowledge of Nuisance Parameters

Many estimation problems in signal processing are characterized by a set of parameters that describe the underlying system configuration, signal features and environment. Among the parameters, which are either unknown or known *a priori*, we are interested only in a subset of their values. In a 2-dimensional range-based location problem using RSS measurements, the system model includes the position parameters (x, y), the path loss exponent n_p, the transmit power P_t, the system loss factor S_t, and transmit antenna gains $\{G_{t,i}\}_{i=1}^{m}$. Among these parameters, our main interest is the position coordinates, while other parameters are just "nuisances." Nevertheless, we need to know the values of the nuisance parameters to determine the position coordinates. The nuisance parameter values are either known *a priori* or estimated jointly with the position parameters.

In estimation theory, it is a fundamental rule to exploit the prior knowledge of the nuisance parameters, if the knowledge is feasible and reliable. From both a classical and Bayesian perspective, the prior knowledge allows the use of a more precise probabilistic model by improving the "closeness" between the observed data and parameters of interest while reducing the uncertainty [57]. Regarding the treatment of the nuisance parameters for location security, an important question is: "*Should we obey this fundamental rule in location estimation, particularly for location security?*" We answer this question by discussing three important factors in the following: (a) feasibility, (b) optimal exploitation and (c) security risk.

First, it is not practical to assume *a priori* knowledge of nuisance parameters in many localization scenarios. While many previous studies in localization presume accurate knowledge of the unwanted parameters (particularly n_p), it is an oversimplification in many cases where reliable off-line training procedures are not feasible. Even if reliable measurement data are

given *a priori*, the data need to be updated regularly due to the time-varying nature of the radio channel. Further, the environmental parameter values are usually determined to be optimal "on the average" (*e.g.*, in the LSE or MSE sense) for the environment. As a consequence, it may not accurately reflect a specific radio propagation condition which changes with target position.

Second, it is often a better strategy for location estimators to estimate nuisance parameters jointly with position parameters, *even though the prior knowledge is available*. It is quite counterintuitive since, in estimation theory, we seek to exploit the prior knowledge of nuisance parameters, if available [57]. However, the recent theoretical studies show that it is actually better to estimate the nuisance parameters jointly with parameters of interest when the MSE criterion is minimized through an ML/LS estimator or, in many cases, a biased estimator [113,114]. In the same sense, most practical RSS-based estimators including ML/LS estimators are inherently *biased* as derived in Section 5.2 and cannot *optimally* exploit the prior knowledge of nuisance parameters in the MSE sense.

Lastly, there is a security risk associated with nuisance parameters, as adversaries can take advantage of the estimator's prior knowledge. More specifically, we have discussed that attackers can falsify transmitter-dependent parameter values such as P_t and G_t under their control. The effect of the falsification can be detrimental as shown in the previous chapter. Further, they can disguise environmental parameter values by modifying LOS/NLOS paths through beamforming or taking advantage of nearby obstacles.

Therefore, in many application scenarios, particularly location security, it is desirable to estimate both types of parameters jointly, even if prior knowledge of the nuisance parameters is available. This argument agrees with previous theoretical studies from a general estimation perspective [113,114]. However, the RMS error behavior of Known-PL and Joint-PL observed in Chapter 4 (see Fig. 4.5) contradicts this. Specifically, the location accuracy of Joint-PL is worse than Known-PL when an SS attack level is higher than approximately −10 dB.

To examine this inconsistency, let us explore an LS error surface or objective function $\phi_R(\boldsymbol{\theta})$ of an RSS-based location estimator in Eq. (5.24) which contains important information about location accuracy. This investigation is useful because in nonlinear, nonconvex optimization, the shape and complexity of the error surface–as evidenced by local minima/maxima, saddle points and curvature/flatness–impact the optimization characteristics such as global optimality, convergence rate, and stability [99]. Since these characteristics decide the accuracy and reliability of location estimation, the performance of a location estimator is closely related to the topographic features of its LS error surface.

Typical LS objective functions of Known-PL and Joint-PL under SS attacks on a logarithmic scale (σ_S = 5 dB, n_p = 3) are shown in Figs. 5.1 and 5.2, respectively. By comparing the two figures, it can be noticed that Joint-PL exhibits better shaped objective functions and lower objective values–that is better residual error–than their counterparts using Known-PL. Interestingly, the most noticeable improvement with Joint-PL compared to Known-PL is when the SS attack level is +30 dB at which Joint-PL has the worst error performance

(see Fig. 4.5). The reason for this inconsistent result can be explained by the *heavy-tailed error behavior* of a location estimator presented next. This issue can also be described by observing the LS error surface. Specifically, the objective function of Joint-PL with high positive-bias SS attacks is occasionally not well-formed, thus leading to anomalously large location error and consequently the heavy-tail of the error distribution.

5.4 Heavy-Tailed Error Distributions

When dealing with location or measurement error e, it is customary to assume the normal distribution which is a function of the variable e^2. This assumption of the *second Laplace law* or *Gauss's law*–that states the frequency of the error is an exponential function of the square of the error–permits a nice mathematical analysis. However, due to undesirable effects in localization such as non-linearity, bad node geometry and non-Gaussian noise, many practical location estimators exhibit heavy- or fat-tails in their error distributions, which is referred to as *heavy-tailed behavior*. In comparison with the Gaussian distribution, the heavy-tail issue can be described by an exponential function of the numerical magnitude of the error $|e|$, referred to as the *first Laplace law* [115]. In this case, there exists no analytical framework, thus leading to considerable mathematical difficulties in obtaining a solution.

Further, if the distribution of location error is heavy-tailed, a small number of excessive errors dominate the MSE performance criterion in Eq. (2.1). Thus, this abnormal phenomenon needs to be taken into account when evaluating the performance of location estimators. However, many localization studies employ a performance metric which does not reflect the heavy-tail behavior (*e.g.*, median). Also, previous statistical studies on location estimation (mostly based on the normal or Rayleigh distribution) do not incorporate this heavy-tail issue, hence leading to overly-optimistic results.

To look further into the heavy-tail issue, in Fig. 5.3 we compare the performance of Known-PL and Joint-PL by focusing on the impact of the heavy-tailed behavior. Specifically, we show the CDFs of location error and two metrics, which are robust to large errors, in Figs. 5.3a and 5.3b, respectively. In Fig. 5.3a, it can be observed that Joint-PL under +30 dB SS attacks performs better than Known-PL in the *lower* error region (*i.e.*, error $\lesssim 45$ m) which is not associated with the heavy tail. The same result can also be found in Fig. 5.3b, where the RMSE disregarding the errors beyond the 95th percentile (which cause the heavy tail) (top) and the median which is robust statistic against data outliers (bottom) are shown over a range of SS attack levels. It can be seen that Joint-PL is better than Known-PL, particularly under effective attacks (*i.e.*, positive-bias attacks with larger SS attack levels). This analysis implies that due to a small number of excessively large errors, a potentially good estimator can be found to be a considerably bad estimator. This is the main reason that the attractive Joint-PL performs worse than Known-PL in terms of the RMS error, particularly with higher SS attack levels. In other words, if the heavy-tail issue is addressed, the performance of the estimator will be improved significantly (as we will show in Chapter

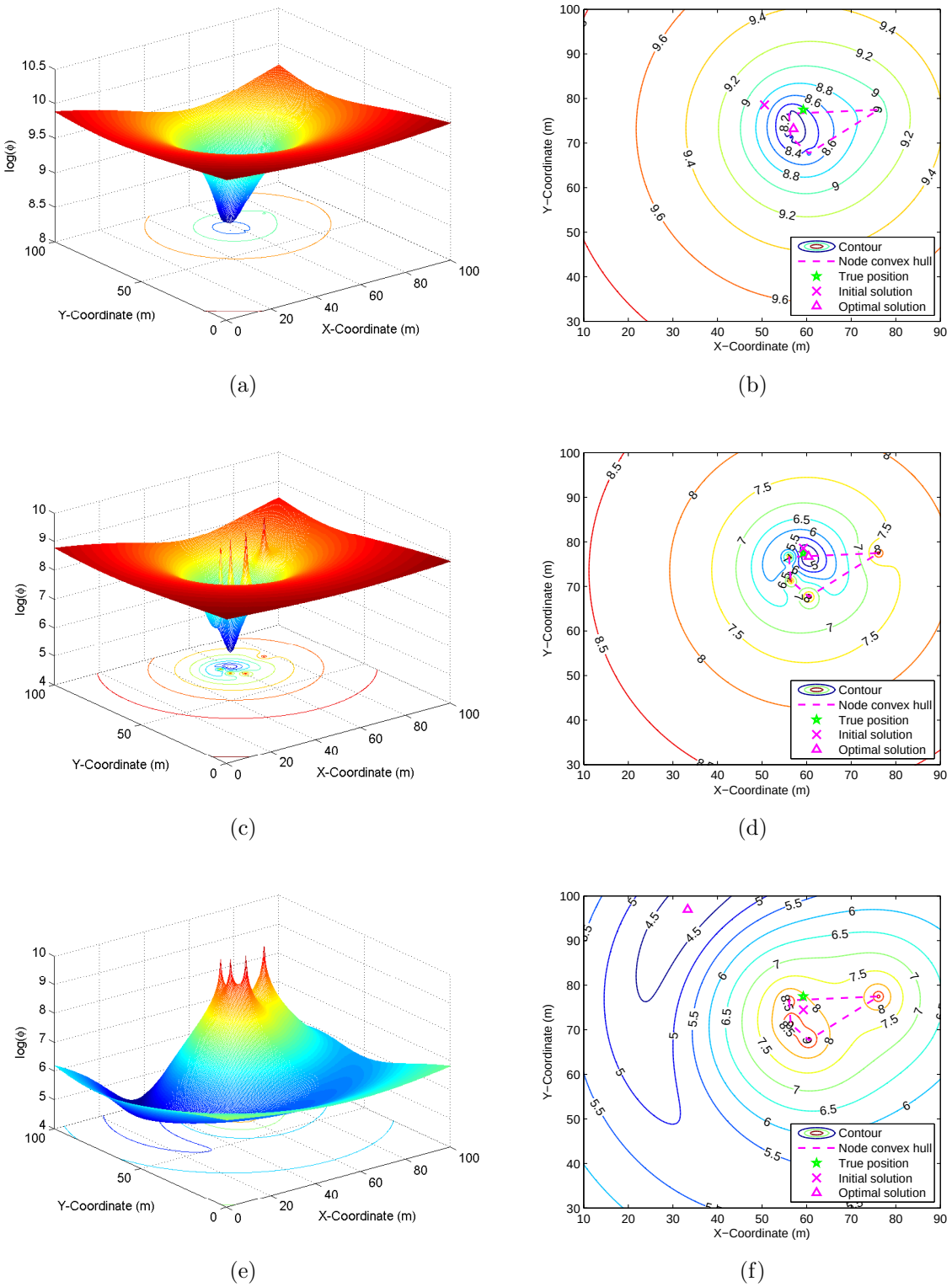


Figure 5.1: The objective function (left column) and the corresponding contour plot (right column) of an LS estimator with *known* n_p (*i.e.*, Known-PL) (σ_S = 5 dB). (a,b) −30 dB SS attack. (c,d) No attack. (e,f) +30 dB SS attack.

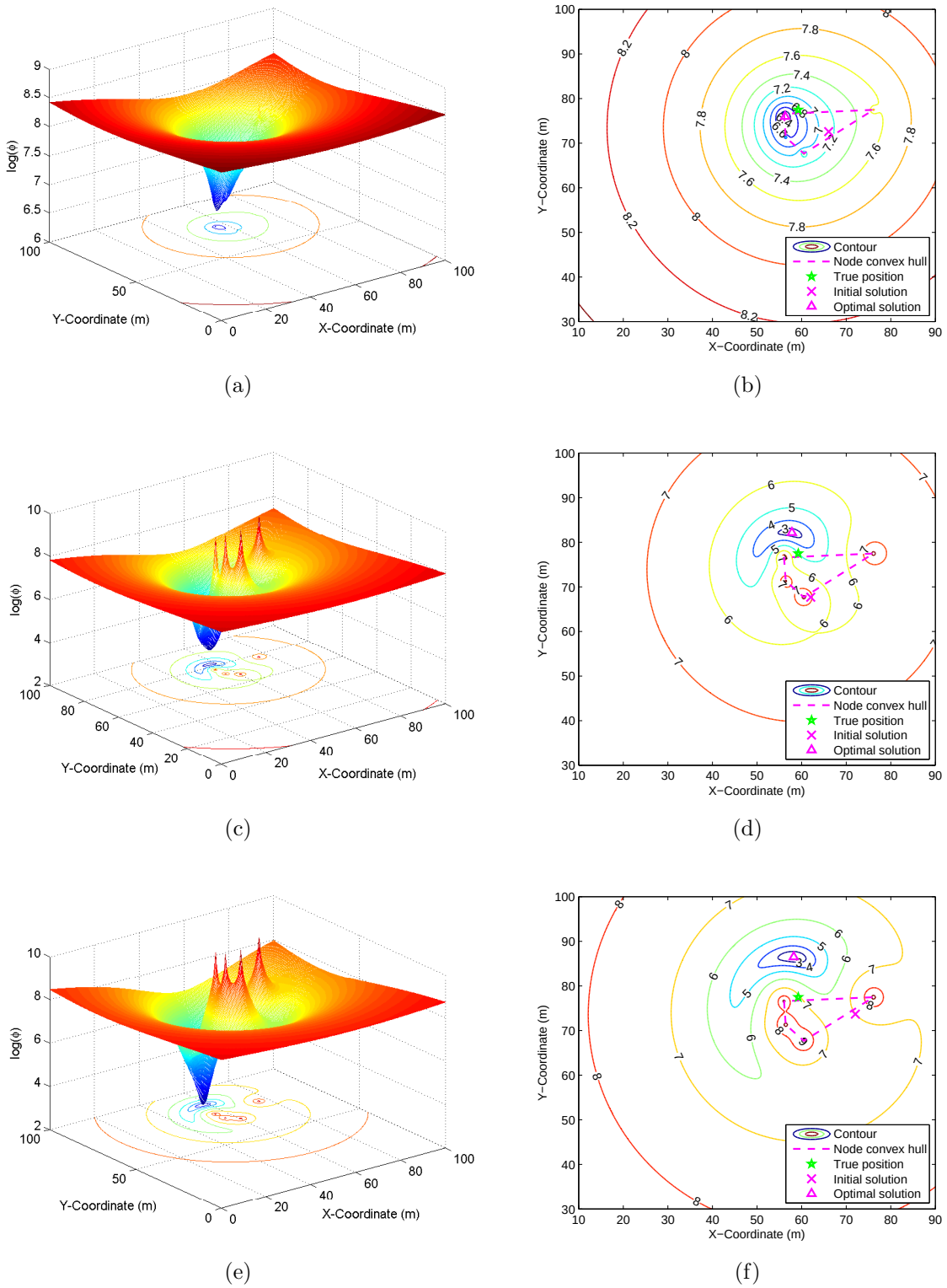
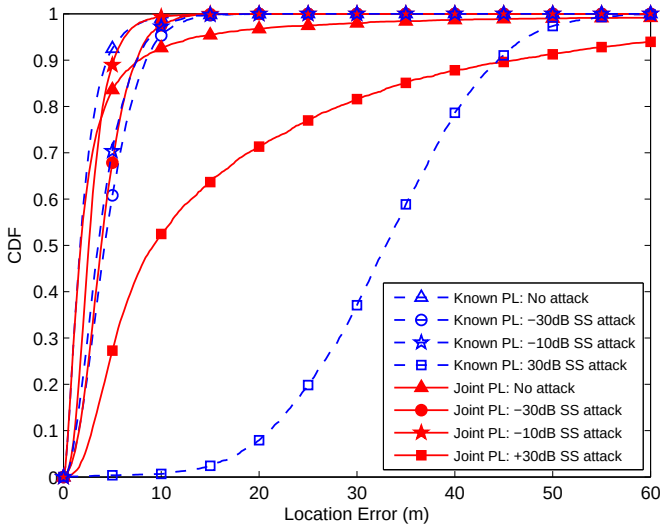
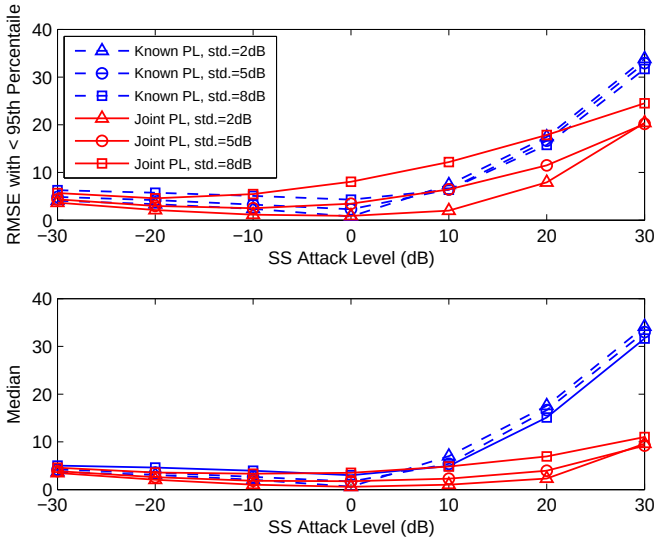


Figure 5.2: The objective function (left column) and the corresponding contour plot (right column) of an LS estimator with jointly estimated n_p (*i.e.*, Joint-PL) ($\sigma_S = 5$ dB). (a,b) −30 dB SS attack. (c,d) No attack. (e,f) +30 dB SS attack.



(a)



(b)

Figure 5.3: Analysis of the effect of SS attacks (associated with Fig. 4.5a), which shows the heavy-tailed error distribution of a location estimator under effective attacks (*e.g.*, +30 SS attack). (a) Cumulative distribution function (CDF) of location error with different SS attack levels (σ_S = 5 dB, n_p = 4). (b) RMSE with estimates below the 95th percentile (*i.e.*, denoted by "< 95th" percentile in the figure) of the error distribution (top) and the median of location error (bottom).

7).

The heavy-tail issue is of particular concern from a security perspective, noting that abnormal estimates with larger error occur when an attack is present. This anomalous behavior can be clearly seen through the complementary CDF (CCDF) in logarithm as given in Fig. 5.4 (associated with Fig. 4.5), where the heavy-tails are observed particularly in the presence of effective or positive-bias attacks. The lower the slope of the CCDF (that is exhibiting greater flatness), the more the estimator exhibits the heavy-tailed error behavior. In fact, attackers are capable of inducing this abnormal error by exploiting the weakness of a location estimator. As a consequence, if there is no countermeasure, even good location systems will not meet desired accuracy requirements, and their location estimates are neither reliable nor secure. In Fig. 5.4 we can see that the heavy tails are hardly observed with negative-bias attacks (*i.e.*, attacks in the negative SS attack region). In this attack region, Joint-PL performs better than Known-PL for different values of shadowing variability. We discussed earlier that this reason can be found from the fact that negatively biased range estimators form well-shaped, stable LS error surfaces, where a solution is near the true position as shown in Figs. 5.1 and 5.2. Note that the well-formed objective functions facilitate better global convergence and stability for numerical optimization algorithms. We will go into further details about the heavy-tail issue and countermeasures in Chapters 6 and 7.

The following is a summary of our key observations as seen by the CCDFs of location error in Fig. 5.4:

- As found in Chapter 4, for both of the estimators, the effects of attacks are very different depending upon which type of bias is added to the range. Positive-bias attacks are very detrimental, whereas the effect of negative-bias attacks is insignificant. Particularly, in practice, Joint-PL is more susceptible to higher positive-bias attacks because its objective function tends to be more ill-formed with a larger feasible region, thus exhibiting the heavy-tailed behavior;
- In the presence of positive-bias attacks, the overall MSE performance of Known-PL is better than that of Joint-PL, yet Joint-PL outperforms Known-PL in the *lower* error region. Under negative-bias attacks, on the other hand, Joint-PL is somewhat better. This is because under negative-bias attacks, the objective function is well-formed over the feasible region constrained around the solution. Also, theoretically, a biased ML/LS estimator performs better with a joint estimation strategy than assuming the prior knowledge of n_p in the MSE sense [113, 114];
- When BF attacks are coupled with positive-bias SS attacks, the estimator performance becomes worse with higher SS attack levels. On the other hand, when coupled with negative-bias SS attacks, the estimator performance under BF attacks can become better, particularly in the case of Joint-PL. This implies that a location estimator which is more susceptible to attacks tends to be stable when negatively biased, as can be inferred from Fig. 5.2 This issue will be further investigated in the next section.

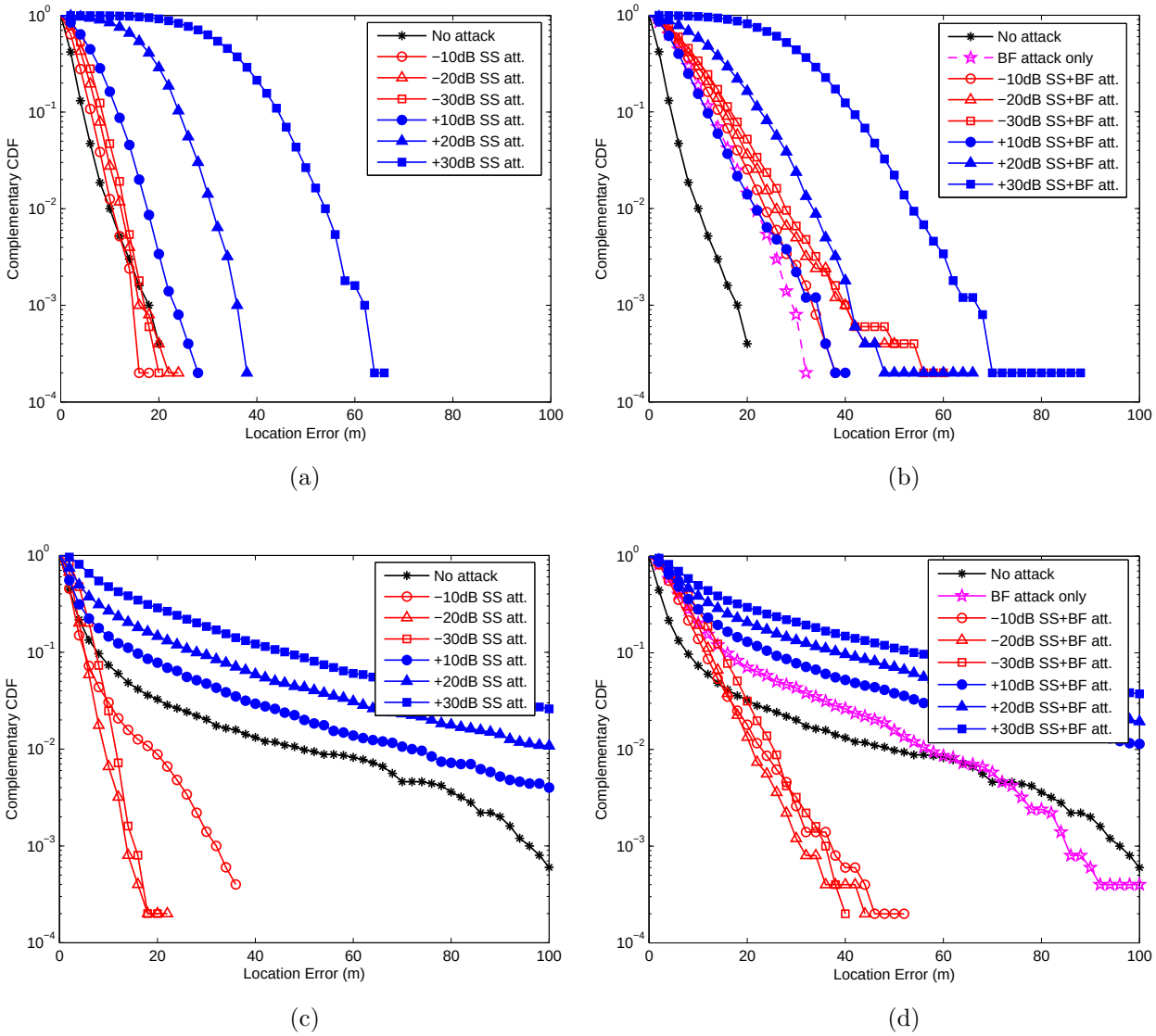


Figure 5.4: Complementary CDF (CCDF) of location error, showing the heavy-tailed error behavior of of a location estimator under effective attacks (associated with Fig. 4.5) ($\sigma_S = 5$ dB, $n_p = 4$). (a) Known-PL under SS attacks. (b) Known-PL under BF attacks. (a) Joint-PL under SS attacks. (b) Joint-PL under BF attacks.

5.5 Bias-Variance Tradeoff

We next describe the last key issue found in Chapter 4, where the MMSE (*i.e.*, best location accuracy) was observed when an attack is *present* as shown in Fig. 4.5. Specifically, the issue will be examined by exploring the *bias-variance tradeoff*, which has been virtually unexplored in relation to location estimation and location security. Although this statistical relationship is not directly exploited in the following chapters, it enables us to examine the impact of location attacks in more detail. While the MSE is the most widely used performance measure in many applications including location estimation, it can be decomposed into bias square and variance terms. Thus, the investigation of the two statistical terms rather than only examining the values of the MSE provides a more thorough view of the estimation error and its source, which is an attack here.

As defined in Eq. (2.1), the MSE is the second moment of the location error which incorporates the variance of the estimator and its bias. More specifically, we can decompose the MSE into two important statistical measures–the variance and bias–as

$$\mathrm{MSE}(\hat{\boldsymbol{\theta}}) = \mathrm{Tr}\left(\mathrm{C}(\hat{\boldsymbol{\theta}})\right) + \|E(\hat{\boldsymbol{\theta}}) - \boldsymbol{\theta}\|^2 \tag{5.28a}$$

$$= \sum_k \left\{\mathrm{var}(\hat{\theta}_k) + \mathrm{bias}^2(\theta_k)\right\} \tag{5.28b}$$

in which $\mathrm{Tr}(\cdot)$ indicates the trace of a matrix. The first and second terms represent the total *variance* and *bias*–the sum of the variances and biases in estimating each position coordinate parameter θ_k–respectively. The square root of the variance is a measure of variability that is the average deviation of the estimator from its average value, whereas the bias reflects the sensitivity/mismatch of the average value of the estimator to the true value.

In signal processing, it is customary to search for an unbiased estimator first, and then seek the one that exhibits the least variability, hoping that estimates are close to the true value. This goal is generally achieved by determining the minimum variance unbiased (MVU) estimator through the derivation of CRLB or using the theory of sufficient statistics [57]. It should be noted from Eq. (5.28) that the direct minimization of the MSE generally leads to an unrealizable estimator due to the fact that the bias is a function of the unknown parameter θ_k (*i.e.*, not exclusively dependent on the observables). Further, the existence of the MVU estimator does not mean that there exists an optimal estimator in which the optimality criterion is typically defined in terms of the MSE.

Noting that the bias square and variance contribute to the MSE *in equal measure*, one may attempt to reduce the both quantities simultaneously. However, there is usually a conflict between these two goals, referred to as the bias-variance tradeoff. Recent studies have claimed that the lower MSE can be achieved by *balancing* the bias and variance values [94, 95, 116]. Specifically, we can often reduce the variance of an estimator substantially at the expense of a small increase in its bias, thus improving the overall MSE. This biased estimator (which may be intentionally achieved, for example, by *scaling* the estimator directly) is preferred

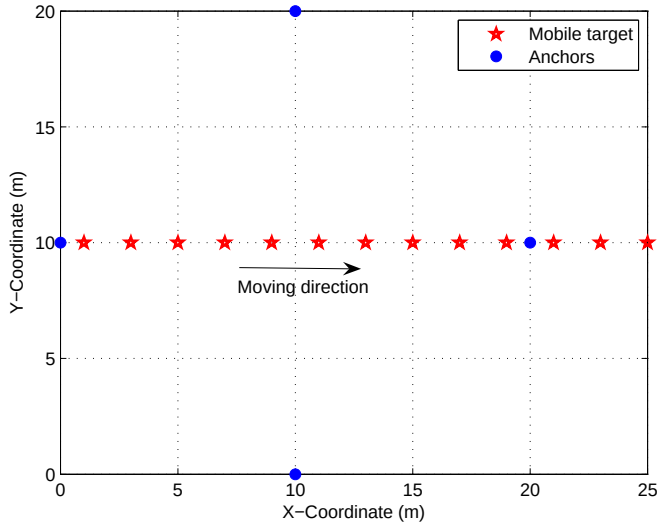
over the MVU estimator in many practical applications in signal processing, particularly with small data records and/or low signal-to-noise ratios (SNRs).

From the perspective of an estimator, the estimator bias and variance are two primary statistical sources of error which are associated with the estimator's error behavior and the effect of attacks. In Section 5.2 we showed that an attack is basically a source of systematic bias. Thus, this bias will affect the estimator's variance and thus the resulting MSE. Before looking further into the bias-variance issue in relation to attacks, let us first examine the tradeoff from the perspective of general location estimation. In relation to the statistical issue we also discuss the fundamental limits of the estimator's location accuracy. This study, based on theoretical measures and their comparison with practical LS estimators, will complement the following numerical analysis of the impact of attacks on a nonlinear location estimator.

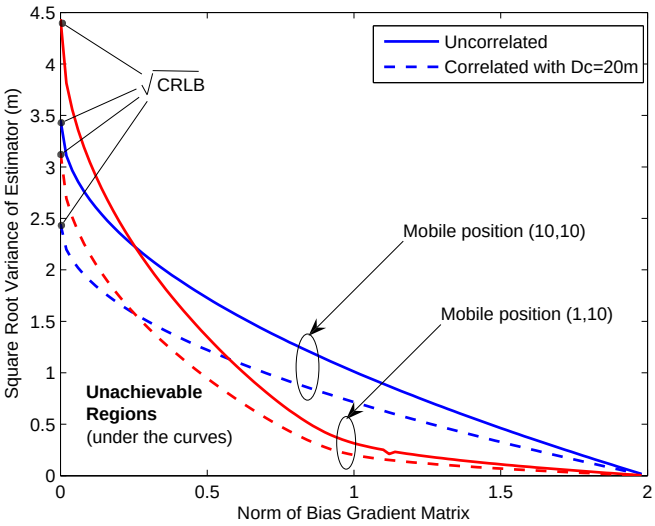
Bias-Variance Characteristics and Theoretical Accuracy Limits

Suppose a basic position location network of four anchors, configured as in Fig. 5.5a, where the mobile target is localized and tracked by an RSS-based estimator. The mobile moves from $X = 1$ to the right along the x-axis with the fixed y-coordinate $Y = 10$. Since the geometry of nodes is one of the primary factors that affect the estimator performance, two distinct positions $\boldsymbol{x} = (10, 10)$ (*i.e.*, the center of the network) and $\boldsymbol{x} = (1, 10)$ (*i.e.*, close to one of the anchors) are chosen to examine the corresponding bias-variance tradeoff. As presented in Fig. 5.5b, given the mobile's true position and the statistical properties of shadow fading we can obtain the theoretical bias-variance tradeoff curves. These curves are closely related to the theoretical accuracy bounds known as the uniform CRLB (UCRLB) which generalizes the CRLB (which can only provide a lower bound on the covariance of an *unbiased* estimator) so as to be applied to both the biased and unbiased cases [94,116,117]. In relation to the UCRLB, we can compute the unachievable performance region (*i.e.*, under the curves) according to the bias-variance characteristics of an estimator. As noted, depending on the mobile position, the bias and variance characteristics change substantially as does the estimator's MSE performance.

The details of the estimator bias-variance tradeoff and its impact on location accuracy (*i.e.*, RMSE) are presented in Fig. 5.6. Here LS estimators using RSS and DRSS are employed to compare their bias-variance characteristics along with the CRLB and UCRLB. As can be inferred from Figs. 5.5 and 5.6, the estimator's statistical characteristics vary depending on the factors affecting location accuracy. Among many factors are unknown mobile position, node geometry, fading variation, and spatial correlation of shadowing. For instance, when the mobile is close to one of the anchors, the RMSE performance is nearly the minimum due to a significant reduction in the estimator's variance at the expense of a relatively small increase in its bias. The increase in the bias at $\boldsymbol{x} = (1, 10)$ is mainly due to the directional tendency of the node geometry toward the right (*i.e.*, impacted by more anchors on the right).

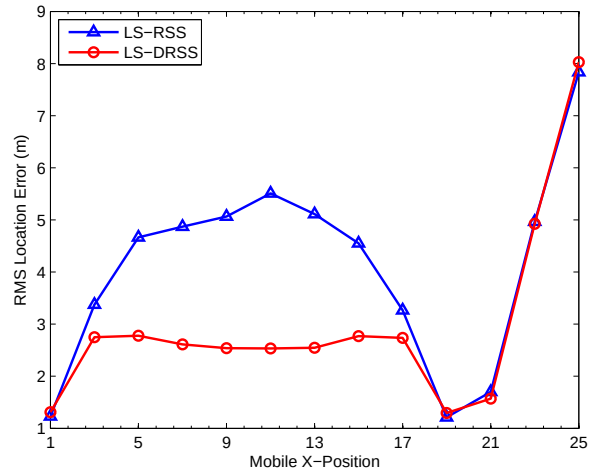


(a)

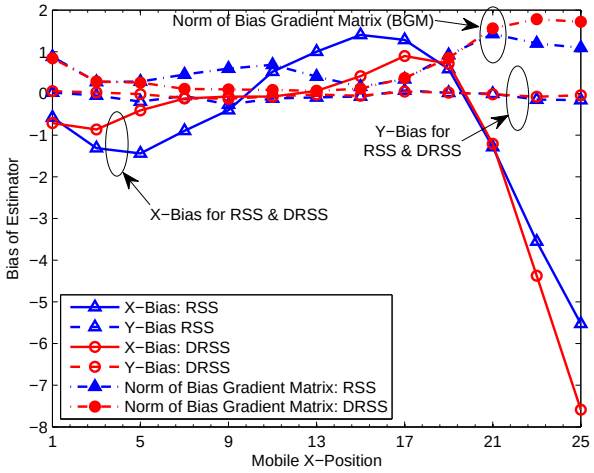


(b)

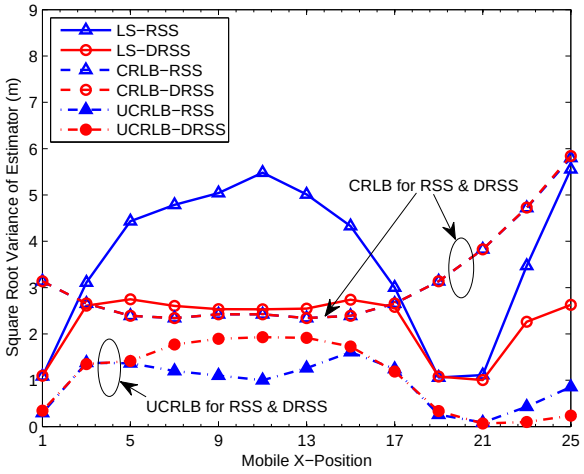
Figure 5.5: Analysis of the bias-variance tradeoff and the achievable estimator performance in general location estimation with spatially correlated shadowing (D_c: the correlation distance). (a) Network scenario considered where a mobile target moves from $X = 1$ to the right along the x-axis with $Y = 10$. (b) The bias-variance tradeoff curve and unachievable region when the mobile is at either $(10, 10)$ or $(1, 10)$.



(a)



(b)



(c)

Figure 5.6: Detailed analysis of the bias-variance tradeoff in relation to Fig. 5.5 as the mobile moves from $X = 1$ to the right along the x-axis with $Y = 10$ ($D_c = 20$ m). Least-squares (LS) estimators based on RSS and DRSS are employed to compare their bias-variance characteristics. (a) Corresponding RMS location error. (b) Associated bias of the estimators. (c) Associated square root variance of the estimators as well as $\sqrt{\text{CRLB}}$ and $\sqrt{\text{UCRLB}}$.

Another major observation from the figure is that the UCRLB can provide a theoretical lower bound on the covariance of an estimator regardless of the degree of bias. On the other hand, as pointed out above, the CRLB cannot be used as a limit to location accuracy. Nevertheless, it should be noted that with an increase in the number of anchors, the CRLB can be a theoretical limit to the estimator's covariance since an ML estimator (as well as an LS estimator in many cases) is *asymptotically* efficient. In other words, with a sufficient number of RSS measurements, a location estimator becomes unbiased. To investigate this asymptotic bound, we repeat the above study with an increasing number of anchors and the mobile near one of the anchors as shown in Fig. 5.7a. The mobile position was chosen such that estimator bias can be substantial due to a strong directional effect of node geometry. As presented in Fig. 5.7, given m equidistant anchor nodes are placed on a circle with radius $r = 10\ m$, the CRLB provides a lower bound on the estimator's covariance when $m \geq 10$. In this case, the CRLB is a tighter bound than the UCRLB. Also, note that the bias as well as the variance decrease with additional anchors so that, as expected, the overall RMSE improves.

Relationships Between the Bias-Variance Tradeoff and Location Spoofing

Earlier in this chapter we characterized location spoofing attacks by a scaling factor which scales or biases an original location estimator subject to natural biases (discussed in Section 5.2). This scaling effect can be found when deriving a location estimator as a function of naturally biased range estimators $\{\hat{d}_i^{(\mathrm{ML})}\}_{i=1}^m$ in Eq. (5.5) and attack coefficients $\{\mathcal{C}_i\}_{i=1}^m$ in Eq. (5.17). As given in Eq. (5.25), the location estimator can be derived as

$$\hat{\boldsymbol{\theta}}_R = \arg\min_{\boldsymbol{\theta}} \left\{ 50 n_p^2 \sum_{i=1}^{m} \left[\log_{10} \left(\frac{\hat{d}_i^{(\mathrm{ML})} / \mathcal{C}_i}{d_i(\boldsymbol{\theta})} \right) \right]^2 \right\}. \tag{5.29}$$

where an RSS location estimator $\hat{\boldsymbol{\theta}}_R$ is a function of the naturally biased range estimator $\hat{d}_{\mathrm{ML},i}$ which is then additionally scaled by a location attack characterized by $\mathcal{C}_i$. In other words, *a location attack can be considered as a scaling factor for an RSS estimator whose bias-variance characteristics are modified by the attack*. Consequently, as can be observed from Fig. 4.5, some range of attack levels may improve the estimator performance by rescaling its range estimators–which is definitely against the purpose of the adversaries. This tradeoff can be understood better by relating it to Fig. 5.5b, where the characteristics of estimator bias and its variance on the curve can be modified by any source of error including an attack. An increase in the estimator bias due to an attack (note the typical range of small bias values) reduces the variance considerably, and thus improves the overall RMSE performance.

We now quantify the effects of the attack coefficient $\mathcal{C}_i$ in Eq. (5.17) and the attack-induced bias $(\mathcal{S}_i - 1)d_i$ in Eq. (5.19) with respect to the MMSE in Fig. 4.5. Note that it is difficult to derive an analytic solution for finding the best scaling value or attack level leading to

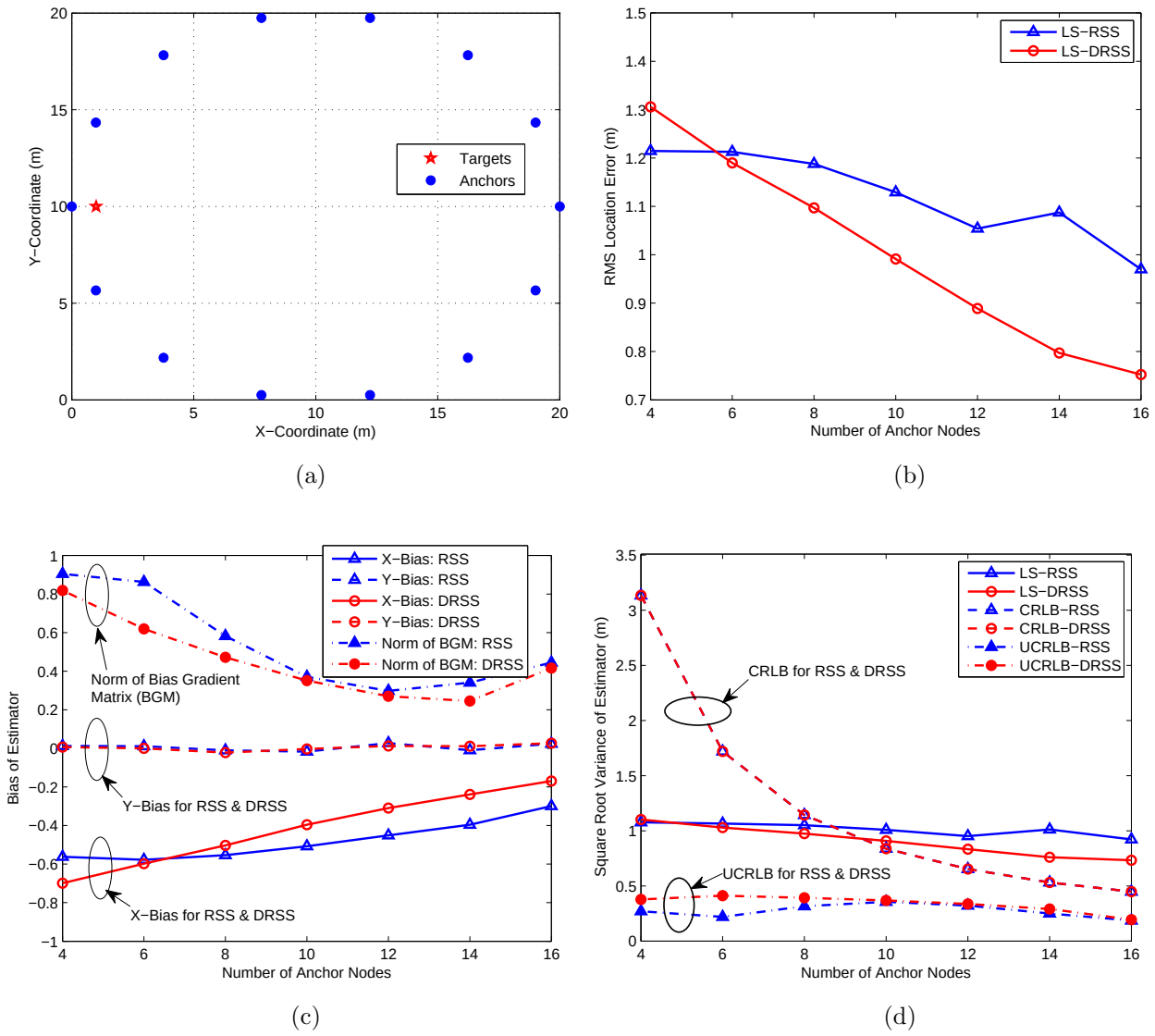


Figure 5.7: Analysis of the theoretical limits to location accuracy and the bias-variance tradeoff ($D_c = 20\ m$). LS estimators based on RSS and DRSS are employed to compare their bias-variance characteristics. (a) Network configuration considered. (a) Corresponding RMS location error. (b) Associated bias of the estimators. (c) Associated square root variance of the estimators as well as $\sqrt{\text{CRLB}}$ and $\sqrt{\text{UCRLB}}$.

the MMSE, unless nonlinear complexities in Eq. (5.29) are simplified. Nevertheless, we can estimate the best scaling value numerically. As an example, in our specific simulation settings with a range of SS attack levels $\in [-30, 30]$ dB ($n_p = 4$, $\sigma_S \in [2, 8]$ dB), $\mathcal{B}$ ranges approximately from 1.007 to 1.112 (bias: +0.7 ~ +11.2 %). On the other hand, $\mathcal{C}_i$ varies from 0.178 to 5.623, leading to the attack-induced range bias of approximately −82 ~ +462 %. The total range bias due to a combination of the natural and unnatural biases is thus −82 ~ +525 % depending on the shadow fading variance. In Fig. 4.5, the MMSE of Joint-PL was achieved when the SS attack level was between −20 and −10 dB (*i.e.*, $\sum_{k=1}^{3} \Delta\psi_{i,k}$ of 10 ~ 20 dB), thus leading to the attack-induced bias of approximately −68 ~ −44 %. As a result, the total range bias is approximately −68 ~ −38 %, depending on the shadow fading variance. This result is consistent with our previous discussion that some degree of negative bias improves the performance of a range-based RSS location estimator whose bias is inherently positive.

5.6 Conclusion

In this chapter we characterized location spoofing attacks and analyzed the behavior of a location estimator under attack. More specifically, the chapter first provided a characterization of the impact of signal strength and beamforming attacks on range estimates and the resulting position estimate. It was shown that such attacks are either uniform or selective in terms of their impact on the individual range estimates. Further, we showed that these attacks add either a positive or negative bias to the range estimate depending on the type of attack. This categorization allowed us to identify the more severe types of attacks, and will lead us to an attack detection and localization approach which does not rely on *a priori* knowledge (either statistical or environmental) later in this dissertation. In the previous chapter, it was shown that positive-bias attacks are much more detrimental than negative-bias attacks. The reason for this different estimator behavior was examined here through the issues with nuisance parameters and heavy-tailed errors.

This chapter also explored the error behavior of a location estimator from fundamental estimation aspects–namely, prior knowledge of the nuisance parameters, heavy-tail issues and the bias-variance tradeoff. Through this analysis, we have explained our observations and simulation results in detail regarding the effects of both signal strength and beamforming attacks given in the previous chapter. From this investigation we have reached three key conclusions. First, it is often a better strategy to optimize nuisance parameters jointly with position parameters of interest, even if prior knowledge of the nuisance parameters is available. Second, the impact of the heavy-tailed error behavior on the estimator performance is significant. Therefore, we should deal with such an abnormal error particularly for location security. Lastly, a location attack can be regarded as a scaling factor for an RSS-based location estimator whose bias-variance behavior or tradeoff is modified by the attack. Due to the bias-variance tradeoff, counter-intuitively, an attack could *improve* the accuracy of a location estimator.

Chapter 6

Detection of Location Attacks

6.1 Introduction

In any type of security system, the primary objective is to identify security risks and detect malicious activities. With our understanding of location attacks and their impact described in the previous chapters we now investigate the detection of location spoofing attacks, specifically the detection of a wireless node which is attempting to falsify (degrade) its position estimate through signal strength (SS) and beamforming (BF) attacks. In classical detection problems in signal processing, it is important to fully exploit our knowledge of signal information and observed data. In location security, however, it is typically not valid to make deterministic or statistical assumptions about the data subject to attacks whose (statistical) characteristics are inherently unknown and unpredictable. Further, a lack of knowledge of the statistical properties of the radio environment (*e.g.*, spatial correlation and the variance of shadow fading) further complicates the problem.

Despite increasing research activity in relation to location security, few studies are dedicated to the detection of location spoofing attacks. Chen et al. [45, 106] propose a statistical approach using an LLS estimator with its residual errors as a test statistic. This detection scheme (as well as other similar approaches) is possible given that the statistical properties of the residual error with the LLS estimator when operating in attack-free conditions are known *a priori*. In order to obtain this *a priori* information, it is vital to construct a reliable radio map or RSS database (usually built offline) prior to localization [15]. However, this approach demands considerable effort and cost (due to offline measurements, manual calibration, *etc.*) as it needs to reflect the time-varying nature of the wireless channel. As we will discuss later in this chapter, the residual error alone is only weakly correlated with location attacks and makes an unreliable test statistic for attack detection. Further, few of these recent studies deal with antenna beamforming attacks, which is one of the more easily envisioned location attack strategies.

Due to the difficulties in detecting location attacks using signal measurements without resorting to prior environmental or statistical knowledge, one may consider a system-level (or algorithmic) approach based on system or cryptographic protocols. Recently, there has been an increasing interest in the secure location discovery of sensors in relatively large-scale networks, typically assuming a communications link between all sensors, including to any adversaries. The security of a node's location information is verified by challenging (unlocalized) nodes through network protocols or algorithmic solutions (*e.g.*, distance bounding [47–49], voting-based schemes [50, 51]) or by employing additional hardware (*e.g.*, sector antennas). The success of this approach will depend on system/hardware requirements, assumptions and/or application scenarios. Among the requirements are a directional antenna in each node (or anchor), sufficient radio resources, the absence of jamming/interference, a majority of benign observations and common control channels.

A strong aspect of the work described in this chapter is that the problem of location attack detection is addressed based solely on signal strength or SS observations which can readily be acquired in (nearly) every wireless system. Since there is no reliance on prior statistical information, predefined system protocols, additional hardware or offline training, our approach is not limited to a specific set of applications or scenarios. This SS-based framework can also be integrated into another type of location system (*e.g.*, TOA) as a hybrid approach. Despite our focus on network-based attack detection using SS measurements, this study can be readily extended to mobile-based positioning with malicious anchors, jammers or rogue APs. The work can also be applied to systems using other measurement types if desired.

The main contributions of this chapter are as follows:

1. A framework for assessing the quality of a mobile's location estimate in the presence of an attack;
2. Development of the novel concept of bilateral dissimilarity detection (BDD) to detect the presence of a location attack regardless of the channel state;
3. Development of statistical and pattern matching techniques for BDD using point and topological error signatures, respectively;
4. Showing that the performance of attack detection is significantly impacted by the geometry of nodes and can be improved by reducing the adverse geometric effect.

The chapter is organized as follows. In Section 6.2 we describe the challenges of measuring anomalous location estimates. With this understanding we introduce the bilateral similarity of two SS-based estimators (*i.e.*, using RSS and DRSS observations) in the absence of an attack which can be used as a metric of the security risk of a mobile's position estimate. Then, it is shown that the two estimators exhibit the dissimilar behavior in the presence of an attack termed the bilateral dissimilarity. By exploiting this two-sided behavior we develop two detection techniques for BDD using point and topological error signatures in Sections

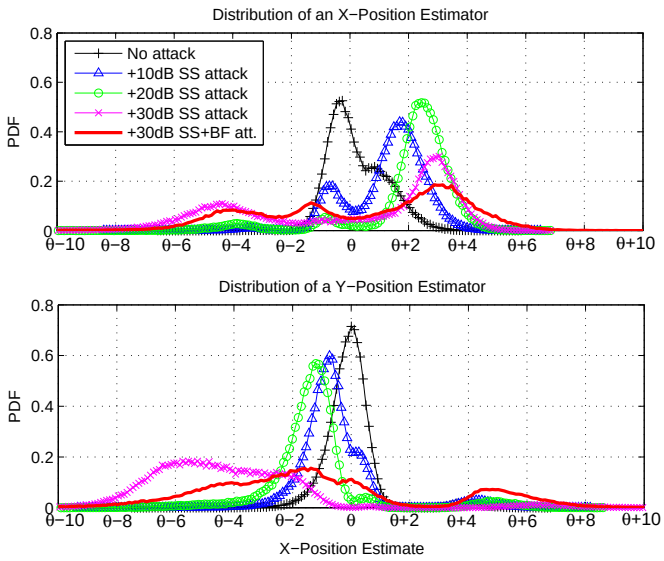


Figure 6.1: The distributions of RSS location estimates along each coordinate axis in the absence or presence of an attack with the scenario in Fig. 6.3.

6.3 and 6.5, respectively. In Section 6.4 we discuss the adverse impact of node geometry on detection performance and how to improve the geometric adversity. Then, in Section **??**, the performance results of the approach are presented. Finally, we conclude the chapater in Section 6.7.

6.2 Measuring Location Anomalies

In Chapter 4 we found that the falsification of position-related parameters $\mathbf{\Psi}_i$ in Eq. (4.1) induces an abnormal bias in the range estimate, resulting in anomalous location error. This error is much larger than what we typically would expect in the absence of an attack as shown in Figs. 4.5 and 4.6. The effect that the induced range bias has on the position estimate can be better understood by examining the distribution of the estimated position $\hat{\boldsymbol{\theta}}$ for a specific scenario. The simulated distributions of the x- and y-positions for different attack cases are plotted in Fig. 6.1 given the scenario in Fig. 6.3. We can see that in the absence of an attack, the estimated values $\hat{x}$ and $\hat{y}$ are near their true values. Although we cannot say that the location estimator is strictly unbiased in the absence of an attack, in general the estimated location is near the true location. The impact of location attacks is to substantially deviate $\hat{\boldsymbol{\theta}}$ from its true value $\boldsymbol{\theta}$. Thus, *if* a location estimate anomaly (*i.e.*, large location error) could be measured, the presence of an attack could be detected and, further, more effective attacks would be easier to detect.

A location *anomaly* can be characterized by a scalar function termed the *absolute anomaly*

measure $\mathcal{M}_A$ (≥ 0) as

$$\mathcal{M}_A(\hat{\boldsymbol{\theta}}) \triangleq d(\hat{\boldsymbol{\theta}}, \boldsymbol{\theta}) \tag{6.1}$$

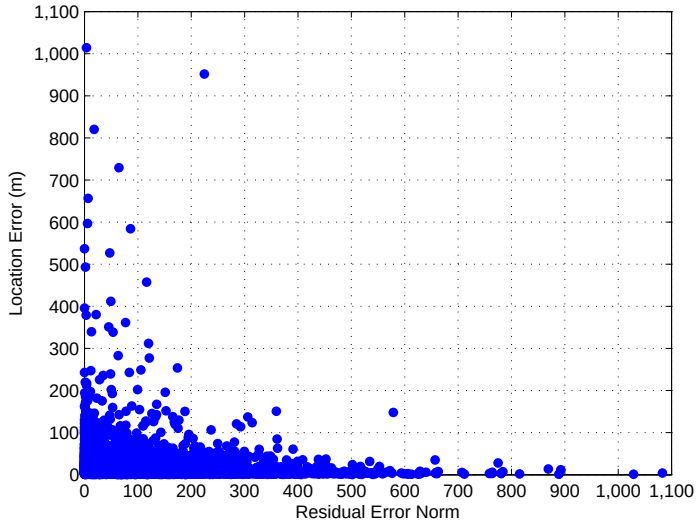
where

$$d(\boldsymbol{u}, \boldsymbol{v}) = \|\boldsymbol{u} - \boldsymbol{v}\|_p = \left(\sum_{k}^{dim(\boldsymbol{u})} |u_k - v_k|^p \right)^{\frac{1}{p}}. \tag{6.2}$$

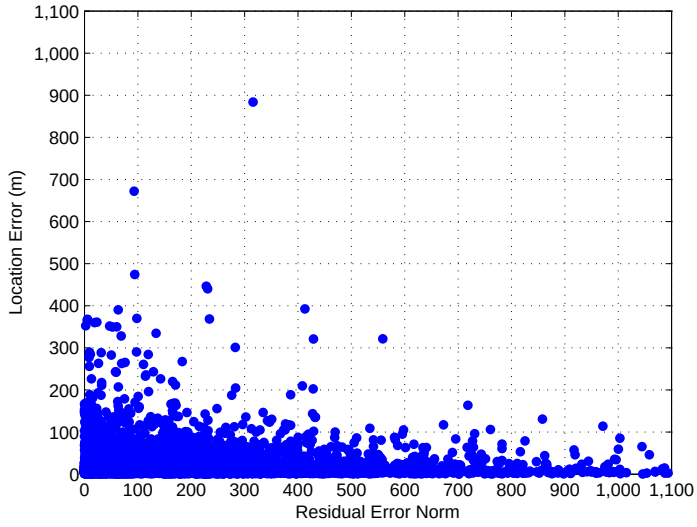
The p-norm $\|\cdot\|_p$ is used as a measure of distance on the finite-dimensional vector space [75]. The value of $p \in [1, \infty)$ is chosen based on the desired degree of similarity or closeness between the estimates. With larger p values, the measure $\mathcal{M}_A$ is less sensitive to estimator variances. When $p = 2$, $\mathcal{M}_A$ measures location error. Although such a measure is intuitive and should be effective for detecting location attacks, since it depends on the unknown true position $\boldsymbol{\theta}$ (as do the distributions in Fig. 6.1), it is not a practical measure.

A practical, and intuitive, measure which could be used for anomaly detection is the LS residual error or $\|\boldsymbol{v} - \boldsymbol{L}(\theta)\|_2^2$ which is an observable measure. Unfortunately, as discussed in Chapter 5, the residuals $\boldsymbol{r}$ or their norm alone cannot be used as a reliable measure for attack detection in most practical localization scenarios, even though the range or location estimator is accurate and robust to natural sources of error (*i.e.*, $var\left[d_i(\boldsymbol{\theta})\right]$ is small and $\hat{d}_i^{(\mathrm{ML})} \mathrm{E}\left[d_i^{-1}(\boldsymbol{\theta})\right] \approx 1$ in Eq. (5.23). This is mainly because the impact of an attack on the residual which increases location error is negated by the factor $\hat{d}_i^{(\mathrm{ML})} d_i^{-1}(\hat{\boldsymbol{\theta}})$ so that the residual is not correlated with location error. The weak correlation when an RSS-based estimator is under attack can be verified through a scatter plot given in Fig. 6.2 which reveals relationships between two variables–that is, the residual error norm and the location error, treated as predictor and response variables, respectively.

Also, many well-known statistical or machine learning techniques used for detecting a *data anomaly* [118] are generally not effective to assess/detect a location anomaly, especially in a stationary scenario. For example, suppose that based on $\mathcal{T}$ sets of m anchors' RSS data $\{\boldsymbol{P}(t) : \boldsymbol{P} = (P_1, P_2, \ldots, P_m)\}_{t=1}^{\mathcal{T}}$ measured over time t, a location estimator outputs $\mathcal{T}$ location estimates $\{\hat{\boldsymbol{\theta}}(t) : \hat{\boldsymbol{\theta}} = [\hat{x}, \hat{y}]^T\}_{t=1}^{\mathcal{T}}$. If the signal source or node is stationary, there is little variation in the measurements over the static channel. Thus, with only one meaningful estimate we cannot assess whether or not it is an anomaly. Even if we have a mobile target, if its time-series location estimates exhibit sufficient variability, a majority of the estimates could be severely corrupted in a systematic manner. Consequently, good estimates can be flagged as anomalous, hence making them difficult to distinguish. Thus, we wish to find a measure which is not subject to these limitations.



(a)



(b)

Figure 6.2: Scatter plots which reveal a weak or no correlation between the *residual error norm* and the location error in the presence of attacks (σ_S = 5 dB, n_p = 4). (a) +30 dB SS attack. (b) +30 dB SS+BF attack.

6.2.1 Bilateral Similarity of Point Estimates

The study of the behavior of a location estimator is closely related to the topological features of its objective function or error surface $\phi(\boldsymbol{\theta})$. Among the most salient features of the error surface are its critical points at which the magnitude of a gradient vector $\nabla\phi(\boldsymbol{\theta})$ or flow vanishes. The goal of a location estimator is to find the global minimizer $\hat{\boldsymbol{\theta}}$ among the critical points. A classic approach to finding the solution is LS estimation. As explained in Chapter 3, an LS solution $\hat{\boldsymbol{\theta}}$ can be obtained by using a system of nonlinear path loss equations which constructs a smooth scalar field

$$\phi(\boldsymbol{\theta}) = \frac{1}{2}\|\boldsymbol{r}(\boldsymbol{\theta})\|_2^2, \tag{6.3}$$

where the residuals $\boldsymbol{r}(\boldsymbol{\theta}) = \boldsymbol{v} - \boldsymbol{L}(\boldsymbol{\theta})$. Its gradient vector field (which implies the direction to the solution) is the first derivative of ϕ with respect to $\boldsymbol{\theta}$ written as

$$\nabla\phi(\boldsymbol{\theta}) = -\boldsymbol{J}(\boldsymbol{\theta})^T\boldsymbol{r}(\boldsymbol{\theta}), \tag{6.4}$$

where the ith row vector ($i = 1, \ldots, m$) of $\boldsymbol{J}$ for the RSS-based location estimator (RLE) or $\hat{\boldsymbol{\theta}}_R$ is

$$\boldsymbol{J}_i^{(R)} = -\frac{10n_p}{\ln 10}\left[\frac{u_{i,x}}{d_i},\ \frac{u_{i,y}}{d_i}, -\frac{\ln d_i}{n_p}\right], \tag{6.5}$$

$$u_{i,x} = \frac{x_i - x}{d_i} \quad \text{and} \quad u_{i,y} = \frac{y_i - y}{d_i}. \tag{6.6}$$

For the DRSS-based location estimator (DLE) or $\hat{\boldsymbol{\theta}}_D$, the ijth row vector ($i, j \in \{1, \ldots, m\}, i < j$) of $\boldsymbol{J}$ is given by

$$\boldsymbol{J}_{ij}^{(D)} = -\frac{10n_p}{\ln 10}\left[z_{ij,x}, z_{ij,y}, -\frac{1}{n_p}\ln\left(\frac{d_j}{d_i}\right)\right], \tag{6.7}$$

$$z_{ij,x} = \frac{u_{j,x}}{d_j} - \frac{u_{i,x}}{d_i} \text{ and } z_{ij,y} = \frac{u_{j,y}}{d_j} - \frac{u_{i,y}}{d_i}. \tag{6.8}$$

Geometrically, $u_{i,x}$ and $u_{i,y}$ are x- and y-elements of the unit vector $\boldsymbol{u}_i = u_{i,x}\boldsymbol{e}_x + u_{i,y}\boldsymbol{e}_y$, where $\mathbf{e}_x$ and $\mathbf{e}_y$ are the basis vectors in the direction of x- and y-axes, respectively. $\boldsymbol{u}_i$ represents a geometric vector from the source to each anchor node. $z_{ij,x}$ and $z_{ij,y}$ are x- and y-elements of the *difference* vector $\boldsymbol{z}_{ij} = z_{ij,x}\boldsymbol{e}_x + z_{ij,y}\boldsymbol{e}_y$.

Both of the estimators ($\hat{\boldsymbol{\theta}}_R$ and $\hat{\boldsymbol{\theta}}_D$) use the same SS measurements and are constructed based on the same framework. In nominal conditions, as demonstrated in Fig. 6.3 (top) for a typical example, location estimates based on RSS and DRSS are geographically close. Accordingly, the error statistics of the estimates (μ_Λ and σ_Λ denote the mean and standard deviation of location error Λ, respectively) are similar. However, when there is an attack the two estimators behave substantially different as shown in Fig. 6.3 (bottom) where we have added a SS attack added to the same example. The bilateral similarity of the two location estimators, $\hat{\boldsymbol{\theta}}_R$ and $\hat{\boldsymbol{\theta}}_D$, can thus be exploited for attack detection as we will show.

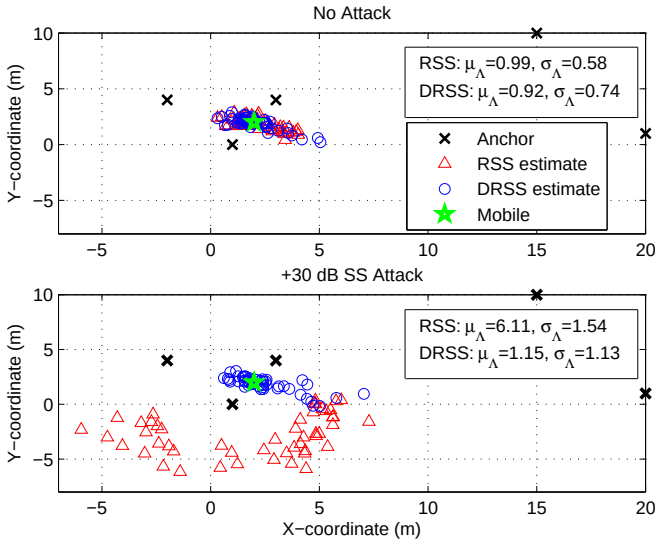


Figure 6.3: Instances of RSS and DRSS location estimates (i) in the absence of an attack (top) and (ii) in the presence of a +30 dB SS attack (bottom).

6.2.2 Bilateral Similarity of Topological Features

Although the emphasis of location estimation is placed on the *point estimate* $\hat{\boldsymbol{\theta}}$–that is the minimizer of the error functional $\phi(\boldsymbol{\theta})$, the *entire* error surface carries information about the *true* position $\boldsymbol{\theta}$ and the associated error. Thus, other topological features such as level sets will also give useful information about the presence of an attack. Note that the observed scalar field ϕ is an *objective* quantity. It is objective in the sense that the model function $\boldsymbol{L}(\boldsymbol{\theta})$ is empirical, and no subjective modifications such as linearization/approximations–which involve a subjective decision on the reference point $\boldsymbol{\theta}_0$–are made.

In particular, our attention is focused on a special region, termed the *node convex hull* (or *node convex polytope* in $\mathbb{R}^n$), on the residual error map produced by taking the logarithm of ϕ. The node convex hull is defined as the smallest convex set $\mathcal{H}_C(\mathcal{X})$ that geometrically contains a set $\mathcal{X}$ of hearable anchors $\mathcal{X} = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\}$ as shown in Fig. 6.4 (top). $\mathcal{H}_C(\mathcal{X})$ can be found using any of many efficient algorithms for convex hull formation which do not require the computation of angles among nodes (which can be numerically erroneous) (*e.g.*, *Graham's scan* with time complexity $\mathrm{O}(m \log m)$ [119]). We examine this specific region since the RSS/DRSS residual error maps behave differently outside the polygon $\mathcal{H}_C(\mathcal{X})$ even in the absence of an attack, whereas their inner region exhibits very similar topography in the absence of an attack and dissimilar topography when under attack, as seen in Fig. 6.4 (top row). The geometric (dis)similarity can be explained theoretically through the geometric dilution of precision (GDOP) (despite different scaling factors) which is a measure of the geometric effect on location error [67]. In Fig. 6.4 (bottom row), using Eqs. (6.3)–(6.8) we plot the inverse of GDOP for RLE and DLE, assuming four anchors (denoted by "×"), each

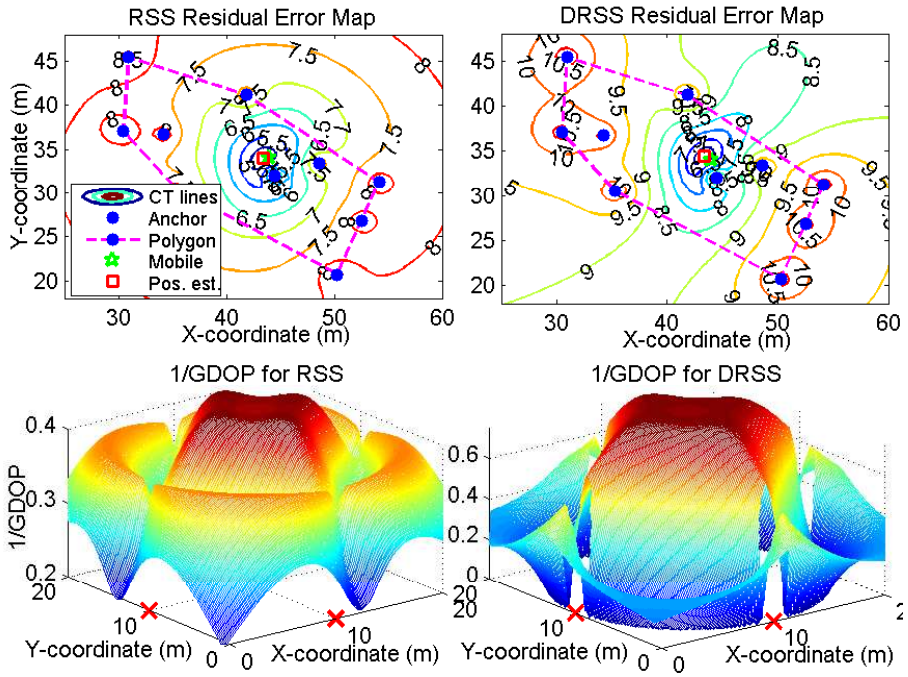


Figure 6.4: The LS residual error map (top row) and the surface of GDOP^{-1} (bottom row) with RSS (left column) and DRSS (right column).

located at the middle of each side of a $20m$-by-$20m$ square area. Due to space constraints, the derivation is omitted here, but can be done in a similar manner as in [67]. This bilateral similarity will also be exploited for attack detection in the next section.

6.2.3 Attack Detection using Bilateral Dissimilarity

As stated previously, it is infeasible to assess whether or not an estimate is a statistical anomaly (due to an attack) using absolute error as a measure since the true location is unknown. Thus, we turn our attention to assessing the anomalous behavior by exploiting the bilateral similarity of two estimators to examine their *relative* error. This approach is referred to as bilateral dissimilarity detection or BDD. As detailed later, the BDD employs two relative anomaly measures $\hat{\mathcal{M}}_A$–using point and topological error signatures, respectively–using two SS-based estimators. As shown in Eqs. (6.3)–(6.8), the estimators take the same SS observations, but process them differently. As a result, in nominal conditions, the two estimates $\hat{\boldsymbol{\theta}}_R$, $\hat{\boldsymbol{\theta}}_D$ are close, and the two scalar fields ϕ_R, ϕ_D in the domain of the node convex hull $\mathcal{H}_C(\mathcal{X})$ are topographically similar. The latter means that the two level curves (or surfaces) or equivalently

$$\mathcal{H}_C(\phi) \triangleq \{\boldsymbol{x} \preccurlyeq \mathcal{H}_C(\mathcal{X}) : \phi(\boldsymbol{x}) = \alpha, \ \forall \alpha \in \mathbb{R}\} \tag{6.9}$$

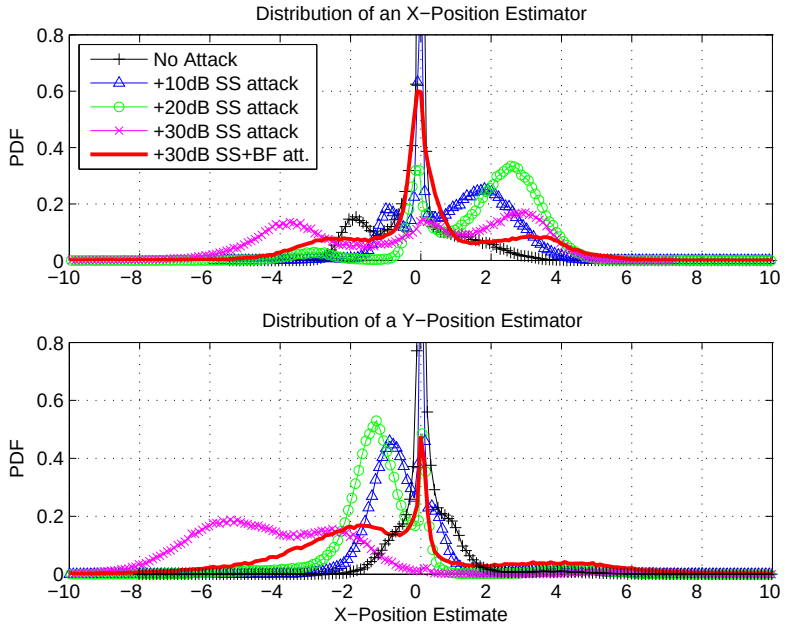


Figure 6.5: The distributions of $\hat{\boldsymbol{\theta}}_R - \hat{\boldsymbol{\theta}}_D$ along each coordinate axis in the absence or presence of SS and BF attacks with the scenario in Fig. 6.3.

are similar, where $\preccurlyeq$ denotes geometrically-inside and α is a constant value. Inherently, location attacks disturb this bilateral similarity. The higher the intensity of an attack, the more likely the degree of bilateral dissimilarity increases. Thus, more effective attacks are more likely to be detected. We next present techniques for detecting SS and BF attacks by using specific bilateral dissimilarity measures.

6.3 Statistical Detection Using Point Error Signatures

The relative error detector (RED) for BDD is a statistical detector using the norm of the relative error as an anomaly measure. The relative error norm $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}}) \in [0, \infty)$ which estimates $\mathcal{M}_A$ in Eq. (6.1) is defined as

$$\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}}) \triangleq d(\hat{\boldsymbol{\theta}}_R, \hat{\boldsymbol{\theta}}_D) = \|\hat{\boldsymbol{\theta}}_R - \hat{\boldsymbol{\theta}}_D\|_p, \tag{6.10}$$

where $p = 2$ here, corresponding to the Euclidean distance between the two position vectors $\hat{\boldsymbol{\theta}}_R$, $\hat{\boldsymbol{\theta}}_D$. In Fig. 6.5, the simulated distributions of $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})$ in the absence or presence of attacks are shown for the same simulation scenario as given in the previous results. Notice the similarity between the general behavior of $\mathcal{M}_A$ and its estimate $\hat{\mathcal{M}}_A$ by comparing Figs. 6.1 and 6.5. Further, in these figures we can observe two important characteristics of $\hat{\mathcal{M}}_A$.

First, true position $\boldsymbol{\theta}$ is not required, making the measure practical. Second, the attack-free distribution is highly concentrated near zero which aids in attack detection.

The relative error norm in Eq. (6.10), which is used as a test statistic by RED, is strongly correlated with location error in the presence of an attack. The high correlation is shown in Figs. 6.6a (+30 dB SS attack) and 6.6b (+30 dB SS+BF attack), where the relative error norm (observable) and the location error (non-observable) are the predictor and response variables, respectively. In comparison to Fig. 6.2, the two variables have a very high linear relationship which increases with larger location error as the slope of the regression line (*i.e.*, correlation coefficient) is nearly unity. This result is promising since in location attack detection, of primary interest is detecting attacks leading to large location error. Note that position falsification attempts with larger attack strength do not always lead to larger location error due to various environmental and system effects. As an example, positive-bias (or negative-bias) SS attacks can be negated by constructive (or destructive) interference or shadow fading. We will show the correlation between actual detection performance and location error in Section 6.6.

Consider that the location error is caused either by a random vector $\boldsymbol{\zeta}$ due solely to nominal radio conditions/noise (*i.e.*, no attack) or by a combination of $\boldsymbol{\zeta}$ and attack-induced factors $\boldsymbol{\eta}$ (*i.e.*, the estimator is under attack). By denoting $\boldsymbol{e}_R = \hat{\boldsymbol{\theta}}_R - \boldsymbol{\theta}$ and $\boldsymbol{e}_D = \hat{\boldsymbol{\theta}}_D - \boldsymbol{\theta}$, we define the relative error $\Delta\boldsymbol{e} = [\delta e_x, \delta e_y]^T$ in the absence of an attack as $\Delta\boldsymbol{e}(\hat{\boldsymbol{\theta}}_R, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta}) = \boldsymbol{e}_R(\boldsymbol{\theta}, \hat{\boldsymbol{\theta}}_R; \boldsymbol{\zeta}) - \boldsymbol{e}_D(\boldsymbol{\theta}, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta})$, whereas $\Delta\boldsymbol{e}$ when under attack is $\Delta\boldsymbol{e}(\hat{\boldsymbol{\theta}}_R, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta}+\boldsymbol{\eta}) = \boldsymbol{e}_R(\boldsymbol{\theta}, \hat{\boldsymbol{\theta}}_R; \boldsymbol{\zeta}+\boldsymbol{\eta}) - \boldsymbol{e}_D(\boldsymbol{\theta}, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta}+\boldsymbol{\eta})$. Then, using Eq. (6.10) we form a hypothesis testing problem, where the null hypothesis $\mathscr{H}_0$ is defined as

$$\mathscr{H}_0 \text{ (no attack)} : \hat{\mathcal{M}}_A = \|\Delta\boldsymbol{e}(\hat{\boldsymbol{\theta}}_R, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta})\|_2, \tag{6.11}$$

whereas the alternative hypothesis $\mathscr{H}_1$ is defined as

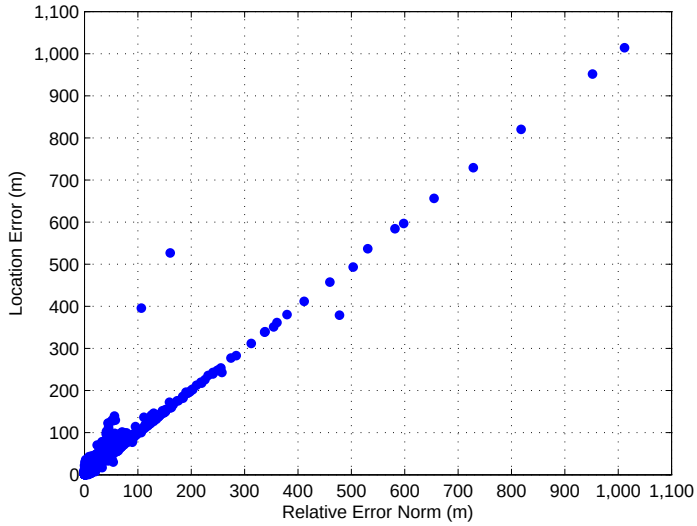
$$\mathscr{H}_1 \text{ (under attack)} : \hat{\mathcal{M}}_A = \|\Delta\boldsymbol{e}(\hat{\boldsymbol{\theta}}_R, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta} + \boldsymbol{\eta})\|_2. \tag{6.12}$$

In detection theory, the detection performance depends on the discrimination between the two hypotheses through a test statistic and the threshold of the detector [120]. In this work, the test statistic $\mathfrak{T}$ is defined as an average of the scaled relative error norms $\{\hat{\mathcal{M}}_{A_t}\}_{t=1}^{\mathcal{T}}$ over the observation period $\mathcal{T}$. Then, our decision on the occurrence of a location anomaly or attack is based on a binary hypothesis test with a decision threshold γ as

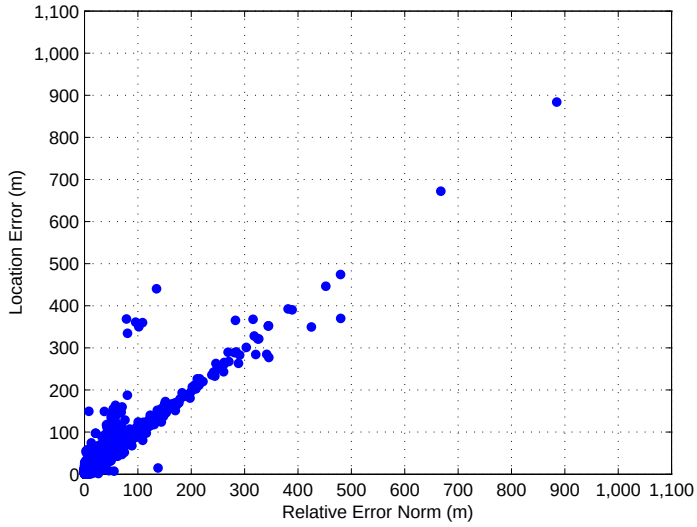
$$\mathfrak{T}(\hat{\boldsymbol{\theta}}) = \frac{1}{\mathcal{T}} \sum_{t=1}^{\mathcal{T}} \frac{\hat{\mathcal{M}}_{A_t}}{\sigma_{R_t}} \underset{\mathscr{H}_0}{\overset{\mathscr{H}_1}{\gtrless}} \gamma, \tag{6.13}$$

where $\sigma_{R_t}^{-1}$ is a weighting factor regarding the reliability of the tth observation (set to 1 in this work). The threshold γ is chosen to satisfy the constraint of a false alarm rate P_{fa}.

As noticed in each hypothesis, the true position vector $\boldsymbol{\theta}$–which is the common *unknown* for RLE and DLE–is canceled out. That is, *the major uncertainty of the true position parameter*



(a)



(b)

Figure 6.6: Scatter plots which reveal a very high correlation between the *relative error norm* and the location error in the presence of attacks (σ_S = 5 dB, n_p = 4). (a) +30 dB SS attack. (b) +30 dB SS+BF attack. This result is notable especially by comparing it with Fig. 6.2

is eliminated from the detection problem. Thus, RED has practical advantages over other detection techniques which require prior (statistical) information or training samples as a benchmark. Further, as shown in Fig. 6.7 (which shows the simulated PDFs and CDFs of $\hat{\mathcal{M}}_A$ for various attacks), the PDF of $\hat{\mathcal{M}}_A$ has a sharp peak at $\hat{\mathcal{M}}_A = 0$ (always known *a priori*) in nominal conditions, thus highlighting the null hypothesis. When an attack is present, the peak disappears and, under more effective attacks, the position with the maximum PDF moves further away from $\hat{\mathcal{M}}_A = 0$. As a consequence, the two hypotheses become more separated. This implies that the value of $\hat{\mathcal{M}}_A$ increases with higher attack strength so that more effective attacks result in an increasing detection rate.

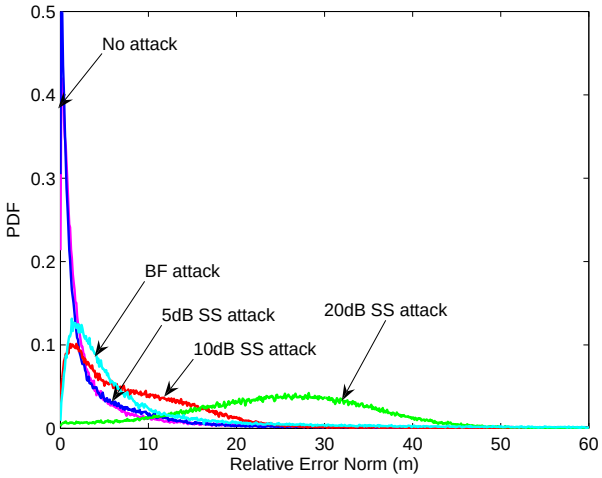
6.4 Improving the Heavy-Tailed Estimator Behavior

Conventionally, when dealing with errors, we commonly assume them to be Gaussian, hence leading to a nice analytic solution. Similarly, many studies in localization ignore location estimates with excessive error or simply assume that location error is Rayleigh (or Gaussian) distributed given the Gaussian distribution of error in each of the coordinates. However, due to various sources of error in practice, the error distribution tends to be non-Gaussian (as stated by Laplace's first law of error [121]) and heavy-tailed as validated by experimental data in [122]. Regarding the relative error or $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})$, assuming a random deployment of nodes we found that its measure $\hat{\mathcal{M}}_A$ in $\mathscr{H}_0$ (*i.e.*, no attack) follows the distribution of the 2-norm of a Laplacian random vector $\Delta\boldsymbol{e} = [\delta e_x, \delta e_y]^T \sim \mathscr{L}(0, \lambda_L)$ as shown in Fig. 6.7:

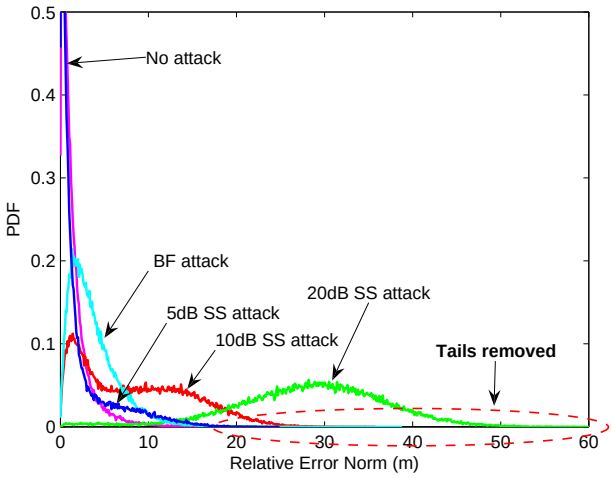
$$f(\delta e_k) = \frac{1}{2\lambda_L} \exp\left(\frac{-|\delta e_k|}{\lambda_L}\right), \; k = x, y : \lambda_L > 0, \tag{6.14}$$

with which the x- or y-error δe fluctuates symmetrically about zero mean along each coordinate axis. Note that location studies based on the Gaussian or Rayleigh assumption *overestimate* the "practical" estimator performance due to the fatter tail, but *underestimate* the "potential" estimator performance due to the sharper peak (if the heavy tail can be eliminated). For attack detection, the resulting heavy tail as seen in Fig. 6.7 will increase both Type I errors (*i.e.*, rejecting the null hypothesis $\mathscr{H}_0$ in the absence of an attack) and Type II errors (*i.e.*, accepting $\mathscr{H}_0$ in the presence of an attack). Thus, it is important to minimize this adverse yet natural effect which can severely bias a location estimator as a function of mobile position $\boldsymbol{\theta}$.

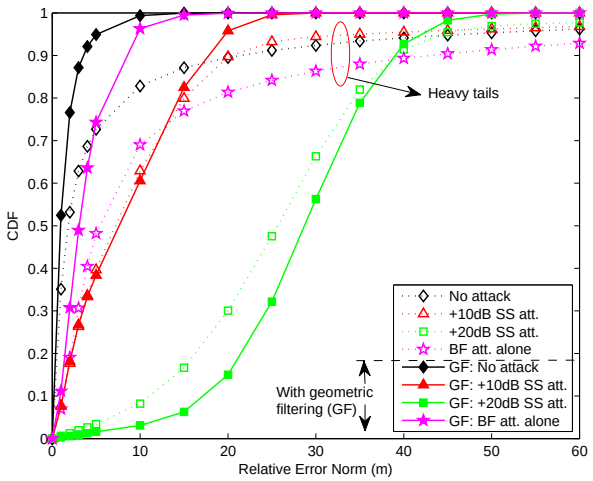
Due to a lack of knowledge of mobile position and error sources, in practice it is impossible to totally eliminate the adverse effect of node geometry. Thus, we now present a heuristic scheme termed geometric filtering (GF) which estimates the geometric impact on location estimates and improves it by using our knowledge of the node convex hull $\mathcal{H}_C(\mathcal{X})$. The method of GF (which is not required for the proposed detection techniques) is developed based on the principle of GDOP, where a smaller GDOP implies a lower impact of node geometry on performance. The geometric reliability of location estimates can be evaluated



(a)



(b)



(c)

Figure 6.7: Frequency distributions of the relative error norm $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})$ before/after geometric filtering (GF). (a) PDFs of $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})$ before GF. (b) PDFs of $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})$ after GF. (a) The corresponding CDFs of $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})$ before/after GF.

based on whether the estimates are geometrically contained by $\mathcal{H}_C(\mathcal{X})$ in which the GDOP is minimum and nearly constant as demonstrated in Fig. 6.4.

Further, the impact (mixed with the shadowing effect) can be reduced by iteratively selecting a subset $\mathcal{X}'$ of the set $\mathcal{X}$ of active anchors so as to produce a location estimate inside or, if impossible, closest to $\mathcal{H}_C(\mathcal{X}')$. Our simulation experiments reveal the feasibility and effectiveness of this iterative method. Alternatively, one may consider other ways of reconfiguring $\mathcal{H}_C(\mathcal{X})$. For example, the network can direct the device of interest to connect to another anchor or access point. The task can be done by a simple, legitimate[1] dissociation/association mechanism in wireless networks or via pilot/beacon power control which is also a common, legitimate mechanism in many types of wireless systems. Another possibility is the use of a mobile anchor [123] or nearby devices which keep their neighbors' RSS levels for ad-hoc modes. Note that in anchor reselection, only one additional anchor will suffice for reforming $\mathcal{H}_C(\mathcal{X})$. The performance improvement with GF is shown in Fig. 6.7 where the heavy tails are removed (notice the CDFs approach unity very quickly with GF in Fig. 6.7c), as well as in Fig. 6.9. This tells us that when the node estimate is inside the convex hull we can obtain much better detection performance. Thus, we can either flag estimates which are outside the convex hull for further examination, or force the node to increase power to hopefully increase the convex hull.

6.5 Detection Using Topological Error Signatures

The main advantage of RED is its simplicity while being effective against UA or SS attacks (as we will see). However, there are some cases where the measure $\hat{\mathcal{M}}_A$ based on *point estimates* provides insufficient discrimination capability. As an example, in Figs. 6.5 and 6.7, the distributions of $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})$ under BF attacks alone overlap substantially with attack-free and weak SS attack cases. Thus, to improve performance in the presence of BF attacks, we wish to compare $\mathcal{H}_C(\phi_R)$ and $\mathcal{H}_C(\phi_D)$ in Eq. (6.9) for BDD from a *global* viewpoint.

With a group of observed data, there are many ways to examine how two sets of variables are related or dissimilar. One of the simplest methods is correlation analysis which measures the association using a single value. However, the correlation coefficient only reveals the *linear* similarity between the two observed error functionals. $\phi(\boldsymbol{\theta})$ in Eq. (6.3) is inherently nonlinear and thus similarities cannot be captured properly through a linear coefficient. Further, the comparison/visualization of the residual error maps based on large data sets on a 2-D or 3-D grid will be computationally expensive. This cost increases rapidly with the network size or mobility.

In this work, we assess the dissimilarity between $\mathcal{H}_C(\phi_R)$ and $\mathcal{H}_C(\phi_D)$ for BDD using a pair of topological error signatures. The signature is termed the *topological "residual fingerprint"* $\mathcal{F}$ (REF) that represents the global structure of the vector field $\nabla\phi(\boldsymbol{\theta}) = [\phi_x, \phi_y, \phi_z]^T$ in relation

[1]This means that a suspect (potential attacker) does not sense that it is actually under surveillance.

to $\mathcal{H}_C(\phi)$ as shown in Fig. 6.8 (2-dimensional case). Specifically, the residual fingerprint $\mathcal{F}$ is a matrix that characterizes a (partially connected) graph or skeleton consisting of critical points and their connection lines, which are instantaneously tangent to $-\nabla\phi$, in the domain of $\mathcal{H}_C(\phi)$. Assuming a 3-dimensional localization problem, the tangent curves $\boldsymbol{s} = [s_x, s_y, s_z]^T$, which are known as *streamlines* in fluid mechanics [124], form column vectors of a $3 \times n$ matrix $\mathcal{F}$ (n depends on the number of the curves and their samples). With two residual fingerprints $\mathcal{F}_R$ and $\mathcal{F}_D$ for RLE and DLE, respectively, we define a relative anomaly measure $\hat{\mathcal{M}}_A[\mathcal{F}(\phi)]$

$$\hat{\mathcal{M}}_A[\mathcal{F}(\phi)] \triangleq d(\mathcal{F}_R, \mathcal{F}_D) = \|\mathcal{F}_R - \mathcal{F}_D\|_F, \tag{6.15}$$

where the Frobenius norm $\|\cdot\|_F$ is chosen as a measure of matrix distance [75]. Then, $\hat{\mathcal{M}}_A[\mathcal{F}(\phi)]$ is compared to a threshold for a decision as to whether or not a location estimate is anomalous. Alternatively, one may calculate a ratio of such columns $\mathcal{F}(:, i)$ to the total number of columns where $\|\mathcal{F}_R(:, i) - \mathcal{F}_D(:, i)\|_2 > r_S$, and r_S is some local similarity range, as illustrated in Fig. 6.8. The column vectors or tangent curves can be found from the equation $-\nabla\phi(\boldsymbol{\theta}) \times d\boldsymbol{s} = 0$ (with "$\times$" denoting the vector cross product), or equivalently

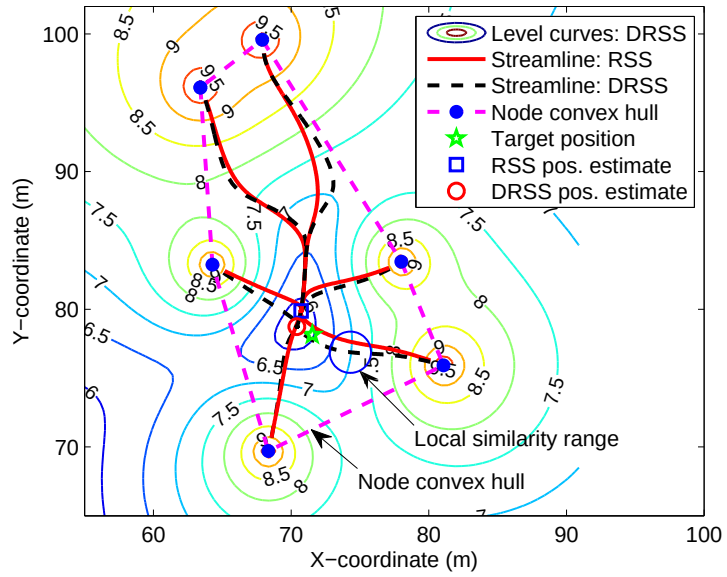
$$\frac{ds_x}{\phi_x} = \frac{ds_y}{\phi_y} = \frac{ds_z}{\phi_z}. \tag{6.16}$$

By definition, these curves never cross each other except at critical points, namely the originators (*i.e.*, anchors) and terminator (*i.e.*, minimizer), and only one of them can be defined at a specific point. Since Eq. (6.16) cannot be defined at the critical points, it is necessary to perturb the starting positions of the streamlines at the originators. As can be seen in Fig. 6.8, the RSS and DRSS topological error signatures $\mathcal{F}_R$ and $\mathcal{F}_D$ tend to be similar in the absence of an attack, but different in the presence of an attack.

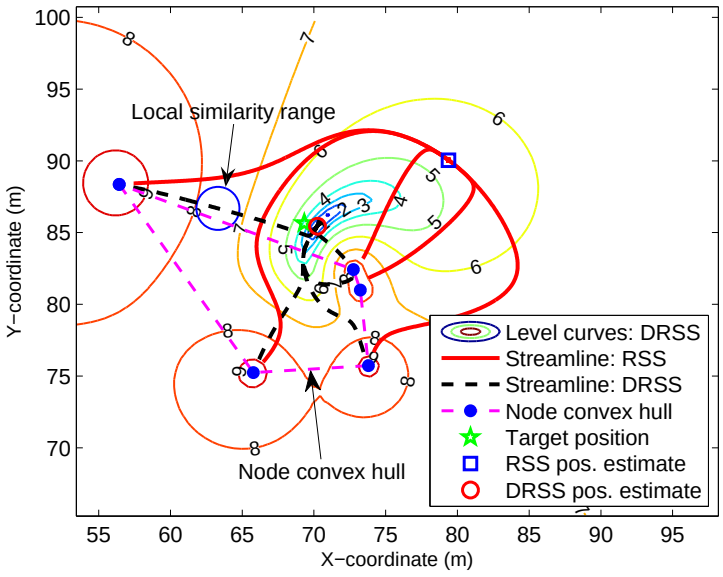
A similar topological concept has received a lot of attention, particularly in the area of flow pattern analysis and visualization [124]. One reason is its capability of reducing yet representing a large set of data in a manner that is both mathematically rigorous and perceptually tractable.

6.6 Performance Evaluation

In detection theory, a popular measure of detector's performance is the trade-off between P_d and P_{fa}, known as the receiver operating characteristic (ROC), as shown for RED and REF in Fig. 6.9. The results show the effectiveness of RED and REF which increases with more harmful attacks. Although lower strength attacks are more difficult to detect, they also have lower impact in terms of location spoofing (refer to Fig. 4.6). Indeed, the 5 dB SS attack level is similar to or smaller than the level of shadow fading assumed and thus it is expected to be difficult to detect while causing little additional location error.

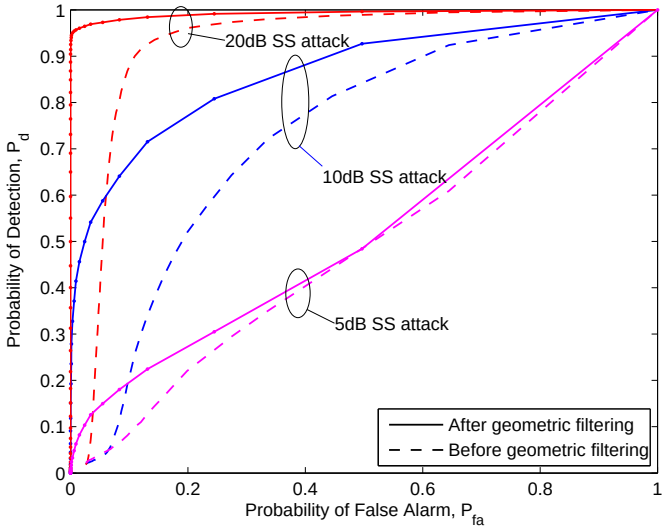


(a)

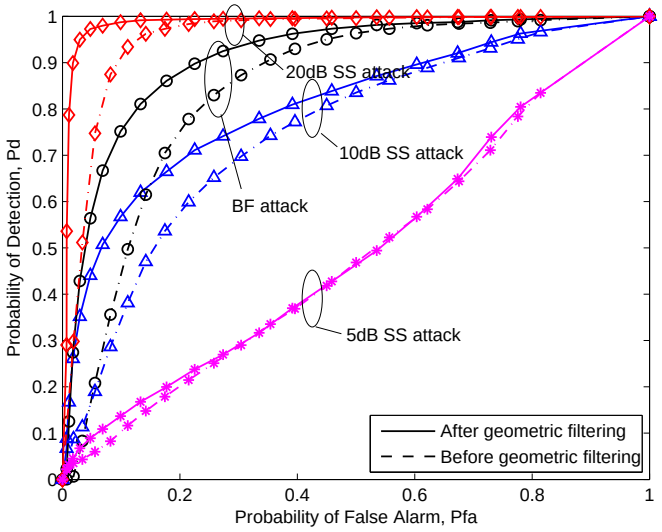


(b)

Figure 6.8: Visualization of comparing a pair of topological residual fingerprints $\mathcal{F}_R$ and $\mathcal{F}_D$. (a) No attack. (b) +10 dB SS attack.



(a)



(b)

Figure 6.9: A family of receiver operating characteristics (ROCs) for attack detection with (a) RED and (b) REF.

Examining Fig. 6.9a, the detection rate P_d of RED with GF for $P_{fa} = 0.2$ is about 0.28, 0.78 and 0.99 for positive-bias SS attack of 5 dB, 10 dB, and 20 dB, respectively. RED is not particularly effective against BF attacks, which require the more sophisticated REF approach. Regarding the detection performance of REF shown in Fig. 6.9b, we see that REF is similar to RED in terms of its effectiveness against SS attacks. However, unlike RED, it is also effective against BF attacks. Specifically, for $P_{fa} = 0.2$, P_d is found to be approximately 0.88 with GF. Additionally, as a design trade-off we can improve the detection rate of REF relative to RED (which is computationally simpler than REF) by adjusting (*e.g.*, reducing) the node convex hull.

We next present the results of another simulation experiment in Fig. 6.10 in order to show how the both detectors operate in real time against both SS and BF attacks. Figures 6.10a and 6.10c show the network scenario, where either an SS attacker or a BF attacker is attempting to spoof its own position while RSS- and DRSS-based estimators determine the position. Specifically, it is assumed that an attacker randomly moves through the network in the right direction with 5 m steps, from $X = 0$ to $X = 100$ (with a random Y-coordinate). The attacker, which is monitored by RED and REF simultaneously, begins to launch a +30 dB SS attack (top figures) or +30 dB SS+BF attack (bottom figures) when $X = 30$ and continues to attack the network up to the end point $X = 100$. Note that there is no attack from $X = 0$ to $X = 20$ in order to show how the detectors behave in normal conditions and perform differently during the presence of an attack. In Figs. 6.10b and 6.10d (right column), the detection performance and RSS location error associated with each attack scenario (left column) are shown. The detection performance is translated into the security risk $\mathcal{L}_S \in [0, 1]$ of localization defined as the normalized relative anomaly levels of $\hat{\mathcal{M}}_A$. Regarding $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})$ in Eq. (6.10) we use $\mathcal{L}_S = 1 - \exp\left[-k\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})\right]$ where $k \in [0, \infty)$ is set to 0.08 here, whereas for $\hat{\mathcal{M}}_A[\mathcal{F}(\phi)]$ in Eq. (6.15), $\mathcal{L}_S$ is a ratio of such columns $\mathcal{F}(:, i)$ to the total number of columns where $\|\mathcal{F}_R(:, i) - \mathcal{F}_D(:, i)\|_2 > r_S$.

A combination of the two detectors can be employed to monitor the security of a location system from different perspectives as follows. As can be seen in Figs. 6.10b (+30 dB SS attack) and 6.10d (+30 dB SS+BF attack) , the RED which monitors *point* error signatures only reacts against effective attacks (*i.e.*, inducing large location error) while being insensitive to ineffective attacks (*i.e.*, at $X = 70, 90, 100$ for SS attacks and $X = 30, 80, 90$ for SS+BF attacks). Thus, we can determine the quality of location estimates among which those of good quality can still be used even under attack. On the other hand, the REF which monitors *global* or topological error signatures is alert to any attacker's malicious attempts regardless of their impact. Thus, we can handle the misbehavior of an attacker or unreliable node accordingly.

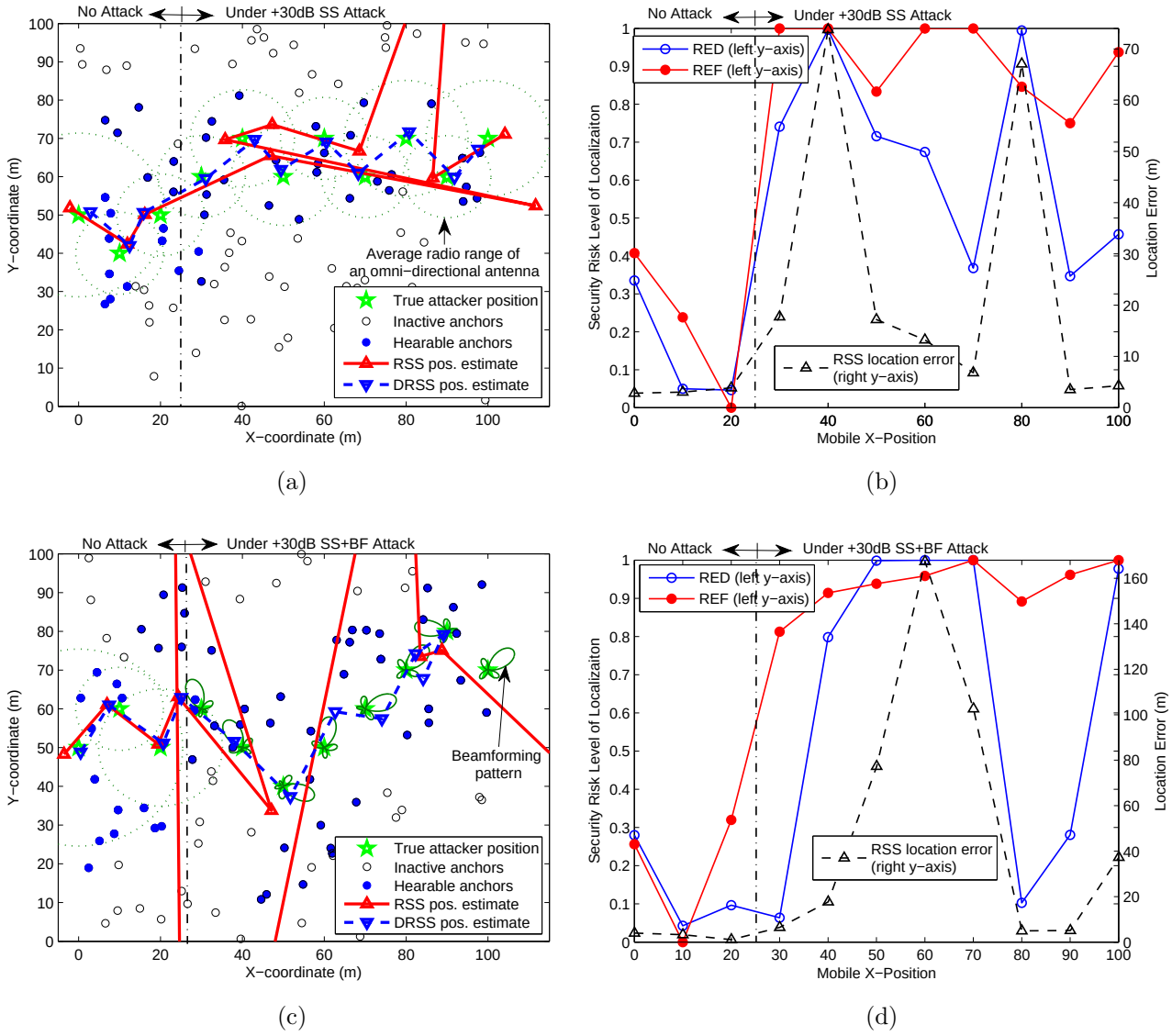


Figure 6.10: Simulation of location attack detection while tracking a mobile attacker which begins to attack the network (*i.e.*, spoof its position) at $X = 30$ and moves right through to $X = 100$. (a) A +30 dB SS attacker. (b) A +30 dB SS+BF attacker. (c) Associated potential risk (or reliability) levels $\mathcal{L}_S \in [0, 1]$ measured by RED and REF.

6.7 Conclusion

The main motivation of this work was to avoid the requirements of prior statistical assumptions, system training, pre-established infrastructure or other application-specific assumptions while providing a means for location attack detection. Due to the difficulty of assessing the anomalous behavior of a location estimator directly, we developed a novel approach for measuring a relative anomaly through two bilateral similarity measures. The first measure captures the similarity of two location estimates which provides a simple statistical detector. The second measure used the similarity of the topological features which was exploited to assess the estimator behavior more thoroughly while reducing large data sets effectively. We demonstrated that a combination of the two detectors can be used to monitor the security of a location system from different perspectives while defending from both SS and BF attacks. Specifically, regardless of the type of attack, REF can detect any malicious attempts to spoof a position estimate, while REF is only sensitive to effective location attacks and thus indicates the quality of a location estimate under attack. In this chapter we also showed that another bias effect due to the geometry of nodes is a key factor affecting the detection of location attacks, which was handled here through geometric filtering.

Chapter 7

Attack-Resilient Position Location with Anomalous Error Correction

7.1 Introduction

The purpose of a location system is to determine the position of a wireless device or node as accurately as possible subject to system and environmental constraints. Although the natural constraints pose technical challenges in location estimation, their impact is inherently limited. Further, there are cases where we can characterize the primary sources of natural error either statistically or experimentally, and thus exploit the knowledge to increase the reliability and accuracy of position location. On the other hand, the characteristics and behavior of location spoofing attacks can be neither known *a priori* nor predictable. Even if an attack is detected successfully, the uncertainty on radio parameters $\boldsymbol{\psi}_i$ of $\boldsymbol{\Psi}_i$ in Eq. (4.1), which can be falsified by an attacker to the extent possible, still remains and enables the attacker to be geographically anonymous.

In the previous chapters we showed that passive location algorithms widely adopted by current location systems are susceptible to both signal strength (SS) and beamforming (BF) attacks. Due to this security issue, there have been recent efforts to make location estimation resilient to attacks using robust statistical methods [53] and range-free localization schemes [48, 50, 54]. These approaches usually improve the resiliency to attacks at the expense of either location accuracy in the non-attack case or high computational/hardware complexity. As a result, this tradeoff limits the applicability of the approach and, moreover, increases the security risk of location information due to the fact that location security is fundamentally associated with location accuracy and availability (please see the definition of location security in Chapter 1). On the other hand, a proactive localization approach such as cryptography or handshaking schemes (*e.g.*, a distance-bounding algorithm [49,107]) typically requires pre-established infrastructure and/or a system protocol installed both in

the network and mobile devices which are potentially adversarial. Thus, this latter approach faces the same tradeoff issues mentioned above.

As discussed in Chapter 1, the security of location information is closely related to the reliability issues of location estimation. Even in the absence of any malicious spoofing attack, due to system nonlinearity, non-Gaussian error and bad node geometry, it is inevitable to encounter large or anomalous location error which impacts the estimator performance significantly. Obviously, the resulting degradation in location accuracy will also be a concern for secure positioning. We have seen in the previous chapters that a small number of anomalous location estimates (or "position outliers") with excessive error dominate the error performance of an estimator, thus resulting in a heavy tail in the error distribution. When the channel state is dynamic, it is possible to deal with such anomalies using popular adaptive techniques in signal processing such as Bayesian filters [65, 66]. However, the techniques normally cannot be employed over static wireless channels (*e.g.*, stationary nodes) and, moreover, many of them are too computationally expensive for many location applications. In relation to the reliability issues in location estimation, there remain many open problems. Two of the most important problems are the development of (a) an *observable* metric for assessing the quality of a node's location estimate and (b) an error correction or improvement algorithm. Since the nature of location attacks is to deteriorate the reliability of location estimates, we address the both problems in this chapter, particularly from a security perspective.

The main purpose of this chapter is to develop an approach to attack-resilient position location which not only can determine the position of an attacker, but also is robust to various sources of anomalous location error. Specifically, the approach is developed to deal with the security and reliability issues concerning location systems discussed in the previous chapters, that is (a) the passive reliance on signal source for localization, (b) heavy-tail issues of a location estimator, and (c) the adverse effect of node geometry. To address these issues, our approach incorporates the following principles. First, it is a better strategy to estimate system's nuisance parameters $\mathbf{\Psi}_i$ in Eq. (4.1) jointly with position parameters of interest without cooperation from the signal source. Second, to make this strategy effective we should avoid the heavy-tail behavior of a location estimator in relation to location estimates with large error. The anomalous behavior deteriorates substantially further under more harmful attacks (*i.e.*, positive-bias attacks with larger SS attack levels) or other systematic biases. Third, despite the proactive effort prior to localization, it is impossible to always avoid large location error due to various nonlinear complexities in the problem of location estimation. Thus, it is desired to find a way to correct large location error, which is particularly caused by location attacks, when it occurs.

In this chapter we present a unified framework for secure, reliable positioning without requiring any prior statistical and environmental knowledge. Within this framework three localization tasks–namely, the *reduction* of anomalous location error (which is not observable directly), and the *discovery* and *correction* of the residual anomalous error–are performed to tackle various challenges in location estimation. Note that this framework can be employed

regardless of whether the location security is concerned or not, while improving the overall localization performance. As we will show, this approach is possible with only a single RSS observation at each anchor regardless of the state of the channel. The benefits come at the cost of insignificant overheads, specifically only one additional parameter (independent of the number of links) in typical optimization routines for the anomalous error reduction (AER) and either one redundant test position estimate (without any additional measurement) or node convex hull computation for residual anomalous error discovery (AED) and correction (AEC).

The rest of the chapter is organized as follows. In Section 7.2, a penalized joint location estimator is developed for AER to jointly estimate nuisance system parameters and position coordinates. Then, we show that the heavy-tail behavior of a location estimator can be improved significantly by the proposed estimator. Section 7.3 introduces an observable metric for assessing the security risk of a location estimate as well as discovering anomalous location error for AED. In Section 7.4, by exploiting the risk measure we develop a novel algorithm for AEC that selectively corrects large location error. Then, Section 7.5 presents simulation results for the approach, where the performance of the penalty-based estimator improves significantly with the aid of AEC. In Section 7.6 we conclude the chapter.

7.2 Penalized Joint Location Estimator

In Chapter 4 we discussed the security risks associated with nuisance parameters $\mathbf{\Psi}_i$ in Eq. (4.1) for position location. The primary security concern is the dependence of RSS measurements $\{\boldsymbol{v}_i\}_{i=1}^m$ on the uncertainty in the extra parameters $\mathbf{\Psi}_i = (n_p, \boldsymbol{\psi}_i)$ which are a combination of the channel parameter n_p and transmitter parameters $\boldsymbol{\psi}_i = (P_t, S_t, G_{t_i})$. P_t, S_t and G_{t_i} are the transmit power, system loss factor and transmitter antenna gain seen by the ith anchor, respectively. These parameters are "nuisance" in the sense that even though their values are not of interest, a location estimator must know their values to determine the unknown position coordinates (x, y) of interest. When the prior knowledge of the channel parameter n_p is not available or reliable, the only viable option is to estimate it jointly with the position parameters. As discussed in Chapter 5, even with perfect knowledge of the nuisance parameter, estimating it jointly with position parameters is still considered a winning strategy in terms of the MSE, particularly under biased, correlated wireless localization conditions. Besides this estimation issue, the transmitter parameters, which are inherently uncertain variables to a positioning system, need to be estimated without the aid of the transmitter (*i.e.*, potential attacker) who can falsify their values deliberately or erroneously.

However, there are technical challenges associated with such a joint estimation strategy in practice. First, in dealing with a nonlinear, nonconvex optimization framework as in Eqs. (3.33) and (3.40), there exists no closed-form solution, thus requiring a numerical optimization algorithm. With more variables in the framework which increase the search space, the computational complexity and convergence time become higher. Second, due to the mul-

timodal objective function, we encounter adverse optimization issues including no global optimality guaranteed, ill-conditioning and other nonlinear effects [99]. The optimization issues would lead to excessively large location errors, thus making the tail of the error distribution heavier (or fatter) as identified in Chapter 5. This heavy-tail issue thus impedes the adoption of such a joint estimation strategy despite its potential localization capability. Recall that the potential location accuracy can be found by examining the lower error region or domain of the cumulative distribution function (CDF) of location error (see Fig. 5.3a). To substantially reduce the anomalous location error for AER and tackle the optimization issues, we employ a penalty-function scheme as follows.

Consider a 2-dimensional source localization problem based on RSS measurements $\{P_i\}_{i=1}^{m}$ at a set of m hearable (*i.e.*, "in range") anchor nodes with known coordinates $\boldsymbol{x}_i$. With the adoption of a non-cooperative, joint estimation strategy, the behavior of a location estimator depends primarily on its optimization characteristics. Particularly, due to the joint estimation approach, location spoofing attacks can only corrupt RSS measurements through either the signal power change, beamforming, or both. To substantially alleviate the estimator's anomalous behavior, we employ a non-cooperative *penalized joint estimator* (PJE) with simple bound constraints in the form

$$\arg\min_{\boldsymbol{\theta}'} \quad \phi_R(\boldsymbol{\theta}') = \underbrace{\frac{1}{2}\sum_{i=1}^{m} f_i^2(\boldsymbol{\theta}')}_{\text{original term}} + \underbrace{\lambda_p \sum_{j=1}^{\tilde{m}} g_j^2(\boldsymbol{\theta}')}_{\text{penalty term}} \tag{7.1a}$$

$$\text{subject to} \quad n_p^{\min} \le n_p \le n_p^{\max} \tag{7.1b}$$

where

$$f_i(\boldsymbol{\theta}') = P_i - P_0 + 10 n_p \log_{10} \|\boldsymbol{\theta} - \boldsymbol{x}_i\|_2 \tag{7.2}$$

$$g_j(\boldsymbol{\theta}') = \max\left\{\bar{P}[d_j(\boldsymbol{\theta}')] - S_{rx}, 0\right\}. \tag{7.3}$$

Now the estimator's variables are $\boldsymbol{\theta}' = [\boldsymbol{\theta}^T, \boldsymbol{\eta}]^T$, where $\boldsymbol{\theta} = [x, y]^T$ and $\boldsymbol{\eta} = (n_p, P_0)$. Note that the link-selective nuisance vector $\boldsymbol{\Psi}_i$ in Eq. (4.1) is simplified to $\boldsymbol{\eta}$, which is now *independent* of the number of links or anchors, thus significantly improving the computational complexity and convergence rate. The bounds $n_p^{\min}$ and $n_p^{\max}$ of n_p are limited to $n_p \in [1.6, 6]$ in most wireless environments [40]. The observed power levels (*i.e.*, RSS) and unknown reference power are denoted by $\boldsymbol{v} = [P_1, \ldots, P_m]^T$ and P_0, respectively. Note that the original residual $\boldsymbol{r}(\boldsymbol{\theta}) = \boldsymbol{v} - \boldsymbol{L}(\boldsymbol{\theta})$ in Eq. (6.3) is expanded with additional penalty terms with a coefficient λ_p (> 0) to suppress the heavy-tail behavior (or anomalous location errors) by penalizing any violation of the constraints. The first term with $f_i(\boldsymbol{\theta}')$ is the original LS objective function. The second term $g_j(\boldsymbol{\theta}')$ is a penalty function added to the objective function. $\bar{P}(d_j(\boldsymbol{\theta}'))$ is the average power received at d_j in Eq. (4.2), S_{rx} is the receiver sensitivity level, and $\tilde{m}$ is the number of unhearable or inactive anchors nearby. In other words, g_j is the constraint for the jth anchor that does not sense a target signal, which is *additional information* about

the mobile position. Thus, $\tilde{m}$ nodes are selected depending on the radio coverage range and the network size.

By denoting the updated residual vector $\bar{\boldsymbol{r}} = [f_1, \ldots, f_m, \lambda_p g_1, \ldots, \lambda_p g_{\tilde{m}}]^T$, we can rewrite Eq. (7.1) as $\phi(\boldsymbol{\theta'}) = \frac{1}{2}\|\bar{\boldsymbol{r}}(\boldsymbol{\theta'})\|_2^2$ in the original form as in Eq. (6.3). The key advantages of PJE in the form of Eq. (7.1) are:

- We can employ many state-of-the-art optimization algorithms to solve the problem in Eq. (7.1) due to its canonical form of a bound-constrained LS problem;
- Through the penalty coefficient λ_p, we can incorporate "soft" constraints on the radio coverage region $\{\bar{P}(d_j) < S_{rx}\}_{j=1}^{\bar{m}}$ for $\bar{m}$ unhearable nodes nearby. The soft constraints enable the estimator to reduce the feasible region effectively while taking into account irregular radio propagation patterns.

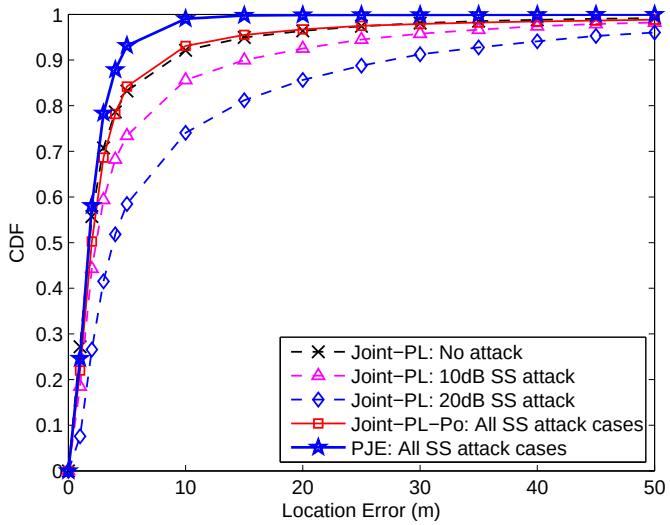
In Eq. (7.1), the unknown system parameters $\boldsymbol{\psi}_i = (P_t, S_t, G_{t_i})$ are incorporated into the single variable P_0 for better optimization properties and simplicity. While this approach is appropriate against SS or uniform attacks with omni-directional antenna patterns $\{G_{t_i}\}_{i=1}^m = G_t$, it may not be appropriate against BF or selective attacks with $G_{t_i} \neq G_{t_j}$ for $\exists i \neq j$. To examine the efficacy of PJE in the presence of BF attacks, we employ a *benchmark* estimator for linear array beamforming, called a linear array BF estimator (LBE), with knowledge of beam direction[1] Θ_0 and estimated array gain

$$g_t(N_a) = \left| \frac{\sin(N_a \varpi_l/2)}{\sin(\varpi_l/2)} \right| \tag{7.4}$$

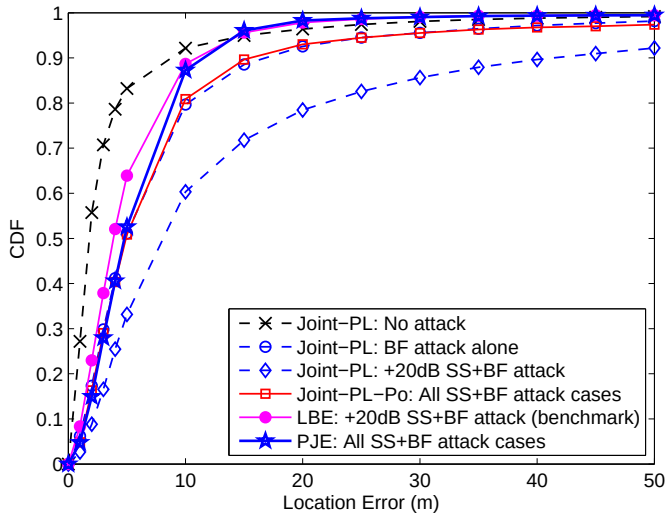
where the unknown array size N_a is jointly optimized, *i.e.*, $\boldsymbol{\theta'} = [\boldsymbol{\theta}^T, \boldsymbol{\eta'}]^T$ where $\boldsymbol{\eta'} = (n_p, P_t, N_a)$ to be related to Θ_0 through the parameter ϖ_l (as similarly done for UCA in Eq. (2.2)) [72]. Alternatively, one may consider jointly estimating antenna gains $\{G_{t_i}\}_{i=1}^m$ for all of the active links. However, we found it too computationally intensive and, moreover, PJE typically performs better.

In Fig. 7.1, we compare the performance of PJE (with $\lambda_p = 1$) and other joint estimators (which do not employ the penalty-function scheme) as well as LBE using adversary and simulation models given in Chapter 2. All of the simulation results presented in this chapter are based on the same simulation settings. The analysis leads to three key results. First, PJE performs without any interference from SS attacks, and improves the heavy-tailed behavior significantly. Note that the tails approach the unity of the CDF much more quickly than other estimators. Second, given that an uniform circular array (UCA) with Eq. (2.2) is used to launch a beamforming attack, the performance of practical and simpler PJE is comparable to LBE with exact knowledge of the beamforming direction. Third, despite the significant

[1]This assumption is probably unrealistic, but provides the benchmark performance to which PJE is compared under BF attacks. Note that the knowledge of the beam direction is required for the array gain model in Eq. (7.4) because it is not defined at $\Theta_0 = n\pi$ for any integer n.



(a)



(b)

Figure 7.1: Comparison of the penalized joint estimator (PJE) and other location estimators which jointly estimate n_p (*i.e.*, Joint-PL) or both n_p and P_0 (*i.e.*, Joint-PL-Po) to show the effectiveness of the anomalous error reduction (AER). CDFs of location error (a) under SS attacks and (b) under SS+BF attacks.

improvement of the estimator performance, PJE (and any other estimators) cannot always avoid anomalous location estimates with large error, which substantially degrade the MSE performance. As an example, in the case of PJE, there are situations where no unhearable nodes or neighbors exist (*e.g.*, at the edge of the network) so that PJE cannot penalize the constraints on improbable mobile positions. The resulting heavy-tail behavior will be shown later in this chapter. Therefore, it is desired to discover and correct residual anomalous errors once they occur.

7.3 Assessing the Security Risk and Anomalous Error of a Location Estimate

The problem of this section is to measure the excessive error or anomaly of a location estimate due to an attack. While this issue was handled in Chapter 6 for attack detection, our goal here is to use the metric for a different purpose. Thus, we restate the problem in terms of measuring the security risk which will also be used to correct residual anomalous errors in the next section.

In location estimation, it is invaluable to know the quality or anomaly of a node's location estimate. Through the use of the quality metric we can quantify how much a location estimate deviates from the true position. Then, it is possible to develop an algorithm which improves the location accuracy or error in real time by, for example, either repeating signal measurements (with additional anchors) and location estimation to meet the predefined "target quality of location." Further, the observable metric can be used as a security risk measure for secure positioning in the presence of an attack. However, it is technically challenging to develop an *observable* metric of the quality of a location estimate without prior knowledge of the (statistical or environmental) characteristics of error. Many well-known statistical measures including CRLB cannot be used for this purpose due to their dependency on the unknown true position and error statistics known *a priori*. Note that adversaries (which are obviously the unknown source of error) will take advantage of the prior statistical or environmental assumptions to compromise position location systems.

The difficulty can be seen by examining the direct metric $\mathcal{M}_A$ (≥ 0) of the error or anomaly of a location estimate $\hat{\boldsymbol{\theta}}$:

$$\mathcal{M}_A(\hat{\boldsymbol{\theta}}) \triangleq d(\hat{\boldsymbol{\theta}}, \boldsymbol{\theta}) \tag{7.5}$$

where

$$d(\boldsymbol{u}, \boldsymbol{v}) = \|\boldsymbol{u} - \boldsymbol{v}\|_p = \left(\sum_{k}^{dim(\boldsymbol{u})} |u_k - v_k|^p \right)^{\frac{1}{p}}. \tag{7.6}$$

As described in Chapter 6, the p-norm $\|\cdot\|_p$ is used for a measure of distance on the finite-dimensional vector space [75]. The value of $p \in [1, \infty)$ is chosen for the desired degree of

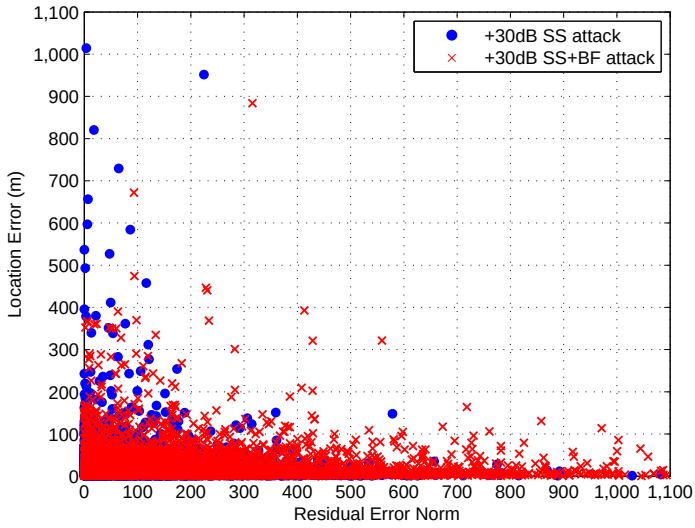


Figure 7.2: Scatter plots of the residual error norm and the location error in the presence of signal strength and beamforming attacks (σ_S = 5 dB, n_p = 4)

similarity or closeness between the estimates. With larger p values, the metric $\mathcal{M}_A$ is less sensitive to estimator variances. When $p = 2$, $\mathcal{M}_A$ measures location error. Even though the direct measure $\mathcal{M}_A$ in Eq. (7.5) is intuitive, unfortunately it is not observable due to its dependence on the unknown true position $\boldsymbol{\theta}$.

One may consider LS residuals to measure the location reliability as previously done for NLOS bias or outlier mitigation. Specifically, researchers have proposed algorithms that selectively remove or scale NLOS measurements by examining the residual errors $\boldsymbol{r}$ of the measurements or their norm $\|\boldsymbol{r}\|_2$ for TOA [60], TDOA [61], and AOA [62]. They assume that a majority of the signal observations are reliable LOS measurements, almost error-free or statistically known over benign localization conditions (*e.g.*, good node geometry). Clearly, this assumption cannot be applied for typical attack scenarios, where all or most of the observations can be severely corrupted or biased by the unknown attack. Also, we do not know which measurements are less corrupted. Without this strong assumption, it is difficult to adopt LS residuals for the location security risk measure. We demonstrate the unreliability of the residuals as a quality (or security) metric through a scatter plot in Fig. 7.2 under the attack-prone environment simulated as before. Here, a typical Joint-PL estimator (which is prone to attacks) is used as an RSS location estimator $\boldsymbol{\theta}_R$. It can be clearly seen that there is little correlation between the residual error norm and the location error.

7.3.1 The Security Risk of a Location Estimator

Despite the challenges of assessing the quality of a location estimate without *a priori* information, this chapter addresses the problem of measuring the quality of a location estimate under attack (*i.e.*, the security risk in terms of location accuracy) or the impact of an attack. More specifically, the security risk is measured through the *relative error norm*, which is related to point error signatures employed for attack detection in Chapter 6. The relative error norm $\hat{\mathcal{M}}_A \in [0, \infty)$ which estimates $\mathcal{M}_A$ in Eq. (7.5) is defined as

$$\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}}) \triangleq d(\hat{\boldsymbol{\theta}}_R, \hat{\boldsymbol{\theta}}_D) = \left\| \hat{\boldsymbol{\theta}}_R - \hat{\boldsymbol{\theta}}_D \right\|_p \tag{7.7}$$

where $p = 2$ here, corresponding to the Euclidean distance between the two points $\hat{\boldsymbol{\theta}}_R$ and $\hat{\boldsymbol{\theta}}_D$. Note that $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})$ using a pair of position estimates is a practical metric (in meters) as the two estimators use the same RSS observations, and no additional measurements or radio resources are required to obtain $\hat{\mathcal{M}}_A$. The metric is clearly observable which can also be shown mathematically as follows. Suppose that location error is caused either by a random vector $\boldsymbol{\zeta}$ due solely to natural sources of error (*i.e.*, no attack) or by a combination of $\boldsymbol{\zeta}$ and an attack $\boldsymbol{\eta}$ (*i.e.*, under attack). By denoting $\boldsymbol{e}_R = \hat{\boldsymbol{\theta}}_R - \boldsymbol{\theta}$ and $\boldsymbol{e}_D = \hat{\boldsymbol{\theta}}_D - \boldsymbol{\theta}$, the relative error $\Delta\boldsymbol{e} = [\delta e_x, \delta e_y]^T$ can be defined as $\Delta\boldsymbol{e}(\hat{\boldsymbol{\theta}}_R, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta}) = \boldsymbol{e}_R(\boldsymbol{\theta}, \hat{\boldsymbol{\theta}}_R; \boldsymbol{\zeta}) - \boldsymbol{e}_D(\boldsymbol{\theta}, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta})$ in the absence of an attack , whereas $\Delta\boldsymbol{e}$ is written as $\Delta\boldsymbol{e}(\hat{\boldsymbol{\theta}}_R, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta}+\boldsymbol{\eta}) = \boldsymbol{e}_R(\boldsymbol{\theta}, \hat{\boldsymbol{\theta}}_R; \boldsymbol{\zeta}+\boldsymbol{\eta}) - \boldsymbol{e}_D(\boldsymbol{\theta}, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta}+\boldsymbol{\eta})$ in the presence of an attack. Thus, we can rewrite $\hat{\mathcal{M}}_A$ in Eq. (7.7) as

$$\hat{\mathcal{M}}_A = \left\| \Delta\boldsymbol{e}(\hat{\boldsymbol{\theta}}_R, \hat{\boldsymbol{\theta}}_D; \boldsymbol{\zeta} + \boldsymbol{\eta}) \right\|_2 \tag{7.8}$$

where $\boldsymbol{\eta}$ is a zero vector when an attack is absent. Note that $\Delta\boldsymbol{e}$ and thus $\hat{\mathcal{M}}_A$ depend on neither the unknown true position $\boldsymbol{\theta}$ nor the unmeasurable location error.

As can be seen in Eq. (7.8), the relative error norm $\hat{\mathcal{M}}_A$ is a function of relative location error $\Delta\boldsymbol{e}$, not the true location error. Hence, its performance as a metric of the quality of a node's location estimate under attack (or location security risk) will depend on how strong the relative error norm and location error are correlated in the presence of various attacks. Note that as discussed in Chapter 6, higher attack levels (*e.g.*, SS attack levels or beamforming) do not always lead to higher location error or higher security risks. This is mainly due to the effects of natural error sources which can increase or reduce the impact of an attack. As a result, a good attack detection metric does not imply a good security measure with respect to location accuracy. In Fig. 7.3 we examine the correlation between the residual error norm (observable) and the location error (non-observable) using a scatter plot under the same attack-prone environment as in Fig. 7.2. We can clearly notice a significant correlation between the predictor and response variables, and their relationships are nearly linear with the slope (*i.e.*, correlation coefficient) of positive unity.

In this work we define the security risk level $\mathcal{L}_S \in [0, 1]$ of a location estimate $\hat{\boldsymbol{\theta}}$ as

$$\mathcal{L}_S(\hat{\mathcal{M}}_A) = 1 - e^{-k\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})} \tag{7.9}$$

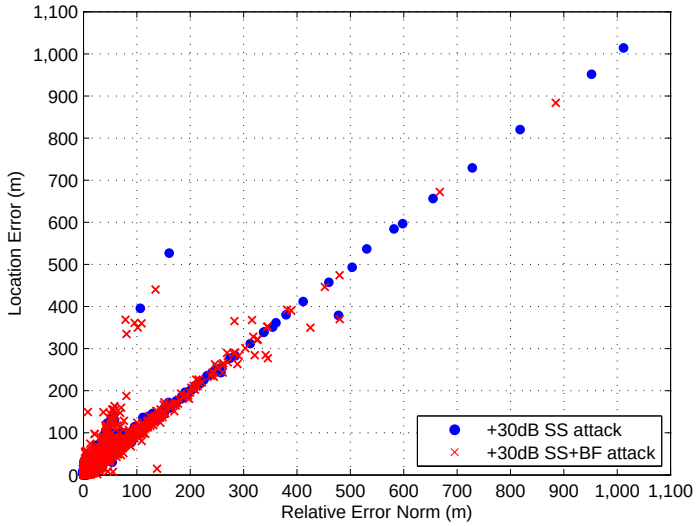


Figure 7.3: Scatter plots of the relative error norm and the location error in the presence of signal strength and beamforming attacks (σ_S = 5 dB, n_p = 4)

where $k \in [0, \infty)$ is the location threat sensitivity (0 = no security) which is set to 0.08 here. We will demonstrate how the security risk of a mobile's position estimate is evaluated through the normalized measure $\mathcal{L}_S$ in Section 7.5.

7.3.2 Discovery of Anomalous Location Errors

As anticipated from the correlation analysis in Fig. 7.3 and will be shown later, the relative error norm $\hat{\mathcal{M}}_A$ is a simple, yet effective metric to assess the quality of an attack-prone location estimate. This metric can be used in to assess the security and reliability of location estimates in attack-prone localization conditions. However, if the bias of a location estimator is insignificant over benign localization conditions (*i.e.*, $\mathrm{E}(\hat{\boldsymbol{\theta}})/\boldsymbol{\theta} \approx 1$ and $var(\hat{\boldsymbol{\theta}})$ is small), $\hat{\mathcal{M}}_A$ is not strongly correlated with the location error. On the one hand, this weak correlation is good since it implies that the impact of an attack and natural effects will be well discriminated through $\hat{\mathcal{M}}_A$, and the security risk can be measured reliably. On the other hand, we would not use $\hat{\mathcal{M}}_A$ directly for assessing the quality of a node's location estimate in non-attack conditions and improve the accuracy of a location estimator. The same argument is applied to the penalized joint estimator or PJE in Eq. (7.1) since it is resistant to most location spoofing attacks. Therefore, our next goal is to further improve the performance of PJE, particularly by addressing its remaining heavy-tail behavior. This issue will be tackled by discovering residual anomalous location estimates (which cause the heavy-tail of the error distribution) as follows and correcting the associated error in the next section. Note that the same principles can also be applied to other range-based estimators under nominal,

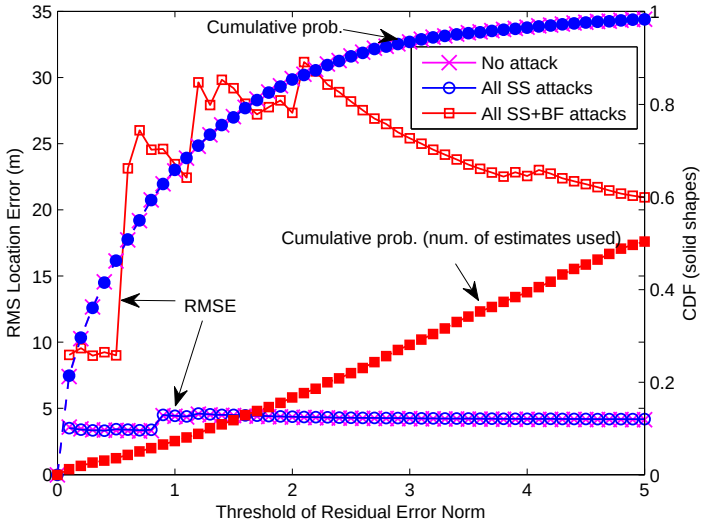
non-attack situations.

The main principles underlying the anomalous error discovery or AED are as follows. We discussed that the location accuracy or MSE performance of an estimator is dominated by a small number of anomalous location estimates with large error (*e.g.*, due to bad node geometry). This anomalous error can be detected by two methods. One of the methods is to use the relative error norm $\hat{\mathcal{M}}_A(\hat{\boldsymbol{\theta}})$ in Eq. (7.7) which can discover anomalous estimates with severe error even in the absence of an attack. This is because that RSS- and DRSS-based estimators (which use the same signal power observations) process the observed data in a different manner as shown in Eqs. (6.3)–(6.8). As a result, they behave differently under natural yet abnormal localization conditions such as system nonlinearity, optimization issues, and bad node geometry. Since we are only concerned with anomalous location errors which will be corrected when discovered, in this work we define a filter threshold for $\hat{\mathcal{M}}_A$ (*i.e.*, target $\hat{\mathcal{M}}_A$) beyond which a location estimate is flagged as "anomalous." In Fig. 7.4 we show relationships (or the correlation) between the RMS location error of PJE and the threshold of the residual error norm (in Fig. 7.4a) as well as the threshold of the relative error norm (in Fig. 7.4b). The RMS error was calculated since we need to incorporate all of the estimates under the threshold value. The CDF of the number of the estimates filtered through (or survival rate) is shown together in Fig. 7.4. It can be noticed that there is a desirable relationship between the threshold of $\hat{\mathcal{M}}_A$ and the RMS location error. With smaller values of the threshold, the location accuracy of PJE improves. This observation suggests that if the *observable* relative error can be reduced somehow, it is likely to improve the location accuracy without resort to any knowledge about the error. As can be inferred from Fig. 7.4, the filter threshold will be used as the target $\hat{\mathcal{M}}_A$ by an anomaly error correction or AEC algorithm to achieve the desired RMS error performance in the next section.

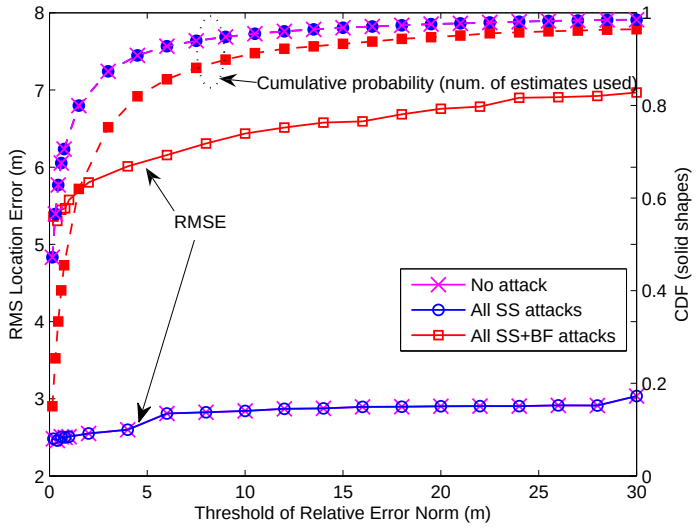
The second method for AED is to use our knowledge of the node convex hull which can be computed easily. As described in Section 7.2, PJE is substantially more reliable than other RSS location estimators even outside the node convex hull due to the use of additional information about radio range constraints. Nevertheless, there are cases where the constraints cannot be applied, for example, when the mobile is at the edge of the network. Thus, the major source of anomalous location error for PJE (which is robust to SS attacks) is the adverse effect of node geometry which would be deteriorated by a BF attack. Thus, when a location estimate is found to be outside the convex hull, it is marked as "geometrically unreliable." Then, as described in the next section, the AEC algorithm tries to improve the geometric adversity with the aid of geometric filtering (GF). The details of the node convex hull and the principles of GF can be found in Chapter 6.

7.4 Correction of Residual Anomalous Errors

In Section 7.2 and Chapter 4 we have described the impact of the heavy-tail of the error distribution (*i.e.*, related to location estimates with large error) on location accuracy, partic-



(a)



(b)

Figure 7.4: Relationships (or the correlation) between the RMS location error and threshold value of (a) the residual error norm and (b) the relative error norm. The CDF of the number of location estimates filtered though which are used for the RMSE calculation (*i.e.*, survival rate).

ularly for location security. Even with good estimators, the anomalous estimator behavior is inevitable in practice due to data outliers, non-linearities, and other complexities in location systems. Upon the detection of an anomalous location estimate, our next goal is to correct it without the aid of its signal source rather than simply rejecting it. If the estimate is rejected or filtered out, the availability of location information cannot be ensured. In particular, the position of a (stationary) attacker cannot be localized. To deal with the anomaly of location estimates, one may consider a robust statistics method such as least median squares estimators (LMSE) [53,125]. However, it does not permit an analytical form so that neither analytical nor state-of-the-art numerical methods can be applied. Further, in benign conditions, LMSE will be outperformed by typical LS estimators.

We now present a novel iterative algorithm termed the residual *anomalous error correction* (AEC) which can be implemented using two risk measures introduced earlier–either the relative error norm (REN) $\hat{\mathcal{M}}_A$ for AEC-REN or the node convex hull $\mathcal{H}_C(\mathcal{X})$ in GF (where $\mathcal{X}$ denotes a set of hearable anchor nodes) for AEC-GF. The two schemes can be integrated for better reliability at the expense of more iterations. It should be noted that the penalty-function scheme and AEC are developed to address the heavy-tail issues by complementing each other. While the penalty method for AER intends to reduce anomalous error *prior to* localization, AEC attempts to correct the remaining excessive error *after* the node's position is estimated. Their combination is especially valuable when only a *single meaningful* RSS observation is available at each anchor (*e.g.*, static radio channels).

The unified framework developed for location estimation, the security risk assessment via $\mathcal{L}_S$ in Eq. (7.9) and AEC is provided in Fig. 7.5 and the algorithm given in Algorithm 7.1 (using the same notations as in this chapter and Chapter 6). AEC-REN weights the RSS observations based on the related heuristic LS residuals to meet the target $\hat{\mathcal{M}}_A^*$ (*i.e.*, the filter threshold in Section 7.3). The LS residuals are not used here as an anomaly measure, but to improve the convergence rate of the algorithm. Since the task of finding the optimal weights on the observations is computationally too expensive and challenging (if not infeasible), AEC iteratively chooses a subset of the observations with binary weights and compares the result to the target value $\hat{\mathcal{M}}_A^*$ or $\mathcal{H}_C$. The details can be found in Algorithm 7.1.

In Algorithm 7.1, once the security alert indicator $\mathcal{I}_S$ is turned on, the network may record the target's MAC/IP addresses and other identifying (*e.g.*, login ID, location information) for network security measures and access control. If the risk of location $\mathcal{R}_S(t) = \mathcal{I}_S(t) \times \mathcal{L}_S(t)$ at $t = t_0$ or its sum $\sum_{t=1}^{\mathcal{T}} R_S(t)$ over some period $\mathcal{T}$ is too high, it may disconnect its connection with the client device.

7.5 Performance Evaluation

We now evaluate the performance results of PJE, AEC-REN and AEC-GF. Specifically, two experiments are considered by (a) simulating a mobile attacker tracking scenario and (b)

Algorithm 7.1 Residual Anomalous Error Correction and Risk Assessment

Input: $\hat{\boldsymbol{\theta}}_R(t)$, $\hat{\boldsymbol{\theta}}_D(t)$, $\boldsymbol{r}$, (or $\mathcal{F}_R$, $\mathcal{F}_D$) from Eq. (7.1), $\mathcal{M}_A^*$, $\mathring{\mathcal{X}}$, $\mathring{\mathcal{H}}_C(\mathcal{X})$

Initialize: $k \leftarrow 1$, $\hat{\mathcal{M}}_A^{(k)}$ from Eq. (6.10) (or Eq. (6.15)), $\{w_i\}_{i=1}^m \leftarrow 1$, $p \leftarrow 1$, $\mathring{X} \leftarrow \{x_i\}_{i=1}^m$, $\mathring{Y} \leftarrow \{y_i\}_{i=1}^m$, $\mathring{\boldsymbol{\theta}}_C \leftarrow \left[\frac{\min(X)+\max(X)}{2}, \frac{\min(Y)+\max(Y)}{2}\right]$, $\mathcal{I}_S(t) \leftarrow 0$, $\mathcal{L}_S(t) \leftarrow 0$, $\mathring{d}_A^{(k)} \leftarrow \|\boldsymbol{\theta}_C - \hat{\boldsymbol{\theta}}_R\|_2$, $D_A^* \leftarrow \hat{\mathcal{M}}_A^{(k)}$ or $\mathring{D}_A^* \leftarrow d_A^{(k)}$

1. **If** $\hat{\mathcal{M}}_A^{(k)} \le \mathcal{M}_A^*$ or $\hat{\boldsymbol{\theta}}_R^{\circ}(t) \preccurlyeq \mathring{\mathcal{H}}_C(\mathcal{X})$

   $\mathcal{I}_S(t) \leftarrow 0$, $\mathcal{L}_S(t) \leftarrow D_A^*$; **Stop**

   Otherwise $\mathcal{I}_S(t) \leftarrow 1$, $\mathcal{L}_S(t) \leftarrow D_A^*$

2. Sort $\boldsymbol{r}$ and return its index set I *s.t.* $\boldsymbol{r}(I_i) \ge \boldsymbol{r}(I_{i+1}), \forall i$

3. $q \leftarrow I_p$, $w_q \leftarrow \varnothing$

   Update: $\{P_i \leftarrow P_i \times w_i\}_{i=1}^m$; $\hat{\boldsymbol{\theta}}_R(t)$, $\hat{\boldsymbol{\theta}}_D(t)$, $\boldsymbol{r}$, (or $\mathcal{F}_R$, $\mathcal{F}_D$)

   Reinitialize: Same as above initialization; $k \leftarrow k+1$

5. **If** $\hat{\mathcal{M}}_A^{(k)} \le \mathcal{M}_A^*$ or $\hat{\boldsymbol{\theta}}_R^{\circ} \preccurlyeq \mathring{\mathcal{H}}_C(\mathcal{X})$

   $\mathcal{I}_S(t) \leftarrow 1$, $\mathcal{L}_S(t) \leftarrow D_A^*$; **Stop**

   Elseif $\hat{\mathcal{M}}_A^{(k)} < D_A^*$ or $\mathring{d}_A^{(k)} < D_A^*$

   $D_A^* \leftarrow \hat{\mathcal{M}}_A^{(k)}$ or $\mathring{D}_A^* \leftarrow d_A^{(k)}$;

   Remove I_p from I

   Otherwise $w_q \leftarrow 1$, $p \leftarrow p+1$

6. **If** $p \le size(I)$ and $size(I) > 3$

   Go to Step 3

   Elseif $t < \mathcal{T}$

   Direct the target to connect to other anchor(s) or to raise P_t;

   If Successful

   $t \leftarrow t+1$; *Resume the algorithm*

   Otherwise $\mathcal{I}_S(t) \leftarrow 1$, $\mathcal{L}_S(t) \leftarrow D_A^*$; **Stop**

Notation– ($\mathring{\cdot}$): For AEC-GF, $\mathcal{M}_A^*$: Target $\hat{\mathcal{M}}_A$, $\mathcal{I}_S$: Security alert indicator, $\mathcal{L}_S$: Security risk level (not normalized here), k: Iteration num., t: Observation index.

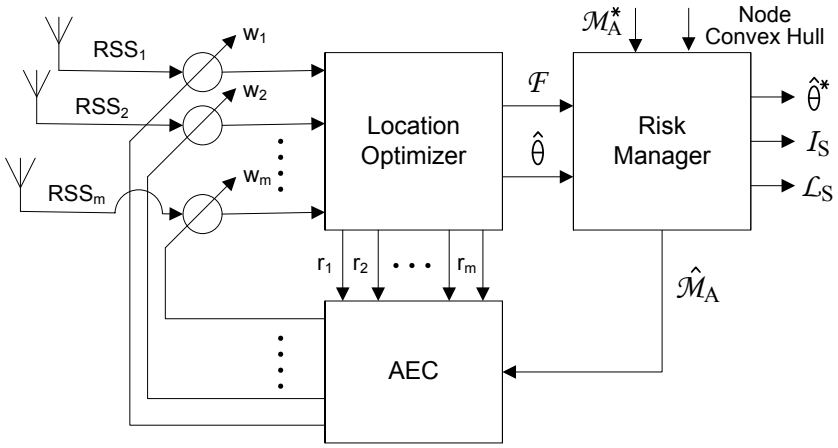
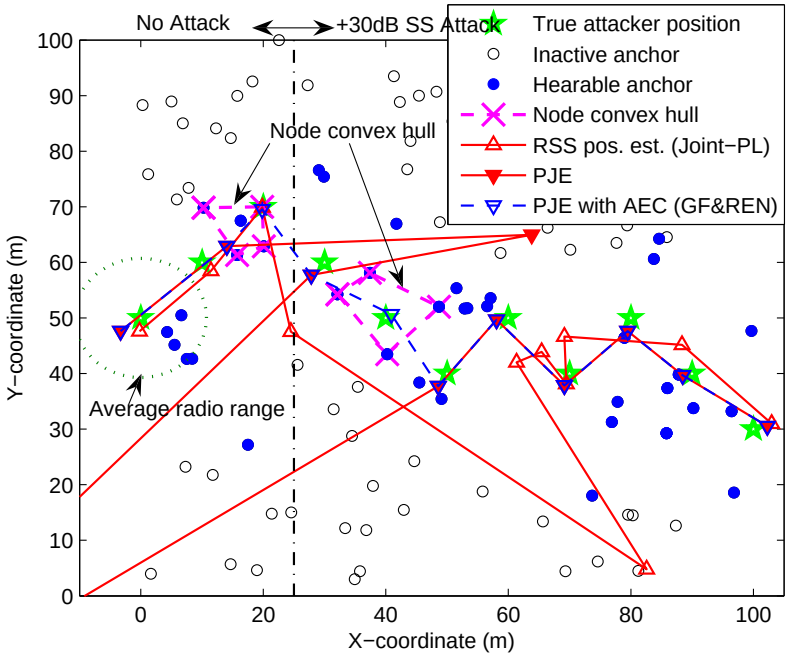


Figure 7.5: A unified framework for location estimation, the security risk assessment (via $\mathcal{L}_S$ in Eq. (7.9)) and the residual anomalous error correction (AEC) which iteratively improves the anomalous location error through the use of either the relative error norm $\hat{\mathcal{M}}_A$ or the node convex hull $\mathcal{H}_C(\mathcal{X})$.

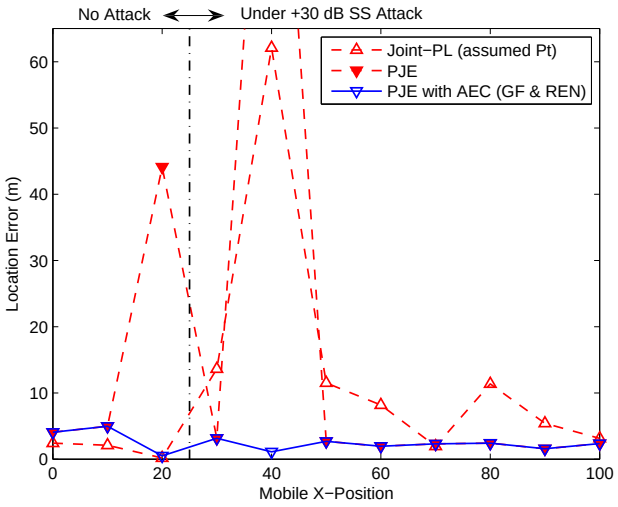
evaluating the "average" performance of the estimator/approach in terms of two statistical performance measures. The measures–that is the RMS and median (50th percentile) of location error–are compared to reveal the impact of the heavy-tail on estimator performance (target $\mathcal{M}_A^* = 5\ m$). As an attack scenario, an adversary launches either positive-bias SS attacks or BF attacks coupled with positive SS attack levels.

In the first experiment, as shown in Figs. 7.6 and 7.7, an attacker randomly moves through the network, from the coordinates $[0, 50]$ to the end of the site. While an attacker takes a random walk with 5 m steps along the X-axis, we employ different location estimators, Joint-PL, PJE, PJE with AEC-GF, PJE with AEC, and LBE with AEC-REN, to locate the attacker under the same environmental/external conditions (*i.e.*, node positions, shadowing levels, spatial correlation, *etc.*). We demonstrate how the estimators track the mobile with SS attacks in Fig. 7.6 and with SS+BF attacks in Fig. 7.7, while recording the resulting location errors and security risk levels over the course of the mobile. The attacker, which is monitored through the relative error detector (RED) (using the relative error norm) and the residual error fingerprinting (REF) technique presented in Chapter 6, begins to launch an attack when $X = 30$ and continues to attack the network up to the end point $X = 100$. Note that there is no attack from $X = 0$ to $X = 20$ in order to show how the detectors behave in normal conditions and perform differently during the presence of an attack.

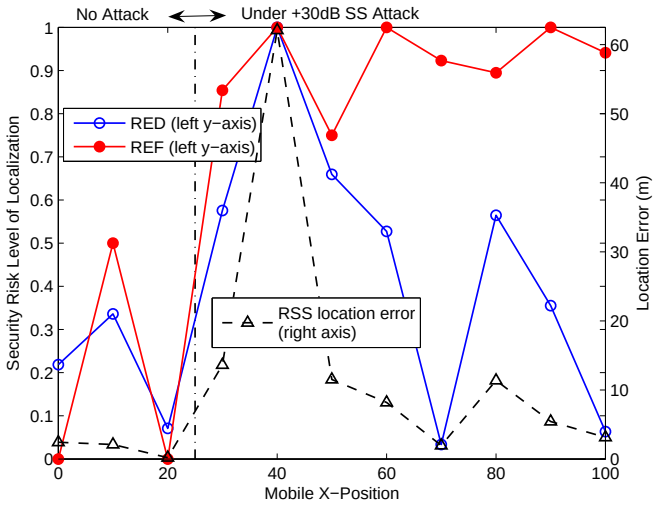
From the results, non-cooperative, penalty-based PJE significantly outperforms the typical estimator Joint-PL under the same conditions (regardless of the presence/absence of an attack). This result can be clearly seen in Fig. 7.1 and will be confirmed in the following simulation results. However, in Figs. 7.6 and 7.7 we deliberately chose one of the worst yet



(a)

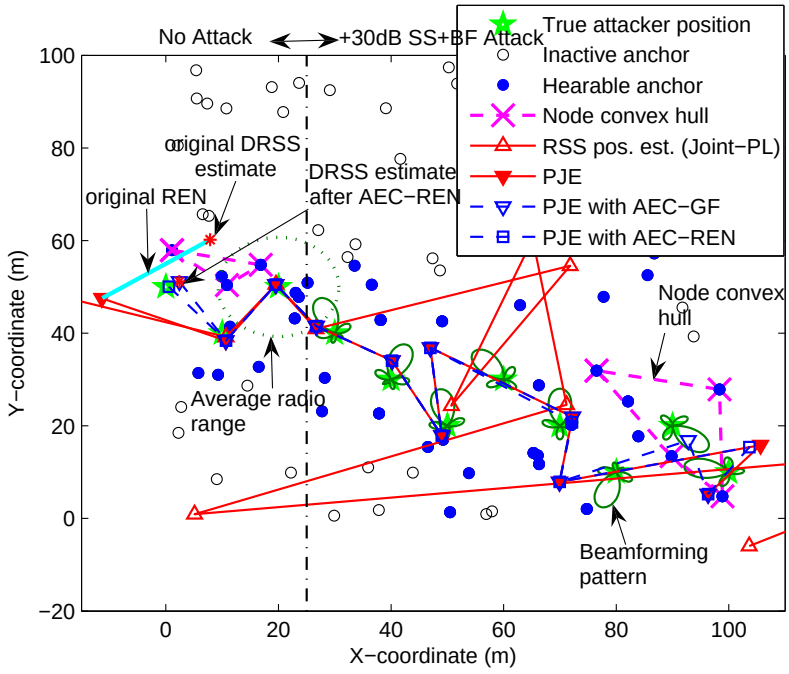


(b)

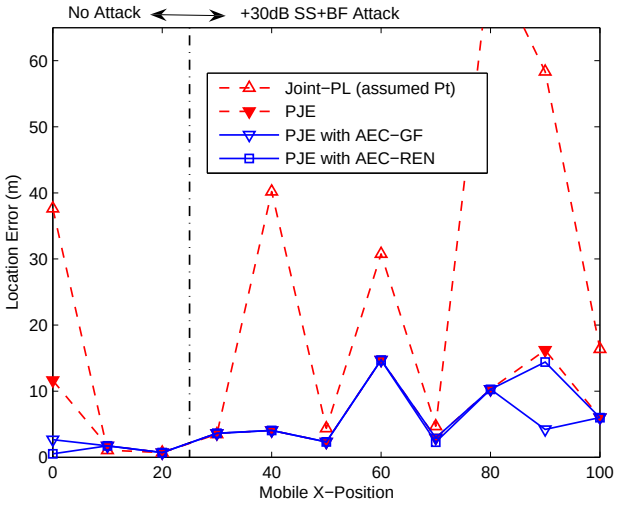


(c)

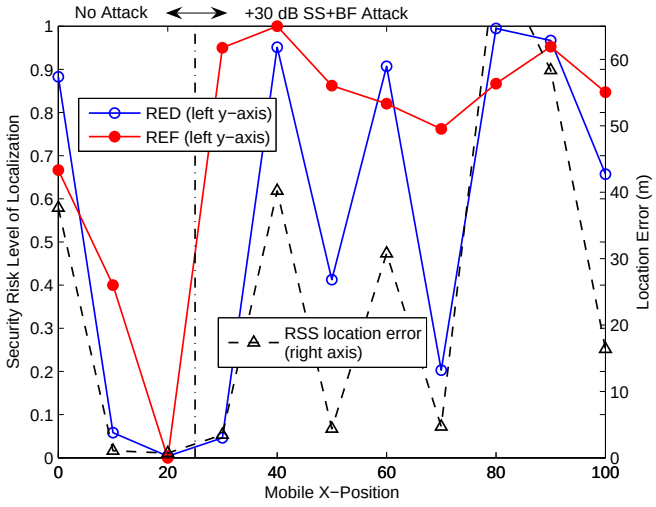
Figure 7.6: Simulation of tacking a mobile +30 dB SS attacker which begins to attack the network (*i.e.*, spoof its position) at X = 30 and moves right through to X = 100. (a) Sample network configuration and positioning activities. (b) Associated location error. (c) Associated security risk levels $\mathcal{L}_S$ using RED and REF.



(a)



(b)



(c)

Figure 7.7: Simulation of tacking a mobile beamforming attacker (with + 30 dB SS levels) which begins to attack the network (*i.e.*, spoof its position) at X = 30 and moves right through to X = 100. (a) Sample network configuration and positioning activities. (b) Associated location error. (c) Associated security risk levels $\mathcal{L}_S$ using RED and REF.

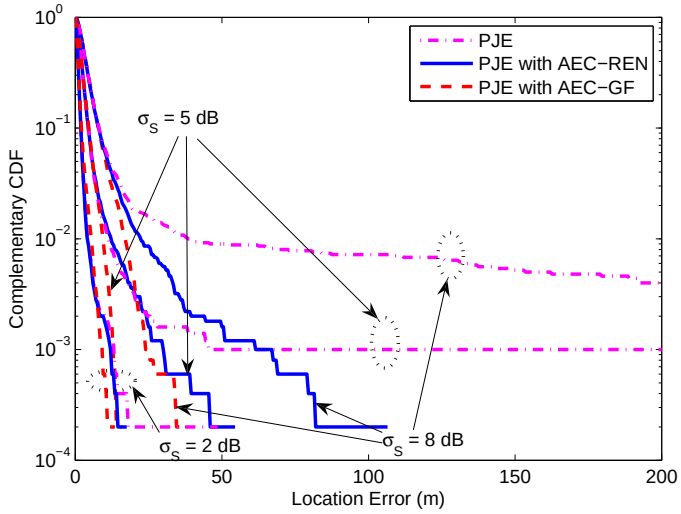
σ_S (dB)	Measure (meters)	+20 dB SS Attack				+20 dB SS+BF Attack			
		PJE_1		PJE_2		PJE		LBE	
		-	AEC-GF	-	AEC-REN	-	AEC-REN	-	AEC-REN
2	Median	0.72	0.72	0.72	0.72	4.45	4.45	2.73	2.69
	RMSE	1.53	1.44	1.52	1.34	8.10	5.85	13.54	4.45
5	Median	1.71	1.75	1.70	1.72	4.84	4.83	3.56	3.50
	RMSE	68.19	2.93	23.01	3.47	53.05	7.26	22.29	6.05
8	Median	2.84	2.88	2.85	2.83	5.63	5.57	5.32	5.17
	RMSE	83.01	5.12	43.82	6.35	56.77	9.80	133.33	8.78

Table 7.1: The performance of PJE and LBE under either +20 dB SS attacks or +20 dB SS+BF attacks as well as its improvements with AEC-REN and AEC-GF. The median which is resistant to outliers or anomalous errors (not good metric of location accuracy) is compared with the RMS location error to reveal how much anomalous error is corrected by AEC.

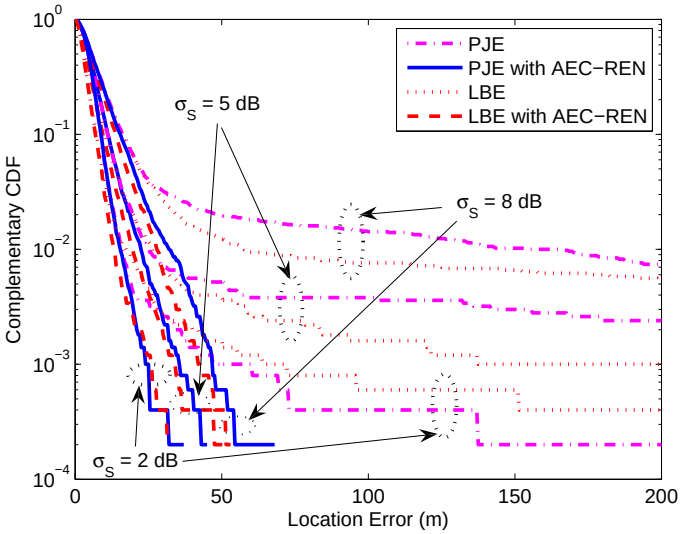
very rare cases for PJE, where the error of PJE is higher than that of Joint-PL to show how AEC performs in the presence of anomalous location estimates. Another key observation is that when PJE is integrated with one of the AEC algorithms (*i.e.*, AEC-REN or AEC-GF), its performance is substantially improved, particularly in the beamforming attack case in Fig. 7.7. Even in the absence of any attack (nominal conditions), AEC is so effective that anomalous error can be (mostly) corrected, as can be seen at $X = 20$ for the SS attack case in Fig. 7.6 and at $X = 0$ for the SS+BF attack case in Fig. 7.6. Regarding the security risk assessment, it is clear in the both figures that the security risk measured through RED (using the relative error norm) is strongly correlated with location error. On the other hand, another detector, REF, using topological error signatures detects the presence of an attack regardless of its impact on location accuracy.

In the second experiment, rather than focusing on a specific simulation scenario, our goal is to compare the average performance of the estimators under different environmental effects. Specifically, noting that PJE outperforms Joint-PL, we test three methods under +20 dB SS attacks (*i.e.*, PJE alone, PJE with AEC-GF and PJE with AEC-REN), and four methods under +20 SS+BF attacks (*i.e.*, PJE alone, PJE with AEC-REN, LBE alone, and LBE with AEC-REN). In Table 7.1, the final numerical values for the median and RMSE performances are given, whereas their error distributions using the complementary CDF (CCDF) are shown in Fig. 7.8. In the legends, the number after "PJE" denotes a simulation index that AEC is applied.

As shown in Table 7.1, AEC improves the RMS location error of PJE and LBE dramatically. In particular, the improvement increases with larger shadowing variance which causes more



(a)



(b)

Figure 7.8: Complementary CDFs of location error associated with Table 7.1. (a) PJE with or without AEC-REN/GF under +20 dB SS attacks. (b) PJE and LBE with or without AEC-REN under +20 dB SS+BF attacks.

excessive location error. The largest improvement rate is found when the location anomaly tends to be the worst–that is under the SS+BF attack with σ_S = 8 dB. In this case, the improvement rate is found to be significant ($\approx 93.4\%$). The existence of location anomalies and their correction/improvement can be more clearly seen in Fig. 7.8. The horizontally linear (flat) behavior of the right tail of the CCDF is the evidence of the heavy-tailed error distribution. From this figure, the above observations concerning the results in Table 7.1 can be visually identified. Note that when the heavy tails are "ignored" (or rejected) through the median, the performance of PJE or LBE alone is comparable to that combined with AEC. This indicates that anomalous errors that cause the heavy tail can be (almost) corrected by AEC.

Another key observation is that PJE with AEC tends to perform better with *worse* location anomalies or heavy-tailed behavior. This is because more anomalous location estimates are more likely to be discovered by AED (presented in Section 7.3) and then corrected by AEC. As as result, the estimator performance can be improved even better than more benign localization conditions. This better correction capability can also be identified by comparing the right tails of the CCDFs under SS attacks alone in Fig. 7.8a and their counterparts under SS+BF attacks in Fig. 7.8b. Lastly, much simpler/faster PJE (particularly with AEC) exhibits comparable performance to the benchmark estimator, LBE which uses a linear array BF model with known beam direction.

7.6 Conclusion

The main motivation of the chapter was to reliably determine the position of an attacker or unreliable signal source without requiring prior statistical or environmental knowledge. This condition is important since the prior information is usually neither available, reliable nor secure. To accomplish this task, this chapter deals with the reduction and discovery of anomalous location errors as well as the correction of the residual anomalous errors which considerably degrade the performance of a location estimator in both attack-prone and attack-free localization situations. We described that the severe errors cause the heavy-tailed behavior of the estimator. Since anomalous location errors and the heavy-tailed behavior are fundamentally the source of location security risks, we developed several new methods to reduce the abnormal errors substantially, and then discover and correct the residual anomalous errors which cannot be measured directly. For anomalous error reduction, a penalized joint estimator was developed to exploit additional information about the radio coverage as soft optimization constraints while jointly estimating attack-prone nuisance parameters. For the discovery and correction of residual anomalous errors, we used the relative error norm which is highly correlated with anomalous location error due to an attack. This metric was then used by an algorithm for the anomalous error correction, where a subset of RSS observations are selectively chosen (or weighted) to reduce the measure and thus correct the anomaly of an estimate. The fact that the proposed approach, based on widely available RSS data,

require neither (statistical) knowledge of error sources, off-line training, nor any type of prior information makes them attractive for various applications and practical scenarios.

Chapter 8

Conclusion

8.1 Summary

In this dissertation we have studied the problem of securing position location from location spoofing in wireless networks. This study is particularly important as there is an increasing concern about the security of location information in wireless devices. From a location security standpoint, every network client and unidentified wireless device could be a potential threat to position location systems or networks, even if they are legitimate or have successfully acquired a network authentication through secret cryptography. Further, the research effort to thwart location attacks facilitates both reliable location estimation and wireless network security. In order to build a location system or algorithm that is resilient to location spoofing, it is fundamentally important to make it robust to natural sources of systematic error or bias. We also noted that secure location information can be used to complement conventional network security schemes.

The main results and contributions of this dissertation are summarized as follows:

- **Fundamental Issues in RSS-Based Location Estimation (Chapter 3)**

  Since this dissertation tackles the security issues related to RSS-based location estimation, we investigated the fundamentals of RSS-based position location, particularly focusing on range-based localization. Specifically, two fundamental approaches to SS-based positioning were studied from various aspects including the LS optimization framework, numerical optimization methods, geometric interpretations and location estimators. We evaluated and compared the performance of the two approaches while taking into account the spatial correlation of shadow fading. The study showed that the location accuracy of the DRSS-based approach improves with higher spatial correlation of shadowing, where many other positioning techniques may struggle. Further, it was found that while spatial correlation deteriorates the localization performance

of the RSS-based approach when the number of anchor nodes is large (*e.g.*, $m > 9$, if $\alpha = 3, \sigma_S = 5$ dB), its performance improves with smaller numbers of anchors. We also found that the RSS-based approach is more robust to the adverse effect of node geometry than its counterpart using DRSS.

- **Security Issues for Wireless Position Location (Chapter 4):**

  Location attacks were classified into three primary types–attack position spoofing, anchor signal spoofing, and location disclosure–and we described the security issues and recent work related to each attack type. The effects of location spoofing, particularly through signal strength and beamforming attacks, were examined by solving simple examples and through a practical simulation study. We found that attacks in the positive SS attack region (*i.e.*, positive-bias attacks) are the most detrimental with respect to location accuracy, and the impact can be increased by coupling positive-bias SS attacks with beamforming. We also examined the impact of inaccurate knowledge of the path loss rate, and it was found that it is very detrimental when the value is underestimated.

- **Characterization of Location Spoofing Attacks (Chapter 5):**

  Since a location spoofing attack can be regarded as a source of systematic error, the characterization of location attacks enabled us to better understand the security issues and facilitate the design of a secure location system. We showed that location spoofing attacks can be characterized by a scaling factor which appears to bias individual range estimators and the resulting position estimator. Depending on the form of bias, location spoofing attempts were categorized into positive- and negative-bias attacks. These attacks were further classified as either uniform or selective attacks–which correspond to SS or BF attacks against RSS-based positioning, respectively–according to the impact of the attack-induced bias on individual range estimators.

- **Analysis of the Behavior of a Location Estimator Under Attack (Chapter 5):**

  Location security issues can be related to fundamental localization issues in harsh environments. This observation led us to examine the behavior of a location estimator under attack from fundamental estimation aspects, namely prior knowledge of nuisance parameters, heavy-tailed error distributions and the bias-variance tradeoff. Through the analysis we could explain the effects of both SS and BF attacks as follows. First, it is typically a better strategy to estimate nuisance parameters jointly with position parameters of interest, even when prior knowledge of the nuisance parameters is available. Second, the impact of a small number of position estimate outliers, which leads to the heavy-tail of the error distribution, is significant in terms of location accuracy, and deteriorates in the presence of an attack. Thus, we argued the importance of addressing the anomalous heavy-tailed behavior. Lastly, it was observed that an attack can be viewed as a scaling factor which impacts a location estimator by modifying the

estimator's bias-variance characteristics, referred to as the bias-variance tradeoff. Due to this tradeoff we found an interesting result that some attacks actually improve the location accuracy of a location estimator, and thus expose their position more.

- **Detection of Location Spoofing Attacks (Chapter 6):**

  To detect both SS and BF attacks, we presented statistical and pattern matching techniques in addition to a geometric approach to improving the detection performance. The statistical approach uses point error signatures which are strongly correlated with location error. On the other hand, topological error signatures are employed by the pattern matching approach to examine RSS measurements (corrupted by an attack) from a global viewpoint. The two approaches enabled us to examine the presence and effect of an attack from different perspectives. We also showed that the detection performance is subject to the adverse effect of node geometry which was tackled through the use of geometric filtering.

- **Attack-Resilient, Reliable Location Estimation (Chapter 7):**

  To achieve attack-resilient, reliable location estimation, our primary emphasis was to handle anomalous location estimates with excessively large error which cause the heavy-tailed behavior of a location estimator. To this end we developed a unified framework that consists of the reduction of anomalous location error, and the discovery and correction of residual anomalous errors. In order to reduce the anomalous error substantially, a joint optimization framework with a penalty function was developed. Despite the significant improvement in location accuracy made by the effort, it is inevitable that one will encounter anomalous location errors which cannot be observed directly. Thus, the relative error norm was developed to discover the residual anomaly and measure its security risk. Another method employed a geometric filtering scheme based on the node convex hull. Upon its detection, an algorithm for the correction of residual anomalous errors was employed to further improve location accuracy by correcting the residual anomalous errors.

In this dissertation, the primary goal in developing an approach to the detection and localization of location spoofing attacks was to use only RSS measurements without resort to prior statistical or environmental knowledge. The prior information is usually assumed in the literature through pre-established infrastructure, additional radio resources/hardware, offline training procedures, system protocols and/or statistical assumptions.

8.2 Design of a Secure Location System

With our understanding of location attacks and their impact we now design a secure location system which incorporates the approaches developed in this work.

8.2.1 Goal of the System

The design goal of a secure location system is to ensure location security, that is the *availability*, *integrity* and *reliability* of location information about the mobile which is potentially malicious or unreliable. To accomplish this goal we consider the following approach:

- **Availability**–In position location networks, location information should be always available. Thus, the system is designed to only utilize SS features for operation which can readily be acquired in (nearly) every wireless system without additional hardware, structure modification or pre-existing localization infrastructure/protocols. Also, it does not require the cooperation of the signal source, which is potentially an attacker. Thus, it is widely applicable regardless of radio type, wireless technology, network scenario, and other system constraints.
- **Integrity**–In location security, the integrity means that location estimates are not modified or disrupted. However, passive location algorithms adopted by many existing systems are prone to violations of integrity by nature. Therefore, the system does not relay on the signal source (which may be malicious, erroneous or unreliable) for localization while monitoring and detecting location security risks to ensure the location integrity.
- **Reliability**–The task of localization can be severely hampered by non-linearity, bad node geometry, and noise in addition to attacks, where tractable statistical methods are typically not applicable. Thus, we make an effort to improve the reliability of location estimates, while reducing excessively large error even with a single RSS observation at each anchor. Further, the system provides a measure of the reliability of a node's location estimate without any assumptions on the statistics of error.

8.2.2 Overview of the System

We now describe a specific design framework for the system which is composed of four major design components as given in Fig. 8.1. The system incorporates various methods developed in this work. The main components are the *signal observer*, the *location estimator*, the *node coordinator* and the *location security monitor* as summarized below:

- **Signal observer**–This collects two SS features, RSS and DRSS, from a mobile target based on RSS measurements as described in Chapter 3.
- **Location estimator**–Based on the observed SS features, the optimizer finds the "best" (based on observations) position estimate of the mobile position. The resulting residuals and residual error maps are acquired by the residual error monitor/handler for detecting location spoofing attacks (see Chapter 6) and handling excessive location errors (see Chapter 7).

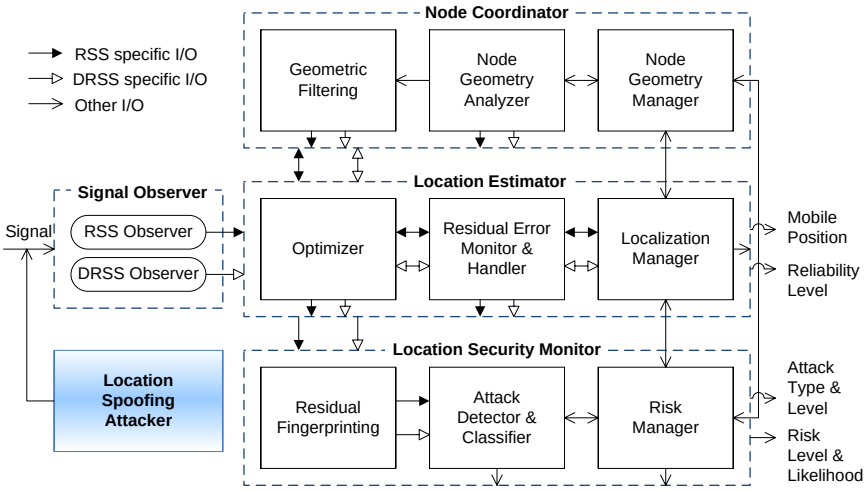


Figure 8.1: Structure of a secure location system based on the hybrid RSS/DRSS framework.

- **Location security monitor**–Provided location estimates and residual error maps, the location security monitor assesses and detects any security risks by either measuring the *relative error norm* or matching *topological residual fingerprints* (see Chapters 6 and 7). The risk manager controls security system parameters (*e.g.*, detection threshold, relative error norm threshold) according to location security policies, and may enforce security access control with respect to the mobile position in the network.

- **Node coordinator**–This module improves the reliability of localization and detection by exploiting the geometry of active anchors (see Chapters 6 and 7). This geometric approach is valuable particularly for locating a stationary target whose channel characteristics are static. In static channel conditions we usually have a single *meaningful* RSS observation at each anchor position, which may be severely corrupted by systematic/environmental bias and error.

8.3 Future Research Directions

As discussed, most location security aspects have been overlooked. Although increasingly more studies are being devoted to this research area, there are still many open research problems. One of the important problems is a theoretical characterization of location uncertainty while generalizing a variety of attack strategies against diverse location systems. Among the many possible views of location uncertainty, one may associate this issue most naturally with classical information uncertainty. Then, we can measure the location uncertainty through its entropy. It can be expected that as the location uncertainty increases (due to a location attack or per user request for his/her privacy), its information entropy becomes higher. An-

other interesting open security issue is regarding the fundamental limits of location security risks. The limits are closely related to theoretical estimator bounds and the bias-variance tradeoff discussed in this work due to the similarity between location security and classical estimation problems. Also, one may design a hybrid TOA/TDOA secure location system based on the principles and results presented here (*i.e.*, replacing the signal observer block in Fig. 8.1). Also, the framework in Fig. 8.1 can be applied to existing TOA/TDOA location systems as a hybrid approach. It is envisioned that the new hybrid system will provide better location accuracy while being secured against location spoofing attacks.

Bibliography

[1] E. Vos, "Survey shows 84 percent want citywide Wi-Fi, 91 percent expect it when traveling," *MuniWireless news*, January 28, 2009, http://www.muniwireless.com/2009/01/28/survey-shows-84-percent-want-citywide-wi-fi/.

[2] L. Luna, "Verizon's Seidenberg: 500 percent penetration achievable," *FierceWirless news*, April 1, 2009, http://www.fiercewireless.com/ctialive/story/verizons-seidenberg-500-percent-penetration-achievable/2009-04-01.

[3] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: scalable coordination in sensor networks," in *Proc. ACM/IEEE Int. Conf. Mobile Computing and Networking*, 1999, pp. 263–270.

[4] J. Mitola III and G. Q. Maguire, Jr., "Cognitive radio: making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, 1999.

[5] G. Lawton, "Machine-to-machine technology gears up for growth," *Computer*, vol. 37, no. 9, pp. 12–15, 2004.

[6] J. Weatherall and A. Jones, "Ubiquitous networks and their applications," *IEEE Wirel. Commun.*, vol. 9, no. 1, pp. 18–29, 2002.

[7] G. Sun, J. Chen, W. Guo, and K. J. R. Liu, "Signal processing techniques in network-aided positioning: a survey of state-of-the-art positioning designs," *IEEE Signal Proc. Mag.*, vol. 22, no. 4, pp. 12–23, 2005.

[8] J. H. Reed, K. J. Krizman, B. D. Woerner, and T. S. Rappaport, "An overview of the challenges and progress in meeting the E-911 requirement for location service," *IEEE Commun. Mag.*, vol. 36, no. 4, pp. 30–37, 1998.

[9] M. Vossiek, L. Wiebking, P. Gulden, J. Wieghardt, C. Hoffmann, and P. Heide, "Wireless local positioning," *IEEE Microwave Mag.*, vol. 4, no. 4, pp. 77–86, 2003.

[10] Y.-B. Ko and N. H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks," in *Proc. Int. Conf. Mobile Computing and Networking*, 1998, pp. 66–75.

[11] A. H. Sayed, A. Tarighat, and N. Khajehnouri, "Network-based wireless location: challenges faced in developing techniques for accurate wireless location information," *IEEE Signal Proc. Mag.*, vol. 22, no. 4, pp. 24–40, 2005.

[12] N. Patwari, J. N. Ash, S. Kyperountas, I. Hero, A.O., R. Moses, and N. Correal, "Locating the nodes: cooperative localization in wireless sensor networks," *IEEE Signal Processing Mag.*, vol. 22, no. 4, pp. 54–69, 2005.

[13] G. Mao, B. Fidan, and B. D. O. Anderson, "Wireless sensor network localization techniques," *ACM Computer Net.*, vol. 51, no. 10, pp. 2529–2553, 2007.

[14] J. H. Lee and R. M. Buehrer, "Location estimation using differential RSS with spatially correlated shadowing," in *Proc. IEEE Global Commun. Conf.*, 2009, pp. 4613–4618.

[15] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proc. IEEE Conf. Comp. Commun.*, vol. 2, 2000, pp. 775–784.

[16] N. Patwari and A. O. Hero III, "Using proximity and quantized RSS for sensor localization in wireless networks," in *Proc. ACM Int. Conf. Wirel. Sensor Net. and Appl.*, 2003, pp. 20–29.

[17] J. Hightower, G. Boriello, and R. Want, "SpotON: An indoor 3D location sensing technology based on RF signal strength," Univ. of Washington, Tech. Rep. CSE 2000-02-02, February 2002.

[18] P. Castro, P. Chiu, T. Kremenek, and R. R. Muntz, "A probabilistic room location service for wireless networked environments," in *Proc. Int. Conf. Atlanta Ubiquitous Computing*, September 2001, pp. 18–34.

[19] B. Parkinson and J. J. Spiker (Ed.), *Global Positioning System: Theory and Applications.* American Institute of Aeronautics & Astronautics, 1996, vol. 1, 2.

[20] G. M. Djuknic and R. E. Richton, "Geolocation and assisted GPS," *IEEE Computer*, vol. 34, no. 2, pp. 123–125, 2001.

[21] R. J. Fontana and S. J. Gunderson, "Ultra-wideband precision asset location system," in *Ultra Wideband Systems and Technologies, 2002. Digest of Papers. 2002 IEEE Conference on*, 2002, pp. 147–150.

[22] J. J. Caffery and G. L. Stuber, "Subscriber location in CDMA cellular networks," *IEEE Trans. Veh. Technol.*, vol. 47, no. 2, pp. 406–416, 1998.

[23] J. Zhang, P. V. Orlik, Z. Sahinoglu, A. F. Molisch, and P. Kinney, "UWB systems for wireless sensor networks," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 313–331, 2009.

[24] D. Dardari, A. Conti, U. Ferner, A. Giorgetti, and M. Z. Win, "Ranging with ultrawide bandwidth signals in multipath environments," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 404–426, 2009.

[25] J. A. Pierce, "An introduction to Loran," *IEEE Aerospace and Electronic Systems Mag.*, vol. 5, no. 10, pp. 16–33, 1990.

[26] A. Savvides, C.-C. Han, and M. B. Strivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proc. Int. Conf. Mobile Computing and Networking*, 2001, pp. 166–179.

[27] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket location-support system," in *Proc. Int. Conf. Mobile Computing and Networking*, 2000, pp. 32–43.

[28] Y. Zhao, "Standardization of mobile phone positioning for 3g systems," *Communications Magazine, IEEE*, vol. 40, no. 7, pp. 108–116, 2002.

[29] D. Niculescu and B. R. Badrinath, "Ad hoc positioning system (APS) using AOA," in *Proc. IEEE Conf. Comp. Commun.*, April 2003, pp. 1734–1743.

[30] P. Biswas, T.-C. Lian, T.-C. Wang, and Y. Ye, "Semidefinite programming based algorithms for sensor network localization," *ACM Trans. Sen. Netw.*, vol. 2, no. 2, pp. 188–220, 2006.

[31] S. Sakagami, S. Aoyama, K. Kuboi, S. Shirota, and A. Akeyama, "Vehicle position estimates by multibeam antennas in multipath environments," *IEEE Trans. Veh. Technol.,*, vol. 41, no. 1, pp. 63–68, 1992.

[32] J. Kennedy and M. C. Sullivan, "Direction finding and "smart antennas" using software radio architectures," *IEEE Commun. Mag.*, vol. 33, no. 5, pp. 62–68, 1995.

[33] *The U.S. Code Title 44, Chapter 35, Subchapter III, §3542–Information Security*, U.S. government Std. Title 44, Chapter 35, Subchapter III, §3542, http://www.law.cornell.edu/uscode/44/3542.html.

[34] E. Bland, "GPS 'spoofing' could threaten national security," *msmbc news*, October 2, 2008, http://www.msnbc.msn.com/id/26992456.

[35] B. M. Ledvina, M. L. Psiaki, S. P. Powell, and P. M. Kintner, "Bit-wise parallel algorithms for efficient software correlation applied to a GPS software receiver," *IEEE Trans. Wirel. Commun.*, vol. 3, no. 5, pp. 1469–1473, 2004.

[36] N. O. Tippenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, "iPhone and iPod location spoofing: Attacks on public WLAN-based positioning systems," SysSec Technical Report. ETH Zurich, April, 2008.

[37] H. F. Lipson, "Tracking and tracing cyber attacks: Technical challenges and global policy issues," CMU, Tech. Rep. CMU/SEI-2002-SR-009, November 2002.

[38] M. Snow and J.-M. Park, "Link-layer traceback in Ethernet networks," in *Proc. IEEE Workshop on Local & Metropolitan Area Networks*, 2007, pp. 182–187.

[39] D. Harrington, R. Presuhn, and B. Wijnen, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*, ser. RFC 3411. RFC Editor, 2002.

[40] T. S. Rappapport, *Wireless Communications: Principles and Practice*, 2nd ed. New Jersey: Prentice-Hall, 2002.

[41] D. Faria and D. Cheriton, "No long-term secrets: Location-based security in overprovisioned wireless LANs," in *Proc. ACM Workshop on Hot Topics in Networks*, vol. 1, November 2004, pp. 212–222.

[42] J. Yang, Y. Chen, and W. Trappe, "Detecting sybil attacks in wireless and sensor networks using cluster analysis," in *Proc. Int. Conf. Mobile Ad Hoc and Sensor Systems*, 2008, pp. 834–839.

[43] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "Rogue access point detection using temporal traffic characteristics," in *Proc. IEEE Global Telecommun. Conf.*, vol. 4, 2004, pp. 2271–2275.

[44] M. Liran, A. Y. Teymorian, and C. Xiuzhen, "A hybrid rogue access point protection framework for commodity Wi-Fi networks," in *Proc. IEEE Conf. Comp. Commun.*, 2008, pp. 1220–1228.

[45] Y. Chen, W. Trappe, and R. P. Martin, "Attack detection in wireless localization," in *Proc. IEEE Conf. Comp. Commun.*, 2007, pp. 1964–1972.

[46] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker, "The directional attack on wireless localization -or- how to spoof your location with a tin can," in *Proc. IEEE Global Commun. Conf.*, pp. 4125–4130.

[47] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM Workshop on Wirel. Secur.* ACM, 2003, pp. 1–10.

[48] L. Lazos, P. Radha, and S. Capkun, "ROPE: robust position estimation in wireless sensor networks," in *Proc. IEEE/ACM Int. Conf. Information Processing in Sensor Networks*, 2005, pp. 324–331.

[49] S. Capkun and J. P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Selected Areas in Commun.*, vol. 24, no. 2, pp. 221–232, 2006.

[50] L. Lazos and R. Poovendran, "SeRLoc: Robust localization for wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 1, no. 1, pp. 73–100, 2005.

[51] D. Liu, P. Ning, A. Liu, C. Wang, and W. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 4, pp. 1–39, 2008.

[52] W. Du, L. Fang, and P. Ning, "LAD: Localization anomaly detection for wireless sensor networks," in *Proc. IEEE Parallel and Dist. Proc. Symposium*, 2005, p. 41.

[53] Z. Li, W. Trappe, Y. Zhang, and N. Badri, "Robust statistical methods for securing wireless localization in sensor networks," in *Proc. Int. Symp. Info. Proc. in Sensor Networks*, 2005, pp. 91–98.

[54] L. Lazos and R. Poovendran, "HiRLoc: high-resolution robust localization for wireless sensor networks," *IEEE J. Selected Areas in Commun.*, vol. 24, no. 2, pp. 233–246, 2006.

[55] J. H. Lee and R. M. Buehrer, "Fundamentals of received signal strength based position location," in *Position Location–Theory, Practice and Advances: A Handbook for Engineers and Academics*, S. A. Zekavat and R. M. Buehrer, Eds. New York, NY: Wiley-IEEE Press, 2011.

[56] ——, "Security issues for position location," in *Position Location–Theory, Practice and Advances: A Handbook for Engineers and Academics*, S. A. Zekavat and R. M. Buehrer, Eds. New York, NY: Wiley-IEEE Press, 2011.

[57] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory.* New Jersey: Prentice-Hall, 1993.

[58] H. Wymeersch, J. Lien, and M. Z. Win, "Cooperative localization in wireless networks," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 427–450, 2009.

[59] I. Guvenc and C.-C. Chong, "A survey on TOA based wireless localization and NLOS mitigation techniques," *Communications Surveys & Tutorials, IEEE*, vol. 11, no. 3, pp. 107–124, 2009.

[60] P.-C. Chen, "A non-line-of-sight error mitigation algorithm in location estimation," in *Proc. IEEE Wirel. Commun. and Networking Conf.*, 1999, pp. 316–320.

[61] L. Cong and W. Zhuang, "Non-line-of-sight error mitigation in TDOA mobile location," in *Proc. IEEE Global Telecommum. Conf.*, vol. 1, 2001, pp. 680–684.

[62] L. Xiong, "A selective model to suppress NLOS signals in angle-of-arrival (AOA) location estimation," in *Proc. IEEE Symposium on Personal, Indoor and Mobile Radio Commun.*, vol. 1, 1998, pp. 461–465.

[63] J. C. Liberti and T. S. Rappaport, "Statistics of shadowing in indoor radio channels at 900 and 1900 MHz," in *Proc. IEEE Military Commun. Conf.*, vol. 3, 1992, pp. 1066–1070.

[64] K. Zayana and B. Guisnet, "Measurements and modelisation of shadowing cross-correlations between two base-stations," in *Proc. IEEE Int. Conf. Univ. Pers. Comm.*, vol. 1, 1998, pp. 101–105.

[65] V. Fox, J. Hightower, L. Liao, D. Schulz, and G. Borriello, "Bayesian filtering for location estimation," *IEEE Pervasive Computing*, vol. 2, no. 3, pp. 24–33, 2003.

[66] M. S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp, "A tutorial on particle filters for online nonlinear/non-Gaussian Bayesian tracking," *IEEE Trans. Signal Processing*, vol. 50, no. 2, pp. 174–188, 2002.

[67] M. A. Spirito, "On the accuracy of cellular mobile station location estimation," *IEEE Trans. Veh. Technol.*, vol. 50, no. 3, pp. 674–685, 2001.

[68] D. B. Jourdan and N. Roy, "Optimal sensor placement for agent localization," *ACM Trans. Sen. Netw.*, vol. 4, no. 3, pp. 1–40, 2008.

[69] L. M. Kaplan, "Local node selection for localization in a distributed sensor network," *IEEE Trans. Aerospace and Electronic Systems*, vol. 42, no. 1, pp. 136–146, 2006.

[70] ——, "Global node selection for localization in a distributed sensor network," *IEEE Trans. Aerospace and Electronic Systems*, vol. 42, no. 1, pp. 113–135, 2006.

[71] P. Ioannides and C. A. Balanis, "Uniform circular arrays for smart antennas," *IEEE Antennas and Propagation Mag.*, vol. 47, no. 4, pp. 192–206, 2005.

[72] W. L. Stutzman and G. A. Thiele, *Antenna Theory and Design*, 2nd ed. New York: Wiley, 1998.

[73] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electronics Lett.*, vol. 27, no. 23, pp. 2145–2146, 1991.

[74] Z. Wang, E. K. Tameh, and A. Nix, "Simulating correlated shadowing in mobile multi-hop relay/ad-hoc networks," IEEE 802.16 Broadband Wireless Access Working Group, Tech. Rep., 2006.

[75] G. Golub and C. Van Loan, *Matrix Computations*, 3rd ed. Baltimore: Johns Hopkins Univ. Press, 1996.

[76] H. B. Lee, "A novel procedure for assessing the accuracy of hyperbolic multilateration systems," *IEEE Trans. Aerospace and Electronic Systems*, vol. AES-11, no. 1, pp. 2–15, 1975.

[77] D. J. Torrieri, "Statistical theory of passive location systems," *IEEE Trans. Aerospace and Electronic Systems,*, vol. AES-20, no. 2, pp. 183–198, 1984.

[78] J. Smith and J. Abel, "Closed-form least-squares source location estimation from range-difference measurements," *IEEE Trans. Acoustics, Speech and Signal Processing*, vol. 35, no. 12, pp. 1661–1669, Dec 1987.

[79] A. J. Coulson, A. G. Williamson, and R. G. Vaughan, "A statistical basis for lognormal shadowing effects in multipath fading channels," *IEEE Trans. Commun.*, vol. 46, no. 4, pp. 494–502, 1998.

[80] N. Patwari and P. Agrawal, "Effects of correlated shadowing: Connectivity, localization, and RF tomography," in *Proc. IEEE/ACM Int. Conf. Information Processing in Sensor Networks*, 2008, pp. 82–93.

[81] N. Patwari, I. Hero, A. O., M. Perkins, N. S. Correal, and R. J. O'Dea, "Relative location estimation in wireless sensor networks," *IEEE Trans. Signal Processing*, vol. 51, no. 8, pp. 2137–2148, 2003.

[82] J. B. Tenenbaum, V. d. Silva, and J. C. Langford, "A global geometric framework for nonlinear dimensionality reduction," *Science*, vol. 290, no. 5500, pp. 2319–2323, 2000.

[83] S. T. Roweis and L. K. Saul, "Nonlinear dimensionality reduction by locally linear embedding," *Science*, vol. 290, no. 5500, pp. 2323–2326, 2000.

[84] I. Borg and P. Groenen, *Multidimensional Scaling, Theory and Applications.* New York: Springer-Verlag, 1997.

[85] D. L. Donoho and C. Grimes, "Hessian eigenmaps: new locally linear embedding techniques for high-dimensional data," *PNAS*, vol. 100, no. 10, pp. 5591–5596, May 2003.

[86] M. Belkin and P. Niyogi, "Laplacian eigenmaps for dimensionality reduction and data representation," *Neural Computation*, vol. 15, no. 6, pp. 1373–1396, 2003.

[87] W. S. Torgeson, "Multidimensional scaling of similarity," *Psychometrika*, vol. 30, no. 1, pp. 379–393, 1965.

[88] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz, "Localization from mere connectivity," in *Proc. ACM Int. Symp. Mobile Ad Hoc Networking and Computing*, 2003, pp. 201–212.

[89] N. Patwari and I. Hero, A. O., "Manifold learning algorithms for localization in wireless sensor networks," in *Proc. IEEE Conf. Acoustics, Speech, and Signal Proc.*, vol. 3, pp. III–857–860.

[90] G. Peyre, "A toolbox for dimension reduction methods," 2006, http://www.mathworks.com/matlabcentral/fileexchange/.

[91] S. Capkun, M. Hamdi, and J. P. Hubaux, "GPS-free positioning in mobile ad-hoc networks," in *Proc. Hawaii Int. Conf. Sys. Sci.*, 2001, pp. 3481–3490.

[92] H. Wu, C. Wang, and N.-F. Tzeng, "Novel self-configurable positioning technique for multihop wireless networks," *IEEE/ACM Trans. Networking*, vol. 13, no. 3, pp. 609–621, 2005.

[93] X. Li, "RSS-based location estimation with unknown pathloss model," *Wireless Communications, IEEE Transactions on*, vol. 5, no. 12, pp. 3626–3633, 2006.

[94] I. Hero, A. O., J. A. Fessler, and M. Usman, "Exploring estimator bias-variance tradeoffs using the uniform CR bound," *IEEE Trans. Signal Processing*, vol. 44, no. 8, pp. 2026–2041, 1996.

[95] S. Kay and Y. C. Eldar, "Rethinking biased estimation [lecture notes]," *IEEE Signal Processing Mag.*, vol. 25, no. 3, pp. 133–136, 2008.

[96] W. Wothke, "Nonpositive definite matrices in structural modeling," in *Testing Structural Equation Models*, K. Bollen and J. Long, Eds. Newbury Park, CA: Sage, 1993, vol. 67, no. 1, pp. 256–293.

[97] R. H. Byrd, R. B. Schnabel, and G. A. Shultz, "Approximate solution of the trust region problem by minimization over two-dimensional subspaces," *Math. Programming*, vol. 40, no. 1, pp. 247–263, 1988.

[98] W. Hahn and S. Tretter, "Optimum processing for delay-vector estimation in passive signal arrays," *IEEE Trans. Information Theory*, vol. 19, no. 5, pp. 608–614, 1973.

[99] M. S. Bazaraa, Sherali, H. D., and C. M. Shetty, *Nonlinear Programming: Theory and Algorithms*, 3rd ed. New York: Wiley, 2006.

[100] G. A. Shultz, R. B. Schnabel, and R. H. Byrd, "A family of trust-region-based algorithms for unconstrained minimization with strong global convergence properties," *SIAM Journal on Numerical Analysis*, vol. 22, no. 1, pp. 47–67, 1985.

[101] M. A. Branch, T. F. Coleman, and Y. Li, "A subspace, interior, and conjugate gradient method for large-scale bound-constrained minimization problems," *SIAM Journal on Scientific Computing*, vol. 21, no. 1, pp. 1–23, 1999.

[102] T. F. Coleman and Y. Li, "An interior trust region approach for nonlinear minimization subject to bounds," *SIAM Journal on Optimization*, vol. 6, no. 2, pp. 418–445, 1996.

[103] S. Venkatesh and R. M. Buehrer, "A linear programming approach to NLOS error mitigation in sensor networks," in *Proc. IEEE/ACM Int. Conf. Information Processing in Sensor Networks*, 2006, pp. 301–308.

[104] J. J. Caffery, "A new approach to the geometry of TOA location," in *Proc. IEEE Veh. Technol. Conf.*, vol. 4, 2000, pp. 1943–1949.

[105] J. Reed, *Software radio: a modern approach to radio engineering.* Upper Saddle River, NJ: Prentice Hall Press, 2002.

[106] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *Proc. IEEE Sensor, Mesh and Ad Hoc Commun. and Net.*, 2007, pp. 193–202.

[107] S. Brands and D. Chaum, "Distance-bounding protocols," in *Workshop on Theory and Application of Cryptographic Techniques on Advances in Cryptology*, 1994, pp. 344–359.

[108] S. Ray, R. Ungrangsi, P. De, A. Trachtenberg, and D. Starobinski, "Robust location detection in emergency sensor networks," in *Proc. IEEE Conf. Comp. Commun.*, vol. 2, 2003, pp. 1044–1053.

[109] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless LANs," in *Proc. ACM Int. Conf. Mobile Syst., App. and Servi.*, 2007, pp. 246–257.

[110] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Trans. Mobile Computing*, vol. 7, no. 1, pp. 1–18, 2008.

[111] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. ACM Int. Conf. Mobile Systems, Applications, and Services*, 2003, pp. 31–42.

[112] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J.-M. Tang, "Framework for security and privacy in automotive telematics," in *Proc. ACM Int. Workshop Mobile Commerce*, 2002, pp. 25–32.

[113] F. Gini, "Estimation strategies in the presence of nuisance parameters," *Signal Processing*, vol. 55, no. 2, pp. 241–245, 1996.

[114] J. Beyerer, "Is it useful to know a nuisance parameter?" *Signal Processing*, vol. 68, no. 1, pp. 107–111, 1998.

[115] S. Kotz, T. Kozubowski, and K. Podgorski, *The Laplace Distribution and Generalizations: A Revisit With Applications to Communications, Economics, Engineering, and Finance*, Boston.

[116] Y. C. Eldar, "Minimum variance in biased estimation: bounds and asymptotically optimal estimators," *IEEE Trans. Signal Processing*, vol. 52, no. 7, pp. 1915–1930, 2004.

[117] ——, "Uniformly improving the Cramer-Rao bound and maximum-likelihood estimation," *IEEE Trans. Signal Processing*, vol. 54, no. 8, pp. 2943–2956, 2006.

[118] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, 2009.

[119] R. L. Graham, "An efficient algorithm for determining the convex hull of a finite planar set," *Inform. Process. Lett.*, vol. 1, no. 4, pp. 132–133, 1972.

[120] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory, vol. II.* New Jersey: Prentice-Hall, 1998.

[121] E. B. Wilson, "First and second laws of error," *Journal of the American Statistical Assoc.*, vol. 18, no. 143, pp. 841–851, 1923.

[122] S. Slijepcevic, S. Megerian, and M. Potkonjak, "Characterization of location error in wireless sensor networks: analysis and applications," in *Proc. Int. Conf. Information Processing in Sensor Networks*, 2003, pp. 593–608.

[123] N. B. Priyantha, H. Balakrishnan, E. D. Demaine, and S. Teller, "Mobile-assisted localization in wireless sensor networks," in *Proc. IEEE Conf. Comp. Commun.*, vol. 1, 2005, pp. 172–183.

[124] R. A. Granger, *Fluid Mechanics.* New York: Holt, Rinehart, and Winston, 1985.

[125] P. J. Huber, *Robust statistics.* New York: Wiley, 1981.