SECURING WIRELESS LOCALIZATION AGAINST SIGNAL STRENGTH ATTACKS

BY YINGYING CHEN

A dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Computer Science

Written under the direction of

Prof. Richard P. Martin and Prof. Wade Trappe

and approved by

_____

_____

_____

_____

New Brunswick, New Jersey

October, 2007

ABSTRACT OF THE DISSERTATION

Securing Wireless Localization against Signal Strength Attacks

by Yingying Chen

Dissertation Director: Prof. Richard P. Martin and Prof. Wade Trappe

Accurately positioning nodes in wireless and sensor networks is important because the location of devices and sensors is a critical input to many higher-level applications. However, the localization infrastructure can be subjected to non-cryptographic attacks, such as signal attenuation and amplification, that can not be addressed by traditional security services. This thesis aims to provide secure and accurate location information in wireless and sensor networks by characterizing the response of localization algorithms to attacks, detecting attacks, localizing adversaries, and additionally, improving localization performance.

First we studied the robustness of localization algorithms to signal strength attacks. We found the performance of localization algorithms degrades significantly under attacks when signals are attenuated or amplified by an adversary. We then formulated a theoretical foundation for the attack detection problem using statistical significance testing. We proposed attack detection schemes for two broad localization approaches: signal strength and multilateration. We found that different localization systems all contain similar attack detection capabilities. Next, we examined the applicability of localization methods to localize adversaries participating in identity-based spoofing attacks. We proposed a spoofing detector for wireless spoofing that utilizes K-means cluster analysis. We integrated our K-means attack detector into a real-time indoor localization system, which is capable of localizing the positions of attackers. Our

experiments using both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network in two office buildings provide strong evidence of the effectiveness of our approach in attack detection and localizing the positions of the adversaries.

In addition, we investigated the impact of landmark placement on localization performance using a combination of analytic and experimental analysis. We developed a novel algorithm called $maxL - minE$ algorithm that finds an optimized landmark deployment. Our experimental results show that our landmark placement algorithm is generic because the resulting placements improve localization performance significantly across a diverse set of algorithms, networks, and ranging modalities. Finally, we presented our general purpose real time localization infrastructure which targets to localize any radio-enabled wireless devices at anywhere and at anytime.

Acknowledgements

This dissertation is an accumulation of much work, guidance, support, and the friendship of many people.

First and foremost, I am deeply thankful for my two advisers, Prof. Richard P. Martin and Prof. Wade Trappe. Without their invaluable guidance and support, I would not be able to make rapid progress in my research work. Especially, I would like to express my gratitude to them for attending numerous discussions, listening to my practice talks, and helping me improve my writing and presentation skills. I have been very fortunate to have the opportunity to work with both of them.

I must also thank the many professors and researchers that provided me advice and helped my research development during my studies at Rutgers. In particular, I would like to thank Prof. David Madigan, Prof. Dipankar Raychaudhuri, Prof. Yanyong Zhang, Prof. Larry Greenstein, Prof. Naftaly Minsky, and Dr. Wei Su for their advice and feedback throughout different stages of my study.

Further, I would like to thank my colleagues in the Computer Science Department and in WINLAB at Rutgers University who have helped me along the way with stimulating discussions and interesting talks.

My parents, who both are professors in the Physics Department at Nanjing University, deserve much credit. I would like to thank them for the continuous encouragement, support, and advice through these long years.

Finally, to my husband, Jerry Cheng, and lovely son, Jeffrey Cheng, I must thank for giving me the love, support, understanding, and patience to keep me going through the difficult times.

Dedication

To my parents, Kunji Chen and Xinfan Huang

To my husband, Jerry Cheng

To my lovely son, Jeffrey Cheng

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Background and Motivation

Wireless networks are changing the way we work, study, and interact with each other. As wireless networks become increasingly prevalent, they make integrating new information types into applications possible. Location information is one such information source that is very important for many applications. Localization refers to determining the physical position of a wireless device or a sensor node which can be either static or mobile. The location information can be one-dimensional (e.g., location on a long airport corridor), two-dimensional (e.g., location on one floor in a hospital), or three-dimensional (e.g., location within a multi-level shopping mall). For example, in the public arena, doctors want to use location information to track and monitor patients in medical facilities; for wild life observation, biologists can put tags on animals and perform habitat tracking; first responders can track victims and each other during an emergency. In the enterprise domain, location-based access control is needed for accessing the proprietary corporate materials in restricted areas or rooms. For example, during meetings, certain documents may need to be sent only to laptops within the involved conference rooms, which requires location-aware content delivery. In addition, asset tracking also relies on location information. These examples show that accurately positioning nodes in wireless and sensor networks is important as the location of sensors is a critical input to many high-level networking tasks and applications.

With recent great advances in wireless technology, there are three wireless communication standards that have conjoined with our everyday life and have further promised to realize location-based services: First, Wireless Local Area Networks (WLANs) usually refer to networks based on $WiFi$ technology functioning according to IEEE 802.11 standards [4]. The normal infrastructure for a WiFi network consists of one or more Access Points (APs), which

has the ability to do wireless transmission and also serves as a gateway to a wired network. WiFi devices can thus connect to the Internet and talk to each other through APs. The most popular WiFi devices are laptops and Personal Digital Assistants (PDAs). Second, $Bluetooth$ technology uses IEEE 802.15.1 standards [5] and is designed for lower power consumption, and thus has a relatively shorter range around 10 meters. It is mostly used for communication between devices closely located to each other. Currently many devices support Bluetooth including laptops, cell phones, headsets, mouses, and digital cameras. Finally, $ZigBee$ implements IEEE 802.15.4 standards [6] and targets for sensor networks with embedded applications such as environmental monitoring, data collection, and intruder detection. Because of the nature of embedded applications, the corresponding devices utilizing ZigBee protocol are required to be small. The current available ones are about the size of a quarter [3, 7].

In wireless and sensor networks, there are various physical modalities can be employed to perform localization such as Received Signal Strength (RSS), Time of Arrival (TOA), Angle of Arrival (AOA), Hop Counts, and etc.. Among the localization techniques, utilizing RSS is especially attractive since it can reuse the existing deployment of wireless communication networks, rather than require a specialized localization infrastructure such as ultrasound or infrared methods. This provides tremendous cost savings. Also, all current standard commodity radio technologies, such as 802.11, 802.15.4, and Bluetooth provide it, and thus the same algorithms can be applied across different platforms. Further, based on the information obtained from physical modalities, different principles can be used to determine the positions of sensors. There has been active research in developing localization algorithms using lateration [23, 28, 44, 49, 54], angulation [53], probabilistic approaches [59, 69], and statistical supervised learning techniques [12, 27, 52]. We detail these efforts in Chapter 7.

However, in spite of the utility of the location information, it is only useful if the location information is accurate and trustworthy. As more location-dependent services are deployed, they will increasingly become tempting targets for malicious attacks. Unlike traditional systems, the localization infrastructure is sensitive to a variety of attacks, ranging from conventional to non-cryptographic, that can subvert the utility of location information. Conventional attacks, where an adversary injects false messages, can be isolated and protected against using

traditional cryptographic methods such as authentication. However, there is a completely orthogonal set of attacks that are non-cryptographic, where the measurement process itself can be corrupted by adversaries. For instance, an adversary could introduce an absorbing barrier between the transmitter and the target, changing the underlying propagation physics. As the signal propagates through the barrier, it is attenuated, and hence the target would observe a significantly lower received signal strength. Consequently, the receiver would conclude that it is further from the transmitter than it actually is. On the other hand, wormhole attacks tunnel through a faster channel to shorten the observed distance between two nodes. Unfortunately, these non-cryptographic attacks can not be addressed by traditional security services. Thus, it is desirable to study the impact of these attacks on localization algorithms and explore methods to detect and further to eliminate these attacks from the network. This is the focus of this thesis. We are motivated to develop solutions that can be integrated into early generations of localization systems, so that we will not have to apply patchwork solutions to solve security threats that arise after localization systems are deployed.

Specifically, in this thesis work we first performed a thorough study on the robustness of a broad array of localization algorithms to attacks that corrupt signal strength readings. The characterization of the response of algorithms provides important insights to be taken into consideration by system designers when choosing localization systems for deployment. From the robustness study, we observed that attackers can cause large localization errors using simple techniques. Hence, we must detect the presence of attacks in the network. We then formulate the attack detection problem as a generic statistical significance testing problem and proposed several attack detection schemes to broad classes of multilateration and signal strength-based methods. After a localization attack is detected in a wireless network, the next important and challenging step is to localize the positions of adversaries and further to eliminate the attack from the network. We proposed to use K-means cluster analysis to detect identity-based spoofing attacks and applied localization methods to locate adversaries participating in a spoofing attack.

During the course of the security analysis for localization systems, we found that the landmark (a node with known position) placement plays an important role on localization performance. It is desirable to obtain higher location accuracy. In this investigation, we focused on

improving localization performance by repositioning the landmarks, rather than improving the localization algorithms or searching for new algorithms, and this should help a wide variety of algorithms. By using a combination of analytic and experimental analysis, we found geometric descriptions for the optimal deployment of landmark placement to maximize the location accuracy for indoor localization.

Finally, one of the primary goals of localization research is to provide a scalable, general purpose, and real time localization infrastructure that can integrate location information into any computing radio-enabled devices. We are designing and developing a general purpose localization system prototype called GRAIL (Generalized Real-time Adaptable Indoor Localization), which can simultaneously position multiple devices using Bayesian Networks. The deployment of such a system in academic and research environments will allow researchers to explore issues beyond just algorithms and simulation tools, which can facilitate a variety of research topics such as privacy studies, security services, and policy enforcements. In addition, the practical usage of such an approach is significant as it can be applied to a broad array of applications such as monitoring, tracking, routing, and security services.

1.2 Thesis Organization

This thesis is focused on to provide accurate and trustworthy location information to location-based applications, and toward a general purpose localization infrastructure. The structure of the thesis is organized as follows.

In Chapter 2, we characterize the response of localization algorithms to attacks where an adversary attenuates or amplifies the signal strength at one or more landmarks. We study both point-based and area-based methods that employ received signal strength for localization, and propose several performance metrics that quantify the estimator's precision and error, including Hölder metrics, which quantify the variability in position space for a given variability in signal strength space. We then conduct a trace-driven evaluation of several point-based and area-based algorithms, where we measured their performance as we applied attacks on real data from two different buildings. We observed both strong experimental and theoretic evidence that all the algorithms have similar average responses to signal strength attacks.

Next, in Chapter 3, we propose several attack detection schemes for wireless localization systems. We first formulate a theoretical foundation for the attack detection problem using statistical significance testing. Next, we define test metrics for two broad localization approaches: multilateration and signal strength. We then derived both mathematical models and analytic solutions for attack detection for any system that utilizes those approaches. We also studied additional test statistics that are specific to a diverse set of algorithms. Our trace-driven experimental results provide strong evidence of the effectiveness of our attack detection schemes with high detection rates and low false positive rates across both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network in two real office buildings.

Further, wireless and sensor networks are especially vulnerable to identity-based spoofing attacks, which allows for many other forms of attacks in networks. It is desirable to detect the presence of spoofing and eliminate them from the network. Although the identity of a node can be verified through cryptographic authentication, authentication is not always possible because it requires key management and additional infrastructural overhead. In Chapter 4, we take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. Specifically, we proposed a scheme for both detecting spoofing attacks, as well as localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. We describe how we integrated our attack detector into a real-time indoor localization system, which is also capable of localizing the positions of the attackers. We show that the positions of the attackers can be localized using either area-based or point-based localization algorithms with the same relative errors as in the normal case through experimentation using both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network.

In Chapter 5, We investigate the impact of landmark placement on localization performance using a combination of analytic and experimental analysis. Our analysis of landmark placement can find an optimal placement of landmarks in well-defined regular regions, thus making it quite suitable for indoor localization. The analysis places an upper bound of the maximum localization error given a set of landmark placements. We can show that this upper bound is minimized by a combination of minimizing the distance estimation error together with the employment of the optimal patterns for landmark placement. Using this result, we can compare

the maximum error between any two placements. We can then constrain a search of placements to minimize the maximum error. We have developed a simple algorithm called $maxL - minE$ algorithm that finds an optimized landmark deployment for the LLS algorithm.

In summary, to ensure the trustworthiness of the location information, first we characterize the response of localization algorithms to signal strength attacks in Chapter 2. Then, in Chapter 3, we propose attack detection mechanisms in wireless localization. We next propose a method for both detecting and localizing spoofing attacks in Chapter 4. In addition, in order to improve the localization performance, we investigate the impact of landmark placement in Chapter 5. Moreover, we present the system architecture of our general purpose localization infrastructure in Chapter 6. In Chapter 7, we compare and contrast our work to the previous research work. Finally, we conclude our thesis in Chapter 8 and present future research directions.

1.3 Contributions

Our contributions in this thesis are:

We first characterized the response of localization algorithms to signal strength attacks. Specifically, we proposed a new set of metrics, Hölder metrics, which relate the magnitude of the perturbation in signal space to its effect on the localization result in physical space and thus measure the susceptibility of localization algorithms to signal attacks. We found that all the algorithms degraded gracefully, with a linear response as a function of the attack strength. And as a rule of thumb, it is easy to attack by 15 dB and cause localization errors by 20-30 feet. We observed that the localization using Bayesian Networks is more robust than other algorithms under attacks that target individual landmarks.

We developed a theoretical foundation of attack detection using statistical significance testing. We built test statistics for two broad localization approaches: multilateration and signal strength. For multilateration that uses Linear Least Squares, we derived a closed-form representation for the attack detector. Moreover, for localization schemes that employ signal strength, we showed that by utilizing the signal strength as a common feature, the minimum Euclidean distance in the signal space can be used as a test statistic for attack detection independent of

the localization process. The key advantage of our approach for signal strength based methods is that the detection phase can be performed prior to localization and thus results in localization computation cost savings under attack. Further, we derived additional test statistics for a selection of representative localization algorithms.

We validated the effectiveness and generality of our attack detection schemes using a trace-driven evaluation across a diverse set of algorithms, networks, and buildings. we found that the performance of the different attack detection schemes are more similar than different. This result shows that different localization systems have similar attack detection capabilities, and consequently that system designers can focus on using algorithms that provide the highest localization accuracy rather than having to trade off position accuracy against attack detection abilities.

Further, we developed a method for detecting spoofing attacks as well as localizing the adversaries in wireless and sensor networks. We applied our generic statistical significance testing formulation for spoofing detection problem. We then utilized the K-means cluster analysis to derive the spoofing detector.

Moreover, we have built a real-time localization system and integrated our K-means spoofing detector into the system to locate the positions of the attackers and as a result to eliminate the adversaries from the network. our experimental results provide strong evidence of the effectiveness of our approach in detecting the spoofing attacks and localizing the positions of the adversaries.

In addition, we took a distinctive approach to investigate the impact of landmark placement on localization performance. By analyzing the Linear Least Squares algorithm, we derived an upper bound on the maximum location error given the placement of landmarks. Based on this theoretical analysis, we found optimal patterns for landmark placement and further developed a novel algorithm, $maxL - minE$, for finding optimal landmark placement that minimizes the maximum localization error. We found that the performance of a wide variety of algorithms showed significant improvements, about 30%, when using landmarks placed according to our algorithm, as opposed to alternate deployments. The experimental results provide strong evidence that our analysis and algorithm for landmark placement is very generic as the resulting placement has improved localization performance across a diverse set of algorithms, networks,

and ranging modalities.

Finally, we presented a system prototype of a general purpose, real time, and scalable localization infrastructure. It aims to incorporate different localization properties and radios. In university research communities, this general purpose localization infrastructure enables researchers to explore issues beyond theoretical algorithms and simulation approaches. It makes further higher-level integrated research investigation possible including privacy studies and security services.

Chapter 2

Robustness Analysis of Localization Algorithms to Signal Strength Attacks

2.1 Introduction

Out of the myriad of localization methods proposed over the last few years, algorithms that use Received Signal Strength (RSS) as the basis of localization are very attractive options as using RSS allows the localization system to reuse the existing communication infrastructure, rather than requiring the additional cost needed to deploy specialized localization infrastructure, such as ceiling-based ultrasound, GPS, or infrared methods [35, 56, 62]. In particular, all commodity radio technologies, such as 802.11, 802.15.4, and Bluetooth provide RSS values associated with packet reception, and thus localization services can easily be built for such systems. Further, RSS-based localization is attractive as the techniques are technology-independent: an algorithm can be developed and applied across different platforms, whether 802.11 or Bluetooth. In addition, it provides reasonable accuracy with median errors of 1 to 5 meters [27]. However, as more location-dependent services are deployed, they will increasingly become tempting targets for malicious attacks. Adversaries may alter signal strength measurements for the purpose of accessing services that are based on location information (e.g. WLAN access may only be granted to devices inside of a building.). In this chapter, we thus investigate the susceptibility of a wide range of signal strength localization algorithms to attacks on the Received Signal Strength (RSS). Specifically, we examine the response of several localization algorithms to unanticipated power losses and gains, i.e. attenuation and amplification attacks.

Conventional attacks, where an adversary injects false messages, can be isolated and protected against using traditional cryptographic methods, such as authentication. However, there is a completely orthogonal set of attacks that are non-cryptographic, where the measurement process itself can be corrupted by adversaries. Unfortunately, these non-cryptographic attacks

cannot be addressed by traditional security services. Thus, it is desirable to study the impact of these attacks on localization algorithms and explore methods to detect and further to eliminate these attacks from the network. Although there has been recent research on securing localization [17–19, 49, 51, 61], to date there has been no study on the robustness of the existing generation of RSS-based localization algorithms to physical attacks. Our evaluation is a valuable contribution to a wireless sensor network designer. Because it helps drive protocol decisions, and allows the engineer to decide whether more complicated secure localization algorithms are truly necessary.

In the physical attacks that we study, the attacker modifies the RSS of a sensor node or landmark, for example, by placing an absorbing or reflecting material around the node or landmark. Notably, we study the set of representative attack scenarios on amplification or attenuation attacks on single landmark, all-landmark and combinations of landmarks. Further we analyze the results of simultaneous amplification and attenuation on multiple landmarks. We investigate both point-based and area-based algorithms that utilize RSS to perform localization. In order to evaluate the robustness of these algorithms, we provide a generalized characterization of the localization problem, and then present several performance metrics suitable for quantifying performance, including estimator angle bias, estimator distance error, and estimator precision. Additionally, an essential contribution of our work is the introduction of a new family of localization performance metrics, which we call Hölder metrics. These metrics quantify the susceptibility of localization algorithms to perturbations in signal strength readings. We use worst-case and average-case versions of the Hölder metric, which describe the maximum and average variability as a function of changes in the RSS. We then experimentally evaluate the performance of a wide variety of localization algorithms after applying attenuation and amplification attacks to real data measured from two different office buildings.

Using experimentally observed localization performance, we found that the error for a wide variety of algorithms scaled with surprising similarity under attack. The single exception was the Bayesian Networks algorithm, which degraded slower than the others in response to attacks against a single landmark. In addition to our experimental observations, we found a similar average-case response of the algorithms using our Hölder metrics. However, we observed that methods which returned an average of likely positions had less variability and are thus less

susceptible than other methods.

We also observed that all algorithms degraded gracefully, experiencing linear scaling in localization error as a function of the amount of loss or gain (in dB) an attack introduced. This observation applied to various statistical descriptions of the error, leading us to conclude that no algorithm "collapses" in response to an attack. This is important because it means that, for all the algorithms we examined, there is no tipping point at which an attacker can cause gross errors. In particular, we found the mean error of most of the algorithms for both buildings scaled between 1.3-1.8 ft/dB when all the landmarks were attacked simultaneously, and 0.5-0.8 ft/dB when attacked a single landmark. Additionally, the performance of the mean response of algorithms with multiple landmarks under attack is between the all-landmarks attack and the single landmark attack, which scaled at 0.4-1.4 ft/dB. Further we observed that mixed attacks with simultaneous attenuation and amplification cause the mean response of algorithms to move faster, ranging from 0.2-2.3 ft/dB. More powerful affects were witnessed when the mixed attack was applied to landmarks that were further apart from each other. We also showed experimentally that RSS can be easily attenuated by 15 dB, and that, as a general rule of thumb, very simple signal strength attacks can lead to localization errors of 20-30 ft.

Finally, we conducted a detailed evaluation of area-based algorithms as this family of algorithms return a set of potential locations for the transmitter. Thus, it is possible that these algorithms might return a set with a larger area in response to an attack and could have less precision (or more uncertainty) under attack. However, we found all three of our area-based algorithms shifted the returned areas rather than increased returned area. Further, one of the algorithms, the Area Based Probability (ABP) scheme, significantly shrank the size of the returned area in response to very large changes in signal strength.

The rest of this chapter is organized as follows. We begin, in Section 2.2, by giving an overview of the algorithms used in our performance study and discuss how signal strength attacks can be performed in Section 2.3. In Section 2.4, we provide a formal model of the localization problem as well as introduce the metrics that we use in this chapter. We then examine the performance of the algorithms through an experimental study in Section 2.5, and discuss the Hölder metrics for these algorithms in Section 2.6. Finally, we conclude in Section 2.7.

2.2 Localization Algorithms

Signal strength is a common physical property used by a widely diverse set of algorithms. For example, most fingerpriting approaches utilize the RSS, e.g. [12, 14], and many multilateration approaches [52] use it as well. In spite of its several meter-level accuracy, using the RSS is an attractive approach because it can re-use the existing wireless infrastructure — this feature presents a tremendous cost savings over deploying localization-specific hardware. In this chapter we thus focus on localization algorithms that employ signal strength measurements. In this section, we provide an overview of a representative set of algorithms selected for conducting performance analysis under attack. These algorithms use either deterministic or probabilistic methods for location estimation.

There are several ways to classify localization schemes that use signal strength: range-based schemes, which explicitly involve the calculation of distances to landmarks; and RF fingerprinting schemes whereby a radio map is constructed using prior measurements, and a device is localized by referencing this radio map. In this work, we focus on indoor signal strength based localization algorithms utilizing these approaches. We can further break down the algorithms into two main categories: point-based methods, and area-based methods.

2.2.1 Point-based Algorithms

Point-based methods return an estimated point as a localization result. Here we describe a few representative point-based schemes for our study.

RADAR (R1): A primary example of a point-based method is the RADAR scheme [12]. In R1, multiple base stations are deployed to provide overlapping coverage of an area, such as an office building. During set up, a mobile host with known position broadcasts beacons periodically, and the signal strength readings are measured at a set of fixed landmarks. Collecting together the averaged signal strength readings from each of the landmarks for different transmitter locations provides a radio map. After training, localization is performed by measuring a wireless device's RSS at each landmark, and the vector of RSS values is compared to the radio map. The record in the radio map whose signal strength vector is closest in the Euclidean sense

to the observed signal strength vector is declared to correspond to the location of the transmitter. Variations of RADAR, such as *Averaged RADAR* (R2) which returns the average of the closest 2 fingerprints and *Gridded RADAR* (GR) that uses the Interpolated Map Grid (IMG) as a set of additional fingerprints over the basic RADAR have been proposed in [27].

Highest Probability (P1): The P1 method uses a probabilistic approach by applying the statistical Bayes' rule to return the point with the highest probability in the pre-constructed radio map as the location estimation result [59]. There are variations of Highest Probability. *Averaged Highest Probability* (P2) returns the mid-point of the top 2 training fingerprints. And like GR, *Gridded Probability* (GP) uses fingerprints based on an IMG [27].

2.2.2 Area-based Algorithms

On the other hand, area-based algorithms return a *most likely* area in which the true location resides. One of the major advantages of area-based methods compared to point-based methods is that they return a region, which has an increased chance of capturing the transmitter's true location. We study 3 area-based algorithms [27, 52], two of them, Simple Point Matching (SPM) and Area Based Probability (ABP), use an Interpolated Map Grid (IMG) and perform scene matching (fingerprint matching) for localization; and the other, Bayesian Networks (BN), is a multilateration algorithm.

Simple Point Matching (SPM): In SPM, the floor is divided into small tiles. The strategy behind SPM is to find a set of tiles that fall within a threshold of the RSS for each landmark independently, then return the tiles that form the intersection of each landmark's set. We define the threshold as

$$s_i \pm q, \tag{2.1}$$

where s_i is the expected value of the RSS reading from Landmark i and q is an expected noise level. One way to choose q is to use the maximum of the standard deviation σ with

$$\sigma = max\{\sigma_{ij}; i \in \{1..numberoflandmarks\}, j \in \{1..numberofpoints\}\}. \tag{2.2}$$

SPM [27] is an approximation of the Maximum Likelihood Estimation (MLE) method.

Area Based Probability (ABP): ABP returns a set of tiles bounded by a probability that the transmitter is within the returned tile set. The probability is called the confidence α and

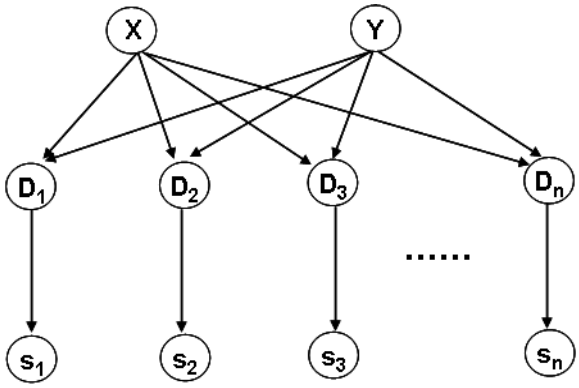


Figure 2.1: The Bayesian Network under analysis.

it is adjustable by user. ABP assumes the distribution of RSS for each landmark follows a Gaussian distribution with mean as the expected value of RSS reading vector $\mathbf{s}$. The Gaussian random variable from each landmark is independent. ABP then computes the probability of the transmitter being at each tile L_i on the floor using Bayes' rule:

$$P(L_i|\mathbf{s}) = \frac{P(\mathbf{s}|L_i) \times P(L_i)}{P(\mathbf{s})}. \tag{2.3}$$

Given that the transmitter must be at exactly one tile satisfying $\sum_{i=1}^{L} P(L_i|\bar{S}_l) = 1$, ABP normalizes the probability and returns the most likely tiles up to its confidence α [27].

Bayesian Networks (BN): BN is a multilateration algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization [52]. In BN, the overall joint density of $x \in X$, where x is a random variable, only depends on the parents of x, denoted $pa(x)$:

$$p(X) = \prod_{x \in X} p(x|\mathrm{pa}(x)). \tag{2.4}$$

Once $p(X)$ is computed, the marginal distribtution of any subset of the variables of the network can be obtained as it is proportional to overall joint distribution. Figure 2.1 shows the basic Bayesian Network used for our analysis. The vertices X and Y represent location; the vertex s_i is the RSS reading from the ith landmark; and the vertex D_i represents the Euclidean distance between the location specified by X and Y and the ith landmark. The value of s_i follows a signal propagation model $s_i = b_{0i} + b_{1i} \log D_i$, where b_{0i}, b_{1i} are the parameters specific to the ith landmark. The distance $D_i = \sqrt{(X - x_i)^2 + (Y - y_i)^2}$ in turn depends on the

location (X, Y) of the measured signal and the coordinates (x_i, y_i) of the ith landmark. The network models noise and outliers by modeling the s_i as a Gaussian distribution around the above propagation model, with variance τ_i:

$$s_i \sim N(b_{0i} + b_{1i} \log D_i, \tau_i). \tag{2.5}$$

The initial parameters (b_{0i}, b_{1i}, τ_i) of the model are unknown, and the training data is used to adjust the specific parameters of the model according to the relationships encoded in the network. Through Markov Chain Monte Carlo (MCMC) simulation, BN returns the sampling distribution of the possible location of X and Y as the localization result.

The algorithms we have described in this section are summarized in Table 2.1. Although there are a variety of other signal strength based localization algorithms that may be studied, our results are general and can be applied to other point-based and area-based methods.

2.3 Conducting Signal Strength Attacks

In this section, we study the feasibility of conducting signal strength attacks. We first discuss the possible attacks on signal strength. We then provide experimental results for signal strength going through various materials. Finally, we derive an attack model for our performance analysis of the robustness of localization algorithms.

2.3.1 Signal Strength Attacks

The first step to tackle a security problem is to put oneself in the role of the adversary and attempt to understand the attacks. To attack signal-strength based localization systems, an adversary must attenuate or amplify the RSS readings. This can be done by applying the attack at the transmitting device, e.g. simply placing foil around the 802.11 card; or by directing the attack at the landmarks. For example, we may steer the lobes and nulls of an antenna to target select landmarks. A broad variety of attenuation attacks can be performed by introducing materials between the landmarks and sensors [49].

In order to support the claim that physical attacks on received signal strength are feasible and capable of significantly affecting the results of a localization algorithm, we first examined the possibility of signal strength attacks. Next, we report results of actual experiments to

Table 2.1: Algorithms under study

Algorithm	**Abbreviation**	**Description**
Area-Based		
Simple Point Matching	SPM	Maximum likelihood matching of the RSS to an area using thresholds.
Area Based Probability	ABP-α	Bayes rule matching of the RSS to an area probabilistically bounded by the confidence level α%.
Bayesian Network	BN	Returns the most likely area using a Bayesian network approach.
Point-Based		
RADAR	R1	Returns the closest record in the Euclidean distance of signal space.
Averaged RADAR	R2	Returns the average of the top 2 closest records in the signal map.
Gridded RADAR	GR	Applies RADAR using an interpolated grid signal map.
Highest Probability	P1	Applies maximum likelihood estimation to the received signal.
Averaged Highest Probability	P2	Returns the average of the top 2 likelihoods.
Gridded Highest Probability	GP	Applies likelihoods to an interpolated grid signal map.

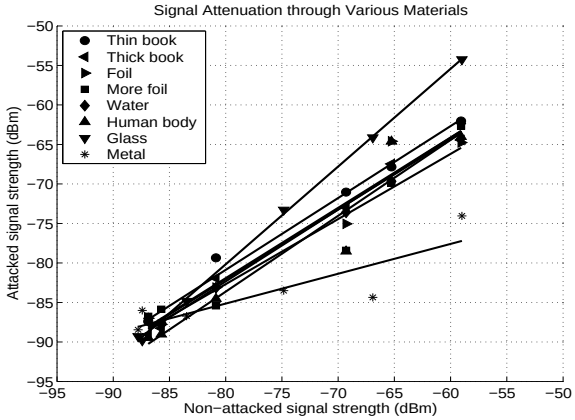


Figure 2.2: Signal strength when going through a barrier.

quantify the effectiveness of various ways of attenuating/amplifying signal strength.

2.3.2 Experimental Results of Attacks

Our experiments were performed in our laboratory in the 3rd floor of the CoRE building at Rutgers University, as shown in Figure 2.4 (a). There are 4 landmarks deployed in the 3rd floor of CoRE. We measured the RSS of beacon signals coming from each of the landmark. The RSS readings were collected using a laptop with an Orinoco Silver wireless card, using `iwlist` to sample the signal strength. In order to mitigate the effect of fluctuations, we collected samples once every second for 10 minutes, and averaged the signal strength over 600 samples.

As noted earlier, an adversary may attack the signal strength by attenuating or amplifying the RSS readings. This can be done either at the receiver or at the transmitter. Our aim is to find the results of power loss in dB by simple attacks. Therefore, in the experiments, we placed various obstruction materials close to the laptop's wireless card and measured the RSS values from each landmark at the laptop. The following obstructions were used: a thin book, a thick book, a layer of metal foil, three layers of foil (referred to as more foil), a mug filled with water (referred to as water), a glass mug (referred to as glass), a metal cabinet (referred to as metal), and a human body. These materials are easy to access and attacks utilizing these kind of materials can be simply performed with low cost. The original signal strength values, together with the signal strength measurements in the presence of these objects, are provided in Figure 2.2.

The points represent the measured data from experimental results for various materials, while the lines are the linear least-squares fitting. From these results, we have the following general observations: placing a blocking object between the transmitter and receiver can attenuate the signal strength; and, across different blocking objects, metal, foil, and human body are more effective than other blocking materials. Interestingly, we found that glass has the amplification effect on the signal strength. A more comprehensive study of propagation loss through common materials can be found in [58], and we note that more powerful attenuation loss is possible by using more advanced materials (such as RF-absorptive carbon fabric). Finally, we note that these results also imply that amplification is possible by removing a barrier (e.g. a door) of the corresponding material or through antenna-based methods.

2.3.3 Attack Model

Based upon the results in Figure 2.2, we further see that there is a linear relationship between the unattacked signal strength and the attacked signal strength in dB for various materials. The linear relationship implies that there is an easy way for an adversary to perform and control the effect of an attack on the observed signal strength by appropriately selecting different materials. Specifically, we envision that an adversary may suitably introduce and/or remove barriers of appropriate materials so as to attenuate and amplify the signl strength readings at one or more landmarks. Due to the observed linear relationship illustrated in Figure 2.2, we refer to this as the ”linear attack model”.

In the remainder of the chapter, we will use the linear attack model to describe the effect of an attack on the RSS readings at one or more landmarks. The resulting attacked readings are then used to study the consequent effects on localization for the algorithms surveyed above. In particular, in this study, we apply our attacks to individual landmarks, which might correspond to placing a barrier directly in front of a landmark, as well as to the entire set of landmarks, which corresponds to placing a barrier around the transmitting device. Similar arguments can be made for amplification attacks, whereby usually barriers are removed between the source and receivers. Moreover, we apply attenuation, amplification, or a mixture of simultaneous

attenuation and amplification attacks to multiple landmarks and study the performance of localization algorithms. The broad collection of our attack scenarios has covered the set of possibilities that an adversary could attempt to accomplish. Although there are many different and more complex signal strength attack methods that can be used, we believe their effects will not vary much from the linear signal strength attack model we use in this paper, and note that such sophisticated attacks could involve much higher cost to perform.

2.4 Measuring Attack Susceptibility

The aim of a localization attack is to perturb a set of signal strength readings in order to have an effect on the localization output. When selecting a localization algorithm, it is desirable to have a set of metrics by which we can quantify how susceptible a localization algorithm is to varying levels of attack by an adversary. In this section, we shall provide a formal specification for an attack, and present several measurement tools for quantifying the effectiveness of an attack.

2.4.1 A Generalized Localization Model

In order to begin, we need to specify a model that captures a variety of RF-fingerprinting localization algorithms. Let us suppose that we have a domain D in two-dimensions, such as an office building, over which we wish to localize transmitters. Within D, a set of n landmarks have been deployed to assist in localization. A wireless device that transmits with a fixed power in an isotropic manner will cause a vector of n signal strength readings to be measured by the n landmarks. In practice, these n signal strength readings are averaged over a sufficiently large time window to remove statistical variability. Therefore, corresponding to each location in D, there is an n-dimensional vector of signal readings $\mathbf{s} = (s_1, s_2, \cdots, s_n)$ that resides in a range R.

This relationship between positions in D and signal strength vectors defines a fingerprint function $F : D \rightarrow R$ that takes our real world position (x, y) and maps it to a signal strength reading $\mathbf{s}$. F has some important properties. First, in practice, F is not completely specified, but rather a finite set of positions (x_j, y_j) is used for measuring a corresponding set of signal strength vectors $\mathbf{s}_j$. Additionally, the function F is generally one-to-one, but is not onto. This

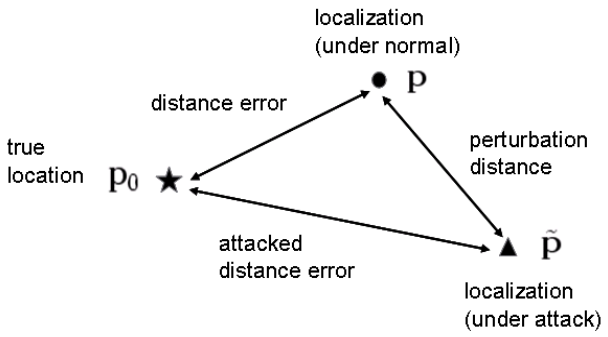


Figure 2.3: Interpretation of distances in location estimation.

means that the inverse of F is a function G that is not well-defined: There are holes in the n-dimensional space in which R resides for which there is no well-defined inverse.

It is precisely the inverse function G, though, that allows us to perform localization. In general, we will have a signal strength reading $\mathbf{s}$ for which there is no explicit inverse (e.g. perhaps due to noise variability). Instead of using G, which has a domain restricted to R, we consider various pseudo-inverses G_{alg} of F for which the domain of G_{alg} is the complete n-dimensional space. Here, the notation G_{alg} indicates that there may be different *algorithmic* choices for the pseudo-inverse. For example, we shall denote G_R to be the RADAR localization algorithm. In general, the function G_{alg} maps an n-dimensional signal strength vector to a region in D. For point-based localization algorithms, the image of G_{alg} is a single point corresponding to the localization result. On the other hand, for area-based methods, the localization algorithm G_{alg} produces a set of likely positions.

An attack on the localization algorithm is a perturbation to the correct n-dimensional signal strength vector $\mathbf{s}$ to produce a corrupted n-dimensional vector $\tilde{\mathbf{s}}$. Corresponding to the uncorrupted signal strength vector $\mathbf{s}$ is a correct localization result $\mathbf{p} = G_{alg}(\mathbf{s})$, while the corrupted signal strength vector produces an attacked localization result $\tilde{\mathbf{p}} = G_{alg}(\tilde{\mathbf{s}})$. Here, $\mathbf{p}$ and $\tilde{\mathbf{p}}$ are set-valued and may either be a single point or a region in D.

2.4.2 Attack Susceptibility Metrics

We wish to quantify the effect that an attack has on localization by relating the effect of a change in a signal strength reading $\mathbf{s}$ to the resulting change in the localization result $\mathbf{p}$. We

shall use $\mathbf{p}_0$ to denote the correct location of a transmitter, $\mathbf{p}$ to denote the estimated location (set) when there is no attack being performed, and $\tilde{\mathbf{p}}$ to denote the position (set) returned by the estimator after an attack has affected the signal strength. Figure 2.3 illustrates the relationship between the true location and the estimated locations. There are several performance metrics that we will use:

- **Estimator Angle Bias:** The perturbation on the signal strength vector caused by an attack will result in the variability of location estimation in the physical space. We want to investigate the bias along the angular dimension. That is, if we plot the relative error position in polar coordinates, for an unbiased estimator the error would have an equal probability of falling along any angle. However, when attacking a single landmark, we may expect an angular bias to be introduced. The estimation angle bias is studied by calculating the estimated position for different experimental trials, and comparing these results, in a spatial sense, to the true position. An angularly-unbiased algorithm should uniformly cover the 360 degrees around the true location. For area-based methods, we replace $\tilde{\mathbf{p}}$, which is a set, with its median (along the x and y dimensions separately) to get a point. The angular bias is an important metric as it can serve as an indication as to whether an attacker can skew the localization result in a specific direction - algorithms with more angular bias are more skewable and hence worse choices for deployment since an adversary can use this knowledge to its advantage.

- **Estimator Distance Error:** An attack will cause the magnitude of $\mathbf{p}_0 - \tilde{\mathbf{p}}$ to increase. For a particular localization algorithm G_{alg} we are interested in the statistical characterization of $\|\mathbf{p}_0 - \tilde{\mathbf{p}}\|$ over all possible locations in the building. The characterization of $\|\mathbf{p}_0 - \tilde{\mathbf{p}}\|$ depends on whether a point-based method or an area-based method is used, and can be described via its mean and distributional behavior. For a point-based method, we may measure the cumulative distribution (cdf) of the error $\|\mathbf{p}_0 - \tilde{\mathbf{p}}\|$ over the entire building. For area-based metrics, we calculate the CDF of the distance between the median of the estimated locations $\tilde{\mathbf{p}}_{med}$ and the true location, i.e. $\|\mathbf{p}_0 - \tilde{\mathbf{p}}_{med}\|$.

  The CDF provides a complete statistical specification of the distance errors. It is often more desirable to look at the average behavior of the error. For point-based methods,

the average distance error is simply $E[\|\mathbf{p}_0 - \tilde{\mathbf{p}}\|]$, which is just the average of $\|\mathbf{p}_0 - \tilde{\mathbf{p}}\|$ over all locations. Area-based methods allow for more options in defining the average distance error. First, for a particular value of $\mathbf{p}_0$, $\tilde{\mathbf{p}}$ is a set of points. For each $\mathbf{p}_0$, we get a collection of error values $\|\mathbf{p}_0 - \mathbf{q}\|$, as $\mathbf{q}$ varies over points in $\tilde{\mathbf{p}}$. For each $\mathbf{p}_0$, we may extract the minimum, 25th percentile, median, 75th percentile, and maximum. These quartile values of $\|\mathbf{p}_0 - \mathbf{q}\|$ are then averaged over the different positions $\mathbf{p}_0$.

- **Estimator Precision:** An area-based localization algorithm returns a set $\mathbf{p}$. For localization, precision refers to the size of the returned estimated area. This metric quantifies the average value of the area of the localized set $\mathbf{p}$ over different signal strength readings $\mathbf{s}$. Generally speaking, the smaller the size of the returned area, the more precise the estimation is. When an attack is conducted, it is possible that the precision of the answer $\tilde{\mathbf{p}}$ is affected.

- **Precision vs. Perturbation Distance:** The perturbation distance is the quantity $\|\mathbf{p}_{med} - \tilde{\mathbf{p}}_{med}\|$. The precision vs. perturbation distance metric depicts the functional dependency between precision and increased perturbation distance.

- **Hölder Metrics:** In addition to error performance, we are interested in how dramatically the returned results can be perturbed by an attack. Thus, we wish to relate the magnitude of the perturbation $\|\mathbf{s} - \tilde{\mathbf{s}}\|$ to its effect on the localization result, which is measured by $\|G_{alg}(\mathbf{s}) - G_{alg}(\tilde{\mathbf{s}})\|$. In order to quantify the effect that a change in the signal strength space has on the position space, we borrow a measure from functional analysis [43], called the Hölder parameter (also known as the Lipschitz parameter) for G_{alg}. The Hölder parameter H_{alg} is defined via

$$H_{alg} = \max_{\mathbf{s},\mathbf{v}} \frac{\|G_{alg}(\mathbf{s}) - G_{alg}(\mathbf{v})\|}{\|\mathbf{s} - \mathbf{v}\|} \tag{2.6}$$

where $\mathbf{s}$ and $\mathbf{v}$ are all the possible combinations of signal strength vectors in signal space. For continuous G_{alg}, the Hölder parameter measures the maximum (or worst-case) ratio of variability in position space for a given variability in signal strength space. Since the traditional Hölder parameter describes the worst-case effect an attack might have, it is natural to also provide an average-case measurement of an attack, and therefore we

introduce the average-case Hölder parameter

$$\overline{H}_{alg} = \text{avg}_{\mathbf{s},\mathbf{v}} \frac{\|G_{alg}(\mathbf{s}) - G_{alg}(\mathbf{v})\|}{\|\mathbf{s} - \mathbf{v}\|}. \tag{2.7}$$

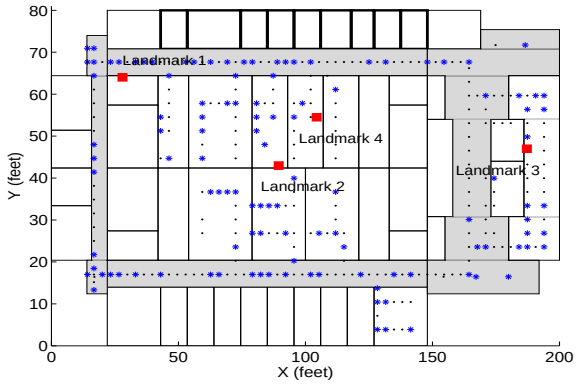
These parameters are only defined for continuous functions G_{alg}, and many localization algorithms are not continuous. For example, if we look at G_R for RADAR, the result of varying a signal strength reading is that it will yield a *stair-step* behavior in position space, i.e. small changes will map to the same output and then suddenly, as we continue changing the signal strength vector, there will be a change to a new position estimate (we have switched over to a new Voronoi cell in signal space). In reality, this behavior does not concern us too much, as we are merely concerned with whether adjacent Voronoi cells map to close positions. We will revisit this issue in Section 2.6. Finally, we emphasize that Hölder metrics measure the perturbability of the returned results, and do not directly measure error.

2.5 Experimental Results

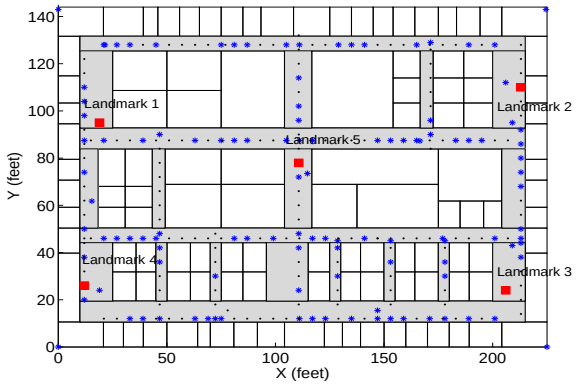
In this section we present our experimental results. We first describe our experimental method. Next, we examine the impact of attacks on the RSS to localization bias and localization error under different attacking scenarios. We then quantify the algorithms' linear responses to RSS changes. Finally, we present a precision study that investigates the impact of attacks on the returned areas for area-based algorithms.

2.5.1 Experimental Setup

Figure 2.4 shows our experimental set up. The floor map on the left, (a) is the 3rd floor of the CoRE building at Rutgers, which houses the computer science department and has an area of 200x80ft (16000 ft^2). The other floor shown in (b) is an industrial research laboratory (we call the Industrial Lab), which has an area of 225x144ft (32400 ft^2). The stars are the training points, the small dots are testing points, and the larger squares are the landmarks, which are 802.11 access points. Notice that the 4 CoRE landmarks are more co-linear than the 5 landmarks in the Industrial Lab.



(a) CoRE Building

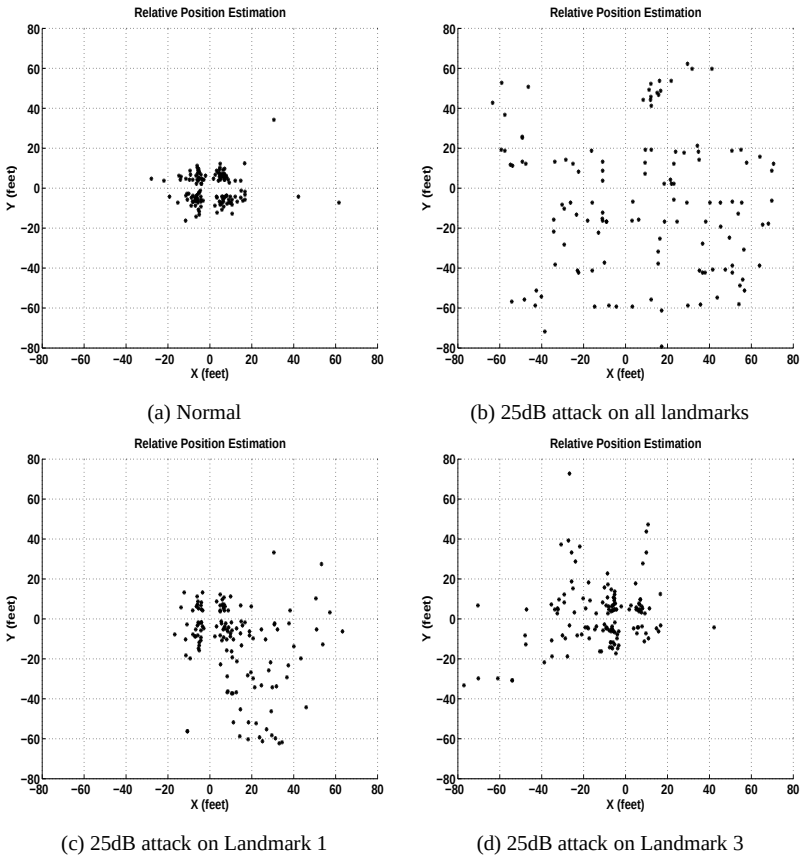


(b) Industrial Lab

Figure 2.4: Deployment of landmarks and training locations on the experimental floors

For both attenuation and amplification attacks, we ran the algorithms but modified the RSS of the testing points. We altered the RSS by +/-5 dB to +/-25 dB, in increments of 5 dB. We experimented with different ways to handle signals that would fall below the detectable threshold of -92 dBm for our cards. We found that substituting the minimal signal (-92 dBm) produced about the same localization results and did not require changing the algorithms to special case missing data.

We experimented with different training set sizes, including 20, 35, 60, 85, 115, 145, 185, 215, 245, 253, and 286 points. Experimental data was collected at a total of 286 locations in the CoRE building and at a total of 253 locations in the Industrial Lab. Although there are some small differences, we found that the behavior of the algorithms matches previous results [27] and varied little after using 115 training points. We therefore chose to use a training set size of 115 for this study.



(a) Normal

(b) 25dB attack on all landmarks

(c) 25dB attack on Landmark 1

(d) 25dB attack on Landmark 3

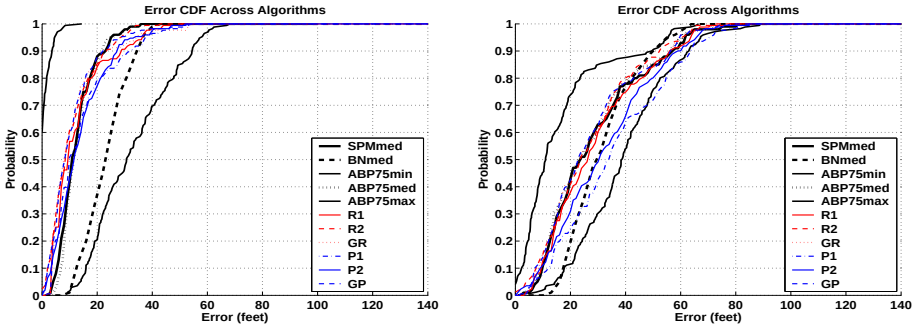
Figure 2.5: ABP: Localization estimation relative to the true locations for the Industrial Lab.

2.5.2 Localization Angle Bias

In this section, we study the angular bias of the localization schemes introduced by signal strength attacks. For the Industrial Lab, Figure 2.5(a) shows the localization result of ABP under no attack for the relative estimation positions to the true locations, setting as the origin, over all the localization attempts. The normal performance of the algorithms are unbiased with the localization results uniformly distributed around the true locations.

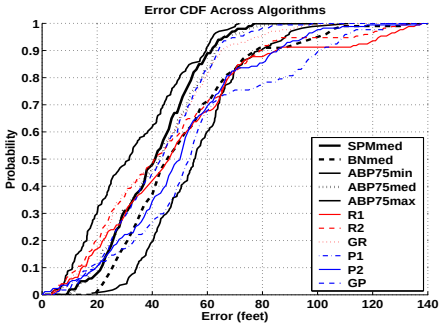
Figure 2.5(b) is the relative position estimation results under 25dB attenuation attack on all landmarks, while Figure 2.5(c) and Figure 2.5(d) show the attacked results on single landmarks, landmark 1 and landmark 3, respectively. Figure 2.4(b) shows that landmark 1 and landmark 3 are placed in diagonal positions across the Industrial Lab. We have observed that signal strength attacks have affected the localization schemes by introducing angular bias on the results with the location estimation more likely to be in the fourth quadrant relative to the true location

when landmark 1 is attacked, as shown in Figure 2.5(c). Because landmark 1 is placed in the upper left corner in the building floor map shown in 2.4, signal attenuation on landmark 1 made the localization system think the sensor node is farther away from landmark 1, and thus the resulting localization results under attack have been pushed into the fourth quadrant. This effect has been proved by examining the localization results when landmark 3 is under attack. As presented in Figure 2.5(d), the relative localization results are mostly in the second quadrant since landmark 3 is placed in the lower right corner of the building floor map. Further, as expected, for simultaneous landmark attacks, the localization results are distributed around the true locations randomly, but with much larger estimation errors as presented in Figure 2.5(b). We have observed similar effects for the other algorithms in the Industrial Lab and the CoRE building.

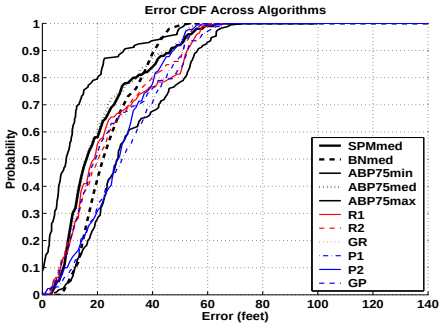


(a) CoRE: No attack

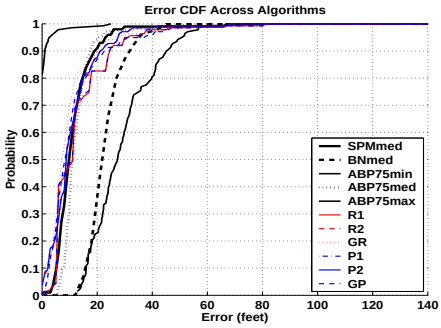
(b) CoRE: 10dB attenuation



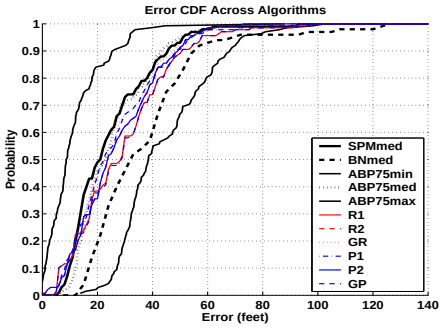
(c) CoRE: 25dB attenuation



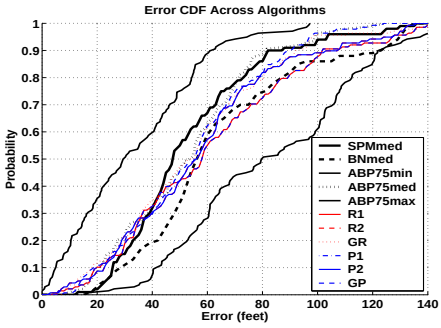
(d) CoRE: 10dB amplification



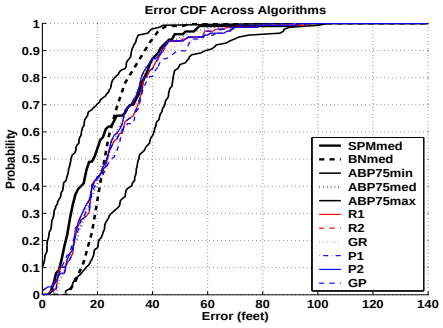
(e) Industrial: No attack



(f) Industrial: 10dB attenuation

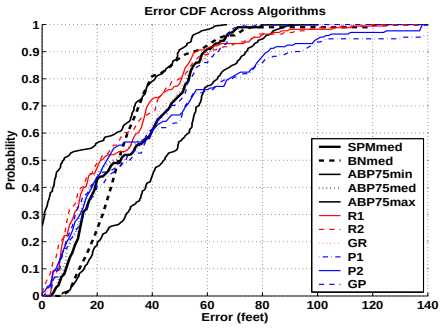


(g) Industrial: 25dB attenuation

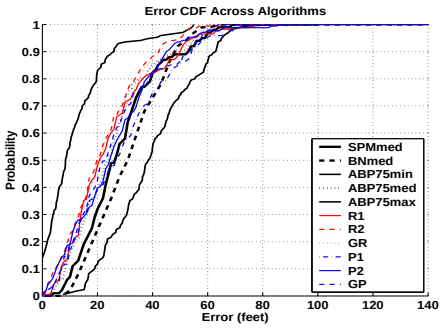


(h) Industrial: 10dB amplification

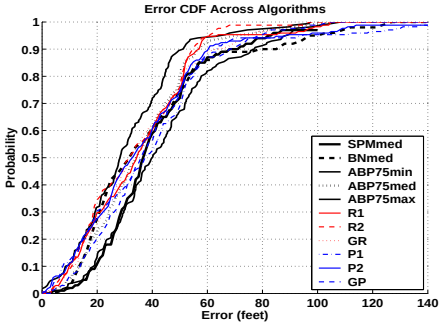
Figure 2.6: Error CDF across localization algorithms when attacks are performed on all the landmarks.



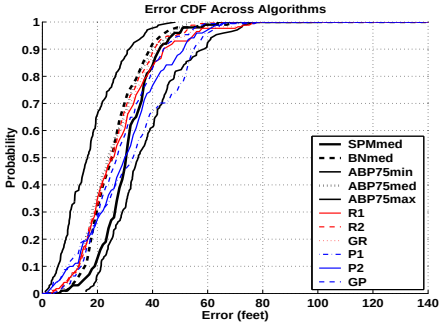
(a) CoRE: Attenuation, Landmark 1



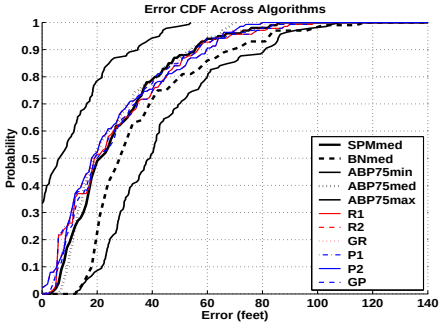
(b) CoRE: Attenuation, Landmark 2



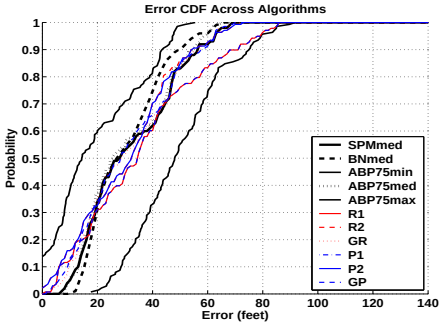
(c) CoRE: Amplification, Landmark 1



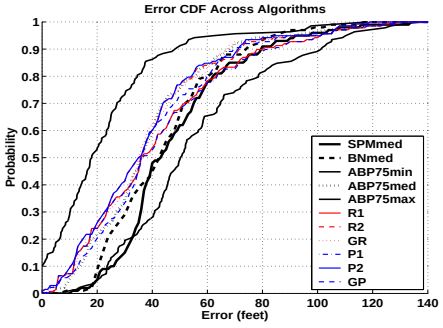
(d) CoRE: Amplification, Landmark 2



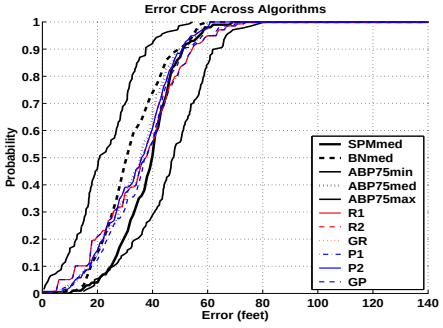
(e) Industrial: Attenuation, Landmark 4



(f) Industrial: Attenuation, Landmark 5

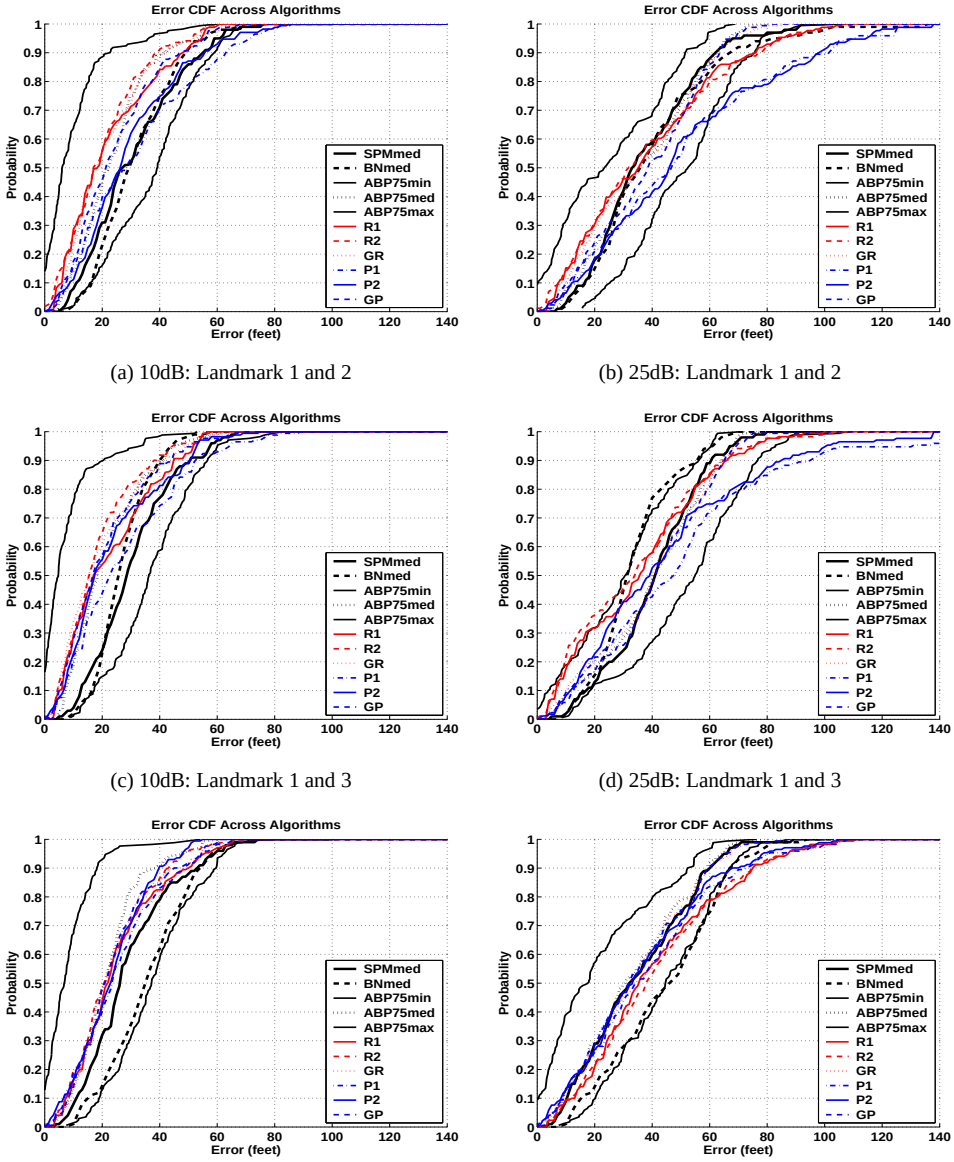


(g) Industrial: Amplification, Landmark 4



(h) Industrial: Amplification, Landmark 5

Figure 2.7: Error CDF across localization algorithms when attacks are performed on an individual landmark. The attack is 25dB of signal attenuation and signal amplification respectively.



(a) 10dB: Landmark 1 and 2

(b) 25dB: Landmark 1 and 2

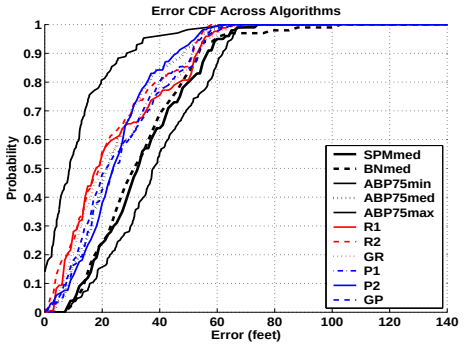
(c) 10dB: Landmark 1 and 3

(d) 25dB: Landmark 1 and 3

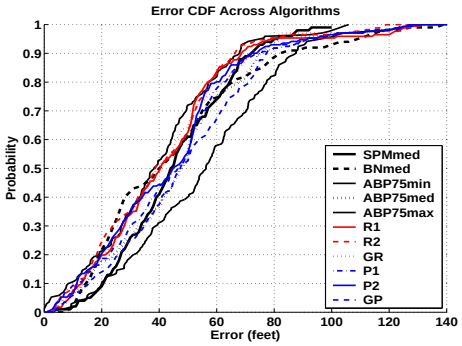
(e) 10dB: Landmark 2 and 4

(f) 25dB: Landmark 2 and 4

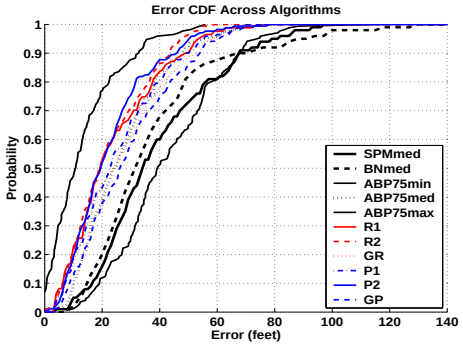
Figure 2.8: CoRE: Error CDF across localization algorithms when attenuation attacks are performed on multiple landmarks.



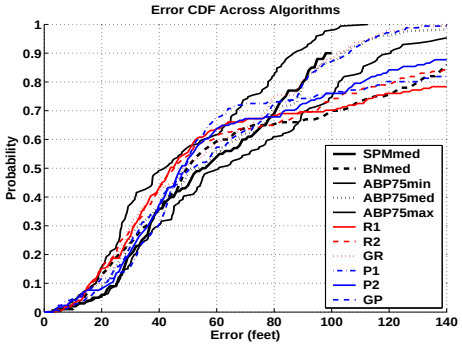
(a) 10dB: Landmark 1 amplification and landmark 2 attenuation



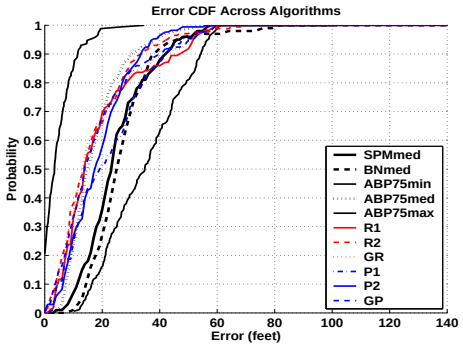
(b) 25dB: Landmark 1 amplification and landmark 2 attenuation



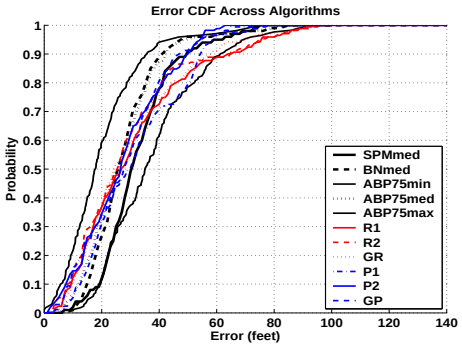
(c) 10dB: Landmark 1 amplification and landmark 3 attenuation



(d) 25dB: Landmark 1 amplification and landmark 3 attenuation



(e) 10dB: Landmark 2 amplification and landmark 4 attenuation



(f) 25dB: Landmark 2 amplification and landmark 4 attenuation

Figure 2.9: CoRE: Error CDF across localization algorithms when amplification and attenuation attacks are simultaneously performed on multiple landmarks.

2.5.3 Localization Error Analysis

In this section, we analyze the estimator distance error through the statistical characterization of $\|\mathbf{p}_0 - \tilde{\mathbf{p}}\|$ by presenting the error CDFs of all the algorithms as a function of attenuation and amplification attacks. The CDF provides a complete statistical specification of the distance errors. Specifically, we study the localization error under four attack scenarios: an all-landmark attack; a single landmark attack; attacks involving multiple landmarks; and attacks involving simultaneous amplification and attenuation on multiple landmarks.

As a baseline, Figure 2.6(a) shows the normal performance of the algorithms for the CoRE building and (e) shows the results for the Industrial Lab. For the area-based algorithms, the median tile error is presented, as well as the minimum and maximum tile errors for ABP-75. As in previous work, the algorithms all obtain similar performance, with the exception of BN, which slightly under-performs the other algorithms.

First, we look at the performance of localization algorithms under an all-landmark attack. Figures 2.6(b) and 2.6(c) show the error CDFs under simultaneous landmark attenuation attacks of 10 and 25 dB for CoRE, respectively, while Figure 2.6(f) and 2.6(g) show the similar results in the industrial lab. First, the bulk of the curves shift to the right by roughly equal amounts: no algorithm is qualitatively more robust than the others. Comparing the two buildings, the results show that the industrial lab errors are slightly higher for attacks at equal dB, but again, qualitatively the impact of the building environment is not very significant.

Figures 2.6(d) and 2.6(h) show the error CDFs for the CoRE and Industrial Lab under a 10 dB amplification attack. The results are qualitatively symmetric with respect to the outcome of the 10dB attenuation attack. We found that, in general, comparing amplifications to attenuations of equal dB, the errors were qualitatively the same.

An interesting feature is that in CoRE the minimum error for ABP-75 also shifts to the right by roughly the same amount as the other curves. Figures 2.6(a) and 2.6(e) show that, in the non-attacked case, the minimum tile error for ABP-75 is quite small, meaning that the localized node is almost always within or very close to the returned area. However, under attacks, the closest part of the returned area moves away from the true location at the same rate as the median tile. We observed similar effects for the SPM and BN algorithms. We noticed

that under large attacks around 25dB, the median error CDF curves in the Industrial Lab have similar performance to those from the CoRE building, but there are two curves that seem to be outliers, namely ABP75min and ABP75max. These two curves represent the best and the worst cases from the ABP algorithm and we see that they are not moving at the same speed as the median errors, when compared with the results of the CoRE building. This tells us that the variance/spread of the performance of area-based algorithms in the Industrial Lab has increased under an all-landmark attack, but that the average behavior is consistent across the two buildings.

We then examine attacks against a single landmark. We found attacks against certain landmarks had a much higher impact than against others in the CoRE building. Figure 2.7(a) and 2.7(b) show the difference in the error CDF by comparing attacks of landmarks 1 and 2. Figure 2.4(a) shows that landmark 1 is at the left end of the building, while landmark 2 is in the center and is close to landmark 4. The tail of the curves in Figure 2.7(a) are much worse than for 2.7(b), showing that when landmark 1 is attacked, significantly more high errors are returned. Figures 2.7(c) and 2.7(d) show a similar effect for amplification attacks. This is because landmark 1 is at one end of the building alone. The contribution of the signal strength reading from landmark 1 plays an important role in localization, while the contribution of landmark 2 can be reduced by the contribution from the nearby landmark 4 when under attack.

The Industrial Lab results in Figures 2.7(e)-(h) show much less sensitivity to landmark placement compared to the CoRE building. Figure 2.4(b) shows that landmark 5 is centrally located and we initially suspected this would result in increased attack sensitivity. However, the error CDFs show that the remaining 4 landmarks provide sufficient coverage: as landmark 5 is attacked, the error CDFs are not much different from attacking landmark 4. The landmark placement in the CoRE building is colinear (to maximize the signal coverage in the floor), while the landmark placement in the Industrial Lab is more close to the optimal landmark placement for location accuracy. We believe that the better landmark placement for localization [20] in the Industrial Lab can account for the localization performance being less sensitive to landmark placement under attack.

Next, we study attacks on more than one landmark, but not on all landmarks. Figure 2.8 present the localization results in the CoRE building when attenuation attacks are performed on

multiple landmarks, specifically on landmark pairs, *1 and 2*, *1 and 3*, and *2 and 4*. We found that attacks on landmark pair *1 and 3* shown in Figure 2.8(d) cause larger errors compared to results in Figure 2.8(b) and (f) when attacking landmark pairs *1 and 2*, and *2 and 4*. Since landmarks 1 and 3 are placed at two ends of the building alone, the contribution of the RSS reading from these two landmarks is significant compared to the readings from landmark 2 and 4, which are closely placed and can cover each other. In general, the impact of the multiple landmark attacks on the localization performance is between the performance of a single landmark attack and an all-landmark attack.

Fourthly, we look at the attack scenario that the adversary simultaneously performs both amplification and attenuation attacks on multiple landmarks. The localization results are presented in Figure 2.9 for the CoRE building. For a direct comparison, we present results when mixed attacks are applied on landmark pairs, *1 and 2*, *1 and 3*, and *2 and 4*. we should expect that such an attack would be more effective in falsifying the location results, and this is what we observe. But, beyond this, we observe that the performance depends heavily upon which landmarks are attacked. We found that if the attacked landmarks are close to each other such as landmark 2 and 4, which are located in the center of the building, the effects of amplification and attenuation attacks are canceled out. Thus the impact of mixed attacks does not lead to significant perturbation in the localization results, as shown in Figure 2.9(f), which is about the same as under single landmark attacks displayed in Figure 2.7. However, if the attacked landmarks are farther away from each other, such as landmark 1 and 3, which are located at opposite ends of the building, the simultaneous amplification and attenuation attacks can be very harmful and cause larger localization errors for all the algorithms presented in Figure 2.9(d). The behavior of the error CDFs in Figure 2.9(d) is qualitatively different than others with very long tails. The effect of the amplification attack on landmark 1 and the attenuation attack on landmark 3 pushed the localization results further in one direction, and thus introduced large localization bias.

The four attack scenarios we studied have covered a broad collection of possible combinations of signal strength attacks. We found that simultaneously attacking all landmarks has more impact on localization performance than attacking an individual landmark. Further, simultaneous amplification and attenuation attacks on certain landmarks can cause qualitatively larger

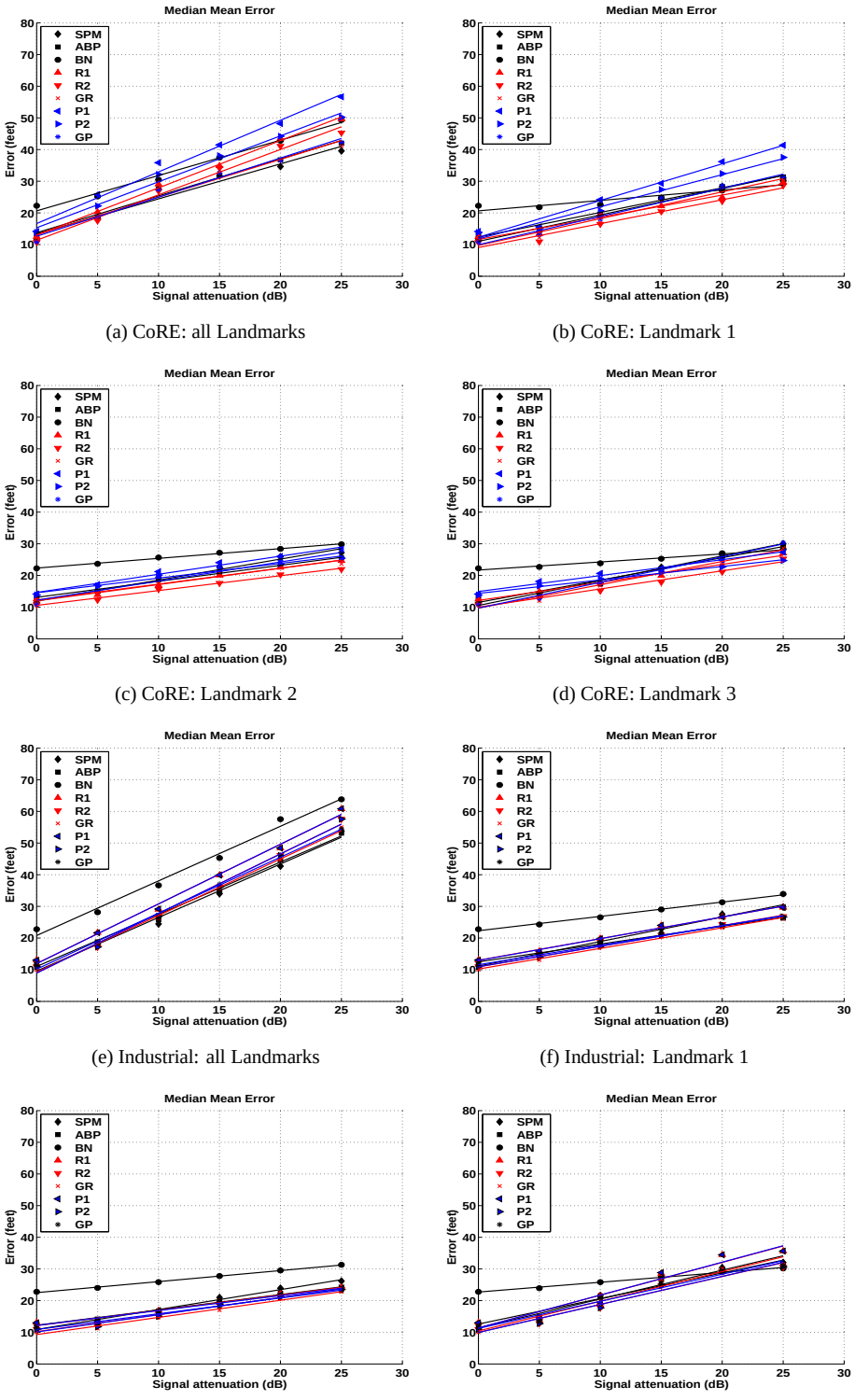
errors than other kinds of attacks. Most importantly, we observed that none of the localization algorithms outperforms the others for the attacks we examined.

2.5.4 Linear Response

In this section, we show that the average distance error, $E[||\mathbf{p}_0 - \tilde{\mathbf{p}}||]$, of all the algorithms scales in a linear way to attacks. That is, the mean localization error changes linearly with respect to the size of the signal strength change introduced in dB (recall dB is a log-scaled change in power).

Figure 2.10 plots the median error vs. RSS attenuation for an all-landmark attack in Figure 2.10(a) and 2.10(e), and for individual landmarks in the other figures. Figure 2.11 plots the median localization error under simultaneous signal strength attenuation and amplification attacks on multiple attacks. Points are data derived from experimental results, and the lines are linear least-squares fits. The most important feature is that, in all cases, the median responses of all the algorithms fits a line extremely well, with an average R^2-statistic of 0.97 for both the CoRE and Industrial Lab. The mixed attacks with amplification attack on landmark 1 and attenuation attack on landmark 3 in CoRE shown in Figure 2.11(d) is an exceptional case with R^2 of 0.86 as the worst case.

Comparing the slopes across all the algorithms presented in Tables 2.2, 2.3, and 2.4, we found a mean change in positioning error vs. signal attenuation of 1.55 ft/dB under an all-landmark attack with a minimum of 1.3 ft/dB and maximum of 1.8 ft/dB. For the single landmark attack, the slope was substantially less, 0.64 ft/dB, although BN degrades consistently less than the other algorithms at 0.44 ft/dB. Under attenuation attacks on multiple landmarks, the localization algorithms move at the speed of 0.9 ft/dB to 1.4 ft/dB, which is between the results of a single landmark attack and an all-landmark attack. However, the median error moves faster under simultaneous amplification and attenuation attacks on landmark 1 and 3, at the speed of 1.8 - 2.2 ft/dB as shown in Table 2.4. We note the mean error tops out when the attack strength is 25dB. This confirms our analysis in Figure 2.9(d) that applying simultaneous amplification and attenuation attacks on landmarks that are farther apart causes larger impacts on the performance of localization schemes, although in practice it is hard for an adversary to



(a) CoRE: all Landmarks

(b) CoRE: Landmark 1

(c) CoRE: Landmark 2

(d) CoRE: Landmark 3

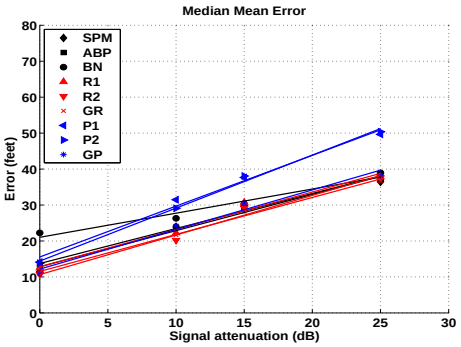
(e) Industrial: all Landmarks

(f) Industrial: Landmark 1

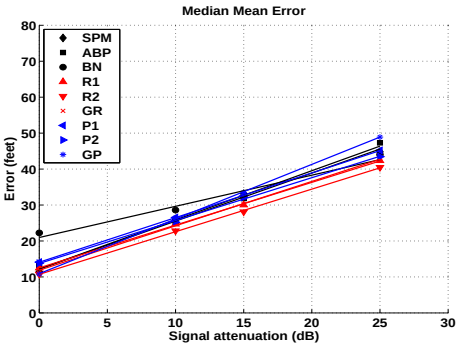
(g) Industrial: Landmark 2

(h) Industrial: Landmark 5

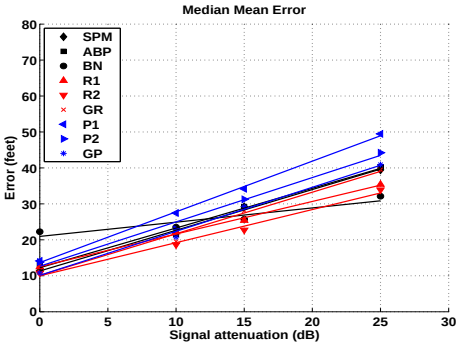
Figure 2.10: Average location estimation error across localization algorithms under signal strength attenuation attack.



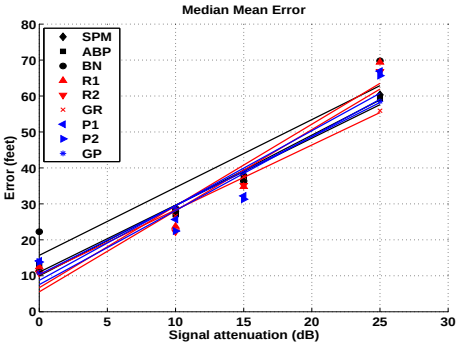
(a) Simultaneous attenuation attacks on landmarks 1 and 2



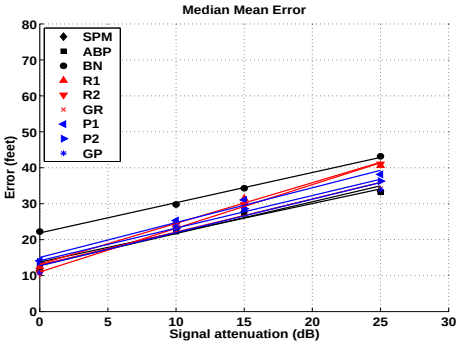
(b) Amplification attack on Landmark 1 and attenuation attack on Landmark 2



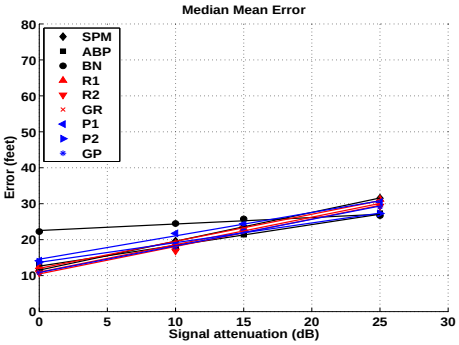
(c) Simultaneous attenuation attacks on landmarks 1 and 3



(d) Amplification attack on Landmark 1 and attenuation attack on Landmark 3



(e) Simultaneous attenuation attacks on landmarks 2 and 4



(f) Amplification attack on Landmark 2 and attenuation attack on Landmark 4

Figure 2.11: CoRE: Average location estimation error across localization algorithms under simultaneous signal strength attenuation and amplification attacks on multiple landmarks.

Table 2.2: CoRE: Slopes of Average Error from Linear Regression for attenuation attacks on all landmarks and individual landmark

Buildings	**CoRE: attenuation attack**				
Landmarks	**All**	**1**	**2**	**3**	**4**
Area-Based					
SPM	1.1048	0.8331	0.662	0.7816	0.6244
ABP-75	1.1656	0.7783	0.5049	0.7052	0.384
BN	1.1157	0.3287	0.3065	0.2544	0.493
Point-Based					
R1	1.4922	0.7006	0.5151	0.5702	0.7941
R2	1.4327	0.7534	0.4687	0.5732	0.7425
GR	1.1896	0.8440	0.5033	0.7357	0.7124
P1	1.6306	1.1597	0.5728	0.5026	0.3644
P2	1.4505	1.0123	0.464	0.4251	0.3063
GP	1.2359	0.8915	0.6028	0.8103	0.4595
Average	1.3131	0.8113	0.5111	0.5954	0.5423

Table 2.3: Industrial: Slopes of Average Error from Linear Regression for attenuation attacks on all landmarks and individual landmark

Buildings	**Industrial Lab: attenuation attack**					
Landmarks	**All**	**1**	**2**	**3**	**4**	**5**
Area-Based						
SPM	1.6901	0.7753	0.6283	0.5485	0.6455	0.9103
ABP-75	1.6479	0.5615	0.4852	0.4146	0.5469	0.8072
BN	1.7249	0.4528	0.3487	0.5215	0.5615	0.3094
Point-Based						
R1	1.8823	0.6827	0.4837	0.4286	0.5867	1.0356
R2	1.8816	0.6524	0.5394	0.4000	0.5861	0.8800
GR	1.7860	0.6514	0.5410	0.4668	0.6331	0.9358
P1	1.8854	0.6856	0.4710	0.4532	0.5881	1.0390
P2	1.8802	0.6448	0.5431	0.4023	0.5875	0.8861
GP	1.7666	0.6148	0.4976	0.4800	0.6213	0.8553
Average	1.7939	0.6357	0.504	0.4573	0.5952	0.8510

conduct simultaneous amplification and attenuation attacks without using sophisticated equipment. In general, the linear fit results are quite important as it means that no algorithm has a cliff where the average positioning error suffers a catastrophic failure under attack. Instead, it remains proportional to the severity of the attack.

While the median error characterizes the overall response to attacks, it does not address whether an attacker can cause a few, large errors. We examined the response of the maximum error as a function of the strength of the attack on an all-landmark attack, i.e. how the 100^{th} percentile error scales as a function of the change in dB under an all-landmark attack. The all-landmark attack corresponds to a common attack scenario. It is thus desirable to study the worst-case situation under an all-landmark attack. We note that this characterization is not

Table 2.4: CoRE: Slopes of Average Error from Linear Regression for mixed attacks of signal attenuation and amplification on multiple landmarks

Buildings	**attenuation attacks**			**amplification and attenuation attacks**		
Landmarks	**1 and 2**	**1 and 3**	**2 and 4**	**1 and 2**	**1 and 3**	**2 and 4**
Area-Based						
SPM	1.0054	1.1328	0.8836	1.3358	1.9556	0.8018
ABP-75	0.9740	1.1050	0.8125	1.3670	1.8628	0.5778
BN	0.6716	0.3965	0.8401	0.8665	1.8868	0.1812
Point-Based						
R1	1.0392	0.9069	1.1326	1.1895	2.2731	0.7522
R2	1.1013	0.9222	1.2148	1.1841	2.2552	0.7633
GR	1.0276	1.1559	0.9196	1.2337	1.8046	0.7642
P1	1.4142	1.4104	0.9683	1.2414	2.0808	0.6492
P2	1.4735	1.2330	0.9054	1.1921	2.0606	0.5472
GP	1.1003	1.2246	0.9271	1.5197	1.9138	0.7387
Average	1.0897	1.0541	0.9560	1.2367	2.0104	0.6417

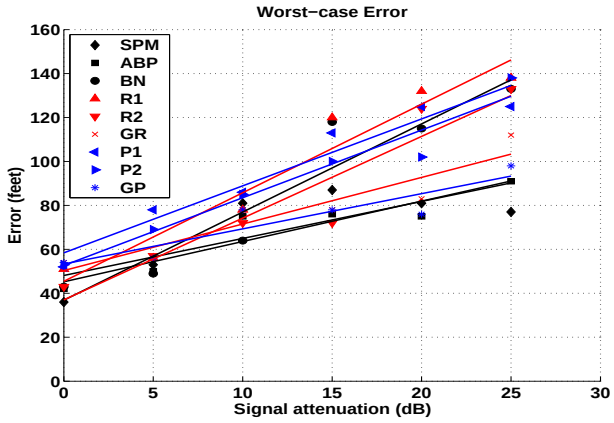
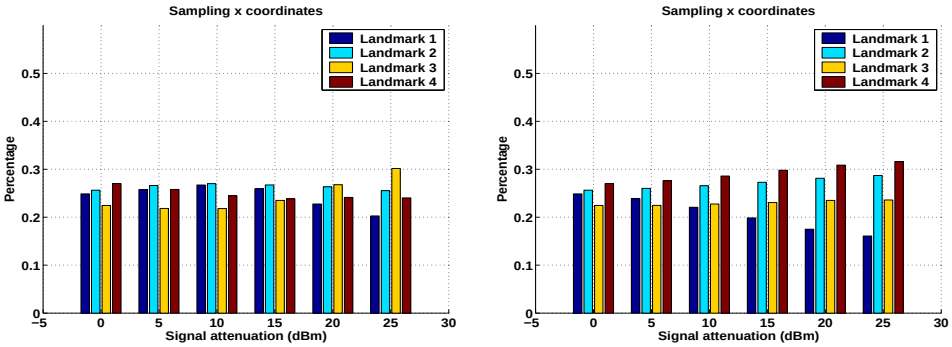


Figure 2.12: CoRE: Maximum error as a function of attack strength from an all-landmark attack.

the same as, nor is directly related to, the Hölder metrics. Those metrics define the rates of change between physical and signal space within the localization function itself, while here we characterize the change in the estimator error to the change in signal, i.e. $\|\mathbf{p}_0 - \tilde{\mathbf{p}}\|/\|\mathbf{s} - \mathbf{v}\|$.

Figure 2.12 plots the worst-case error for each algorithm as a function of signal dB for the CoRE building under an all-landmark attack. The figure shows that almost all the responses are again linear, with least-squares fits of R^2 values of 0.84 or higher, though SPM does not have a linear response. The second important point is the algorithms' responses vary, falling into three groups. BN, R1 and R2 are quite poor, with the worst case error scaling at about 4 ft/dB. P1 and P2, are in a second class, scaling at close to 3 ft/dB. The gridded algorithms, GP and GR,



(a) CoRE: all landmarks

(b) CoRE: Landmark 1

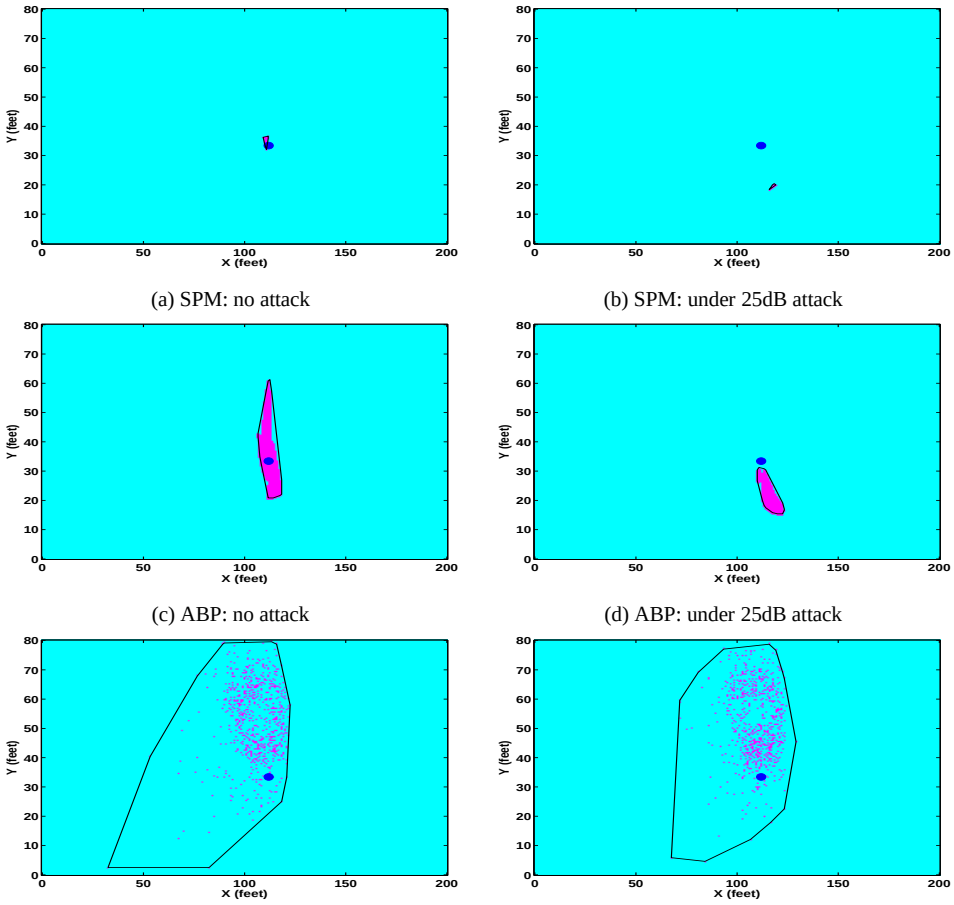
Figure 2.13: Contribution of each Landmark during sampling in the BN algorithm under attenuation attacks.

as well as ABP-75 fair better, scaling at 2 ft/dB or less. Finally, SPM is in a class by itself, with a poor linear fit (R^2 of 0.61) and the maximum error topping out at about 85 ft after 15 dB of attack.

Examining the error CDFs and the maximum errors, we can see that most of the localizations move fairly slowly in response to an attack, at about 1.5 ft/dB. However, for some of the algorithms, particularly BN, R1 and R2, the top part of the error CDF moves faster, at about 4 ft/dB. What this means is that, for a select few points, an attacker can cause more substantial errors of over 100 ft. However, at most places in the building, an attack can only cause errors with much less magnitude.

Figure 2.10 show that BN is more robust compared to other algorithms for individual landmark attacks. Recall BN uses a Monte-Carlo sampling technique (Gibbs sampling) to compute the full joint-probability distribution for not just the position coordinates, but also for every node in the Bayesian network. Under a single landmark attack we found the network reduces the contribution of network nodes directly affected by the attacked landmark to the full joint-probability distribution while increasing other landmarks' contributions. In effect, the network "discounts" the attacked landmark's contribution to the overall joint-density because the attacked data from that landmark is highly unlikely given the training data.

To show this effect we developed our own Gibbs sampler so that we could observe the relative contributions of each node in the Bayesian network to the final answer. Figure 2.13



(a) SPM: no attack

(b) SPM: under 25dB attack

(c) ABP: no attack

(d) ABP: under 25dB attack

(e) BN: no attack

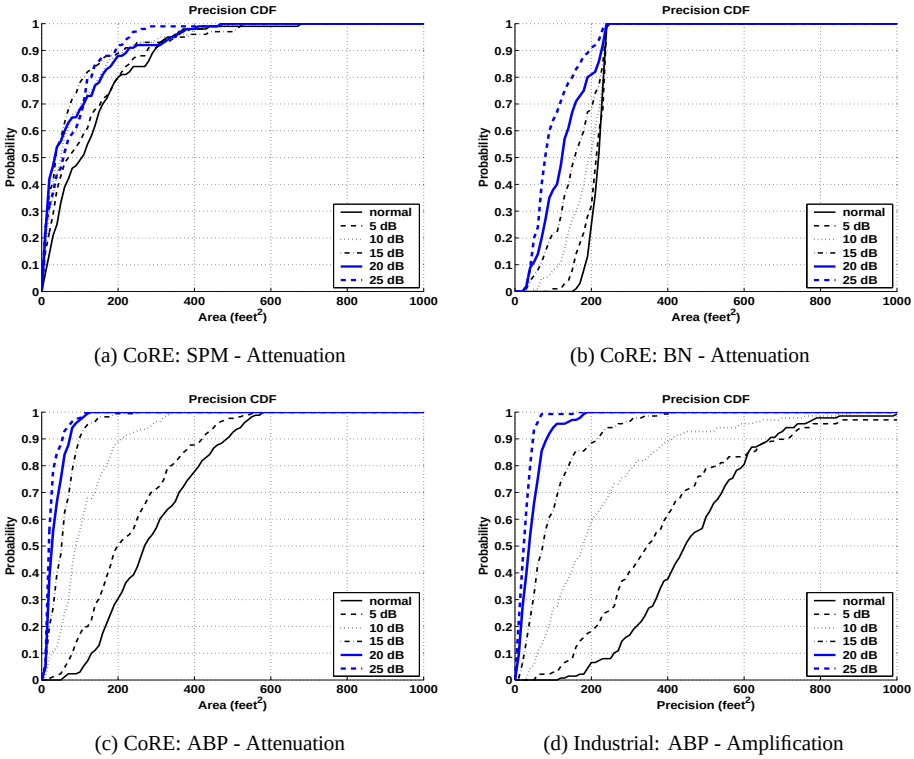
(f) BN: under 25dB attack

Figure 2.14: CoRE: Comparison of localization results from the area-based algorithms for a testing point.

shows the percentage contribution for each landmark to overall joint-density. For instance, in CoRE, the contribution of each landmark starts almost uniformly. When Landmark 1 under attack, the contribution of Landmark 1 goes from 0.25 down to 0.15.

2.5.5 Precision Study

In this section, we examine the area-based algorithms' precision in response to attacks. Figure 2.14 shows a localization example of the area-based algorithms in the CoRE building. The actual point is shown as a big dot and the convex hulls of the returned areas are outlined. Normally, the SPM and ABP algorithms perform similarly, while the BN algorithm has a much



(a) CoRE: SPM - Attenuation

(b) CoRE: BN - Attenuation

(c) CoRE: ABP - Attenuation

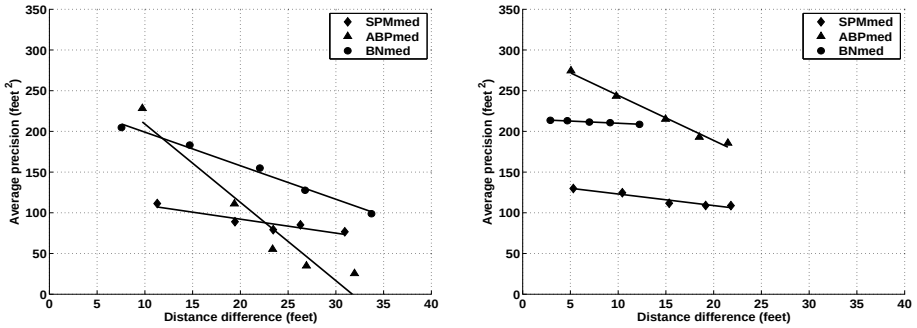
(d) Industrial: ABP - Amplification

Figure 2.15: Analysis of precision CDF across area-based algorithms. The attack is performed on all the landmarks.

different profile by returning the sampling distribution of the possible estimation. Under signal strength attacks, We observed that the returned areas are reduced and shifted from the true location.

Figure 2.15 shows the CDF of the precision (i.e. size of the returned area) for different area-based algorithms under attack for all the landmarks in CoRE and Industrial Lab. We found that overall the algorithms did not become less precise in response to attacks, but rather, the algorithms tended to shift and shrink the returned areas. Figure 2.15(a) shows a small average shrinkage for SPM in the CoRE building, and likewise, 2.15(b) shows a similar effect for BN.

ABP-75 had the most dramatic effect. Figures 2.15(c) and 2.15(d) show the precision versus the attack strength for both buildings. The shrinkages are quite substantial. We found that, under attack, the probability densities of the tiles shrank to small values that were located on a few tiles– reflecting the fact that an attack causes there not to be a likely position to localize a node. We also found that this effect held for amplification attacks, as is shown in



(a) CoRE: all landmarks (b) CoRE: Landmark 1

Figure 2.16: Precision vs. perturbation distance under attenuation attack.

Table 2.5: Analysis of (worst-case) H and (average-case) $\overline{H}$

Algorithms	**CoRE:** H	**LAB:** H	**CoRE:** $\overline{H}$	**LAB:** $\overline{H}$
Area-Based				
SPM	23.7646	11.0659	1.8856	2.3548
ABP-75	20.0347	23.0652	1.8548	2.3424
BN	31.7324	14.9168	2.0595	2.5873
Point-Based				
R1	36.2400	20.7846	1.9750	2.3677
R2	19.8586	8.7313	1.9138	2.3058
GR	35.9880	20.6886	1.9691	2.3628
P1	20.8832	20.7846	1.9793	2.3683
P2	19.8586	8.7313	1.9178	2.3058
GP	21.8303	20.6886	1.9649	2.2882

Figure 2.15(d). The shrinking precision behavior may be useful for attack detection, although a full characterization of how this effect occurs remains for future work.

Examining this effect further, Figure 2.16 presents the precision vs. the perturbation distance $\|\mathbf{p}_{med} - \tilde{\mathbf{p}}_{med}\|$, with a least squares line fit. Figure 2.16(a) shows the effect when attacking all landmarks on the CoRE building. Figure 2.16(b) shows a downward trend, but much weaker, when one landmark is under attack. We observed similar results for the Industrial Lab. We see mostly linear changes in precision in response to attacks, although with great differences between the algorithms. The figures show that the decrease in precision as a function of dB is particularly strong for ABP-75.

2.6 Discussion about Hölder Metrics

In the previous section we examined the experimental results, and looked at the performance of a set of representative localization algorithms in terms of error and precision. We now focus on the performance of these localization algorithms in terms of the Hölder metrics. The Hölder metrics measure the variability of the *returned* answer in response to changes in the signal strength vectors.

We first discuss the practical aspects of measuring H and $\overline{H}$ for different algorithms. In Section 2.4, the Hölder parameters are defined by calculating the maximum and average over the entire n-dimensional signal strength space. In practice, it is necessary to perform a sampling technique to measure H and $\overline{H}$. Additionally, as noted earlier, the definition of H and $\overline{H}$ are only suitable for (Hölder) continuous functions G_{alg}. In reality, several localization algorithms, such as RADAR, are not continuous and involve the tessellation of the signal strength space into Voronoi cells V_j, and thus only a discrete set of localization results are produced (image of V_j under G_{alg}). Hence, for any $\mathbf{s} \in V_j$ we have $G_R(\mathbf{s}) = (x_j, y_j)$. Unfortunately, for neighboring Voronoi cells, we may take $\mathbf{s} \in V_j$ and $\mathbf{v} \in V_i$ such that they are arbitrarily close (i.e. $\|\mathbf{s} - \mathbf{v}\| \to 0$), while $\|G_R(\mathbf{s}) - G_R(\mathbf{v})\| \neq 0$. In such a case, the formal calculation of H and $\overline{H}$ is not possible. However, for our purposes, we are only interested in measuring the notion of adjacency of Voronoi cells in signal space yielding *close* localization results. Thus, our calculation of H and $\overline{H}$ is only performed over the centroids of the various Voronoi cells for localization algorithms that tessellate of signal strength space.

The Hölder parameters for the different localization algorithms are presented in Table 2.5. Examining these results, there are several important observations that can be made. First, if we examine the results for $\overline{H}$ we see that, for each building, all of the algorithms have very similar $\overline{H}$ values. Hence, we may conclude that the average variability of the returned localization result to a change in the signal strength vector is roughly the same for all algorithms. This is an important result as it means, regardless of which RF fingerprinting localization system we deploy, the average susceptibility of the returned results to an attack is essentially identical.

However, if we examine the results for H, which reflects the worst-case susceptibility, then we see that there are some differences across the algorithms. First, comparing H and $\overline{H}$ for

both point-based and area-based algorithms, we see that the worst-case variability can be much larger than the average variability. Additionally, the point-based methods appear to cluster. Notably, RADAR (R1) and Gridded Radar (GR) have similar performance across both CoRE and the Industrial Lab, while averaged RADAR (R2) and averaged Highest Probability (P2) have similar performance across both buildings. A very interesting phenomena is observed by looking at the algorithms that returned an average of likely locations (R2 and P2). Across both buildings these algorithms exhibited less variability compared to other algorithms. This is to be expected as averaging is a smoothing operation, which reduces variations in a function. This observation suggests that R2 and P2 are more robust from a worst-case point-of-view than other point-based algorithms.

2.7 Conclusion

In this chapter, we analyzed the robustness of RF-fingerprinting localization algorithms to attacks that target signal strength measurements. We first examined the feasibility of conducting amplification and attenuation attacks, and observed a linear dependency between non-attacked signal strength and attacked signal strength readings for different barriers placed between the transmitter and a landmark receiver. We provided a set of performance metrics for quantifying the effectiveness of an attenuation/amplification attack. Our metrics included localization angular bias, localization error, the precision of area-based algorithms, and a new family of metrics, called Hölder metrics, that quantify the variability of the returned location results versus change in signal strength vectors.

We conducted a trace-driven evaluation of several point-based and area-based localization algorithms where the linear attack model was applied to data measured in two different office buildings. We found that the localization error scaled similarly for all algorithms under attack. Further, we found that, when attacked, area-based algorithms did not experience a degradation in precision although they experienced degradation in accuracy. We then examined the variability of the localization results under attack by measuring the Hölder metrics. We found that all algorithms had similar average variability, but those methods returned the average of a set of

most likely positions exhibited less variability. This result suggests that the average susceptibility of the returned results to an attack is essentially identical across point-based and area-based algorithms, though it might be desirable to employ either area-based methods or point-based methods that perform averaging in order to lessen the worst-case effect of a potential attack.

Chapter 3

Attack Detection in Wireless Localization

3.1 Introduction

In this chapter, we examine the problem of detecting attacks on wireless localization. We present a general formulation for attack detection using statistical significance testing and then build tests that are applicable to broad classes of multilateration and signal strength-based methods, as well as several other test statistics that are unique to a variety of different localization algorithms.

Multilateration is a popular localization approach that uses Least Squares (LS) techniques to perform localization [23, 28, 44, 49, 54], and has the desirable property of supporting mathematical analysis, in part because LS-based regression has well-known statistical descriptions when operating near ideal conditions. By examining Linear Least Squares (LLS), we build a mathematical model and derive an analytic solution for attack detection using the residuals of an LLS regression. We show that attack detection using LLS is easy to conduct and is suitable for both single-hop and multi-hop ranging methods because it is independent of the ranging modality used by the localization system.

On the other hand, many signal strength based algorithms [12, 27] rely on either statistical inference or machine-learning in the context of scene matching to perform localization, and consequently do not yield closed-form solutions. However, for algorithms based on signal strength, we found that the minimum distance between an observation and the database of signal strength vectors is a good test statistic to perform attack detection. One key advantage of our approach for signal strength based methods is that the detection phase can be performed before localization.

To evaluate the effectiveness of our attack detection mechanisms we first present experimental results illustrating the feasibility of physical attacks on localization. We then conducted a trace driven evaluation using both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network in two real office buildings. In particular, we applied signal strength attenuation and amplification, using a linear attack model obtained from our experiments, to the Received Signal Strength (RSS) readings collected from these two office buildings. We evaluated the performance of our attack detection schemes using detection rates and receiver operating characteristic curves. Our experimental results provide strong evidence of the effectiveness of our attack detection schemes with high detection rates, over 95%, and low false positive rates, often under 5%. Surprisingly, we found that most of the attack detection schemes provide qualitatively similar performance. This shows that the different localization systems have similar attack detection capabilities.

The rest of the chapter is organized as follows. We study the feasibility of attacks and present our experimental methodologies in Section 3.2. We present our generalized theoretical formulation for the attack detection problem in Section 3.3. We next derive an analytic solution for attack detection using Least Squares in Section 3.4. Using common features for attack detection in signal strength based algorithms is presented in Section 3.5. We study the test statistics that are specific to a variety of different algorithms in Section 3.6. Then, we provide a discussion in Section 3.7. Finally, we conclude in Section 3.8.

3.2 Feasibility of Attacks

In this section we provide background on how attackers can impact the localization system. We next discuss the feasibility of conducting these attacks on signal strength, and provide the experimental methodology that we use to evaluate our attack detection mechanisms later in this chapter.

3.2.1 Localization Attacks

Localization mechanisms are built upon different ranging modalities, such as RSS, TOA, AOA, and hop count. These all rely on the measurement of the physical properties of the wireless system. Adversaries can apply non-cryptographic attacks against the measurement processes, bypassing conventional security services, and as a result can affect the localization performance. For example, wormhole attacks tunnel through a faster channel to shorten the observed distance between two nodes [36]. An attenuation attack would decrease the radio range, and thus potentially lengthen the hop-count. Compromised nodes may delay response messages to disrupt distance estimation [49]. RSS readings can be altered due to attenuation or amplification of the signal strength by an adversary [22]. A broad survey of the potential non-cryptographic attacks that are unique to localization can be found in [49].

3.2.2 Signal Strength Attacks

We choose to use RSS as the ranging modality for localization algorithms. An adversary can attack the wireless node directly or compromise the landmarks involved in localization by attenuating or amplifying the signal strength readings. Based on our experimental attacks using real materials, we will use the linear attack model [22] (i.e. a material causes a constant percentage power loss independent of distance) as shown in Figure 3.1 to describe the effect of an attack on the RSS readings at the wireless device or at the landmarks. As presented in the figure, these attacks are easy to conduct with low cost materials. The linear relationship implies that it is easy for an adversary to control the effect of an attack on the observed signal strength by appropriately selecting different materials.

3.2.3 Experimental Methodology

In order to study the generality of our attack detection approaches, we have conducted experiments in two office buildings, one is the 3rd floor of the Computer Science building at Rutgers University (CoRE) as shown in Figure 3.2 (a) and the other is in a floor of an industrial research lab (Industrial Lab) as presented in Figure 3.2 (b). In Figure 3.2 (a), the experiments are performed for both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network. For

the 802.11 (WiFi) network, there are 4 landmarks shown in red squares deployed in a collinear manner to maximize signal strength coverage. While for the 802.15.4 (ZigBee) network, there are 4 landmarks shown in magenta circles placed in a square set to maximize localization accuracy [20]. For experiments conducted in the industrial lab, as depicted in Figure 3.2 (b), we only used an 802.11 (WiFi) network with 5 landmarks. The small green dots are the localization testing points and the small blue stars are the training points. We will present the results of our experiments for each of the proposed attack detection cases in its associated section in this chapter. Across all experiments, we have performed a trace-driven evaluation by either attenuating or amplifying RSS readings collected from these two buildings.

3.3 Generalized Attack Detection Model

In this section we first propose a general formulation for the localization attack detection problem. We then introduce metrics for evaluating the effectiveness of our approaches.

3.3.1 Localization Attack Detection

In general, the error of a localization algorithm is defined as the distance between the true location $\mathbf{x} = [x, y]^T$ and the estimated location $\hat{\mathbf{x}}$, $D_{err} = \|\mathbf{x} - \hat{\mathbf{x}}\|$. We found in prior work that under physical attacks, the localization error D_{err} increases significantly [22]. However, D_{err} is not directly available during run-time, and the challenge in attack detection is to devise strategies for detecting localization attacks that do not use localization errors.

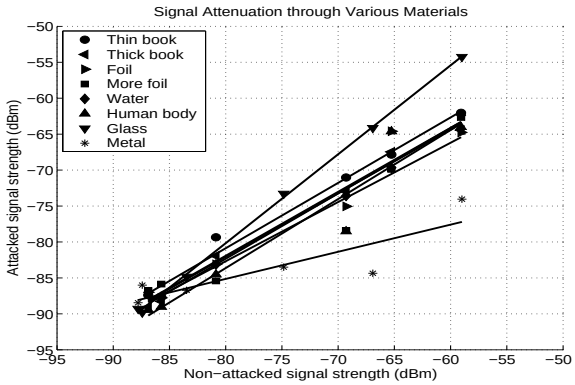
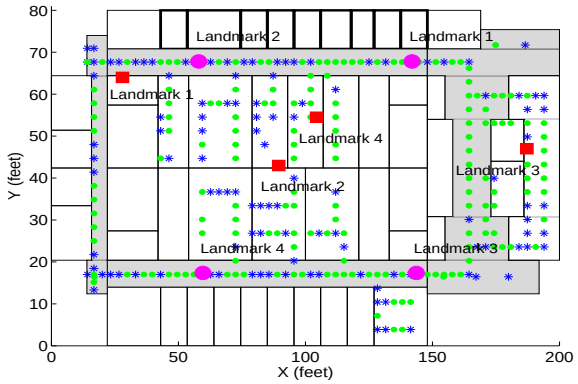
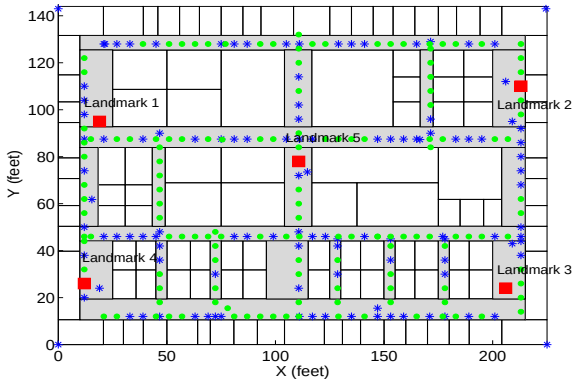


Figure 3.1: Linear attack model on received signal strength for various media.



(a) CoRE Building



(b) Industrial Lab

Figure 3.2: Layout of the experimental floor

We propose to formulate location attack detection as a statistical significance testing problem, where the null hypothesis is

$$\mathcal{H}_0 : \text{normal (no attack)}.$$

In significance testing, a test statistic $\mathbf{T}$ is used to evaluate whether observed data belongs to the null-hypothesis or not. For a particular significance level, α (defined as the probability of rejecting the hypothesis if it is true), there is a corresponding *acceptance region* Ω such that we declare the null hypothesis valid if an observed value of the test statistic $\mathbf{T^{obs}} \in \Omega$, and reject the null hypothesis if $\mathbf{T^{obs}} \notin \Omega$ (i.e. declare an attack is present if $\mathbf{T^{obs}} \in \Omega^c$, where Ω^c is the *critical region* of the test). In our attack detection problem, the region Ω and decision rule is specified according to the form of the detection statistic $\mathbf{T}$ (for example, when using distance in signal strength space for $\mathbf{T}$, the decision rule becomes comparison against a threshold), and

rejection of the null hypothesis corresponds to declaring the presence of an attack.

3.3.2 Effectiveness

In order to evaluate the effectiveness of our attack detection methods, we will utilize the following performance metrics:

Cumulative Distribution Function (CDF): The CDF of the test statistic $\mathbf{T}$ provides the sensitivity of $\mathbf{T}$ under attack. Based on the CDF, we can study the feasibility of using $\mathbf{T}$ for attack detection.

Detection Rate (DR): An attack may cause the significance test to reject $\mathcal{H}_0$. We are thus interested in the statistical characterization of the attack detection attempts over all the localization attempts. The Detection Rate is defined as the percentage of localization attempts that are determined to be under attack, i.e.:

$$DR = \frac{N_{attack}}{N_{total}} \tag{3.1}$$

where N_{total} is the total number of localization attempts and N_{attack} is the number concluded under attack by detection. Note that when the signal is attacked, the detection rate corresponds to the probability of detection P_d, while under normal (non-attack) conditions it corresponds to the probability of declaring a false positive P_{fa}. We will examine DR as a function of the attack strength.

Receiving Operating Characteristic (ROC) curve: To evaluate an attack detection scheme we want to study the false positive rate P_{fa} and probability of detection P_d together. The ROC curve is usually used to measure the tradeoff between false-positives and correct detections. The ROC curve is a plot of attack detection accuracy against the false positive rate. It can be obtained by varying the detection thresholds.

3.4 Using Least Squares

In this section we provide mathematical analysis for attack detection in multilateration algorithms. We first provide background in using LS to perform localization. Next, based on the properties of the LLS estimator, we define an attack detection scheme that utilizes regression

residuals, and give an analytic formulation to specify the acceptance region Ω. Finally, the experimental results are presented to evaluate the effectiveness of the detection scheme.

3.4.1 Localization

To perform localization with LS requires 2 steps: ranging and lateration.

Ranging Step: Recent research has seen a host of variants on the ranging step such as RSS, TOA, TDOA, and hop count. Our attack detection approach works with any ranging modality.

Lateration Step: From the estimated distances d_i and known positions (x_i, y_i) of the landmarks, the position (x, y) of the localizing node can be found by finding $(\hat{x}, \hat{y})$ satisfying:

$$(\hat{x}, \hat{y}) = arg \min_{x,y} \sum_{i=1}^{n} [\sqrt{(x_i - x)^2 + (y_i - y)^2} - d_i]^2 \tag{3.2}$$

where n is the total number of landmarks. We call solving the above problem *Nonlinear Least Squares*, or NLS. Solving the NLS problem requires significant complexity and is difficult to analyze. We may approximate the NLS solution and linearize the problem [20] into the system $\mathbf{Ax} = \mathbf{b}$, where:

$$\mathbf{A} = \begin{pmatrix} x_1 - \frac{1}{n}\sum_{i=1}^{n} x_i & y_1 - \frac{1}{n}\sum_{i=1}^{n} y_i \\ \vdots & \vdots \\ x_n - \frac{1}{n}\sum_{i=1}^{n} x_i & y_n - \frac{1}{n}\sum_{i=1}^{n} y_i \end{pmatrix} \tag{3.3}$$

and

$$\mathbf{b} = \frac{1}{2} \begin{pmatrix} (x_1^2 - \frac{1}{n}\sum_{i=1}^{n} x_i^2) + (y_1^2 - \frac{1}{n}\sum_{i=1}^{n} y_i^2) \\ -(d_1^2 - \frac{1}{n}\sum_{i=1}^{n} d_i^2) \\ \vdots \\ (x_n^2 - \frac{1}{n}\sum_{i=1}^{n} x_i^2) + (y_n^2 - \frac{1}{n}\sum_{i=1}^{n} y_i^2) \\ -(d_n^2 - \frac{1}{n}\sum_{i=1}^{n} d_i^2) \end{pmatrix}. \tag{3.4}$$

Note that $\mathbf{A}$ is described by the coordinates of landmarks only, while $\mathbf{b}$ is represented by the distances to the landmarks together with the coordinates of landmarks. We call the above formulation of the problem *Linear Least Squares*, or LLS. The estimate of $\mathbf{x} = [x, y]^T$ is done via

$$\mathbf{x} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b} \tag{3.5}$$

In addition to its computational advantages, the LLS formulation allows for tractable statistical analysis, as we shall now see.

3.4.2 The Residuals

In practice, there are estimation errors from the ranging step. The LLS formulation can be refined as a linear regression, $\mathbf{b} = \mathbf{A}\mathbf{x} + \mathbf{e}$, where $\mathbf{e}$ corresponds to model errors. The localization result is then $\hat{\mathbf{x}} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}$, and the fitted values $\hat{\mathbf{b}}$ corresponding to the observed values $\mathbf{b}$ are given by

$$\hat{\mathbf{b}} = \mathbf{A}\hat{\mathbf{x}} = \mathbf{A}[(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}] = \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}. \tag{3.6}$$

Further, we define the vector of residuals $\hat{\mathbf{e}}$ as

$$\hat{\mathbf{e}} = \mathbf{b} - \hat{\mathbf{b}} = [1 - \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T]\mathbf{b}. \tag{3.7}$$

When the regression model is performing well we may assume that the model errors are Gaussian [41,65]. Under this assumption, the residuals also follow a Gaussian distribution, $\mathbf{N}(\mu, \mathbf{\Sigma})$, since the residuals are a linear combination of the elements of $\mathbf{b}$ and $\mathbf{e}$. Here, μ is the mean vector and $\mathbf{\Sigma}$ is the covariance matrix. We choose the residuals $\hat{\mathbf{e}}$ as the test statistic $\mathbf{T}$, and will build our attack detection scheme by using the statistical properties of $\hat{\mathbf{e}}$ when LLS is operating in a desirable performance regime.

3.4.3 The Detection Scheme

The LLS attack detection is performed after localization. The residuals are correlated Gaussian random variables and the multivariate Gaussian distribution of $\hat{\mathbf{e}}$ can be expressed as:

$$f(\hat{\mathbf{e}}) = \frac{1}{(\sqrt{2\pi})^n |\mathbf{\Sigma}|^{\frac{1}{2}}} e^{-\frac{1}{2}(\hat{\mathbf{e}}-\mu)^{\mathbf{T}}\mathbf{\Sigma}^{-\mathbf{1}}(\hat{\mathbf{e}}-\mu)}. \tag{3.8}$$

In order to determine whether the location result is compromised by adversaries, we perform attack detection through significance testing. We can define an acceptance region in $\hat{\mathbf{e}}$ space by

$$\Omega = \{\hat{\mathbf{e}} : Pr(\{\mathbf{T} : (\mathbf{T}-\mu)^T\mathbf{\Sigma}^{-1}(\mathbf{T}-\mu) >$$

$$(\hat{\mathbf{e}}-\mu)^T\mathbf{\Sigma}^{-1}(\hat{\mathbf{e}}-\mu)\}) > \alpha\}.$$

In practice, after performing localization using LLS, we have an observed value of residuals $\hat{\mathbf{e}}^{\mathbf{obs}}$. Testing the null hypothesis, we can decide that the localization is under attack if the probability $P = 1 - M < \alpha$, where

$$M = \frac{1}{(\sqrt{2\pi})^n |\mathbf{\Sigma}|^{\frac{1}{2}}} \int ... \int_E e^{-\frac{1}{2}(\hat{\mathbf{e}}-\mu)^{\mathbf{T}}\mathbf{\Sigma}^{-\mathbf{1}}(\hat{\mathbf{e}}-\mu)} d\hat{e}_1 ... d\hat{e}_n \tag{3.9}$$

and E is the integration region defined by $(\hat{\mathbf{e}}-\mu)^{\mathbf{T}}\mathbf{\Sigma^{-1}}(\hat{\mathbf{e}}-\mu) \leq X^2$ with

$$X^2 = (\hat{\mathbf{e}}^{\mathbf{obs}}-\mu)^{\mathbf{T}}\mathbf{\Sigma^{-1}}(\hat{\mathbf{e}}^{\mathbf{obs}}-\mu).$$

We can express the term

$$\begin{aligned}(\hat{\mathbf{e}}-\mu)^{\mathbf{T}}\mathbf{\Sigma^{-1}}(\hat{\mathbf{e}}-\mu) &= (\hat{\mathbf{e}}-\mu)^{\mathbf{T}}\mathbf{D}^{\mathbf{T}}\mathbf{D}(\hat{\mathbf{e}}-\mu) \\ &= (\mathbf{D}(\hat{\mathbf{e}}-\mu))^{\mathbf{T}}(\mathbf{D}(\hat{\mathbf{e}}-\mu)) \\ &= \mathbf{y}^{\mathbf{T}}\mathbf{y}. \end{aligned} \tag{3.10}$$

Substituting $\mathbf{y} = \mathbf{D}(\hat{\mathbf{e}}-\mu)$ into Equation (3.9), we get

$$\begin{aligned} M &= \frac{1}{(\sqrt{2\pi})^n}\int ... \int_{E'} e^{-\frac{1}{2}\mathbf{y}^{\mathbf{T}}\mathbf{y}} dy_1 ... dy_n \\ &= \frac{1}{(\sqrt{2\pi})^n}\int ... \int_{E'} e^{-\frac{1}{2}\sum_{i=1}^{n} y_i^2} dy_1 ... dy_n \end{aligned} \tag{3.11}$$

with E' defined by $\mathbf{y}^{\mathbf{T}}\mathbf{y} \leq X^2$. Changing to polar coordinates, we get

$$\begin{aligned} M &= \frac{1}{(\sqrt{2\pi})^n}\int_0^X \int_0^{2\pi} \int_0^{\pi} ... \int_0^{\pi} [e^{-\frac{r^2}{2}} r^{n-1} dr d\phi_1 \\ &\quad sin\phi_2 d\phi_2 ... sin^{n-2}\phi_{n-1} d\phi_{n-1}] \\ &= \frac{1}{(\sqrt{2\pi})^n}\int_0^X e^{-\frac{r^2}{2}} r^{n-1} dr \times \int_0^{2\pi} d\phi_1 \\ &\quad \times \prod_{i=2}^{n-1} \int_0^{\pi} sin^{i-1}\phi_i d\phi_i \\ &= \frac{2}{(\sqrt{\pi})^{n-2}} \times A_{r,n} \times \prod_{i=2}^{n-1} B_i \end{aligned} \tag{3.12}$$

with

$$A_{r,n} = \frac{1}{(\sqrt{2})^n}\int_0^X e^{-\frac{r^2}{2}} r^{n-1} dr$$

and

$$B_i = \int_0^{\pi} sin^{i-1}\phi_i d\phi_i.$$

Using $v = r^2/2$, we have

$$A_{r,n} = \frac{1}{2}\int_0^{\frac{X^2}{2}} e^{-v} v^{\frac{n-2}{2}} dv = \frac{1}{2} \times \Gamma(\frac{n}{2}, \frac{X^2}{2}) \tag{3.13}$$

where Γ is the incomplete gamma function. Since

$$B_i = \beta(\frac{i}{2}, \frac{1}{2}) = \frac{\Gamma(\frac{i}{2})}{\Gamma(\frac{i+1}{2})} \times \sqrt{\pi}. \tag{3.14}$$

Through further simplification, we can get

$$\prod_{i=2}^{n-1} B_i = (\sqrt{\pi})^{n-2} \times \frac{1}{\Gamma(\frac{n}{2})}. \tag{3.15}$$

Hence, substituting Equations (3.13) and (3.15) into (3.12), we obtain the probability mass

$$M = \frac{\Gamma(n/2, X^2/2)}{\Gamma(n/2)}.$$

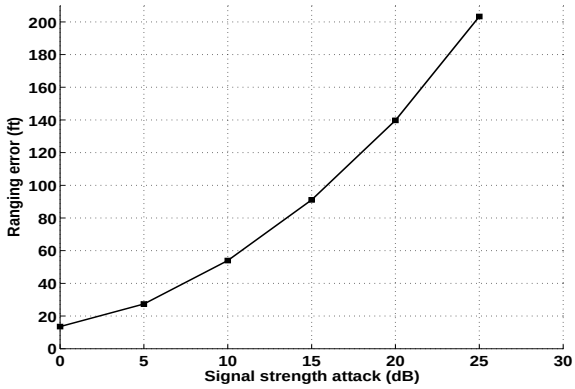
We then further obtain the probability by $P = 1 - M$. Based on the definition in Section 3.3, if the probability is sufficiently low, i.e. $P < \alpha$, then $\hat{\mathbf{e}}^{\mathbf{obs}}$ belongs to the critical region Ω^c and we can conclude that the location result is under attack.

3.4.4 Experimental Evaluation

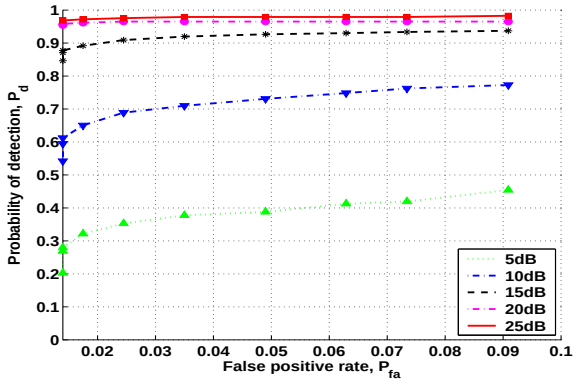
In this section we present the evaluation of the effectiveness of the attack detection scheme. We chose RSS as the ranging modality and performed signal strength attacks according to the experimental methodologies described in Section 3.2.

The average ranging error as a function of the severity of signal strength attacks is shown in Figure 3.3(a). We know that the relationship between the RSS error and the ranging error is multiplicative with distance [20]. Even small random perturbation in RSS readings can cause large ranging errors due to this multiplicative factor. We observed this effect in Figure 3.3(a); the ranging error increases superlinearly to attack severity. Figure 3.4 presents DR vs. the ranging errors when tested against significance level $\alpha = 0.01$ and $\alpha = 0.05$. We found that under a normal situation, where the ranging errors are less than 15 feet, the false alarm probability, P_{fa}, is less than 1.5% and 2.5% for $\alpha = 0.01$ and $\alpha = 0.05$ respectively. Large signal strength attacks, greater than 15dB, can cause ranging errors larger than 90 feet, and then the detection rates are more than 90%. These results strongly indicate that using residuals in LS as a test statistic for attack detection is effective.

Further, the ROC curves in Figure 3.3(b) show that for false positive rates less than 10%, the detection rates are above 90% and close to 99% when the attack strength increases to 20dB and 25dB. This shows that if the adversary wants to cause a large localization error, it is almost certain that our attack detection mechanism will detect it. For small attacks of less than 5dB, the detection rates are about 40%. In this case, it is difficult to distinguish whether the anomaly

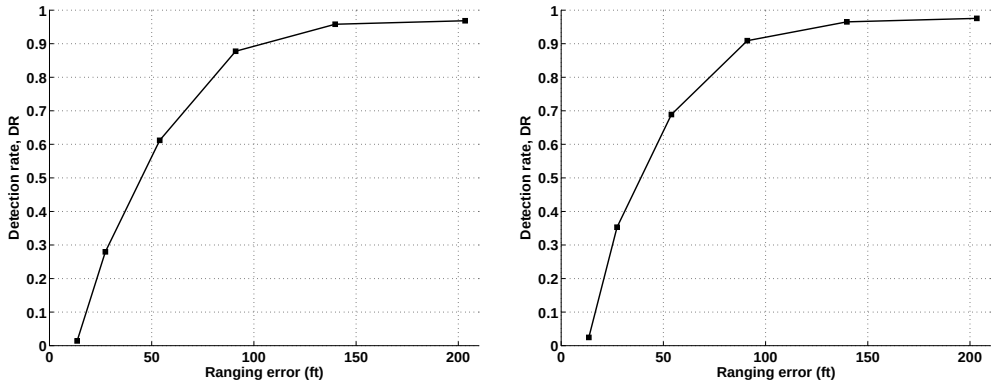


(a) Ranging errors



(b) ROC curves

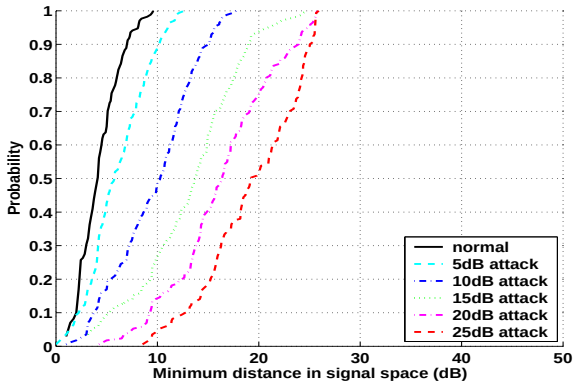
Figure 3.3: CoRE 802.11: (a) Ranging errors under the signal strength attacks (b) LLS residuals: Receiver Operating Characteristic (ROC) curves



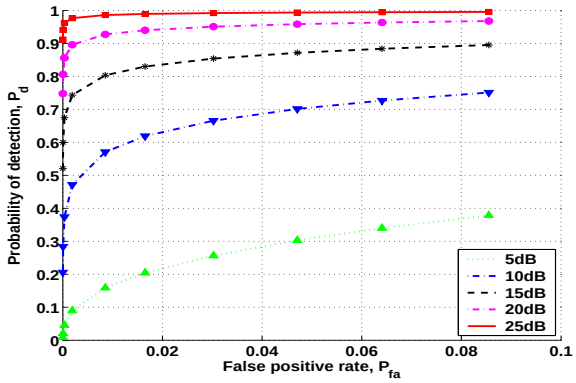
(a) LOA: $\alpha = 0.01$

(b) LOA: $\alpha = 0.05$

Figure 3.4: CoRE 802.11, LLS residuals: effectiveness of attack detection



(a) CDF



(b) ROC curves

Figure 3.5: CoRE 802.11: (a) Cumulative Distribution Function (CDF) of minimum distance D_s in signal space. (b) Minimum distance D_s: Receiver Operating Characteristic (ROC) curves.

in the test statistic is caused by attacks or by measurement errors since the RSS readings can fluctuate around 5dB due to environmental effects. However, for such small attacks, because the resulting impact on the final localization result was shown to be small [22], the consequences of failing to detect such attacks would likely be small as well.

3.5 Distance In Signal Space

RSS is a common physical property used by a widely diverse set of algorithms. For example, most scene matching approaches utilize the RSS, e.g. [12, 14], and many multilateration approaches [52] use it as well. In spite of its several meter-level accuracy, using the RSS is

an attractive approach because it can re-use the existing wireless infrastructure — this feature presents a tremendous cost savings over deploying localization-specific hardware. In this section, we thus derive an attack detection scheme applicable to any signal strength based localization system.

3.5.1 Overview

All of the above algorithms take a vector $\mathbf{s}$ of n RSS readings to (or from) n landmarks for the node to be localized. Note that $\mathbf{s}$ corresponds to a point in a n-dimensional signal space [22]. Under normal conditions, the RSS vectors obtained from the physical positions in a floor form a surface S in the n-dimensional signal space; we can think of this surface as comprising 'valid' points in signal space. Due to measurement noise, multipath effects, and unknown biases, $\mathbf{s}$ will fluctuate around this idealized RSS surface.

A localization attacker would perturb the correct $\mathbf{s}$ to produce a corrupted n-dimensional RSS vector $\mathbf{s}'$. In signal space, $\mathbf{s}'$ will be moved away from the ideal surface constructed by the correct RSS vectors. The stronger the attack, the more likely the vector $\mathbf{s}'$ will be distant from the RSS surface. We thus choose the minimum distance to the surface S, i.e. $D_s = \min\{\|\mathbf{s}' - \mathbf{s}^j\| : \text{where } \mathbf{s}^j \in S\}$, as the test statistic for signal strength based attack detection. The key advantage of this approach is that the attack detection is independent of the localization algorithms and can be performed before the localization process.

Although it is possible to devise a statistical model for D_s based on models for normal measurement errors, in this section we shall take a different approach and apply empirical methodologies from training data to determine thresholds for defining the critical region.

3.5.2 Finding Thresholds

Choosing an appropriate threshold τ will allow the detection scheme to be robust to false detections. In order to obtain the thresholds, we don't need to know the exact RSS surface in the signal space (in practice, it is hard to determine and exhibits discontinuities due to wall boundaries). Instead, we can obtain the thresholds through empirical training. During the offline phase, we can collect the RSS vectors for a set of known positions over the floor and construct

a radio map. During the localization phase, we get an observed vector $\mathbf{s^{obs}}$, and we can then determine whether the $\mathbf{s^{obs}}$ is being attacked by calculating the D_s using the pre-constructed radio map.

We define that if

$$D_s > \tau, \tag{3.16}$$

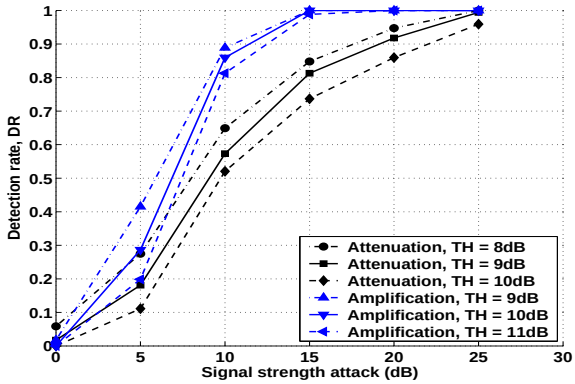
the signal strength readings are under attack. We use the distribution of the training data to help decide on the thresholds. Figure 3.5 (a) shows the CDF of the D_s in signal space. We found that the curve of D_s shifted to the right under signal strength attacks, especially for larger attacks, thereby suggesting that we can use D_s as a test statistic for detecting attacks, and also that we can use the non-attacked CDF to obtain τ for a given α value.

3.5.3 Experimental Evaluation

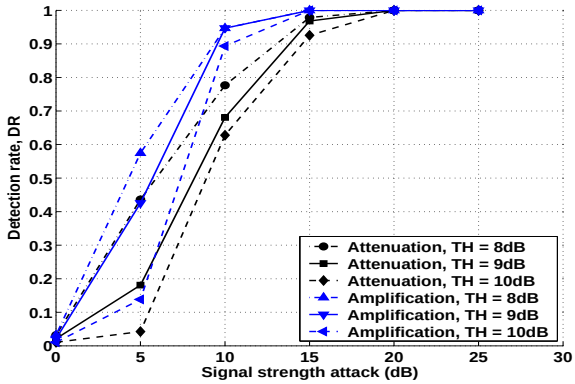
We next present the evaluation of the effectiveness of using minimum distance D_s for attack detection. Figure 3.6 presents the Detection Rate under different threshold (TH) levels as a function of signal strength attacks for both the 802.11 and the 802.15.4 networks in CoRE and the 802.11 network in the Industrial Lab. Figure 3.5 (b) is the corresponding ROC curves under signal attenuation attacks for the 802.11 network in CoRE. We found that, in general, the effectiveness of the attack detection scheme is similar across the different networks and buildings. Interestingly, we found that the performance of the attack detection scheme under signal amplification attacks is uniformly better than those for signal attenuation attacks, although the shapes of the DR curves are similar. Because of the higher detection rates under amplification attacks, we do not present additional amplification results in the remainder of the chapter. All these results are highly encouraging because they show our methods are quite general and do not depend on a specific network or environment.

Further, we observed that the DR under the 802.15.4 network in CoRE outperformed the DR under the 802.11 networks in both CoRE and Industrial Lab for the signal attenuation attacks as well as the signal amplification attacks. For attack strengths of 15dB or larger, the DR in the 802.15.4 network is over 95% and equals 100% when attack severity reaches 20dB and larger. We believe that the better landmark placement for localization [20] of the 802.15.4

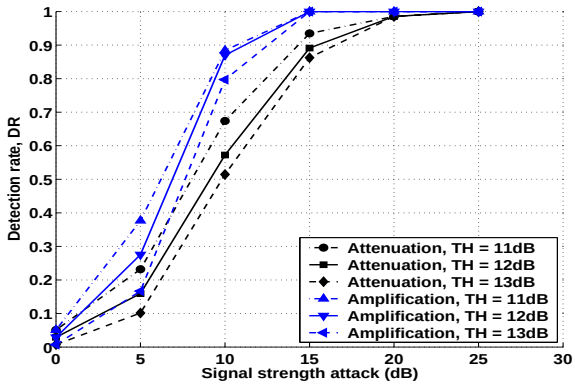
network can account for its higher detection rates, although further investigation of this effect is required.



(a) CoRE 802.11



(b) CoRE 802.15.4



(c) Industrial 802.11

Figure 3.6: Minimum distance in signal space $\mathbf{D_s}$: attack detection across different networks and buildings.

3.6 Other Test Statistics

In this section, we examine algorithm-specific test statistics, which use properties specific to a particular localization algorithm. We have chosen a representative set of diverse algorithms. For the multilateration category, we investigate the NLS algorithm, while for signal strength based algorithms, we study both Area Based Probability (ABP) and Bayesian Networks (BN) algorithms. Detailed descriptions of these can be found in [20, 27, 52].

3.6.1 Nonlinear Least Squares (NLS)

As presented in Section 3.4, NLS is a multilateration algorithm that tries to satisfy the condition shown in Equation (3.2). The estimated $(\hat{x}, \hat{y})$ is the solution that minimizes the Sum of Squared Errors $\mathcal{E}^2$:

$$\mathcal{E}^2 = \sum_{i=1}^{n} [\sqrt{(x_i - \hat{x})^2 + (y_i - \hat{y})^2} - d_i]^2. \tag{3.17}$$

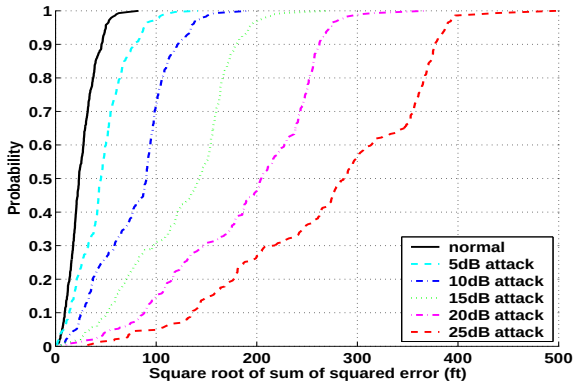
We define a test statistic $\mathcal{E} = \sqrt{\mathcal{E}^2}$ because $\mathcal{E}$ will likely increase under the attack. The CDF of $\mathcal{E}$ presented in Figure 3.7 (a) confirms that the $\mathcal{E}$ grows rapidly with the attack severity. Figure 3.7 (b) and Figure 3.8 show that the performance of attack detection when using $\mathcal{E}$ for the 802.11 network in CoRE is comparable to that using residuals in Section 3.4. The thresholds are also obtained from training.

3.6.2 Area Based Probability (ABP)

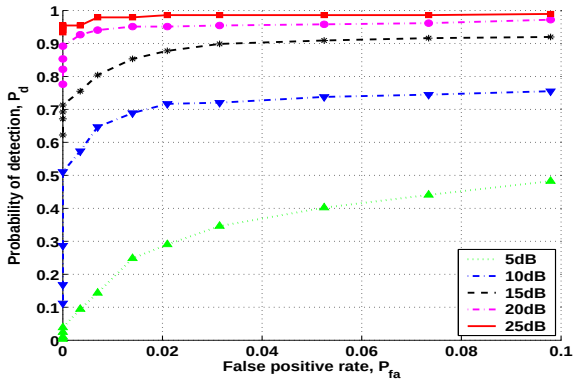
Turning to signal strength based algorithms, ABP is an area-based algorithm that uses Bayes' Rule to return an area which has the highest likelihood of capturing the true location [27]. ABP divides the floor into a set of tiles. The total likelihood that the wireless node resides at each tile is calculated using:

$$P = \prod_{i=1}^{n} P_i \tag{3.18}$$

where n is the total number of landmarks and P_i is the likelihood of observing the measured RSS reading at landmark i which is usually modeled as a Gaussian random variable. The total likelihood is calculated at each tile, and the returned location estimation is either a region whose likelihood is above a certain level, or is the tile with the maximum likelihood.



(a) CDF



(b) ROC curves

Figure 3.7: CoRE 802.11, NLS: (a) Cumulative Distribution Function (CDF) of $\mathcal{E}$. (b) $\mathcal{E}$: Receiver Operating Characteristic (ROC) curves.

When under attack, the corrupted RSS readings reduce the set of likely positions on the floor to localize a node. We found that the highest tile-likelihood denoted as $likelihood_{max}$ decreases significantly under attack, as well as the sum of the likelihoods over all the tiles, $likelihood_{sum}$. We explored both $likelihood_{sum}$ and $likelihood_{max}$ as test statistics. The thresholds are learned from the training data by taking the negative log of the values of the highest likelihood and the sum of the likelihoods.

The effectiveness of using $likelihood_{sum}$ and $likelihood_{max}$ for attack detection in ABP are presented in Figure 3.9 and Figure 3.10. We found that using $likelihood_{sum}$ under threshold equal to 2 had better performance than others in detecting larger attacks, but on the other hand resulted in slightly higher false positive rates around 7%.

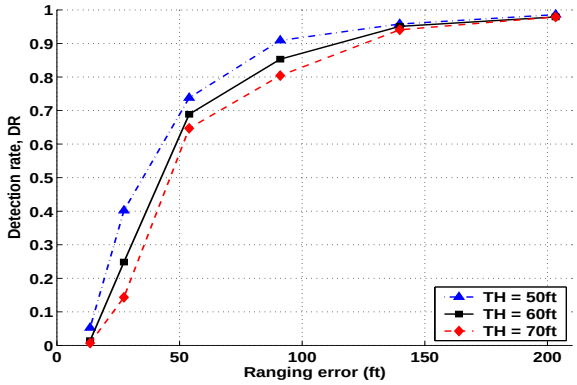


Figure 3.8: CoRE 802.11, NLS using $\mathcal{E}$: effectiveness of attack detection

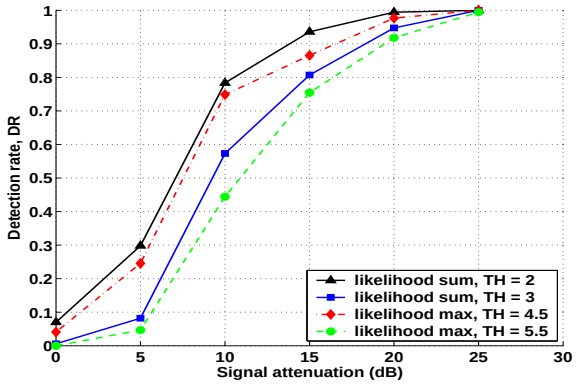


Figure 3.9: CoRE 802.11, ABP: effectiveness of attack detection

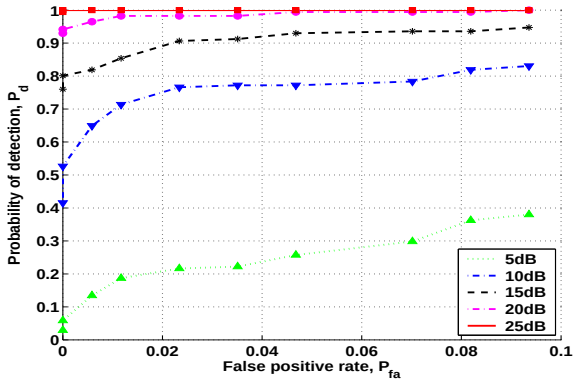


Figure 3.10: CoRE 802.11, ABP: Receiver Operating Characteristic (ROC) curves

3.6.3 Bayesian Networks (BN)

Another representative signal strength based algorithm, BN, utilizes Bayesian networks [52]. With Bayesian statistical inference, BN predicts the probability distribution of the unknown positions. BN uses a Monte-Carlo sampling technique (Gibbs sampling) to compute the full joint-probability distribution for not just the position coordinates, but also for every random variable in the Bayesian network. Without an attack, the contribution from each landmark to the full joint-probability distribution is almost uniform. Under an attack, we found that the contribution from each landmark can become significantly reduced as the attack severity increases. Thus, we can use the fraction of contribution to the joint probability as a test statistic in BN.

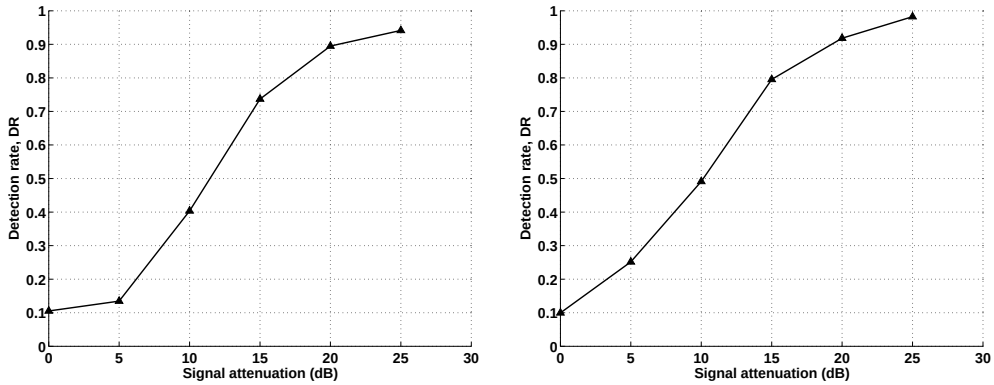
Another method we explored is to use the probability likelihood because the conditional probability distribution of the coordinates in BN relies on the prior and the likelihood. We observed that under an attack, the value of the likelihood became significantly smaller. During the sampling process, the calculation of the likelihood uses the same approach as in Equation (3.18). Because the absolute value of the likelihood is very small, we take the negative log of the likelihood and use it as a test statistic for attack detection in BN.

Figure 3.11 shows the effectiveness of using the fraction of contribution and the likelihood for attack detection in BN. The detection rates are over 90% for attack strength of 20dB or larger. The false positive rates are about 10%. Comparing the absolute performance of these two methods with the other schemes we proposed in this chapter, the performance of these two methods is qualitatively worse.

3.7 Discussion

Comparing all of our detection schemes, Figure 3.12 shows the DR as a function of the signal attenuation attacks for the 802.11 network in the CoRE building. Surprisingly, we found that the performance of all the schemes provided qualitatively similar detection rates, although utilizing the residuals in LLS and the sum of likelihoods in ABP slightly outperformed the others, while using the fraction of contribution and the likelihood in BN underperformed the others.

Based on these similar performance characteristics, it is advantageous to use the minimum



(a) (b)

Figure 3.11: CoRE 802.11, BN: (a) Using fraction of contribution of each landmark for attack detection with threshold = 0.15. (b) Using likelihood in Bayesian inference for attack detection with threshold = 0.25.

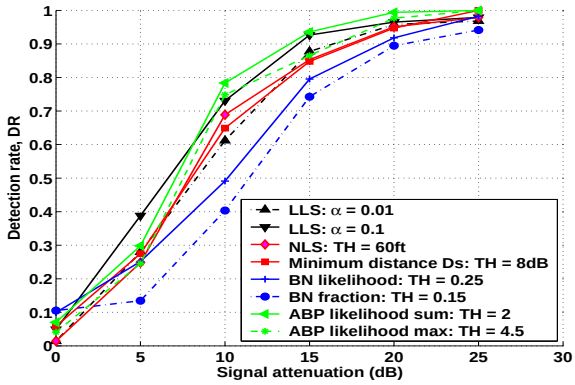


Figure 3.12: CoRE 802.11: Comparison between generic and specific test statistics for attack detection.

distance in the signal space D_s for signal strength based algorithms. Since the attack detection can be performed prior to the localization process and thus results in localization computation cost savings under attack. Additionally, the attack detection performance under the 802.15.4 network when using D_s outperforms the 802.11 network with 100% detection rate for large attacks as shown in Figure 3.6.

Moving to examine the relationship between attack detection and localization error, Figure 3.13 shows the DR when using residuals in LLS for attack detection, and the localization errors under the corresponding signal attacks with different localization algorithms. The figure shows that detection rates are more than 90% for attack strength equal to or greater than 15dB,

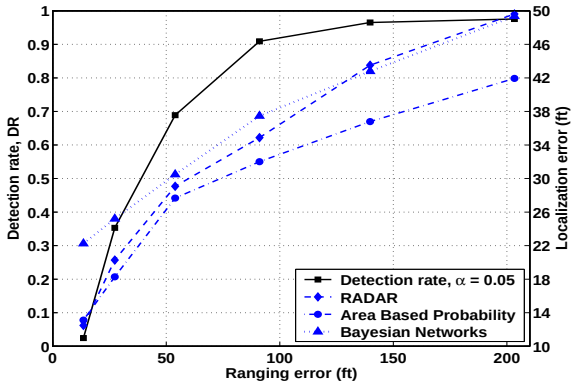


Figure 3.13: CoRE 802.11: Relationships among Detection Rate (DR), ranging error, and localization error.

and at this attack strength the average localization error is about 35ft.

The above result is quite encouraging, as it shows that an attacker cannot cause gross localization errors without there being a very high probability of detection (¿95%). In the case of RSS, with mean errors of 10-15 ft [27], an attacker can not cause errors of about 2-3 times over the average error without a very high probability of detection. Even for detection rates as low as 50%, the attacker's position error is limited to about 20 ft.

3.8 Conclusion

In this chapter, we analyzed the problem of detecting non-cryptographic attacks on wireless localization. We proposed a theoretical foundation by formulating attack detection as a statistical significance testing problem. We then concentrated on test statistics for two broad localization approaches: multilateration and signal strength. For multilateration that uses Linear Least Squares, we derived a closed-form representation for the attack detector. Further, for localization schemes that employ signal strength, we showed that by utilizing the signal strength as a common feature, the minimum Euclidean distance in the signal space can be used as a test statistic for attack detection independent of the localization process. Further, we derived additional test statistics for a selection of representative localization algorithms.

We studied the effectiveness and generality of our attack detection schemes using a trace-driven evaluation involving both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network in two real office buildings. We evaluated the performance of our attack detection schemes in

terms of detection rates and receiver operating characteristic curves. Our experimental results provide strong evidence of the effectiveness of our attack detection schemes with high detection rates, over 95% and low false positive rates, often below 5%. Also, our approach is generic across a diverse set of algorithms, networks, and buildings. Interestingly, we found that the performance of the different attack detection schemes are more similar than different. This result shows that different localization systems have similar attack detection capabilities, and consequently that system designers can focus on using algorithms that provide the highest localization accuracy rather than having to tradeoff position accuracy against attack detection abilities.

After a localization attack is detected in a wireless network, the next important and challenging step is to localize the positions of the adversaries and further to eliminate the attack from the network. In the next chaper, we illustrate this idea further by examining the applicability of localization methods to locate an adversary participating in a spoofing attack. A spoofing attack is an attack where the attacker forges its identity and masquerades as another device, or even creates multiple illegitimate identities. Although the identity of a node can be verified through cryptographic authentication, authentication is not always desirable or possible because it requires key management and additional infrastructure overhead. We will take a different approach by using the physical properties of the radio signal and propose a scheme using K-means cluster analysis for both detecting spoofing attacks as well as localizing the positions of the adversaries without adding any overhead to the wireless devices and sensor nodes.

Chapter 4

Detecting and Localizing Identity-based Spoofing Attacks

4.1 Introduction

Due to the openness of wireless and sensor networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is thus desirable to detect the presence of spoofing and eliminate them from the network.

The traditional approach to address spoofing attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational power associated with distributing, and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In addition, key management often incurs significant human management costs on the network. In this chapter, we take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. Specifically, we propose a scheme for both detecting spoofing attacks, as well as localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. Our scheme does not add any overhead to the wireless devices and sensor nodes.

By analyzing the RSS from each MAC address using K-means cluster algorithm, we have found that the distance between the centroids in signal space is a good test statistic for effective attack detection. We then describe how we integrated our K-means spoofing detector into a real-time indoor localization system. Our K-means approach is general in that it can be applied to almost all RSS-based localization algorithms. For two sample algorithms, we show that

using the centroids of the clusters in signal space as the input to the localization system, the positions of the attackers can be localized with the same relative estimation errors as under normal conditions.

To evaluate the effectiveness of our spoofing detector and attack localizer, we conducted experiments using both an 802.11 network as well as an 802.15.4 network in a real office building environment. In particular, we have built an indoor localization system that can localize any transmitting devices on the floor in real-time. We evaluated the performance of the K-means spoofing detector using detection rates and receiver operating characteristic curve. We have found that our spoofing detector is highly effective with over 95% detection rates and under 5% false positive rates.

Further, we observed that, when using the centroids in signal space, a broad family of localization algorithms achieve the same performance as when they use the averaged RSS in traditional localization attempts. Our experimental results show that the distance between the localized results of the spoofing node and the original node is directly proportional to the true distance between the two nodes, thereby providing strong evidence of the effectiveness of both our spoofing detection scheme as well as our approach of localizing the positions of the adversaries.

The rest of the chapter is organized as follows. In Section 4.2, we study the feasibility of spoofing attacks and their impacts, and discuss our experimental methodologies. We formulate the spoofing attack detection problem and propose K-means spoofing detector in Section 4.3. We introduce the real-time localization system and present how to find the positions of the attackers in Section 4.4. Further, we provide a discussion in Section 4.5. Finally, we conclude our work in Section 4.6.

4.2 Feasibility of Attacks

In this section we provide a brief overview of spoofing attacks and their impact. We then discuss the experimental methodology that we use to evaluate our approach of spoofing detection.

4.2.1 Spoofing Attacks

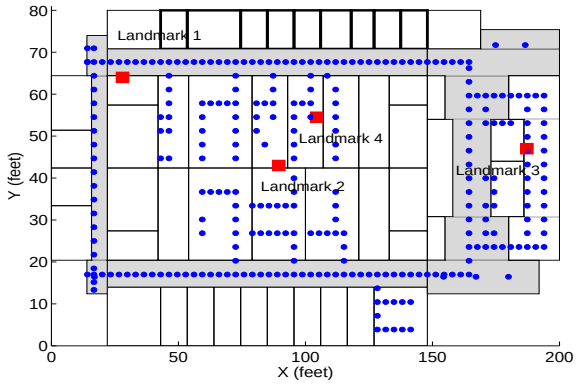
Due to the open-nature of the wireless medium, it is easy for adversaries to monitor communications to find the layer-2 Media Access Control (MAC) addresses of the other entities. Recall that the MAC address is typically used as a unique identifier for all the nodes on the network. Further, for most commodity wireless devices, attackers can easily forge their MAC address in order to masquerade as another transmitter. As a result, these attackers appear to the network as if they are a different device. Such spoofing attacks can have a serious impact on the network performance as well as facilitate many forms of security weaknesses, such as attacks on access control mechanisms in access points [10], and denial-of-service through a deauthentication attack [15]. A broad survey of possible spoofing attacks can be found in [29, 47].

To address potential spoofing attacks, the conventional approach uses authentication. However, the application of authentication requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply authentication because of its infrastructural, computational, and management overhead. Further, cryptographic methods are susceptible to node compromise– a serious concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned.

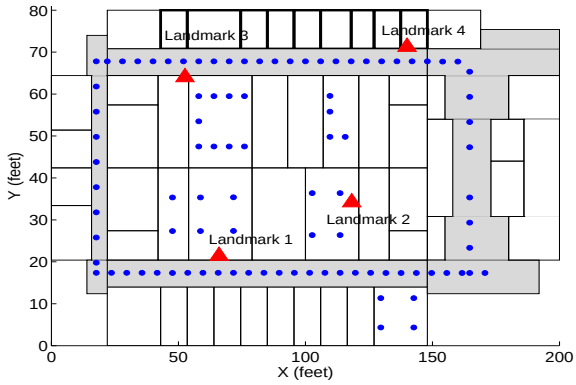
It is desirable to use properties that cannot be undermined even when nodes are compromised. We propose to use received signal strength (RSS), a property associated with the transmission and reception of communication (and hence not reliant on cryptography), as the basis for detecting spoofing. Employing RSS as a means to detect spoofing will not require any additional cost to the wireless devices themselves– they will merely use their existing communication methods, while the wireless network will use a collection of base stations to monitor received signal strength for the potential of spoofing.

4.2.2 Experimental Methodology

In order to evaluate the effectiveness of our spoofing detection mechanisms, which we describe in the next section, we have conducted experiments using both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network on the 3rd floor of the Computer Science Department at Rutgers University. The floor size is 200x80ft (16000 ft^2). Figure 4.1 (a) shows the 802.11



(a) 802.11 network



(b) 802.15.4 network

Figure 4.1: Landmark setups and testing locations in two networks.

(WiFi) network with 4 landmarks deployed to maximize signal strength coverage, as shown in red squares. The 802.15.4 (ZigBee) network is presented in Figure 3.2 (b) with 4 landmarks distributed in a squared setup in order to achieve optimal landmark placement [20] as shown in red triangles. The small blue dots in the floor map are the locations used for spoofing and localization tests.

For the 802.15.4 network, we used 300 packet-level RSS samples for each of the 100 locations. We utilized the actual RSS values attached to each packet. We have 286 locations in the 802.11 deployment. Unlike the 802.15.4 data, the RSS values are partially synthetic. We had access to only the mean RSS at each location, but to perform our experiments we needed an RSS value per packet. To generate such data for 200 simulated packets at each location, we used random draws from a normal distribution. We used the measured RSS mean for the mean

of the distribution. For the standard deviation, we computed the difference in the RSS from a fitted signal to distance function, and then calculated the standard deviation of the distribution from these differences over all locations. To keep our results conservative, we took the maximum deviation over all landmarks, which we found to be 5 dB.

Much work has gone into characterizing the distributions of RSS readings indoors. It has been shown that characterizing the per-location RSS distributions as normal, although not often the most accurate characterization, still results in the best balance between algorithmic usability and the resulting localization error [27, 33].

In addition, we built a real-time localization system to estimate the positions of both the original nodes and the spoofing nodes. We randomly selected points out of the above locations as the training data for use by the localization algorithms. For the 802.11 network, the size of the training data is 115 locations, while for the 802.15.4 network, the size of the training data is 70 locations. The detailed description of our localization system is presented in Section 4.4.

To test our approach's ability to detect spoofing, we randomly chose a point pair on the floor and treated one point as the position of the original node, and the other as the position of the spoofing node. We ran the spoofing test through all the possible combinations of point pairs on the floor using all the testing locations in both networks. There are total 14535 pairs for the 802.11 network and 4371 pairs for the 802.15.4 network. The experimental results will be presented in the following sections for the spoofing detector and the attack localizer.

4.3 Attack Detector

In this section we propose our spoofing attack detector. We first formulate the spoofing attack detection problem as one using classical statistical testing. Next, we describe the test statistic for spoofing detection. We then introduce the metrics to evaluate the effectiveness of our approach. Finally, we present our experimental results.

4.3.1 Formulation of Spoofing Attack Detection

RSS is widely available in deployed wireless communication networks and its values are closely correlated with location in physical space. In addition, RSS is a common physical property

used by a widely diverse set of localization algorithms [12, 27, 60, 69]. In spite of its several meter-level localization accuracy, using RSS is an attractive approach because it can re-use the existing wireless infrastructure. We thus derive a spoofing attack detector utilizing properties of the RSS.

The goal of the spoofing detector is to identify the presence of a spoofing attack. We formulate the spoofing attack detection as a statistical significance test, where the null hypothesis is:

$$\mathcal{H}_0 : \text{normal (no attack)}.$$

In significance testing, a test statistic $\mathbf{T}$ is used to evaluate whether observed data belongs to the null-hypothesis or not. If the observed test statistic $\mathbf{T^{obs}}$ differs significantly from the hypothesized values, the null hypothesis is rejected and we claim the presence of a spoofing attack.

4.3.2 Test Statistic for Spoofing Detection

Although affected by random noise, environmental bias, and multipath effects, the RSS value vector, $\mathbf{s} = \{s_1, s_2, ...s_n\}$ (n is the number of landmarks/access points(APs)), is closely related with the transmitter's physical location and is determined by the distance to the landmarks [27]. The RSS readings at different locations in physical space are distinctive. Each vector $\mathbf{s}$ corresponds to a point in a n-dimensional signal space [22]. When there is no spoofing, for each MAC address, the sequence of RSS sample vectors will be close to each other, and will fluctuate around a mean vector. However, under a spoofing attack, there is more than one node at different physical locations claiming the same MAC address. As a result, the RSS sample readings from the attacked MAC address will be mixed with RSS readings from at least one different location. Based on the properties of the signal strength, the RSS readings from the same physical location will belong to the same cluster points in the n-dimensional signal space, while the RSS readings from different locations in the physical space should form different clusters in signal space.

This observation suggests that we may conduct K-means cluster analysis [34] on the RSS readings from each MAC address in order to identify spoofing. If there are M RSS sample

readings for a MAC address, the K-means clustering algorithm partitions M sample points into K disjoint subsets S_j containing M_j sample points so as to minimize the sum-of-squares criterion:

$$J_{min} = \sum_{j=1}^{K} \sum_{\mathbf{s_m} \in S_j} \|\mathbf{s_m} - \mu_j\|^2 \tag{4.1}$$

where $\mathbf{s_m}$ is a RSS vector representing the mth sample point and μ_j is the geometric centroid of the sample points for S_j in signal space. Under normal conditions, the distance between the centroids should be close to each other since there is basically only one cluster. Under a spoofing attack, however, the distance between the centroids is larger as the centroids are derived from the different RSS clusters associated with different locations in physical space. We thus choose the distance between two centroids as the test statistic $\mathbf{T}$ for spoofing detection,

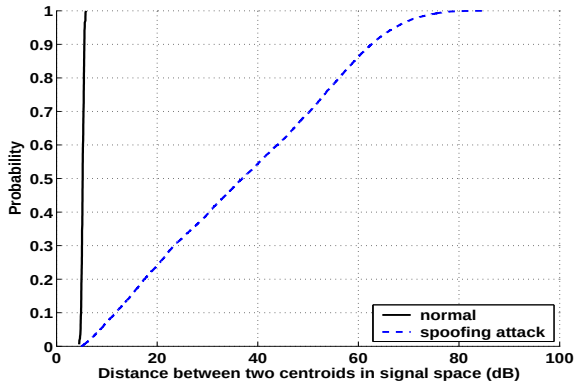
$$D_c = ||\mu_i - \mu_j|| \tag{4.2}$$

with $i, j \in \{1, 2..K\}$. Next, we will use empirical methodologies from the collected data set to determine thresholds for defining the critical region for the significance testing. To illustrate, we use the following definitions, *an original node* P_{org} is referred to as the wireless device with the legitimate MAC address, while *a spoofing node* P_{spoof} is referred to as the wireless device that is forging its identity and masquerading as another device. There can be multiple spoofing nodes of the same MAC address.

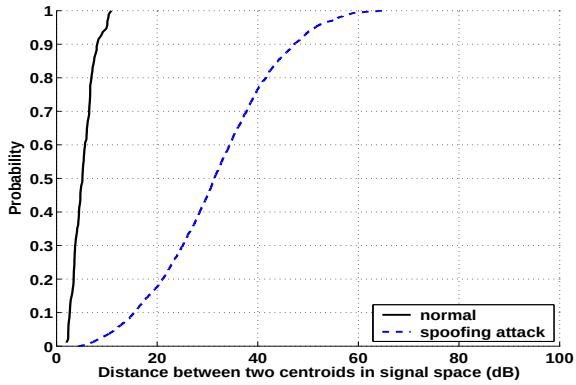
Note that our K-means spoofing detector can handle packets from different transmission power levels. If an attacker sends packets at a different transmission power level from the original node with the same MAC address, there will be two distinct RSS clusters in signal space. Thus, the spoofing attack will be detected based on the distance of the two centroids obtained from the RSS clusters.

4.3.3 Determining Thresholds

The appropriate threshold τ will allow the spoofing detector to be robust to false detections. We can determine the thresholds through empirical training. During the off line phase, we can collect the RSS readings for a set of known locations over the floor and obtain the distance between two centroids in signal space for each point pair. We use the distribution of the training information to determine the threshold τ. At run time, based on the RSS sample readings for



(a) 802.11 network



(b) 802.15.4 network

Figure 4.2: Cumulative Distribution Function (CDF) of D_c in signal space

a MAC address, we can calculate the observed value D_c^{obs}. Our condition for declaring that a MAC address is under a spoofing attack is:

$$D_c^{obs} > \tau. \tag{4.3}$$

Figure 4.2 (a) and (b) show the CDF of the D_c in signal space for both the 802.11 network and the 802.15.4 network. We found that the curve of D_c shifted greatly to the right under spoofing attacks, thereby suggesting that using D_c as a test statistic is an effective way for detecting spoofing attacks.

4.3.4 Performance Metrics

In order to evaluate the performance of our spoofing attack detector using K-means cluster analysis, we use the following metrics:

Network, Threshold	Detection Rate	False Positive Rate
802.11, τ = 5.5dB	0.9937	0.0819
802.11, τ = 5.7dB	0.9920	0.0351
802.11, τ = 6dB	0.9884	0
802.15.4, τ = 8.2dB	0.9806	0.0957
802.15.4, τ = 10dB	0.9664	0.0426
802.15.4, τ = 11dB	0.9577	0

Table 4.1: Detection rate and false positive rate of the spoofing attack detector.

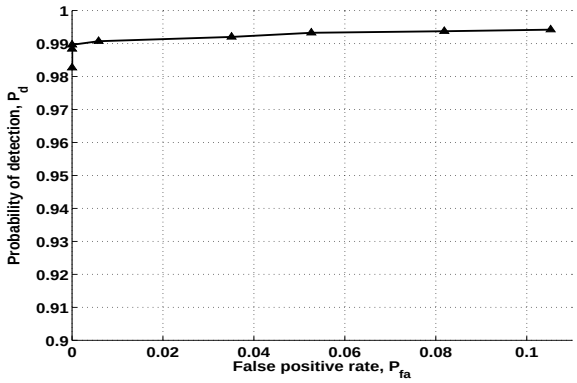
Detection Rate and False Positive Rate: A spoofing attack will cause the significance test to reject $\mathcal{H}_0$. We are thus interested in the statistical characterization of the attack detection attempts over all the possible spoofing attacks on the floor. The detection rate is defined as the percentage of spoofing attack attempts that are determined to be under attack. Note that, when the spoofing attack is present, the detection rate corresponds to the probability of detection P_d, while under normal (non-attack) conditions it corresponds to the probability of declaring a false positive P_{fa}. The detection rate and false positive rate vary under different thresholds.

Receiver Operating Characteristic (ROC) curve: To evaluate an attack detection scheme we want to study the false positive rate P_{fa} and probability of detection P_d together. The ROC curve is a plot of attack detection accuracy against the false positive rate. It can be obtained by varying the detection thresholds. The ROC curve provides a direct means to measure the trade off between false-positives and correct detections.

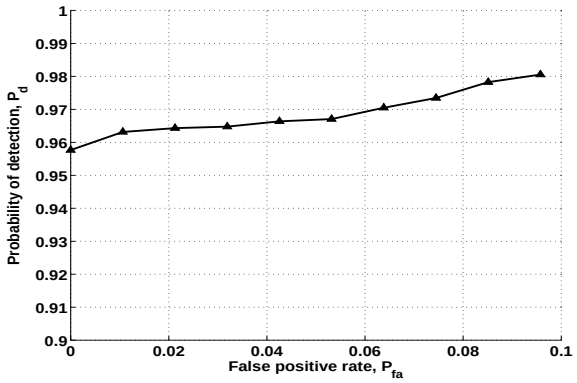
4.3.5 Experimental Evaluation

In this section we present the evaluation results of the effectiveness of the spoofing attack detector. Table 4.1 presents the detection rate and false positive rate for both the 802.11 network and the 802.15.4 network under different threshold settings. The corresponding ROC curves are displayed in Figure 4.3. The results are encouraging showing that for false positive rates less than 10%, the detection rates are above 95%. Even when the false positive rate goes to zero, the detection rate is still more than 95% for both 802.11 and 802.15.4 networks.

We further study how likely a spoofing node can be detected by our spoofing attack detector when it is at varying distances from the original node in physical space. Figure 4.4 presents the detection rate as a function of the distance between the spoofing node and the original node. We found that the further away P_{spoof} is from P_{org}, the higher the detection rate becomes. For the



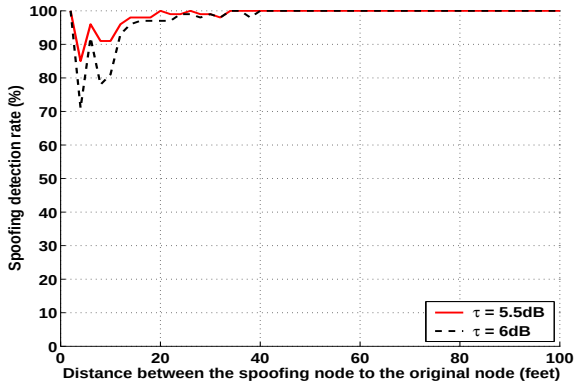
(a) 802.11 network



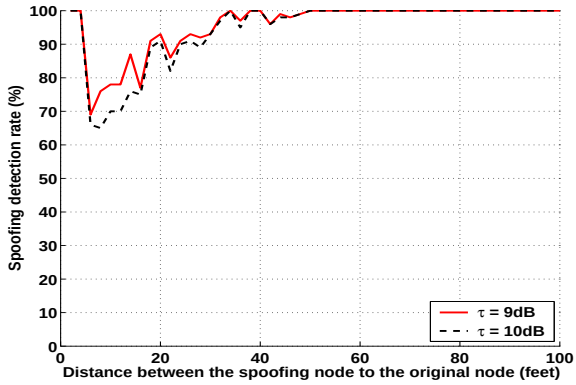
(b) 802.15.4 network

Figure 4.3: Receiver Operating Characteristic (ROC) curves

802.11 network, the detection rate goes to over 90% when P_{spoof} is about 13 feet away from P_{org} under τ equals to 5.5dB. While for the 802.15.4 network, the detection rate is above 90% when the distance between P_{spoof} and P_{org} is about 20 feet by setting threshold τ to 9dB. This is in line with the average localization estimation errors using RSS [27] which are about 10-15 feet. When the nodes are less than 10-15 feet apart, they have a high likelihood of generating similar RSS readings, and thus the spoofing detection rate falls below 90%, but still greater than 60%. However, when P_{spoof} moves closer to P_{org}, the attacker also increases the probability to expose itself. The detection rate goes to 100% when the spoofing node is about 45-50 feet away from the original node.



(a) 802.11 network



(b) 802.15.4 network

Figure 4.4: Detection rate as a function of the distance between the spoofing node and the original node.

4.4 Localizing Adversaries

If the spoofing attack is determined to be present by the spoofing attack detector, we want to localize the adversaries and further to eliminate the attackers from the network. In this section we present a real-time localization system that can be used to locate the positions of the attackers. We then describe the localization algorithms used to estimate the adversaries' position. The experimental results are presented to evaluate the effectiveness of our approach.

4.4.1 Localization System

We have developed a general-purpose localization system to perform real-time indoor positioning. The detailed system architecture is presented in Chapter 6. Here we provide a brief system

overview. This system is designed with fully distributed functionality and easy to plug-in localization algorithms. It is built around 4 logical components: Transmitter, Landmark, Server, and Solver. The system architecture is shown in Figure 6.1 in Chapter 6.

Transmitter: Any device that transmits packets can be localized. Often the application code does not need to be altered on a sensor node in order to localize it.

Landmark: The Landmark component listens to the packet traffic and extracts the RSS reading for each transmitter. It then forwards the RSS information to the Server component. The Landmark component is stateless and is usually deployed on each landmark or access point with known locations.

Server: A centralized server collects RSS information from all the Landmark components. The spoofing detection is performed at the Server component. The Server summarizes the RSS information such as averaging or clustering, then forwards the information to the Solver component for localization estimation.

Solver: A Solver takes the input from the Server, performs the localization task by utilizing the localization algorithms plugged in, and returns the localization results back to the Server. There are multiple Solver instances available and each Solver can localize multiple transmitters simultaneously.

During the localization process, the following steps will take place:

1. A Transmitter sends a packet. Some number of Landmarks observe the packet and record the RSS.

2. Each Landmark forwards the observed RSS from the transmitter to the Server.

3. The Server collects the complete RSS vector for the transmitter and sends the information to a Solver instance for location estimation.

4. The Solver instance performs localization and returns the coordinates of the transmitter back to the Server.

If there is a need to localize hundreds of transmitters at the same time, the server can perform load balancing among the different solver instances. This centralized localization solution also makes enforcing contracts and privacy policies more tractable.

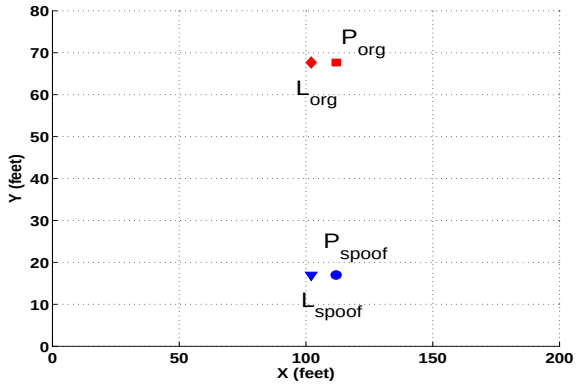


Figure 4.5: Relationships among the original node, the spoofing node, and their location estimation through localization system.

4.4.2 Attack Localizer

When our spoofing detector has identified an attack for a MAC address, the centroids returned by the K-means clustering analysis in signal space can be used by the server and sent to the solver for location estimation. The returned positions should be the location estimate for the original node and the spoofing nodes in physical space. Using a location on the testing floor as an example, Figure 4.5 shows the relationship among the original node P_{org}, the location estimation of the original node L_{org}, the spoofing node P_{spoof}, and the localized spoofing node position L_{spoof}.

In order to show the generality of our localization system for locating the spoofing nodes, we have chosen two representative localization algorithms using signal strength from point-based algorithms and area-based algorithms.

RADAR: Point-based methods return an estimated point as a localization result. A primary example of a point-based method is the RADAR scheme [12]. In RADAR, during the off line phase, a mobile transmitter with known position broadcasts beacons periodically, and the RSS readings are measured at a set of landmarks. Collecting together the averaged RSS readings from each of the landmarks for a set of known locations provides a radio map. At runtime, localization is performed by measuring a transmitter's RSS at each landmark, and the vector of RSS values is compared to the radio map. The record in the radio map whose signal strength vector is closest in the Euclidean sense to the observed RSS vector is declared to correspond to

the location of the transmitter. In this work, instead of using the averaged RSS in the traditional approach, we use the RSS centroids obtained from the K-means clustering algorithm as the observed RSS vector for localizing a MAC address.

Area Based Probability (ABP): Area-based algorithms return a most likely area in which the true location resides. One major advantage of area-based methods compared to point-based methods is that they return a region, which has an increased chance of capturing the transmitter's true location. ABP returns an area, a set of tiles on the floor, bounded by a probability that the transmitter is within the returned area [27]. ABP assumes the distribution of RSS for each landmark follows a Gaussian distribution. The Gaussian random variable from each landmark is independent. ABP then computes the probability of the transmitter being at each tile L_i on the floor using Bayes' rule:

$$P(L_i|\mathbf{s}) = \frac{P(\mathbf{s}|L_i) \times P(L_i)}{P(\mathbf{s})}. \tag{4.4}$$

Given that the transmitter must reside at exactly one tile satisfying $\sum_{i=1}^{L} P(L_i|\mathbf{s}) = 1$, ABP normalizes the probability and returns the most likely tiles up to its confidence α.

Both RADAR and ABP are employed in our experiments to localize the positions of the attackers.

4.4.3 Experimental Evaluation

In order to evaluate the effectiveness of our localization system in finding the locations of the attackers, we are interested in the following performance metrics:

Localization Error CDF: We obtain the cumulative distribution function (CDF) of the location estimation error from all the localization attempts, including both the original nodes and the spoofing nodes. We then compare the error CDF of all the original nodes to that of all the possible spoofing nodes on the floor. For area-based algorithms, we also report CDFs of the minimum and maximum error. For a given localization attempt, these are points in the returned area that are closest to and furthest from the true location.

Relationship between the true and estimated distances: The relationship between the true distance of the spoofing node to the original node $||P_{org} - P_{spoof}||$ and the distance of the location estimate of the spoofing node to that of the original node $||L_{org} - L_{spoof}||$ evaluates

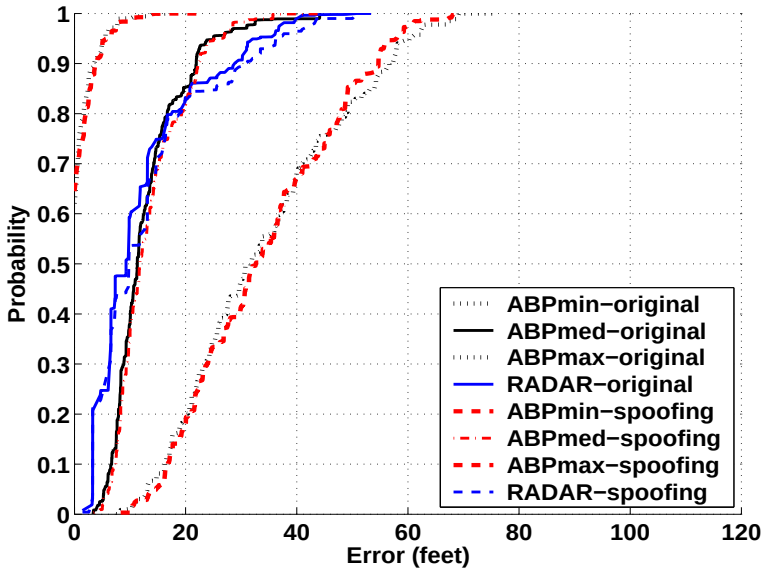
how accurate our attack localizer can report the positions of both the original node and the attackers.

We first present the statistical characterization of the location estimation errors. Figure 4.6 presents the localization error CDF of the original nodes and the spoofing nodes for both RADAR and ABP in the 802.11 network as well as the 802.15.4 network. For the area-based algorithm, the median tile error $ABP - med$ is presented, as well as the minimum and maximum tile errors, $ABP - min$ and $ABP - max$. We found that the location estimation errors from using the RSS centroids in signal space are about the same as using averaged RSS as the input for localization algorithms [27]. Comparing to the 802.11 network, the localization performance in the 802.15.4 network is qualitatively better for both RADAR and ABP algorithms. This is because the landmark placement in the 802.15.4 network is closer to that predicted by the optimal and error minimizing placement algorithm as described in [20].

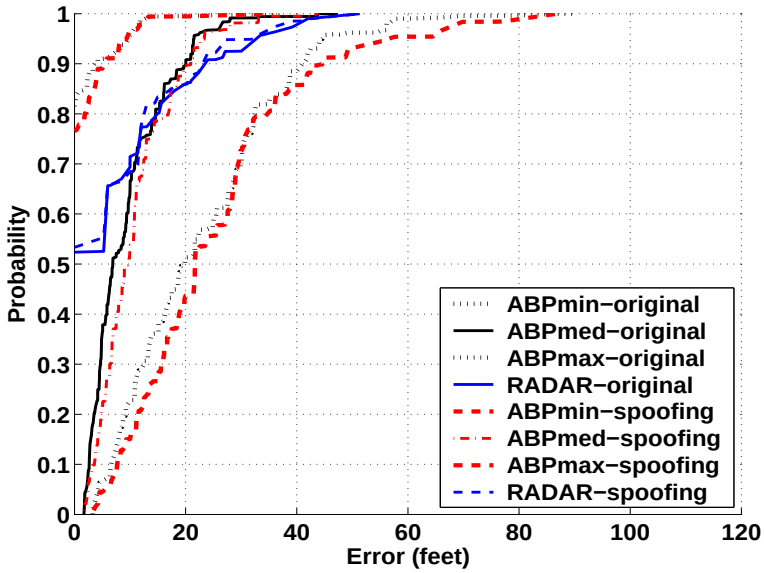
More importantly, we observed that the localization performance of the original nodes is qualitatively the same as that of the spoofing nodes. This is very encouraging as the similar performance is strong evidence that using the centroids obtained from the K-means cluster analysis is effective in both identifying the spoofing attacks as well as localizing the attackers.

The challenge in localizing the positions of the attackers arises because the system does not know the positions of either the original MAC address or the node with the masquerading MAC. Thus, we would like to examine how accurate the localization system can estimate the distance between P_{org} and P_{spoof}. Figure 4.7 displays the relationship between $||L_{org} - L_{spoof}||$ and $||P_{org} - P_{spoof}||$ across different localization algorithms and networks. The blue dots represent the cases of the detected spoofing attacks. While the red crosses indicate the spoofing attack has not been detected by the K-means spoofing detector. Comparing with Figure 4.4, i.e. the detection rate as a function of the distance between P_{org} and P_{spoof}, the results of the undetected spoofing attack cases represented by the red crosses are in line with the results in Figure 4.4, the spoofing attacks are 100% detected when $||P_{org} - P_{spoof}||$ equals to or is greater than about 50 feet.

Further, the relationship between $||L_{org} - L_{spoof}||$ and $||P_{org} - P_{spoof}||$ is along the 45 degree straight line. This means that $||L_{org} - L_{spoof}||$ is directly proportional to $||P_{org} - P_{spoof}||$ and indicates that our localization system is highly effective for localizing the attackers. At a

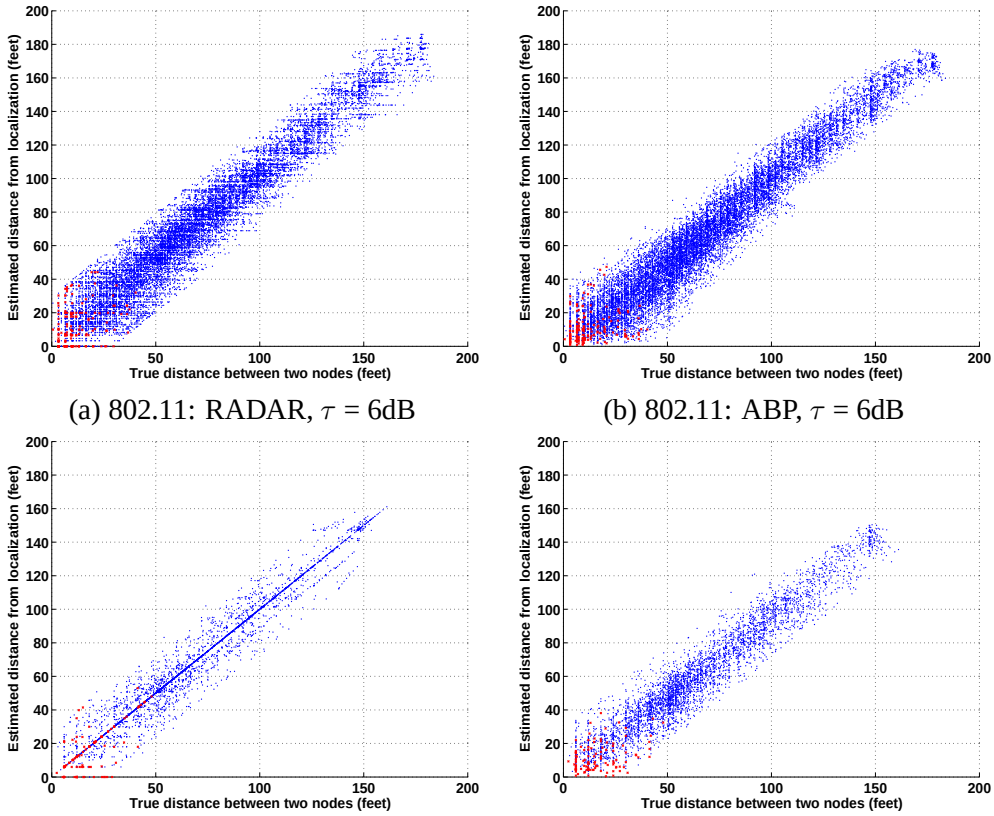


(a) 802.11 network



(b) 802.15.4 network

Figure 4.6: Localization error CDF across localization algorithms and networks.



(a) 802.11: RADAR, τ = 6dB

(b) 802.11: ABP, τ = 6dB

(c) 802.15.4: RADAR, τ = 9dB

(d) 802.15.4: ABP, τ = 9dB

Figure 4.7: Relationship between the true distance and the estimated distance for the original node and the spoofing node across localization algorithms and networks.

fixed distance value of $||P_{org} - P_{spoof}||$, the values of $||L_{org} - L_{spoof}||$ fluctuate around the true distance value. The fluctuation reflects the localization errors of both P_{org} and P_{spoof}. The larger the $||P_{org} - P_{spoof}||$ is, the smaller the fluctuation of $||L_{org} - L_{spoof}||$ becomes, at about 10 feet maximum. This means that if the attacker is farther away from the original node, it is extremely likely that the K-means spoofing detector can detect it. In addition, our attack localizer can find the attacker's position and estimate the distance from the original node to the attacker at about 10 to 20 feet maximum error.

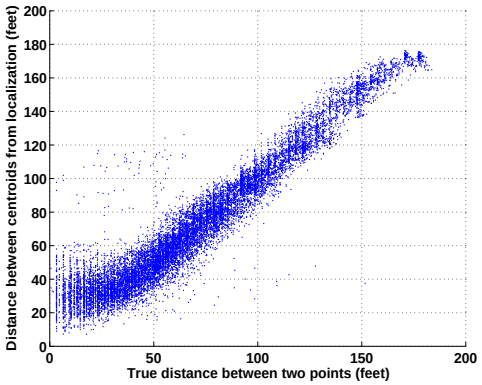


Figure 4.8: Packet-level localization: relationship between the true distance and the estimated distance for the original node and the spoofing node when using RADAR in the 802.11 network.

4.5 Discussion

So far we have conducted K-means cluster analysis in signal space. Our real-time localization system also inspired us to explore packet-level localization at the server, which means localization is performed for each packet received at the landmarks. The server utilizes each RSS reading vector for localization. Over a certain time period (for example, 60 seconds), for a MAC address there will be a cluster of location estimates in physical space. Intuitively, we think that, during a spoofing attack there will be distinctive location clusters around the original node and the spoofing nodes in physical space. Our intuition was that the clustering results from the per-packet localization would allow the detection and localization of attackers in one step.

However, we found that the performance of clustering packet-level localization results for spoofing detection is not as effective as deriving the centroids in signal space. The relationship between $||P_{org} - P_{spoof}||$ and $||L_{org} - L_{spoof}||$ is shown in Figure 4.8. Although it also has a trend along the 45 degree line, it shows more uncertainties along the line. Therefore, we believe that given a set of RSS reading samples for a MAC address, working with the signal strength directly preserves the basic properties of the radio signal, and this in turn is more closely correlated with the physical location, and thus working with the RSS values directly better reveals the presence of the spoofing attacks.

4.6 Conclusion

In this chapter, we proposed a method for detecting spoofing attacks as well as localizing the adversaries in wireless and sensor networks. In contrast to traditional identity-oriented authentication methods, our RSS based approach does not add additional overhead to the wireless devices and sensor nodes. We formulated the spoofing detection problem as a classical statistical significance testing problem. We then utilized the K-means cluster analysis to derive the test statistic. Further, we have built a real-time localization system and integrated our K-means spoofing detector into the system to locate the positions of the attackers and as a result to eliminate the adversaries from the network.

We studied the effectiveness and generality of our spoofing detector and attacker localizer in both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network in a real office building environment. The performance of the K-means spoofing detector is evaluated in terms of detection rates and receiver operating characteristic curves. Our spoofing detector has achieved high detection rates, over 95% and low false positive rates, below 5%. When locating the positions of the attackers, we have utilized both the point-based and area-based algorithms in our real-time localization system. We found that the performance of the system when localizing the adversaries using the results of K-means cluster analysis are about the same as localizing under normal conditions. Usually the distance between the spoofing node and the original node can be estimated with median error of 10 feet. Our method is generic across different localization algorithms and networks. Therefore, our experimental results provide strong evidence of the effectiveness of our approach in detecting the spoofing attacks and localizing the positions of the adversaries.

During the course of the security analysis for localization systems, we found that the landmark placement plays an important role on localization performance. While most research has focused on improving the localization algorithm, we took the viewpoint that it is perhaps just as important to improve the deployment of the localization system. In the next chapter, we will investigate the impact of landmark placement on localization performance using a combination of analytic and experimental analysis.

Chapter 5

Performance Improvement Using Optimal Landmark Placement

5.1 Introduction

Although recent efforts have resulted in a plethora of methods to localize sensor nodes, little work to date has systematically investigated how the placement of the nodes with known locations, or *landmarks*, impacts localization performance. In this chapter we investigate the impact of landmark placement on localization performance using a combination of analytic and experimental analysis.

Our analytic approach focuses on the Least Squares (LS) algorithm, and in particular, a variant we call Linear Least Squares (LLS). Our analysis centers on the algorithm for two reasons. First, LS is a widely used multilateration algorithm, as is evidenced by its application as a step in many recent localization research works [23, 28, 44, 49, 54]. Second, mathematical analysis of LLS is tractable, resulting in equations with closed-form solutions. For a myriad of other algorithms, closed form solutions that describe the localization error as a function of landmark placement are not tractable and as a result heuristic search strategies must be used to find an optimal placement, as was done in [13].

Our analysis of landmark placement can find an optimal placement of landmarks in well-defined regular regions, thus making it quite suitable for indoor localization. The analysis begins with LLS and places an upper bound of the maximum localization error given a set of landmark placements. We can show that this upper bound is minimized by a combination of minimizing the distance estimation error together with the employment of the optimal patterns for landmark placement.

Using this result, we can compare the maximum error between any two placements. We can then constrain a search of placements to minimize the maximum error. We have developed a

simple algorithm called $maxL - minE$ algorithm that finds an optimized landmark deployment for the LLS algorithm.

We show that our placement minimizing the upper bounds of LLS also reduces the Hölder parameter for a variety of algorithms. The Hölder parameter [22] describes the maximum change in physical space that can arise from a change in signal space. This is strong evidence that our $maxL - minE$ algorithm finds a landmark placement that minimizes the errors due to noise, bias, and measurement error.

Another interesting result of our analysis is that for a small number of landmarks, simple shapes such as equilateral triangles and squares result in placements with better localization performance. Interestingly, for higher number of landmarks, we can show that extensions of shapes with equal sides, e.g. a hexagon, are non-optimal. Rather, the simple shapes enclose one another, for example, two enclosing equilateral triangles. We detail these geometries and describe rule-of-thumb for landmark placement in Section 5.2.

To show the generality of our results, we conducted localization experiments with both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network in a real building environment. For the 802.11 network, we used two ranging modalities, Received Signal Strength (RSS) to distance, and Time of Arrival (TOA). In the 802.15.4 network, we used only RSS-to-distance.

We compared the accuracy of a suite of localization algorithms using landmarks placed according to our analysis as well as landmarks placed in positions that provide good signal coverage but ignore localization concerns. While we found that all algorithms improved their performance, over a non-optimal placement for localization, we also observed that LS became competitive with the other algorithms, and that coarse-grained TOA ranging was less accurate than RSS-based approaches.

The remainder of the chapter is as follows. We provide the theoretical analysis in Section 5.2. Then Section 5.3 describes the metrics that we use to characterize the localization performance. The investigation of the number of landmarks and their positions is provided in Section 5.4. Section 5.5 presents the experimental results across localization algorithms, networks, and ranging strategies. Finally we conclude in Section 2.7.

5.2 Theoretical Analysis

In this section we first provide background on using LS algorithms for localization, and then describe the LLS variant. We next present our theoretical analysis of an upper bound on the error, and then discuss our $maxL - minE$ placement algorithm.

5.2.1 Background: Localization with LS

To perform localization with LS requires 2 steps: ranging and lateration.

Ranging Step: Recent research has seen a host of variants on the ranging step. For example, in the APS algorithm [54], hop counts are used to estimate ranges. Other approaches are also possible, [56] used the time-difference of arrival between an ultrasound pulse and a radio packet. In this work, we focus on RSS and TOA as ranging strategies.

Lateration Step: From the estimated distances d_i and known positions (x_i, y_i) of the landmarks, the position (x, y) of the localizing node can be found by finding $(\hat{x}, \hat{y})$ satisfying:

$$(\hat{x}, \hat{y}) = arg \min_{x,y} \sum_{i=1}^{N} [\sqrt{(x_i - x)^2 + (y_i - y)^2} - d_i]^2 \tag{5.1}$$

where N is the total number of landmarks. We call solving the above problem *Nonlinear Least Squares*, or NLS. It can be viewed as an optimization problem where the objective is to minimize the sum of the error squared.

Solving the NLS problem requires significant complexity and is difficult to analyze. We may approximate the NLS solution and linearize the problem by introducing a constraint in the formulation. We start with the $N \geq 2$ equations:

$$\begin{aligned} (x_1 - x)^2 + (y_1 - y)^2 &= d_1^2 \\ (x_2 - x)^2 + (y_2 - y)^2 &= d_2^2 \\ &\vdots \\ (x_N - x)^2 + (y_N - y)^2 &= d_N^2 \end{aligned} \tag{5.2}$$

Now, subtracting the constraint

$$\frac{1}{N} \sum_{i=1}^{N} [(x_i - x)^2 + (y_i - y)^2] = \frac{1}{N} \sum_{i=1}^{N} d_i^2 \tag{5.3}$$

from both sides, we obtain the following set of linear equations

$$\begin{gathered}(x_1 - \frac{1}{N}\sum_{i=1}^{N} x_i)x + (y_1 - \frac{1}{N}\sum_{i=1}^{N} y_i)y = \\ \frac{1}{2}[(x_1^2 - \frac{1}{N}\sum_{i=1}^{N} x_i^2) + (y_1^2 - \frac{1}{N}\sum_{i=1}^{N} y_i^2) - (d_1^2 - \frac{1}{N}\sum_{i=1}^{N} d_i^2)] \\ \vdots \\ (x_N - \frac{1}{N}\sum_{i=1}^{N} x_i)x + (y_N - \frac{1}{N}\sum_{i=1}^{N} y_i)y = \\ \frac{1}{2}[(x_N^2 - \frac{1}{N}\sum_{i=1}^{N} x_i^2) + (y_N^2 - \frac{1}{N}\sum_{i=1}^{N} y_i^2) - (d_N^2 - \frac{1}{N}\sum_{i=1}^{N} d_i^2)].\end{gathered} \tag{5.4}$$

The above can be easily solved linearly using the form $\mathbf{Ax} = \mathbf{b}$ with:

$$\mathbf{A} = \begin{pmatrix} x_1 - \frac{1}{N}\sum_{i=1}^{N} x_i & y_1 - \frac{1}{N}\sum_{i=1}^{N} y_i \\ \vdots & \vdots \\ x_N - \frac{1}{N}\sum_{i=1}^{N} x_i & y_N - \frac{1}{N}\sum_{i=1}^{N} y_i \end{pmatrix} \tag{5.5}$$

and

$$\mathbf{b} = \frac{1}{2}\begin{pmatrix} (x_1^2 - \frac{1}{N}\sum_{i=1}^{N} x_i^2) + (y_1^2 - \frac{1}{N}\sum_{i=1}^{N} y_i^2) \\ -(d_1^2 - \frac{1}{N}\sum_{i=1}^{N} d_i^2) \\ \vdots \\ (x_N^2 - \frac{1}{N}\sum_{i=1}^{N} x_i^2) + (y_N^2 - \frac{1}{N}\sum_{i=1}^{N} y_i^2) \\ -(d_N^2 - \frac{1}{N}\sum_{i=1}^{N} d_i^2) \end{pmatrix}. \tag{5.6}$$

Note that $\mathbf{A}$ is described by the coordinates of landmarks only, while $\mathbf{b}$ is represented by the distances to the landmarks together with the coordinates of landmarks. We call the above formulation of the problem *Linear Least Squares*, or LLS. NLS trades higher computational complexity for better accuracy. The introduction of the constraint collapsed the nonlinear problem into a linear problem, which greatly simplifies the computation needed to arrive at a location estimate. In addition to its computational advantages, the LLS formulation allows for tractable error analysis, as we shall soon provide.

5.2.2 Error Analysis

Our objective is to minimize the location estimation error introduced by LLS. we have matrix $\mathbf{A}$ and vector $\mathbf{b}$ presented in Equations (5.5) and (5.6). In an ideal situation solving for $\mathbf{x} = [x, y]^T$

is done via

$$\mathbf{x} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b} \tag{5.7}$$

However, the estimated distances are impacted by noise, bias, and measurement error. We express the resulting distance estimation error $\mathbf{e}$ in terms of $\tilde{\mathbf{b}}$ with estimated distances and $\mathbf{b}$ with true distances as $\tilde{\mathbf{b}} = \mathbf{b} + \mathbf{e}$, and hence the localization result is

$$\tilde{\mathbf{x}} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\tilde{\mathbf{b}}. \tag{5.8}$$

The location estimation error is thus bounded by

$$\|\mathbf{x} - \tilde{\mathbf{x}}\| \leq \|\mathbf{A}^+\|\|\mathbf{e}\|, \tag{5.9}$$

where the matrix $\mathbf{A}^+$ is the Moore-Penrose pseudo-inverse of $\mathbf{A}$. It can be shown that, under the 2-norm, $\|\mathbf{A}^+\| = \frac{1}{\gamma_2}$, where $\gamma_1 \geq \gamma_2$ are the singular values of $\mathbf{A}$. This means that for a certain size on error $\mathbf{e}$ the LS estimation error is stretched by $\frac{1}{\gamma_2}$. It can be proved that the eigenvalues of $\mathbf{A}^T\mathbf{A}$ are the squares of the singular values of $\mathbf{A}$. Therefore, we can limit our concern to the eigenvalues of $\mathbf{A}^T\mathbf{A}$, where $\mathbf{A}^T\mathbf{A}$ is a matrix of the form:

$$\mathbf{A}^T\mathbf{A} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$$

with:

$$a = \sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i)^2 \tag{5.10}$$

$$b = \sum_{i=1}^{N}[(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i)(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i)] \tag{5.11}$$

$$c = \sum_{i=1}^{N}(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i)^2. \tag{5.12}$$

Note that a, b and c are only related to the coordinates of landmarks (x_i, y_i). The eigenvalues of $\mathbf{A}^T\mathbf{A}$ can be found as the roots of:

$$\lambda^2 - (a+c)\lambda + (ac - b^2) = 0.$$

Thus, we have:

$$\lambda = \frac{(a+c) \pm \sqrt{(a-c)^2 + 4b^2}}{2}, \tag{5.13}$$

where the discriminant, $(a-c)^2 + 4b^2$, is non-negative.

5.2.3 Deployment Patterns

Our goal in this section is to minimize the total error. Recall there are two terms on the right side of Equation (5.9). Our approach is to choose x_i and y_i so as to make λ_2 (the smaller eigenvalue) as close to λ_1 as possible, because this will minimize the first term, $\|\mathbf{A}^+\|$. Given the first term is minimized, we then minimize the second term. Having minimized the second term given the first term is minimized is clearly a local minima. We call such a local minima *an optimal deployment*, because no movement of a single landmark can improve the error bound. However, our piecewise minimization approach still leaves open a proof that this local minima is the true minima over all possible landmark positions. We leave such a proof as future work.

Returning to minimizing the first term $\|\mathbf{A}^+\|$, to minimize $\frac{1}{\sqrt{\lambda_2}}$, a general strategy would be to make $(a-c)$ small or to make b small or both. Interestingly, this is determined only by the coordinates of the landmarks.

Then our next task is to find the landmark positions that satisfy $\lambda_1 \cong \lambda_2$. We found that the optimal landmark deployment setup follows some simple and symmetric patterns. This makes it not only possible to achieve but also easy to deploy practically. Figure 5.1 shows the patterns for an optimal landmark deployment setup when utilizing 3, 4, 5, 6, 7, 8 landmarks in the indoor environment. These patterns consist of squares, equilateral triangles, or the enclosing of them. We observe that for higher number of landmarks, the extensions of shapes with equal sides, e.g. a hexagon, do not satisfy $\lambda_1 \cong \lambda_2$, and thus are not optimal. Instead, simple shapes that enclose one another present optimal solutions.

5.2.4 Finding an Optimized landmark Deployment

The above discussion dealt with deploying the landmarks without considering the physical constraints of the building and, as such, only provide a general guideline as to the ”shape” of the deployment. Placing the landmarks within a particular building requires stretching/shrinking

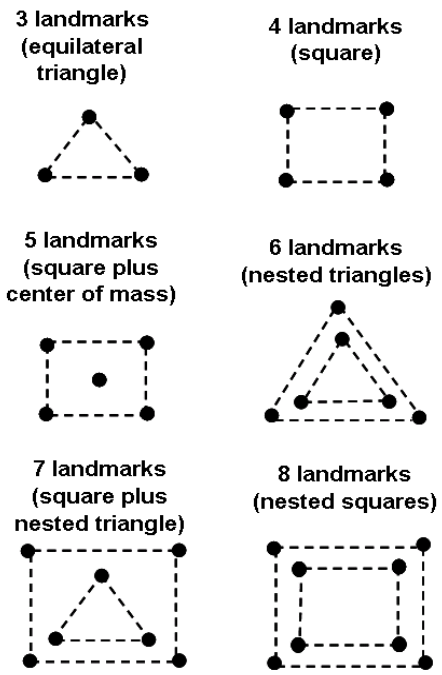


Figure 5.1: Patterns for optimal landmark deployments

the deployment shape so that it fits within the confines of the building. The stretching/shrinking should be done so as to minimize localization errors.

Recall in Equation (5.9), the location estimation error is also contributed by $\|\mathbf{e}\|$, and that $\tilde{\mathbf{b}} = \mathbf{b} + \mathbf{e}$. The term $\|\mathbf{e}\|$ is a result of distance estimation errors introduced by ranging. We have developed an iterative algorithm, called $maxL - minE$ (i.e. maximum lambda and minimum error), which helps to find the real landmark coordinates given the floor size, number of landmarks, and the optimal landmark deployment pattern. Figure 5.2 shows the pseudo-code that implements $maxL-minE$. The algorithm first minimizes $\|\mathbf{A}^{+}\|$ using geometry, then uses an iterative search. The search begins with a maximal sized optimal pattern (e.g. a square) and simply keeps reducing the size of the pattern until such movements stop reducing the distance estimation error $\mathbf{e}$. We observe the algorithm usually converges very quickly within a number of iterations.

5.3 Evaluation Metrics

In this section we describe the three metrics we use throughout the rest of the paper.

---

input $floorSize, numOfLandmark$
output $optimized\ landmark\ coordinates$

[initialize] get optimal pattern based on geometry
fit optimal pattern into maximum floorsize
generate initial landmark coordinates
calculate λ_1 and λ_2

$minError = maxNum$
$thisError = maxNum$
loop until $thisError > minError$
  generate random localizing nodes
  for each localizing node **begin**
    apply random noise or bias
    $B = \|b - \tilde{b}\|$
  end for
  $thisError = \frac{avg(B)}{\sqrt{\lambda_2}}$
  if $thisError < minError$, $minError = thisError$
  [landmark adjustment] move towards the center of mass one step
end loop
return $optimized\ landmark\ coordinates$

Figure 5.2: The maxL-minE algorithm

Average error: All of our observations are the results of many localization trials. This metric takes the average of the distances between the localized result and the true location over all trials. In area-based algorithms, as opposed to point-based ones, the result is a returned area. To compare these two kinds of algorithms, we use the median X and Y of the returned area to the true location to generate a point and then average these distance errors.

Accuracy CDF: We also return the entire cumulative density function (CDF) of all our localization attempts. We simply report all attempts in sorted order, and then normalize the Y axis by the total number of attempts to obtain a domain of $[0, 1]$. For area-based algorithms, we also report CDFs of the minimum and maximum error. For a given attempt, these are points in the returned area that are closest to and furthest from the true location.

Hölder Metrics: In addition to error performance, we are also interested in how dramatically the localization results can be perturbed by changes in signal strength. Hölder metrics for RSS based localization were introduced in a previous work [22]. Intuitively, these metrics

relate the magnitude of a perturbation to its effect on the localization result. The idea here is that certain landmark placements can reduce the impacts of perturbations due to noise or bias, and we should be able to observe these as lower Hölder parameters.

The Hölder parameter H^p_{alg} for a given placement and algorithm is defined as $H^p_{alg} = \max_{\mathbf{s},\mathbf{v}} \frac{\|L^p_{alg}(\mathbf{s}) - L^p_{alg}(\mathbf{v})\|}{\|\mathbf{s}-\mathbf{v}\|}$, where L^p_{alg} is the result of a localization algorithm alg given placement p, with s as a signal strength vector and v as a perturbed vector.

Since the traditional Hölder parameter describes the maximum effect a signal perturbation might have, it is natural to also provide an average-case measurement. We therefore examine the average-case Hölder parameter, $\overline{H}^p_{alg}$, as well. In both cases, we measure the metrics by statistical sampling in the case of simulation, or direct computation over all localization attempts for experimentally measured data.

5.4 Landmark Position and Quantity

In this section we investigate the impact of landmark position and quantity on localization performance. Because the data collection process using many real deployments is prohibitively time-consuming, we use a trace-driven simulation methodology for this section. We first describe our methodology, then present our results investigating both the impact of landmark deployment and quantity using our previously defined metrics.

5.4.1 Simulation Methodology

Our simulation methodology requires we generate a simulated RSS reading for any point on the floor of a building from any landmark. We first begin with the path loss equation that models the received power as a function of the distance to the landmark:

$$P(d)[dBm] = P(d_0)[dBm] - 10nlog(\frac{d}{d_0}) \tag{5.14}$$

We choose the parameters $d_0 = 1m$, $P(d_0) = 58.48$ and $n = 1.523$ from [12]. We then apply a random noise factor to perturb the RSS readings. This corresponds to the random model described in [48], which represents an upper bound on the signal variability.

In many cases, we found that the localization error is large enough such that the estimated

deployment	optimal	horizontal	vertical	diagonal
Topology 200x200ft				
Linear LS				
$error$	59.81	101.26	101.07	141.79
H	58.05	172.23	159.01	206.24
$\overline{H}$	8.03	9.51	9.74	9.84
Nonlinear LS				
$error$	39.48	66.82	66.08	70.27
H	75.44	132.61	180.27	230.52
$\overline{H}$	6.98	7.31	7.58	7.97
Topology 230ftx150ft				
Linear LS				
$error$	57.89	86.97	116.57	146.65
H	66.39	170.98	198.44	352.96
$\overline{H}$	7.22	8.20	9.84	8.86
Nonlinear LS				
$error$	39.00	56.24	74.06	61.19
H	80.69	232.88	267.32	265.68
$\overline{H}$	6.66	7.12	7.21	7.32

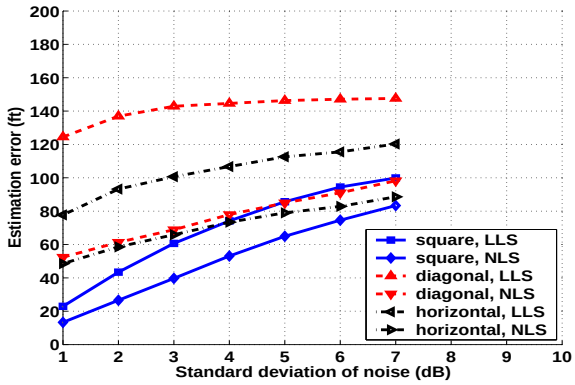
Table 5.1: Localization error (ft) and Hölder metrics when standard deviation of noise on rss is 3dB

position is well outside the floor. This was particularly true for LLS. Because such results are unrealistic in our scenario, we apply a simple truncation rule in these cases: if the X or Y coordinate is outside the floor, we truncate to the maximum or minimum value along that dimension.

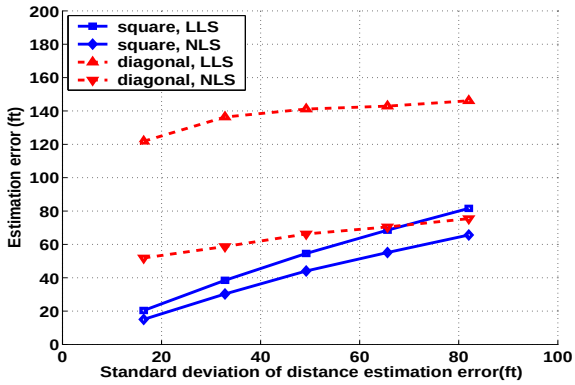
5.4.2 Evaluation of Estimation Error

Table 5.1 presents the average location estimation error after the application of truncation and the Hölder metrics for both LS algorithms under 5 landmarks for our two simulated floors. The optimized landmark deployment setup is obtained from the $maxL - minE$ algorithm. It is encouraging that both NLS and LLS provide smallest estimation errors using our placement algorithm. By comparing the values of the Hölder parameters, the LS algorithm is the least susceptible to random noise with the optimized landmark deployment, which has 4 landmarks positioned as the vertex of a square plus the fifth landmark placed at the center of the mass.

When under the diagonal landmark deployment, the localization results suffer the largest estimation errors and the algorithm is the most susceptible. The following results presented in this section are bounded by the floor boundary.



(a)



(b)

Figure 5.3: In 200x200ft area: (a) Location estimation error vs. random noise in RSS (b) Location estimation error vs. ranging error

5.4.3 Impact of Landmark Deployment

In this section we describe the impact of 3 different deployments on localization performance. We use a representative situation of 5 landmarks deployed in 3 ways to demonstrate the impact of our algorithm in a typical case.

The first deployment we call $square$, and in the 5 landmark case it is an optimal deployment when the shape is a square plus one landmark at the center of the mass. Next, the $horizontal$ deployment is the one where all the landmarks placed in a line along the longest dimension; this will give better signal coverage than the square for rectangular buildings. Finally, we also examine the impact of a poor deployment, in this case $diagonal$, which equally spaces the landmarks along a diagonal line.

Figure 5.3(a) shows the average accuracy of 10000 random trials across the floor for the 3

deployments as a function of increasing the standard deviation σ_{rss} of the noise term applied to each point. The six curves correspond to the NLS and LLS for each deployment.

First, NLS always significantly outperforms LLS. When the σ_{rss} is less than 4dB, which is typical based on our experimental experience, both algorithms under the optimized landmark deployment outperform the two other deployments. When the σ_{rss} is larger than 4dB, under the optimized landmark deployment, the NLS still performs better, while the performance of the LLS is compatible with the performance of the NLS for horizontal and diagonal landmark deployments.

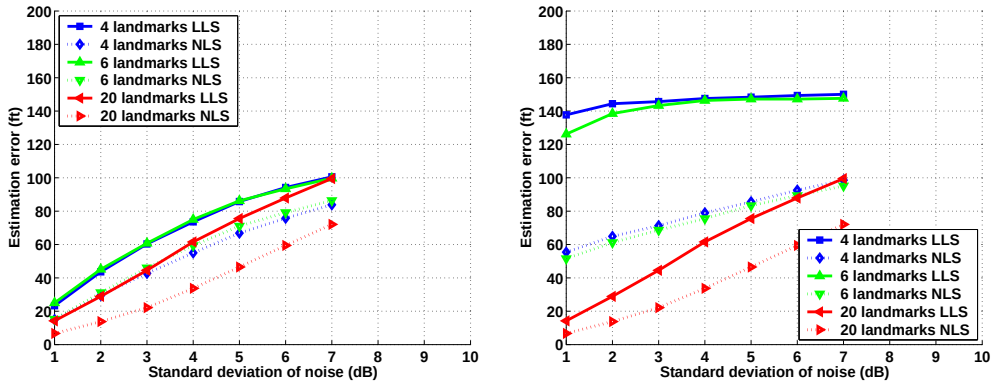
Constant sized deviations in the RSS readings result in wide differences in the distance estimation depending on the distance to the landmark. Note that the relationship between the RSS error and ranging error is multiplicative with distance, i.e., $\tilde{d} = d10^{\frac{ss-\tilde{ss}}{10n}}$. For example, in our simulation a 3dB error corresponds to a multiplicative factor of 1.5, at 10ft distance, $\tilde{d} = 15ft$ with an error of 5ft, while at 100ft distance, $\tilde{d} = 150ft$ with an error of 50ft, a factor of ten larger. We are motivated to study the magnitude of distance estimation error caused by the deviation of the RSS readings.

Figure 5.3(b) shows the location estimation error vs. the standard deviation σ_d of distance estimation error. We observe that a noise σ_{rss} of 2dB corresponds to a distance error σ_d of 32ft. Further, the estimation results when the σ_{rss} is 4dB and 5dB translate to the σ_d of 65ft and 82ft respectively. Thus, even small random perturbation in RSS readings cause large ranging estimation errors due to this multiplicative factor.

5.4.4 Impact of Landmark Quantity

In this section we observe the impact of adding more landmarks. We compare the performance of the LS algorithms with 4, 6 and 20 landmarks under square and diagonal deployments. We use our optimized placement in the case of 4 and 6 landmarks, and a uniform randomized deployment for 20 landmarks.

Figure 5.4 shows a promising result that when deploying 4 landmarks and 6 landmarks under their optimized deployments, the localization results using LS are compatible with the results using a much higher number landmarks, 20, in this case. If a small number of landmarks



(a)Optimized case (b)Worst case

Figure 5.4: Performance of LS algorithms across different number of landmarks in 200x200ft area

provide sufficient coverage, this is an encouraging observation because good localization performance can be achieved without a large number of landmarks.

5.5 Experimental Study

In this section we present our experimental study by using 802.11 PCMCIA cards and Telos Sky motes. The objective is to compare the impact of our landmark deployment analysis on a variety of algorithms and different ranging modalities. Although the mathematics of our analysis is based on LLS, we show that deployments based on $maxL-minE$ algorithm improve localization accuracy in widely diverse scenarios.

We first give a brief description of a set of representative RSS-based localization algorithms. We then describe our experimental method. Next, we quantify the performance across the algorithms provided different landmark deployments. We also compare the localization accuracy and Hölder metrics for these algorithms. Finally, we provide a comparison between the RSS-based and TOA-based LS algorithms using our deployment strategy.

5.5.1 Algorithms

In this study, our main focus is the localization algorithms that employ signal strength measurements. To demonstrate the general applicability of our landmark deployment algorithm, we test

our placement strategy on three widely different localization algorithms, RADAR, ABP, and BN. Although there are many other RSS-based localization algorithms, this set spans various strategies, and given all algorithms have qualitatively similar performance [27] we feel this set is sufficiently representative.

RADAR is a point-based, scene-matching algorithm. The user first builds a training set of RSS values from landmarks matched to known locations. To localize, the object creates a vector of RSS values from the landmarks and the algorithm returns the training point closest to the vector using Euclidean distance as the discriminating function [12]. ABP uses Bayes rule combined with scene-matching to return an area the object is likely to reside in and probabilistically bounds the likelihood with a confidence level [27]. Taking the Bayesian network approach, the BN algorithm uses a Bayesian graphical model based on lateration to find the estimated location [52].

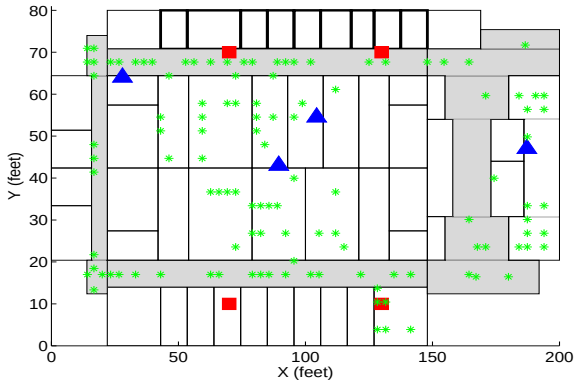
5.5.2 Experimental Setup and Methodology

A series of experiments are conducted in our Computer Science Department which resides the whole 3rd floor of the CoRE building. The floor size is 200x80ft (16000 ft^2). The experiments are performed using 4 landmarks setup in the floor.

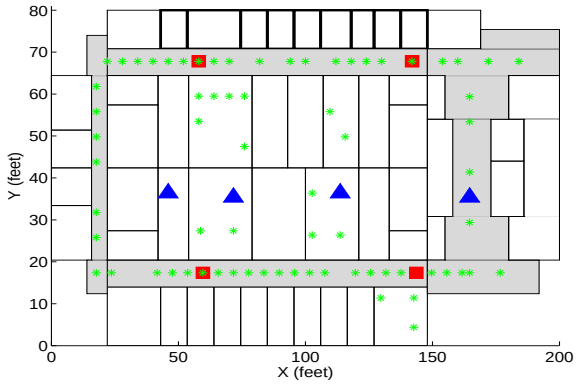
Figure 5.5(a) shows the original collinear landmark deployment setup in triangles and our optimized landmark deployment as squares for the 802.11 network. The networking staff of the department deployed the APs in the collinear deployment specifically to maximize signal strength coverage. The first set of RSS data was collected under this collinear deployment by using a Dell laptop running Linux equipped with an Orinoco silver card (802.11 card). The data was collected at 286 locations on the 3rd floor.

Then we used a trace-driven approach to generate the RSS data set under the optimized landmark deployment. We first performed a least squares fit of the measured data and obtained the parameters of the path loss model in Equation (5.14). Then we directly used measured variance to generate the RSS readings. Finally, we applied environmental bias using the Ray-Sector model described in [48] to obtain the new RSS data set for the optimized deployment case.

To validate that our trace-driven strategy generated realistic radio signal readings, we placed



(a)802.11

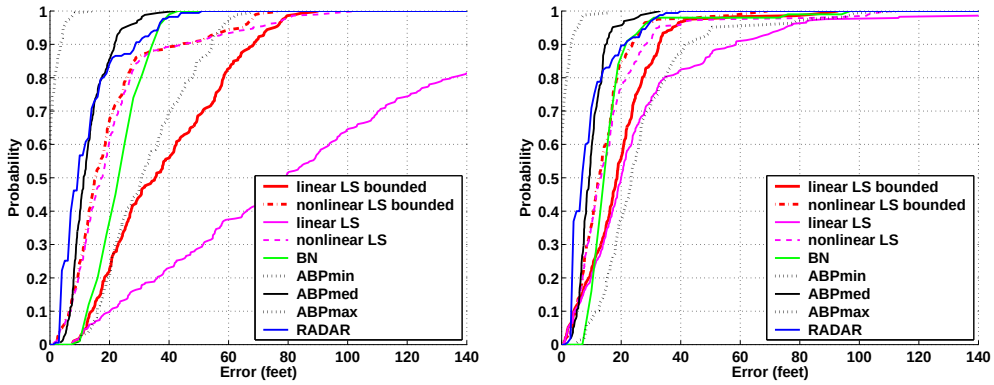


(b)802.15.4

Figure 5.5: Deployment of landmarks and training locations on the experimental floors

4 simulated landmarks at the same positions as the real collinear deployment and then generated synthetic RSS values. We compared the localization performance of using this synthetic data set against the real data. We found the estimation CDFs nearly identical for all of our algorithms under study. Thus we have confidence that our combination of path-loss model fitting, variance application, and bias generation result in RSS readings that generate realistic localization results.

Our second experimental setup was an 802.15.4 network which utilized 4 Telos Sky mote landmarks and deployed two sets of landmark placement positions. Figure 5.5 (b) shows the mote landmarks under an optimized square deployment as squares and a horizontal landmark deployment (again, to maximize signal strength coverage) as triangles. Unlike the 802.11 case, no RSS data was generated; for both deployments the measured data is used in the algorithms.



(a)Collinear case (b)Square case

Figure 5.6: Localization accuracy CDFs across algorithms for 802.11 network

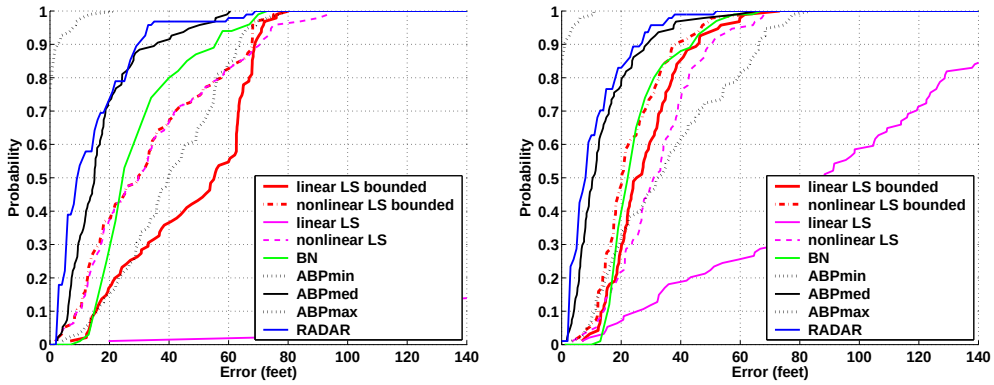
We have experimented with different training set sizes for constructing the radio map for RADAR and ABP. For 802.11 data sets, we show the results with 115 training points. While for 802.15.4 data sets, we use 70 training points. The small stars in Figure 5.5 are the randomly selected training points. The localization at each testing point is performed by using the leave-one-out method.

5.5.3 Localization Accuracy

Figure 5.6 (a) and (b) present the 802.11 accuracy CDF under collinear and square landmark deployments, respectively. A bounded result means we applied truncation. ABP is calculated with confidence level 75%. ABP-med is the error of the median distance of the area, together with ABP-min and ABP-max are the closest and furthest points of the returned area.

Figure 5.6(a) shows that under the horizontal-like deployment, LLS always fairs very poorly, while NLS, RADAR, ABP and BN are qualitatively similar. All the algorithms have long tails. Figure 5.7(a) shows a similar result when using the motes, although in here the perfect collinear deployment, the horizontal case, reduces the performance of the lateration approaches (BN, NLS , and LLS) compared to 802.11.

Figures 5.6(b) and 5.7(b) show the key impact of our work. All of the CDFs have shifted up and to the left compared to those in Figures 5.6(a) and 5.7(a). Thus, a significant fraction of the results are more accurate using the optimized deployments generated by $maxL - minE$



(a)Horizontal case (b)Square case

Figure 5.7: Localization accuracy CDFs across algorithms for 802.15.4 network

algorithm. In addition, for ABP, the gap between the min and max CDFs is much narrower, implying the returned areas are on average smaller than those in the horizontal deployments.

5.5.4 Evaluation of Performance and Sensitivity

Table 5.2 summarizes the average error for each algorithm to further investigate the improvements gained by using an optimal deployment. The table shows the average error improves for all the algorithms. For 802.11 data sets, the LLS algorithm improves over 35% and NLS gains 25% in performance. Both ABP and RADAR have improved over 20% in localization accuracy, while BN has gained 10%. Looking at the 802.15.4 network, the performance improvement results are compatible to the results from the 802.11 network.

The Hölder metrics presented in Table 5.2 for each algorithm under the optimized landmark deployment is smaller than the horizontal deployment. Recall that the Hölder parameter is a measurement of the sensitivity of the algorithm to perturbations of inputs such as RSS, which can model random noise, environmental bias, and measurement errors. The lower Hölder values are strong evidence that an optimized landmark deployment not only can improve the localization performance, but also can make an algorithm less susceptible to the above classes of perturbations.

Average location estimation error (ft)							
Algorithms	**Linear LS**		**Nonlinear LS**		**BN**	**ABP**	**RADAR**
802.11	**w trun**	**w/o trun**	**w trun**	**w/o trun**			
collinear	38.56	94.53	20.23	21.85	22.25	13.11	12.49
square	24.73	31.29	15.37	16.92	20.16	10.09	9.31
802.15.4	**w trun**	**w/o trun**	**w trun**	**w/o trun**			
horizontal	47.89	608.43	33.15	34.44	28.43	17.86	14.28
square	28.27	92.05	23.65	32.17	24.25	14.27	11.33
Hölder	**(worst-case)** H						
Algorithms	**Linear LS**		**Nonlinear LS**		**BN**	**ABP**	**RADAR**
802.11	**w trun**	**w/o trun**	**w trun**	**w/o trun**			
collinear	22.36	48.47	21.55	21.55	31.73	20.03	36.24
square	12.19	15.33	9.62	9.75	15.89	10.64	9.86
802.15.4	**w trun**	**w/o trun**	**w trun**	**w/o trun**			
horizontal	28.88	286.13	91.00	91.00	28.27	64.06	32.58
square	13.86	17.14	10.82	16.32	18.41	11.27	13.42
Hölder	**(average-case)** $\overline{H}$						
Algorithms	**Linear LS**		**Nonlinear LS**		**BN**	**ABP**	**RADAR**
802.11	**w trun**	**w/o trun**	**w trun**	**w/o trun**			
collinear	2.72	5.37	2.06	2.18	2.06	1.85	1.98
square	2.87	3.57	2.45	2.70	1.63	1.79	2.06
802.15.4	**w trun**	**w/o trun**	**w trun**	**w/o trun**			
horizontal	2.66	33.87	2.45	2.50	1.44	2.05	2.21
square	2.95	5.23	2.35	2.69	2.41	1.95	2.27

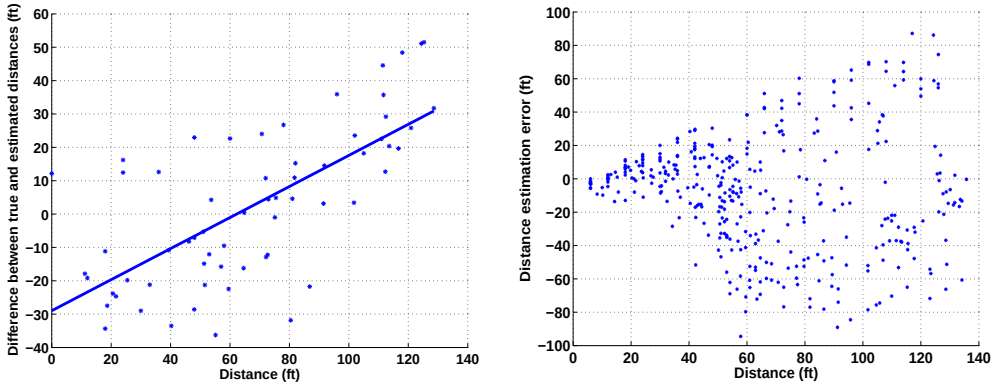
Table 5.2: Location estimation error (ft) and Hölder parameters across algorithms

5.5.5 Using Time of Arrival

In this section we experimentally investigate how well our deployment algorithm works for an alternate ranging modality. In this second modality, we compute the distance to a landmark by measuring many round trip times between a node and a landmark, and then calculate the time-of-flight (ToF) of a packet. Given the ToF and the speed of light, we can estimate the range. This is a Time-of-Arrival (TOA) based approach because the actual time-of-flight is estimated. Space limitations prevent us from describing this approach in more details, but a full description of the technique and an analysis of it can be found in [32].

We used a similar trace-driven based methodology in our TOA investigation as for the 802.11 RSS one. We estimated the TOA based on the round trip times for packets and derived the distance between the localizing node to each landmark. We then built an error distribution of the true distance vs. the estimated distance, and used that to drive a simulation where we could place the landmarks in the same positions as the RSS study. The same hardware is used as for the RSS study.

The linear regression model applied to the distance estimation error of TOA data with 63



(a)TOA (b)RSS

Figure 5.8: Linear regression on TOA data

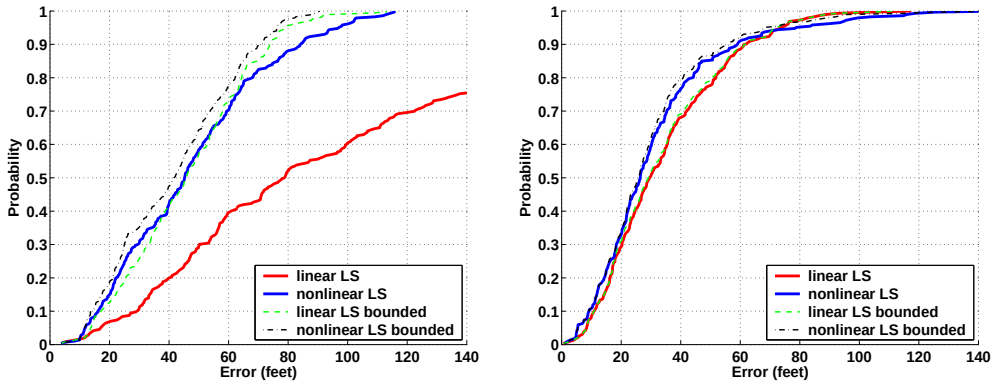
experimental distances is shown in Figure 5.8(a). We observe that shorter the distance to a landmark results in estimated distance longer than the true distance, while longer the distance to a landmark results in estimation distance shorter than the true distance. The corresponding distance estimation error of RSS data is presented in Figure 5.8(b). Comparing the TOA results to RSS distance estimation errors, while the magnitude of the distance estimation error grows with lengthening distance, unlike in TOA the resulted estimation in RSS is either longer or shorter with near equal probability.

With the mean and variance estimated from linear regression, we have modeled distance estimation error of TOA as a Gaussian distribution defined in Equation (5.15):

$$\begin{aligned} error &\sim N(\mu, \sigma^2) \\ with\ \hat{\mu} &= b_0 + b_1 d_i \\ and\ \hat{\sigma^2} &= \frac{\sum_{i=1}^{n} (\tilde{d_i} - \hat{\mu})^2}{n-1}, \end{aligned} \tag{5.15}$$

where d_i is the true distance and $\tilde{d_i}$ is the estimated distance. n is the total number of distances under experimentation. b_0 and b_1 are the coefficients of the linear regression.

We further conducted a trace-driven approach to localize 286 positions on the floor using 4 landmarks setup with collinear and square deployment respectively according to Figure 5.5(a) for the 802.11 network.



(a)Collinear case (b)Square case

Figure 5.9: Localization accuracy CDFs using TOA

Figure 5.9 plots the localization accuracy CDF of the LS algorithms using TOA. The figure shows that as with RSS, the performance of LS increases under an optimized deployment as compared to a horizontal deployment designed for coverage. Quantitatively, the performance improvement is over 30%. Comparing the absolute performance of this technique with RSS, our TOA approach is qualitatively worse. This is likely due to the very coarse grained microseconds-level clocks currently available in standard 802.11. Additional clocks with much higher frequencies would help to reduce much of the measurement uncertainty.

5.6 Conclusion

In this chapter, by analyzing the Linear Least Squares algorithm, we derived an upper bound on the maximum location error given the placement of landmarks. Based on this theoretical analysis, we found optimal patterns for landmark placement and further developed a novel algorithm, $maxL - minE$, for finding optimal landmark placement that minimizes the maximum localization error.

To show the generality of our results, we conducted experiments using both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network. Based on the experimental data, we investigated the impact of landmark position and quantity on localization performance using both the measurements of RSS in an actual building as well as trace-driven simulations that used the RSS measurements. In addition, we apply the trace-driven approach to an alternate ranging

modality, in this case, TOA.

We found that the performance of a wide variety of algorithms showed significant improvements when using landmarks placed according to our algorithm, as opposed to alternate deployments. We evaluated these improvements under several different metrics. The experimental results provide strong evidence that our analysis and algorithm for landmark placement is very generic as the resulting placement has improved localization performance across a diverse set of algorithms, networks, and ranging modalities.

Our results also point out that there is a tension between the ideal landmark deployment for localization vs. deployments that optimize for signal coverage. We found that in our building, the better coverage deployment was very collinear, and this had pronounced negative impact on localization performance. Future work would conversely investigate the impact of a deployment optimized for localization on signal coverage, as well as try to find a method of trading one kind of deployment for another depending on the users' needs.

In the previous chapters we have explored methods and solutions to provide accurate and trustworthy localization results. Further, we would like to provide a scalable, general purpose, and real time localization infrastructure that can localized any radio-enabled devices at any where and any time. In the next chapter, we present a general purpose localization system prototype called GRAIL (Generalized Real-time Adaptable Indoor Localization) which can simultaneously position multiple devices.

Chapter 6

General Purpose Localization System

6.1 Introduction

Utilizing the same infrastructure for both communication and positioning would provide a tremendous cost and deployment savings over a specific localization infrastructure. Thus one of the primary goals of localization research is to provide a scalable, general purpose, and real time localization infrastructure that can integrate location information into any computing radio-enabled devices. We are designing and developing a general purpose localization system prototype called GRAIL (Generalized Real-time Adaptable Indoor Localization) which can simultaneously position multiple devices using Bayesian Networks. The deployment of such a system in academic and research environments will allow researchers to explore issues beyond just algorithms and simulation tools. It would make it possible to conduct higher-level interaged research investigation including privacy studies, security services, and policy enforcement. For instance, we utilized the GRAIL system to conduct research on spoofing attacks in Chapter 4. In addition, the practical usage of such an approach is significant because it can be applied to a broad array of applications such as monitoring, tracking, routing, and security services.

Localization is a diverse area covering everything from lower-layer physical problems to application-level services. GRAIL assumes the localization area to be about the size of a building, where devices have access to gateway nodes, and these in turn can access wired networks. Additional properties of the GRAIL system include:

General Purpose. A primary goal of the GRAIL system is that it should work over a variety of physical modalities and networks. Much as a networking system should support multiple media access layers, a general purpose localization system should support multiple physical modalities and methods of localization.

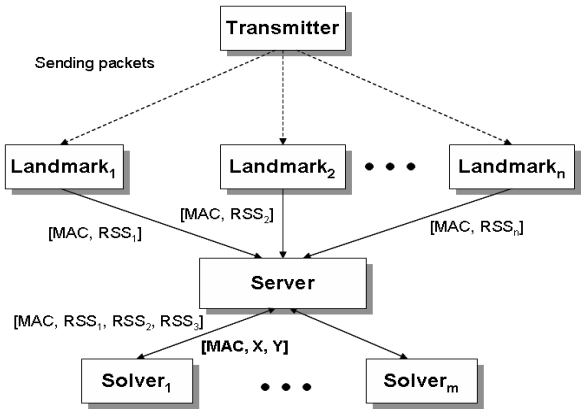


Figure 6.1: GRAIL system architecture

GRAIL is designed to localize using any wireless network that supports physical layer measurements of packet data. It supports to use Received Signal Strength (RSS) as the physical modality and can be easily extended to support Angle-of-Arrival (AoA), and time-of-arrival (TOA).

Real-time. Latency is a key property of localization systems because it defines the maximum mobility that can be supported. Our system can return results in less than one second, allowing us to support both stationary devices as well as those moving at walking speeds (about 1m/s).

Adaptable. A common problem with many systems is that they are too brittle; they require specific environments, hardware, or much training data related to a specific set-up. GRAIL uses real-time feedback to dynamically calibrate its parameters due to changing radio conditions.

Indoor. Indoor environments are especially challenging due to reflections, refractions, and scattering, which result in substantial multi-path effects. GRAIL manages the uncertainly of these effects. GRAIL can expand and contract the possible set of locations as we introduce or reduce the uncertainty in the environment. Specifically, we can show how modifying the antennas can either increase or decrease spatial uncertainty.

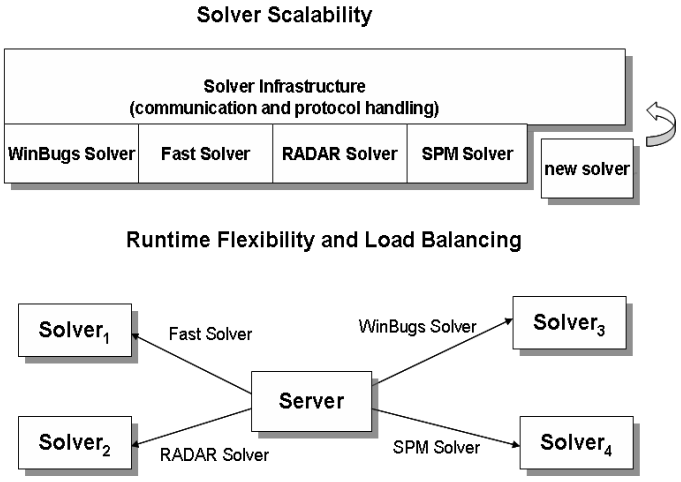


Figure 6.2: Solver scalability and flexibility.

6.2 Architecture Design

The GRAIL system is designed with fully distributed functionality and easy to plug-in localization algorithms. As shown in Figure 6.1, The main software components are Transmitters, Landmarks, the Server, and Solvers. The Landmarks collect the RSS reading for each transmitting device and send it to the Server together with the coordinates of the landmarks. Landmarks are stateless, which greatly simplifies the design, and are deployed in known loations. Often, in other research works, landmarks are called Anchor Points or Access Points. However, we use the term *landmark* because an access point also provides access to the wired network, and in GRAIL, landmarks do no provide this function. Upon receiving the RSS readings from each Landmark module, the Server collects the complete set of RSS readings for each node, decides on which localization algorithm to use, then forwards the RSS information to the corresponding Solver module. The Solver is flexible and easy to scale. Many different kinds of localization algorithms can be plugged in as illustrated in Figure 6.2. The Server and Solver components are fully decoupled.

For localization using Bayesian networks, in addition to the *WinBugs Solver* which utilizes the statistical WinBugs tool [9], we have implemented the *Fast Solver* [40]. The *Fast Solver* is developed by using a novel real-time sampling technique which reduces computational cost significantly and solves Bayesian networks 9 to 17 times faster than the *WinBugs Solver*. The

GRAIL system can localize 1 to 10 sensor nodes in less than half a second, and scales to localize 51 objects simultaneously with no location information in the training data within 6 seconds.

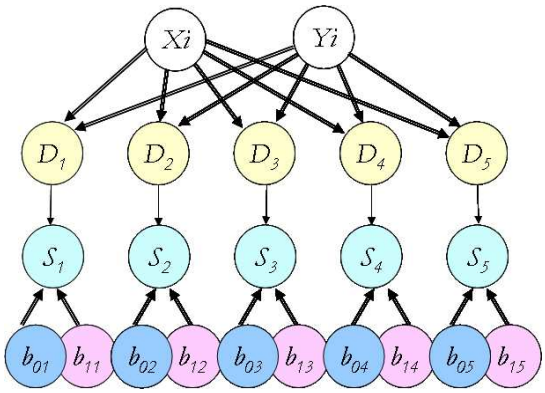
Although our current GRAIL system uses Bayesian networks, its distributed and scalable architecture was designed for maximum flexibility. GRAIL can thus easily accommodate alternative localization modalities and algorithms by using replaceable components. Thus other localization algorithms [12, 27] such as RADAR (R), Simple Point Matching (SPM), and Area Based Probability (ABP) can be added on easily with this flexible architecture design. During localization, there are multiple Solver instances available and each can represent one type of algorithm. Once the localization results are returned by the Solver, the Server displays the positions of the unknown transmitting devices. If there is a need to localize hundreds of transmitting devices simultaneously, the Server can perform load balancing among the different Solver instances as shown in Figure 6.2. Plus, this centralized server also makes enforcing contracts and privacy policies more tractable.

6.3 Bayesian Networks

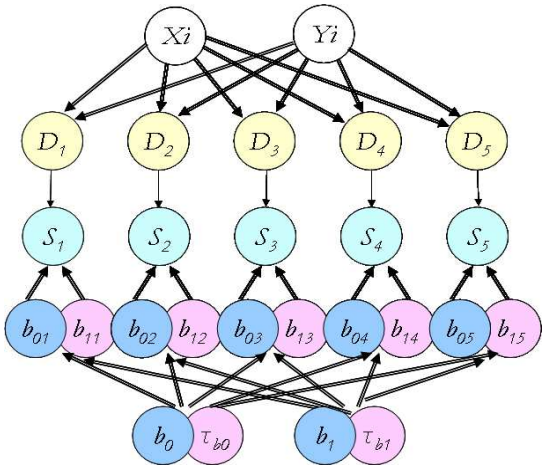
In this section, we give a brief overview of Bayesian Networks that are used in the GRAIL system. The Bayesian network is a graphical model that encodes dependencies and relationships among a set of random variables. The vertices of the graph correspond to the random variables and the edges represent dependencies. Bayesian inference in conjunction with Bayesian networks offers an efficient and principal approach for avoiding the over-fitting of data.

In the GRAIL system, we have developed several Bayesian graphical models to encode the relationship between the RSS and the location based on signal-to-distance propagation model. We have built both non-hierarchical (M1) and hierarchical (M2) Bayesian graphical models as presented in Figure 6.3 (a) and (b).

The location measurement process is slow and labor-intensive. By contrast, gathering RSS readings without the corresponding locations does not require human intervention. For example, sniffing devices can perform RSS measurements repeatedly at essentially no cost. So, we pursue the idea that different access points behave similarly and the prior knowledge may provide sufficient constraints to obviate the need to know the actual locations of the training data



(a) Non-hierarchical Bayesian graphical model



(b) Hierarchical Bayesian graphical model

Figure 6.3: Bayesian Networks

observations. As a result, we have extended the M2 model and built a new model called M3 whose training data comprise solely of signal strengths of unknown locations [52]. This leads to a truly adaptive, zero-profiling technique for location estimation. The GRAIL system fully supports M1, M2 and M3 models for performing localization using either *WinBugs Solver* or *Fast Solver*.

Chapter 7

Related Work

7.1 Introduction

In this chapter, we present the related research work, and compare and contrast our research work with the others. Specifically, we first provide an overview of wireless localization approaches in Section 7.2. Then we show severe impacts of non-cryptographic attacks to localization results in the network and discuss methods to verify localization estimates in Section 7.3. Next, we point out identity-based spoofing attacks are a serious threat in the network and review conventional methods and a few new approaches to address spoofing attacks in Section 7.4. Further, in Section 7.5 we studied the previous work that try to improve localization performance from the point of view of landmark placement. Finally, we give a short review of developing localization systems in both academic and industrial environments in Section 7.6.

7.2 Wireless Localization

There has been much activity toward developing localization systems for wireless and sensor networks. We cannot cover the entire body of works in this section. Rather, we give a short overview of the different localization strategies in this section.

Localization approaches can be categorized using various taxonomies. Range-based algorithms involve distance calculation to landmarks with known positions using the measurement of various physical properties [55] like RSS [12, 27], Time Of Arrival (TOA) [28] and Time Difference Of Arrival (TDOA) [56]. Range-free algorithms use coarser metrics such as connectivity [63] or hop counts [54] to place bounds on node positions.

Another classification method relates how a node is mapped to a location. Lateration approaches [23, 28, 44, 49, 54], try to solve a set of equations involving distances to landmarks;

angulation uses the angles from landmarks [53]; while probabilistic approaches [59, 69] use statistical inferences, and statistical supervised learning techniques [12, 27, 52] utilize training data to help inference the location estimation. Among them, scene matching strategies [12, 14, 27, 59, 69] are originated from machine learning techniques. Usually a radio map of the environment is constructed, either by measuring actual samples, using signal propagation models, or some combination of the two. A node then measures a set of radio properties (often just the RSS of a set of landmarks), the *fingerprint*, and attempts to match these to known location(s) on the radio map. These approaches are almost always used in indoor environments because signal propagation is extensively affected by reflection, diffraction and scattering, and thus ranging or simple distance bounds cannot be effectively employed. Matching fingerprints to locations can be cast in statistical terms [59, 69], as a machine-learning classifier problem [14], or as a clustering problem [12].

Finally, a third dimension of classification extends to aggregate or singular algorithms. Aggregate approaches [25, 63] use collections of many nodes in the network in order to localize (often by flooding), while localization of a node in singular methods only requires it to communicate to a few landmarks with known locations.

In addition, some research have experimented with using ultrasound, infrared, or a combination of infrared and RSS for localization [35, 56, 62, 64, 66]. The goal is to reach centimeter accuracy. These work use specialty hardware or have limited range as in the infrared technology. As such, they can only be deployed in highly engineered and controlled areas, and hence have not become very popular.

Also, this is different from our goals: we conjecture that sacrificing little accuracy for scalability would create more practical positioning systems that are easier to bootstrap. We focus our work on two broad localization mechanisms: multilateration and signal strength. Multilateration clearly applies to both single and multi-hop range-based approaches, while signal strength can be applied to a wider variety of both range-based and scene matching algorithms.

7.3 Secure Localization

There has been considerably less work on the problem of ensuring the trustworthiness of wireless localization. In this section, we review research methods that developed for secure localization.

Cryptographic threats on localization can be addressed through traditional security services [16, 31, 39, 67, 68, 70, 71], e.g. authentication.

However, there is a completely orthogonal set of attacks that are non-cryptographic, where the measurement process itself can be corrupted by adversaries. For example, wormhole attacks tunnel through a faster channel to shorten the observed distance between two nodes [36]. Compromised nodes may delay response messages to disrupt distance estimation [49] and compromised landmarks may even broadcast completely invalid information [51]. Physical barriers can directly distort the physical property used by localization. [49] provided a thorough survey of potential attacks to various localization algorithms based on their underlying physical properties.

Unfortunately, these non-cryptographic attacks can not be addressed by traditional security services. In order to address the non-cryptographic attacks, different strategies are required. This has been the focus of our research. [17, 61] proposed distance bounding protocols for verification of node positions. [18] proposed the Verifiable Multilateration mechanism which is based on the distance bounding protocols for secure position computation and verification. [19] uses hidden and mobile base stations to localize and verify location estimates. [45] uses both directional antennas and distance bounding to achieve security. Compared to all these methods, which employ location verification and discard location estimate that indicates under attack, [24, 49, 51] try to eliminate attack effects and still provide accurate localization. [49] makes use of the data redundancy and robust statistical methods to achieve reliable localization in the presence of attacks. [51] proposes to detect attacks based on data inconsistency from received beacons and to use a greedy search or voting algorithm to eliminate the malicious beacon information.

The closest works to our attack detection work are [26, 51]. A general location anomaly

detection scheme is described in [26] that relied on the neighbor information to detect inconsistencies. However, it assumes a highly dense network where the positions of the nodes follow a Gaussian distribution, which is contrary to the structure of many deployed systems where much lower densities are typical. Our proposed LLS approach is more general than the ARMMSE approach in [51]. Further, our approach provides a broader choices of detectors than that work.

Our work is unique in that we have formulated location attack detection as a general statistical significance testing problem. We showed how the test statistics come naturally out of the localization algorithms themselves without additional assumptions. In addition, our work differs from most previous research in that we experimentally validated our approaches using real networks deployed in two different buildings.

7.4 Coping with Identity Fraud

In wireless networks, attackers can gather useful identity information during passive monitoring and utilize the identity information to launch identity-based spoofing attacks. For instance, it is easy for a wireless device to acquire a valid MAC address and masquerade as another device. The 802.11 protocol suite provides insufficient identity verification during message exchange, including most control and management frames. Therefore, the adversary can utilize this weakness and request various services as if it were another user. Identity-based spoofing attacks are a serious threat in the network since they represent a form of identity compromise and can facilitate a series of traffic injection attacks. There has been active research addressing spoofing attacks as well as those facilitated by adversaries masquerading as another wireless device. In this section, we give a short overview of the attacks that is based on identity-spoofing, and the traditional methods and several new approaches to address spoofing attacks. We then describe the works most closely related to our work.

An adversary can launch a deauthetication attack. After a client chooses an access point for future communication, it must authenticate itself to the access point before the communication session starts. Both the client and the access point are allowed to explicitly request for deauthentication to void the existing authentication relationship with each other. Unfortunately, this deauthentication message is not authenticated. Therefore, an attacker can spoof this

deauthentication message, either on the clients behalf, or on the access points behalf [15]. The adversary can persistently repeat this attack and completely prevent the client from transmitting or receiving. Further, An attacker can utilize identity spoofing and launch the Rogue Access Point (AP) attack against the wireless network. In the Rogue AP attack, the adversary first sets up a rogue access point with the same MAC address and SSID as the legitimate access point, but with a stronger signal. When a station enters the coverage of the rogue AP, the default network configuration will make the station automatically associate with the rogue access point, which has a stronger signal. Then the adversary can take actions to influence the communication. For example, it can direct fake traffic to the associated station or drop the requests made by the station. Besides the basic packet flooding attacks, the adversary can make use of identity-spoofing to perform more sophisticated flooding attacks on access points, such as probe request, authentication request, and association request flooding attacks [30].

The traditional security approach to cope with identity fraud is to use cryptographic authentication. An authentication framework for hierarchical, ad hoc sensor networks is proposed in [16] and a hop-by-hop authentication protocol is presented in [71]. Additional infrastructural overhead and computational power are needed to distribute, maintain, and refresh the key management functions needed for authentication. [68] has introduced a secure and efficient key management framework (SEKM). SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group. [67] implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys. In addition, binding approaches are employed by Cryptographically Generated Addresses (CGA) to defend against the network identity spoofing [11, 38].

Due to the limited resources in wireless and sensor nodes, and the infrastructural overhead needed to maintain the authentication mechanisms, it is not always desirable to use authentication. Recently new approaches have been proposed to detect the spoofing attacks in wireless networks. [47, 57] have introduced a security layer that is separate from conventional network authentication methods. They developed forge-resistant relationships based on packet traffic by using packet sequence numbers, traffic interarrival, one-way chain of temporary identifiers, and signal strength consistency checks to detect spoofing attacks. [50] proposed a lower-layer approach that utilizes properties of the wireless channel at the physical layer to support high-level

security objectives such as authentication and confidentiality. The most closely related work to ours is [29], which proposed the use of matching rules of signal prints for spoofing detection.

Although these methods have varying detection and false alarm rates, none of these approaches provide the ability to localize the positions of the spoofing attackers after detection. Further, our work is novel in that we have integrated our spoofing detector into a real-time localization system which can both detect the spoofing attacks, as well as localize the adversaries in wireless and sensor networks. In addition, we deployed our localization system in a real office building environment which houses our Computer Science Department.

7.5 Localization Performance

In addition to ensure the trustworthiness of the location information, it is also important to pursue higher location accuracy through improving the performance of localization systems. There has been some work to investigate or place bounds on the performance of localization systems using signal strength [14, 27, 37]. They either showed a range of localization algorithms all have similar performance or tried to build theoretical models for the localization environment in order to study the localization performance. They did not propose solutions to improve the localization performance.

In our work, we took a novel approach, instead of improving the localization algorithms themselves, we focus on improving the deployment of landmarks, and this should help a wide variety of algorithms. There are a few works that studied the impact of landmark placement to the localization performance that are related to our work. [21] used simple linear and multiple regression methods to estimate the signal strength model. With simulation, it analyzed the relationship between standard deviation of location error and signal strength error for a few Access Point (AP) configurations. However, they did not analyze for the optimized geometry of AP deployment and provide experimental comparison as we have in our work. Another work presented a theoretical model for RSS-based location estimation accuracy and examined placement, but did not find optimal solutions [41]. [13] developed a set of heuristic search algorithms to find optimal AP deployment for a balance of signal coverage and location errors. Compared to our simple approach, the heuristic search algorithms are more complex and time

consuming. The results were only shown for the probability matching algorithms, thus may not be general for other type of algorithms.

Furthermore, a large body of works have examined AP placement to maximize coverage and throughput properties of wireless LANs and sensor networks. We do not cover these works here, except to say that future work would be to examine the trade offs in landmark and AP deployment assuming they use the same hardware, although this does not need to be the case. Recall that landmarks provide a node with signals from known locations, while APs provide media access control as well as gateways into the wired network.

7.6 Localization Infrastructure

In the academic research environment, the deployment of a general purpose localization system that can localize any radio-enabled devices at any time and at any where will allow researchers to explore various issues beyond just algorithms and simulation, such as privacy study and security services. The localization system that developed in a research setting that mostly related to ours is Place Lab [42, 46]. The Place Lab approach is to allow commodity hardware clients like notebooks, PDAs and cell phones to locate themselves by listening for radio beacons such as 802.11 APs, GSM cell phone towers, and fixed Bluetooth devices that already exist in the environment. Our general purpose localization infrastructure is different from Place Lab in that it is easy for us to extend and support other physical modalities such as TOA and AOA in addition to RSS. Further, our flexible Solver infrastructure makes it easy to plug in and test on different localization algorithms including Bayesian Networks (BN), Area Based Probability (ABP), RADAR, and any new algorithms.

There are several emerging commercial products for indoor localization or intrusion prevention [1, 2, 8]. The problems for these industrial products are: they are not very general, require specific chip sets and operating systems, only focus on Wi-Fi radio, and do not support other physical modalities for localization. Moreover, the performance of these systems are not well-known, lack of independent performance benchmarking. Further, the source code of all these products is not available, which makes them hard to be used in an research environment that frequently needs to incorporate new properties and make extensions for research purposes.

Chapter 8

Conclusions and Future Work

8.1 Dissertation Conclusions

As more wireless networks are deployed, location-based services are becoming increasingly prevalent. It is critical to provide accurate and trustworthy location information. This thesis explored and proposed methods to provide secure and accurate location information for wireless and sensor networks using statistical approaches.

We first characterized the robustness of localization algorithms to attacks that target signal strength measurements. We provided a set of performance metrics for quantifying the effectiveness of signal strength attacks, including a new family of metrics, called Hölder metrics, that quantify the variability of localization changes in physical space related to changes in signal strength vectors. The key observation we found is that all the algorithms have similar average responses to attacks. The median error of all the algorithms degraded gracefully with a linear response as a function of the attack strength.

Since we have found the performance of localization algorithms degrades significantly under signal attacks, it is important to detect the presence of these attacks. The next contribution of our work is several attack detection methods that provide a theoretical foundation of the attack detection problem using statistical significance testing. We then built test statistics for two broad localization classes: multilateration and signal strength. For multilateration that uses Linear Least Squares, we derived a closed-form representation for the attack detector. Further, for localization schemes that employ signal strength, we showed that by utilizing the signal strength as a common feature, the minimum Euclidean distance in the signal space can be used as a test statistic for attack detection independent of the localization process. The key advantage of this approach is that for algorithms employing signal strength, the detection phase is prior to the localization, and thus saves computational cost of localization under attack. The

significant finding is that our experimental results involving both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network in two real office buildings show that different localization system have similar attack detection capabilities, and consequently these provide important insights to system designers that they can focus on using algorithms that provide the highest localization accuracy rather than having to trade off position accuracy against attack detection abilities. Further, we conclude that any significant attacks can be successfully captured by our attack detection schemes.

The next challenging step after detecting attacks is to localize adversaries and eliminate malicious attacks. We thus proposed a method for detecting spoofing attacks utilizing K-means cluster analysis, as well as localizing the adversaries by integrating our K-means spoofing detector into a general purpose, real-time localization system. We found that the performance of the localization system when localizing the adversaries using the centroids of RSS readings from K-means cluster analysis are about the same as localizing using averaged RSS readings under normal conditions. The distance between the spoofing node and the original node can be estimated with median error of 10 feet. Since spoofing attacks are a serious threat as they represent a form of identity compromise and a malicious attacker may create multiple illegitimate identities, we will discuss our future work for detecting multiple illegal spoofing identities in the next section.

Another significant finding of our work in the area of improving the localization performance is that we found the landmark placement plays an important role in location accuracy. By analyzing the Linear Least Squares algorithm, we derived an upper bound on the maximum location error given the placement of landmarks. Based on this theoretical analysis, we found optimal patterns for landmark placement and further developed a novel algorithm, $maxL - minE$, for finding optimal landmark placement that minimizes the maximum localization error. The experimental results provide strong evidence that our analysis and algorithm for landmark placement is very generic as the resulting placement has improved localization performance across a diverse set of algorithms, networks, and ranging modalities. Our results also point out that there is a tension between the ideal landmark deployment for localization vs. deployments that optimize for signal coverage. We found that in our building, the better

coverage deployment was very collinear, and this had pronounced negative impact on localization performance. Future work would conversely investigate the impact of a deployment optimized for localization on signal coverage, as well as try to find a method of trading one kind of deployment for another depending on the users' needs.

8.2 Future Research Directions

We envision the utility of the location information in wireless and sensor network systems will continue to have an increasing impact on our life, ultimately to the point where location-based applications will be an inseparable part of our social fabric. In order to make this vision a reality, there are many open issues that remain to be addressed. Based on current results in this thesis, we think it is important to address future research directions in the following area:

First, from the perspective of basic physical modalities used for localization, utilizing RSS is an attractive approach for localization because it can re-use the existing wireless infrastructure, rather than requiring additional specialized localization infrastructure. However, based on our observations RSS readings can vary largely across different periods of operation. Most of the current localization algorithms do not consider the inherent variation of RSS readings across time (calibration drift) as well as across different devices. This has reduced the practical usage of these algorithms. Our previous results show that the Bayesian approaches can gracefully handle a variety of challenging operational scenarios, and we propose to use Bayesian networks to help retrain and recalibrate RSS readings in order to provide robust, reliable, and trustworthy localization using RSS.

As we discussed, spoofing attacks are a serious threat in the network and can facilitate a variety of attacks. We developed K-means clustering detector to detect the spoofing attacks and further to localize the adversary in the network using our GRAIL system. However, some malicious attackers may create multiple illegitimate identities to facilitate spoofing attacks. In order to address this problem, we would like to further detect multiple illegal spoofing identities by using other statistical analysis methods including Akaikes Information Criteria (AIC) and Minimum Description Length (MDL) methods for order estimation, and Mean Shift clustering techniques.

Next, looking foreword in the application level, as wireless networks become increasingly prevalent, they will provide the means to support new classes of location-based services. One type of location-oriented service that can be deployed are those that make use of spatio-temporal location-information to control access to objects or services, instead of restricting access to services based solely on conventional identity-based authenticators. We propose to study using location information to support spatio-temporal access control. The spatio-temporal access control represents a promising paradigm for the development of new location-oriented applications.

Finally, exploring in the system level, through the characterization of the robustness of localization algorithms to attacks, we found that most of the existing localization algorithms are susceptible to attacks. None of the algorithms outperforms the others under attack. Thus one of the important research goals in localization is to build robust attack-resistant localization algorithms that can detect the presence of attacks, reduce or eliminate their negative impacts, provide high-quality localization estimation, and further to build attack-resistant localization systems which are critical for a general purpose localization infrastructure.

References

[1] Aeroscout enterprise visibility solutions. White paper available at http://www.aeroscout.com.

[2] Airtight networks. White paper available at http://www.airtightnetworks.net.

[3] Crossbow Technology Inc. White paper available at http://www.xbow.com.

[4] IEEE 802.11 Standards. http://standards.ieee.org/getieee802/802.11.html.

[5] IEEE 802.15.1 Standards. http://standards.ieee.org/getieee802/download/802.15.1-2003.pdf.

[6] IEEE 802.15.4 Standards. http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf.

[7] Moteiv Corporation. White paper available at http://www.moteiv.com.

[8] Newbury networks. White paper available at http://www.newburynetworks.com.

[9] The BUGS Project. White paper available at http://www.mrc-bsu.cam.ac.uk/bugs/.

[10] W. A. Arbaugh, N. Shankar, Y.C.J. Wan, and Kan Zhang. Your 802.11 network has no clothes. *IEEE Wireless Communications*, 9(6):44–51, December 2002.

[11] T. Aura. Cryptographically generated addresses (cga). *RFC 3972, IETF*, 2005.

[12] P. Bahl and V. N. Padmanabhan. Radar: An in-building rf-based user location and tracking system. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, pages 775–784, March 2000.

[13] R. Battiti, M. Brunato, and A. Delai. Optimal wireless access point placement for location-dependent services. Technical Report DIT-03-052, Department of Information and Communication Technology, University of Trento, Italy, October 2003.

[14] Roberto Battiti, Mauro Brunato, and Alessandro Villani. Statistical Learning Theory for Location Fingerprinting in Wireless LANs. Technical Report DIT-02-086, University of Trento, Informatica e Telecomunicazioni, October 2002.

[15] J. Bellardo and S. Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *Proceedings of the USENIX Security Symposium*, pages 15 – 28, 2003.

[16] M. bohge and W. Trappe. An authentication framework for hierarchical ad hoc sensor networks. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, pages 79–87, 2003.

[17] S. Brands and D. Chaum. Distance-bounding protocols. In *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, pages 344–359, 1994.

[18] S. Capkun and J. P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, pages 1917–1928, 2005.

[19] S. Capkun and J.P. Hubaux. Securing localization with hidden and mobile base stations. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, March 2006.

[20] Y. Chen, J. Francisco, W. Trappe, and R. P. Martin. A practical approach to landmark deployment for indoor localization. In *Proceedings of the Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, September 2006.

[21] Y. Chen and H. Kobayashi. Signal strength based indoor geolocation. In *Proceedings of the IEEE International Conference on Communications (ICC)*, April 2002.

[22] Yinging Chen, Konstantos Kleisouris, Xiaoyan Li, Wade Trappe, and Richard P. Martin. The robustness of localization algorithms to signal strength attacks: a comparative study. In *Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pages 546–563, June 2006.

[23] K.K. Chintalapudi, A. Dhariwal, R. Govindan, and G. Sukhatme. Ad hoc localiztion using ranging and sectoring. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, March 2004.

[24] D. Liu and P. Ning and W. Du. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. In *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS 05)*, pages 609–619, June 2005.

[25] L. Doherty1, K. S. J. Pister, and L. ElGhaoui. Convex position estimation in wireless sensor networks. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, pages 1655–1663, Apr. 2001.

[26] W. Du, L. Fang, and P. Ning. Lad: Localization anomaly detection for wireless sensor networks. In *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS 05)*, April 2005.

[27] E. Elnahrawy, X. Li, and R. P. Martin. The limits of localization using signal strength: A comparative study. In *Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communcations and Networks (SECON 2004)*, pages 406–414, Oct. 2004.

[28] P. Enge and P. Misra. *Global Positioning System: Signals, Measurements and Performance*. Ganga-Jamuna Pr, 2001.

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

[30] F. Ferreri, M. Bernaschi, and L. Valcamonici. Access points vulnerabilities to dos attacks in 802.11 networks. In *Proceedings of the IEEE Wireless Communications and Networking Conference*, 2004.

[31] S. Garg, N. Singh, and T. Tsai. Schemes for enhancing the denial of service tolerance of srtp. In *Proceedings of the International Conference on Security and Privacy for Emerging Areas in Communication Networks*, 2005.

[32] Andre Gunther and Christian Hoene. Measuring round trip times to determine the distance between WLAN nodes. Technical Report TKN-04-16, Technical University Berlin, Telecommunication Networks Group, December 2004.

[33] A. Haeberlen, E. Flannery, A. Ladd, A. Rudys, D. Wallach, and L. Kavraki. Practical robust localization over large scale 802.11 wireless networks. In *Proceedings of the Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, September 2004.

[34] T. Hastie, R. Tibshirani, and J. Friedman. *The Elements of Statistical Learning, Data Mining Inference, and Prediction*. Springer, 2001.

[35] Mike Hazas and Andy Ward. A high performance privacy-oriented location system. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Dallas, TX, March 2003.

[36] Y.C. Hu, A. Perrig, and D. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, pages 1976–1986, 2003.

[37] K. Kaemarungsi and P. Krishnamurthy. Modeling of indoor positioning systems based on location fingerprinting. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, 2004.

[38] E. Kempf, J. Sommerfeld, B. Zill, B. Arkko, and P. Nikander. Secure neighbor discovery (send). *RFC 3971, IETF*, 2005.

[39] A. Khalili and J. Katz. Toward secure key distribution in truly ad-hoc networks. In *Proceedings of IEEE workshop on Security and Assurance in Ad-Hoc Networks*, 2003.

[40] K. Kleisouris and R. P. Martin. Reducing the computational cost of bayesian indoor positioning systems. In *Proceedings of the Third IEEE International Conference on Sensor and Ad hoc Communcations and Networks (SECON 2006)*, September 2006.

[41] A.S. Krishnakumar and P. Krishnan. On the accuracy of signal strength-based location estimation techniques. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, March 2005.

[42] A. LaMarca, Y. Chawathe, S. Consolvo, J. Hightower, I. Smith, J. Scott, T. Sohn, J. Howard, J. Hughes, F. Potter, J. Tabert, P. Powledge, G. Borriello, and B. Schilit. Place lab: Device positioning using radio beacons in the wild. In *Proceedings of Pervasive*, 2005.

[43] S. Lang. *Real and Functional Analysis*. Springer, 1993.

[44] K. Langendoen and N. Reijers. Distributed localization in wireless sensor networks: a quantitative comparison. *Comput. Networks*, 43(4):499–518, 2003.

[45] L. Lazos, R. Poovendran, and S. Capkun. Rope: robust position estimation in wireless sensor networks. In *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, pages 324–331, 2005.

[46] J. Letchner, D. Fox, and A. LaMarca. Large-scale localization from wireless signal strength. In *Proceedings of the National Conference on Artificial Intelligence (AAAI)*, 2005.

[47] Q. Li and W. Trappe. Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks. In *Proceedings of the Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, September 2006.

[48] Xiaoyan Li and R.P. Martin. A simple ray-sector signal strength model for indoor 802.11 networks. In *Proceedings of the Second IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, November 2005.

[49] Z. Li, W. Trappe, Y. Zhang, and B. Nath. Robust statistical methods for securing wireless localization in sensor networks. In *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, pages 91–98, 2005.

[50] Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via lower layer enforcements. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, 2006.

[51] D. Liu, P. Ning, and W. Du. Attack-resistant location estimation in sensor networks. In *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, pages 99–106, 2005.

[52] D. Madigan, E. Elnahrawy, R.P. Martin, W. Ju, P. Krishnan, and A. S. Krishnakumar. Bayesian indoor positioning systems. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, pages 324–331, March 2005.

[53] D. Niculescu and B. Nath. Vor base stations for indoor 802.11 positioning. In *in Proceedings of the Annual ACM International Conference on Mobile Computing and Networking (MOBICOM)*, pages 2926–2931, 2004.

[54] Dragos Niculescu and Badri Nath. Ad hoc positioning system (APS). In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, pages 2926–2931, 2001.

[55] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal. Locating the nodes. *IEEE Signal Processing Magazine*, July 2005.

[56] N. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location-support system. In *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, pages 32–43, Aug 2000.

[57] Q. Li and W. Trappe. Light-weight detection of spoofing attacks in wireless networks. In *Proceedings of the 2nd International Workshop on Wireless and Sensor Network Security (WSNS)*, October 2006.

[58] R. Wilson. Propagation Loss through Common Building Materials, 2.4GHz vs. 5GHz, 2002. White paper available at http://www.magisnetworks.com.

[59] T. Roos, P. Myllymaki, and H.Tirri. A Statistical Modeling Approach to Location Estimation. *IEEE Transactions on Mobile Computing*, 1(1):59–69, Jan-March 2002.

[60] T. Roos, P. Myllymaki, H.Tirri, P. Misikangas, and J. Sievanen. A probabilistic approach to WLAN user location estimation. *International Journal of Wireless Information Networks*, 9(3):155–164, July 2002.

[61] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Proceedings of the ACM workshop on wireless security*, pages 1–10, 2003.

[62] Andreas Savvides, Chih-Chien Han, and Mani Srivastava. Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors. In *in Proceedings of the Seventh Annual ACM International Conference on Mobile Computing and Networking (MobiCom)*, Rome, Italy, July 2001.

[63] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz. Localization from mere connectivity. In *Proceedings of the Fourth ACM International Symposium on Mobile Ad-Hoc Networking and Computing (MobiHoc)*, pages 201–212, Jun 2003.

[64] Roy Want, Andy Hopper, Veronica Falcao, and Jonathon Gibbons. The active badge location system. *ACM Transactions on Information Systems*, 10(1):91–102, January 1992.

[65] S. Weisberg. *Applied Linear Regression*. Wiley Series in Probability and Mathematical Statistics, 2005.

[66] J. Werb and C. Lanzl. Designing a positioning system for finding things and people indoors. *IEEE Spectrum*, pages 71–78, 1998.

[67] A. Wool. Lightweight key management for ieee 802.11 wireless lans with key refresh and host revocation. *ACM/Springer Wireless Networks*, 11(6):677–686, 2005.

[68] B. Wu, J. Wu, E. Fernandez, and S. Magliveras. Secure and efficient key management in mobile ad hoc networks. In *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, 2005.

[69] Moustafa Youssef, Ashok Agrawal, and A. Udaya Shankar. Wlan location determination via clustering and probability distributions. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 143–150, March 2003.

[70] L. Zhou and Z. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, 1999.

[71] S. Zhu, S. Xu, S. Setia, and S. Jajodia. Lhap: A lightweight hop-by-hop authentication protocol for ad-hoc networks. In *Proceedings of the IEEE International Workshop on Mobile and Wireless Network (MWN)*, pages 749–755, 2003.

Vita

Yingying Chen

1991 B.S. in Physics, Nanjing University.

1994 M.S. in Computer Science, North Carolina State University.

2007 Ph. D. in Computer Science, Rutgers University.

1990 - 1991 Research Assistant, National Laboratory of Solid State Microstructures (LSSMS), Nanjing University, Nanjing, P.R. China.

1991 - 1992 Teaching Assistant, Department of Physics, North Carolina State University, Raleigh, NC.

1992 - 1994 Research Assistant, Department of Physics and Department of Computer Science, North Carolina State University, Raleigh, NC.

1994 - 1995 Embedded System Engineer, Alcatel Network Systems, Raleigh, NC.

1995 - 2007 Member of Technical Staff, Lucent Technologies, Holmdel, NJ.

2003 - 2007 Ph.D. studies in Computer Science, Rutgers University, New Brunswick, NJ.

2007 Instructor, Department of Computer Science, Rutgers University, New Brunswick, NJ.

Selected Publications

2005 Yingying Chen, Constantin Serban, Wenxuan Zhang, Naftaly Minsky. Towards a Decentralized and Secure Electronic Marketplace. In Proceedings of IADIS International Conference on E-Commerce, December, 2005.

2006 John-Austin Francisco, Yingying Chen, Eiman Elnahrawy, Konstantinos Kleisouris, Richard P. Martin. Real Time Bayesian Positioning. Research Poster and Demo at the Third International TinyOS Technology Exchange (TTX), February 2006.

2006 Yingying Chen, Konstantinos Kleisouris, Xiaoyan Li, Wade Trappe, Richard P. Martin. The Robustness of Localization Algorithms to Signal Strength Attacks: A Comparative Study. In Proceedings of International Conference on Distributed Computing in Sensor Systems (DCOSS), June 2006.

2006 Yingying Chen, John-Austin Francisco, Wade Trappe, Richard P. Martin. A Practical Approach to Landmark Deployment for Indoor Localization. In Proceedings of the Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), September 2006.

2006 Yingying Chen, Eiman Elnahraway, John-Austin Francisco, Konstantinos Kleisouris, Xiaoyan Li, Hongyi Xue, Richard P. Martin. Demo Abstract: GRAIL: General Realtime Adaptable Indoor Localization. In Proceedings of the 4th ACM Conference on Embedded Networked Sensor Systems (ACM SenSys), November 2006.

2007 Yingying Chen, Wade Trappe, Richard P. Martin. ADLS: Attack Detection for Wireless Localization Using Least Squares. In Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications WiP (PerCom), March 2007.

2007 Yingying Chen, Wade Trappe, Richard P. Martin. Attack Detection in Wireless Localization. In Proceedings of the IEEE Internationl Conference on Computer Communications (INFOCOM), May 2007.

2007 Yingying Chen, Wade Trappe, Richard P. Martin. Detecting and Localizing Wireless Spoofing Attacks. In Proceedings of the Fourth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), June 2007.