ENHANCING RELIABILITY IN DEVICE-FREE LOCALIZATION

by

Manas Maheshwari

A thesis submitted to the faculty of
The University of Utah
in partial fulfillment of the requirements for the degree of

Master of Science

in

Computing

School of Computing

The University of Utah

August 2011

The University of Utah Graduate School

STATEMENT OF THESIS APPROVAL

The thesis of **Manas Maheshwari**

has been approved by the following supervisory committee members:

Sneha Kasera	, Chair	**06-17-2011** Date Approved
Neal Patwari	, Member	**05-13-2011** Date Approved
Robert Ricci	, Member	**05-13-2011** Date Approved

and by **Alan Davis** , Chair of

the Department of **School of Computing**

and by Charles A. Wight, Dean of The Graduate School.

ABSTRACT

Location of an object or person in in-door environments is a vital piece of information. Traditionally, global positioning system-based devices do an excellent job in providing location information but are limited in in-door environments due to lack of an unobstructed line of sight. Wireless environments, with their extreme sensitivity to the positioning of objects inside them, provide excellent opportunities for obtaining location information of subjects. Received signal strength (RSS) based localization methods attract special attention as they can be readily implemented with "off-the-shelf" hardware and software. Device-free localization (DFL) presents a new and promising dimension in RSS-based localization research by providing a non-intrusive method of localization. However, existing RSS-based localization schemes assume a fixed or known transmit power. Any unexpected change in transmit power, not known to the receivers in the wireless network, can introduce errors in location estimate. Previous work has shown that meticulously planned power attacks can result in expected errors, in location of a transmitting sensor, in excess of 18 meters for an area of 75 X 50 m^2. We find that the localization error in DFL can increase by four-fold when under power attack of 15 dB amplitude by multiple adversaries. Certain nonadversarial circumstances can also lead to unexpected changes in transmit power which would result in increased localization error. In this thesis, we focus on detection and isolation of wireless sensor nodes in a network which vary their transmit power to cause unexpected changes in RSS measurements and lead to increased localization errors in DFL. In the detection methods presented in this thesis, we do not require a training phase and hence, our methods are robust for use in dynamic environments where the training data may get obsolete frequently. We present our work with special focus on DFL methods using wireless sensor networks. However, the methods developed are generic and can be easily extended to active localization

methods using both wireless sensor networks (WSN) and IEEE 802.11 protocols. To evaluate the effectiveness of our detection method, we perform extensive experiments in indoor settings using a network of 802.15.4 (Zigbee) compliant wireless sensor nodes and present evaluation results in the form of average detection rate, ROC curves, probability of missed detection and false alarm.

To my parents and my beloved sister

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

It is a great pleasure to thank those who have made this thesis possible with their continued guidance and support. First and foremost, I would like to express my utmost gratitude for my advisor, Professor Sneha Kumar Kasera, for providing me an opportunity to get involved in quality research and accomplish my goals at graduate school with his invaluable guidance. He has been a constant source of motivation and at times shown more faith in my abilities than I had myself. Working with him has been a joy and great learning experience. I am grateful to Professor Neal Patwari for his active involvment and willingness to spend numerous hours discussing my research. Thanks to him, I got introduced to the exciting field of Radio Tomography and was able to make my own small contribution.

I would like to thank Professor Robert Ricci for being on my committee and drawing my attention on several ways to improve my research with his insightful questions and suggestions. I also appreciate Joey Wilson for helping me better understand the fundamentals of Radio Tomography. I feel indebted to Arijit Banerjee and Sai Ananthanarayanan for their time during our discussions and their tremendous help during the experiments.

I would like to thank Shashank Pandey, Manav Seth, Vimal Kasagani, Vishay Vanjani, Ravin Abraham, Prarthana Gowda and Shobhit Gupta for making me feel at home in Salt Lake City. My sincere thanks to Ann Carlstrom and Karen Feinauer for being such wonderful graduate advsiors.

Finally and most importantly, my gratitude goes to my parents, Manjula and Ved Prakash Maheshwari, who have always given utmost importance to my education and valued my well-being above any of their comforts. I cannot imagine any of my success without the sacrifices they have made. My sister, Shobhi Maheshwari, has

always been a source of love and support. For all their support, I dedicate this thesis to my family.

CHAPTER 1

INTRODUCTION

Location of an object or person in in-door environments is a vital piece of information. The capability to know the whereabouts of a subject has wide ranging applications from search and rescue operations, where location information can help in reducing human and monetary losses, to organizing a supermarket where accurate tracking of shoppers can be used for more efficient placement of goods. A large number of location-based applications have been proposed which use the location information to add to a user's experience [1][2][3][4]. Traditionally, global positioning system (GPS) based devices do an excellent job in providing location information but are limited in in-door environments due to lack of an unobstructed line of sight [5]. Several extensions of GPS for indoor applications have also been proposed [6][7][8] but they are still limited in use.

Wireless environments, with their extreme sensitivity to the positioning of subjects inside them, provide excellent opportunities for obtaining location information. Several localization schemes using features of wireless signals like received signal strength (RSS), angle of arrival(AoA), time of arrival (ToA) and time difference of arrival (TDoA), have been proposed which can work with existing IEEE 802.11 wireless local area networks (WLAN) as well as IEEE 802.15 wireless sensor networks (WSNs). Among these schemes, those using RSS measurements attract special attention as they can be readily implemented with "off-the-shelf" hardware and software.

Existing RSS-based localization methods can be divided into two broad categories:

1. *Active localization*: Methods in which the subject being localized actively participates in the localization process by transmitting wireless signals through a sensor attached to it. Such methods use RSS to estimate location of a transmitter by

calculating path lengths in multilateration positioning algorithms [9] or by using a precalculated RSS-to-location map in fingerprint-based localization algorithms [10][11][12][13][14].

2. *Device-free localization (DFL)*: More recent works do not require the subject being monitored to carry any device and thus, the subjects remain passive to the localization process. These DFL methods use changes in RSS measurements on static links to monitor movement of the subject [15][16][17][18][19][20][21][22].

DFL presents a new but promising dimension in RSS-based localization research. Since the subject is not carrying any device, it has the advantage of being nonintrusive. In general, DFL also does not require cooperation from the subject and hence, can be extremely useful in hostile situations where the subject being monitored is not expected to cooperate. Another interesting application of DFL is through-wall monitoring [22] which makes DFL applicable in situations where traditional methods of monitoring like optical and infra-red cameras do not work.

1.1 Problem statement

While the pervasiveness of wireless networks makes DFL using RSS measurements a widely applicable localization method, the untethered nature of wireless networks raises security concerns. WLANs are susceptible to access-point spoofing [23][24][25]. WSNs are often deployed in unmonitored and possibly hostile situations where they are susceptible to node capturing attacks by adversaries [26][27]. With DFL methods being proposed for use in mission critical operations involving emergency responders, police, and military personnel [22], timely and accurate detection of compromised nodes becomes increasingly important.

While the most common attack form in wireless networks is stealing secret keys used for authentication and encryption, DFL methods can also be targets of another, not so common attack technique. The existing DFL methods use a path loss model to model the channel perturbations resulting from movement in the network. In this model, the RSS measurements are given by:

$$P_r = P_t - P_{loss} \tag{1.1}$$

where P_t (P_r) is the transmit (received) power in dBm and P_{loss} is the path loss in dB.

Here, path loss, P_{loss} , is the component which is directly affected by the channel perturbations due to the movements and contains information about the location of the subject. However, RSS measurements P_r are often used as a surrogate for P_{loss} with the assumption that the transmit power stays constant. This assumption may not hold true in adversarial circumstances where a compromised node varies its transmit power to introduce unexpected variations in RSS measurements. These unexpected variations when erroneously attributed to P_{loss} can result in increased errors in localization. Existing works have shown that meticulously planned transmit power changes in active RSS-based localization schemes result in expected errors in excess of 18 meters for an area of 75 X 50 m^2 [28]. Further, it has been observed that mean error for most existing active localization schemes range between 0.5-1.8 ft per dB of transmit power change [29]. In our experiments with DFL, we find that the localization error increases up to four-fold when there is a 15 dB variation in transmit power by multiple adversaries.

Further, certain nonadversarial circumstances can also lead to unexpected changes in transmit power. For example, faults in sensor nodes, due to physical damage and varying transmit power levels due to depleting batteries [30], can manifest as changes in transmit power. Power control algorithms are often used in WSNs in order to preserve battery life and to reduce interference with other nodes [31][32] which, again, may vary the transmit power. Under such circumstances, any change in the transmit power level must be communicated to the receiver nodes in the network. However, uncertainty (due to sensor faults), data corruption (due to packet errors, etc.) or software bugs can result in cases when a node's transmit power changes without the receiver nodes in the network finding out about the change.

The effect of power attack, on both active and device-free localization methods, serves as a strong motivation for us to develop a common yet robust method to detect a power attack and isolate the adversarial nodes in both approaches of localization. In this thesis, we present our main work with special focus on DFL methods using wireless sensor networks. However, the methods developed are generic and can be easily extended to active localization methods using both WSN and IEEE 802.11 protocols.

1.2 Contributions

In this thesis, we focus on detection and isolation of nodes which vary their transmit power to cause unexpected changes in RSS measurements and lead to increased localization errors in DFL. In the rest of this thesis, we denote such transmit power changes by *power attack* irrespective of their adversarial or non-adversarial origins. The amount by which transmit power changes is defined as *power attack amplitude*. Any transmission in which the transmit power changes unexpectedly from the previous transmission by the same transmitter is defined as a *malicious transmission*. A node which is not an adversary is called a *normal node*.

In this thesis, we make the following main contributions:

1. We experimentally determine the increased localization error in DFL under adversarial circumstances.
2. We present two different methods to detect power attacks and identify adversarial nodes.
3. We evaluate the performance of the proposed methods with extensive experimental data.
4. We design a simple, yet robust, protocol to isolate adversarial nodes from the network and add in new nodes as replacements.

In both the detection methods presented in this thesis, we do not require a training phase. This makes our methods robust for use in dynamic environments where training data may get obsolete frequently. The algorithms developed are of low complexity and hence, can be implemented on nodes with few resources. For the

isolation of adversarial nodes, we propose *Enhanced Spin or eSpin*, an enhancement of the Spin scheduling protocol [33]. We provide an algorithm for node removal as well as node addition using the eSpin protocol.

To evaluate the effectiveness of our detection method, we perform extensive experiments in indoor settings using a network of 802.15.4 (Zigbee) compliant wireless sensor nodes. We present evaluation results in the form of average detection rate, ROC curves, probability of missed detection and probability of false alarm under two different experimental environments.

The remainder of this thesis is organized as follows. In Chapter 2, we discuss related work. Chapter 3 presents our adversary model and the notations used in this thesis. In Chapter 4, we present experimental evidence of adversarial affect on DFL by showing the increase in localization error under power attack. In Chapter 5 and Chapter 6, we formulate our detection methods, M1 and M2, and provide evaluation results under two different adversarial environments using extensive experimental data. In Chapter 7, we propose our Enhanced-Spin protocol and discuss the mechanism followed to isolate and replace adversarial nodes. Chapter 8 concludes the thesis and indicates directions for future work.

CHAPTER 2

RELATED WORK

In this section, we present a brief discussion on existing work for detecting power attacks.

Traditionally, crypto-based approaches are used to secure WSN against an adversary whose aim is to extract the secret keys or eavesdrop the communication between sensor nodes. These would, in general, not be suitable for securing against power attacks as discussed below.

- *Key based authentication and encryption methods*: Significant work has involved securing WSNs using traditional key based authentication and encryption protocols [34][35]. These methods, although resource intensive, do provide admission control and some level of security as long as the adversary is assumed not to gain physical control over the sensor nodes. However, if the adversary has physical control over the nodes, it can obtain security keys and passwords and maliciously insert cloned nodes in the network. The adversary can even reprogram a node to make it behave maliciously while still using the original security keys and passwords.
- *Using Device signatures* [36]: Device signatures can be used as alternative to traditional key based encryption methods. These signatures can protect the system from maliciously inserted cloned nodes. However, most device signatures depend on hardware characteristics and would not change with the software installed on the nodes. Hence, this method is not robust against malicious reprogramming.
- *Tamper proof memory* [26]: This provides a method to secure a node from being reprogrammed by an adversary and when combined with security passwords and

keys, can serve to protect a malicious node from affecting the system. However, use of tamper proof memory would result in an increase in the implementation cost of the system.

Power attacks have been previously considered for active RSS-based localization algorithms. [29] provides a survey for power attacks in common active RSS-based localization methods. However, due to the fundamental difference between the active and device-free localization method, none of the existing methods to secure active RSS-based localization can be applied or extended to DFL. Further, most of the works on developing a secure RSS-based localization scheme, like SPINE [37], ROPE [38], SeRLoc [39] and HirLoc [40], assume the availability of some reference points, special nodes with known locations or key-based secure communication between anchor nodes to prevent against a variety of attacks in WSNs. These methods are thus vulnerable to capture of critical nodes by the adversary.

There has been considerably less work towards providing a method for detection of power attacks which could be applied to existing localization schemes. Chen *et al.* [41] proposed a generic method which works for two broad ranges of active localization methods: multilateration-based and RSS-based. However, their method is also not applicable to DFL.

CHAPTER 3

ADVERSARY MODEL AND NOTATIONS

3.1 Adversary model and assumptions

We assume that the adversarial nodes are never present in majority in the network and all nodes have equal probability of developing fault or being targeted by an adversary. We allow multiple adversaries to be active at the same time but they do not collude with each other to carry out a coordinated power attack. We make the assumption that even though an adversary can vary its transmit power to create localization errors, it does not report report false readings of RSS values it receives from other transmitters. This would be considered in future works.

We assume a network of N transceivers nodes. Hereafter, a transceiver is referred to as a transmitter when it is transmitting and as a receiver when it is receiving. A fully connected network is not required for our detection method. A transmitter's neighborhood is defined as the set of receivers capable of receiving wireless signals from it. In a network where a transmitter's neighborhood can change with time, we assume availability of a suitable protocol which can disseminate the neighborhood information quickly. In our analysis, we assume such information is disseminated instantly and the current neighborhood information is always available at the nodes.

Since faulty nodes are just a weaker form of the adversary being considered, all further discussions apply to both adversarial and faulty nodes.

3.2 Notations

Table 3.1 lists the symbols used frequently in this thesis. We discuss a few of them in detail here and the rest are defined as needed.

We define the set of RSS measurements being analyzed for the presence of a power attack as the *detection window*. During a power attack, an adversary can affect a

Table 3.1. List of frequently used symbols

Symbol	Meaning
N	Number of nodes in the network
$\mathcal{H}_k$	Neighborhood of transmitter k
$r_{k,j}(i)$	RSS measurement at receiver j from transmitter k at time i
$L_{k,j}$	Link between transmitter k and receiver j, $j \in \mathcal{H}_k$
$a_k, \hat{a}_k$	Power attack amplitude and its estimate
n	Power attack interval
$M1, M2$	Method 1 and Method 2 for detecting power attacks
T	Vector transpose
$S_k(i), Q_k(i)$	Detection windows for M1 and M2 ending at time i
p	Size of detection window
$\mathcal{L}$	Line with slope 1 and passing through origin
γ	Distance threshold
$\gamma_h(i)$	Heuristically chosen distance threshold for window $Q_k(i)$
P_D, P_{MD}, P_{FA}	Probability of detection, missed detection and false alarm
w_{min}	Minimum power attack window size
a_{min}	Minimum power attack amplitude

RSS-based localization system by changing the transmit power of a node. We define the following parameters related to this change in RSS:

- *Power attack interval* (n): It is defined as the time interval between two periodic power changes by the adversary. For an ideal detector, probability of detection would be 1 for a detection window size p greater than and equal to n.
- *Minimum power attack window size* (w_{min}): Power changes by an adversary may not always be periodic. For such cases, we define w_{min} as the smallest set of contiguous transmissions which would always contain at least one malicious power change. In real scenarios, w_{min} is not expected to be known beforehand; however, an educated guess of w_{min} can be made based on the expected movement activity and noise in WSNs. For $p \geq w_{min}$, we expect our detection methods to achieve nearly 100 % detection rate. In this thesis, we only evaluate our methods for a periodic n. Experimental evaluation for nonperiodic power variations is to be considered in future research.
- *Minimum attack amplitude* (a_{min}): It is defined as the minimum power change

that is required to perform a power attack with significant changes in the estimated location. Power attacks with an amplitude less than a_{min} are not considered significantly harmful to the application and thus are not important to detect. We use a_{min} in the formulation of M2. The value of a_{min} is determined by the application and the environment.

CHAPTER 4

LOCALIZATION ERROR IN DFL

In this chapter, we demonstrate the affect of power attack by adversaries on localization error in DFL. We perform experiments using variance-based radio tomographic imaging (VRTI) [22] which performs device-free localization by measuring link variance. We show that an adversary can introduce significant errors in VRTI by varying its transmit power and thus creating artificial variance on the links. Through our experiments, we also determine the dependence of localization error on the number of adversaries and on the power attack amplitude.

We first present a little background on the VRTI method used for our experiments. We then explain our experimental setup and finally present our findings.

4.1 VRTI background

VRTI uses RSS variance caused on static links in a WSN due to motion in the network area. The entire network area is divided into N equal voxels and the estimated image vector $\mathbf{x}$ describes the presence of motion in the network area. Each element of image vector $\mathbf{x}$ is given by:

$$x_i = \begin{cases} 1, & \text{if there is motion in voxel } i \\ 0, & \text{otherwise} \end{cases} \tag{4.1}$$

The image vector $\mathbf{x}$ is estimated using the RSS variance vector $\mathbf{s}$ which contains a measure of the RSS variance on each of the M links in the network. The variance vector $\mathbf{s}$ and the image vector $\mathbf{x}$ have a linear relationship which can be expressed as:

$$\mathbf{s} = \mathbf{W}\mathbf{x} + \mathbf{n} \tag{4.2}$$

where $\mathbf{W}$ is an MXN matrix representing the variance weighting for each pixel, and $\mathbf{n}$ is an M X 1 noise vector. $\mathbf{W}$ is the elliptical weighing model given by:

$$[W]_{l,j} = \frac{1}{\sqrt{d_l}} \begin{cases} \psi, & \text{if } d_{lj}(1) + d_{lj}(2) < d_l + \lambda \\ 0, & \text{otherwise} \end{cases} \tag{4.3}$$

where d_l is the distance between two nodes on a link, $d_{lj}(1)$ and $d_{lj}(2)$ are the distances from the center of the voxel j to the respective node locations on the link, λ and ψ are two tunable parameters. For estimating the position vector **x,** Tikhonov regularization is used. The inversion formula can be written as:

$$\hat{\mathbf{x}} = (\mathbf{W}^T\mathbf{W} + \alpha\mathbf{Q}^T\mathbf{Q})^{-1}\mathbf{s} \tag{4.4}$$

where $\mathbf{Q}$ is the Tikhonov matrix, and α is the regularization parameter.

4.2 Experimental setup

In this section, we provide detailed description of the experimental environment and the experiments performed to obtain the localization error. The same experimental setup is again used for experiments performed later in Chapter 5 and 6.

4.2.1 Environment

We perform our experiments in a typical classroom with a testbed of 20 wireless sensors deployed at equal distances from one another in a network area of 6 X 6 m^2. We refer to this as the *In-room* environment. An In-room environment setup with (o) representing the deployed node's locations is shown in Figure 4.1. The room has a number of static objects like chairs and tables present near the deployment area which would result in lots of multipaths for the wireless signals, providing a perfect indoor environment. TelosB wireless sensors nodes are used for all the experiments. The nodes operate in the 2.4 GHz frequency band. Spin [33] is used as the data collection protocol for normal nodes. For adversarial nodes, we modify the standard Spin protocol as per the requirements of the experiment. For completeness, we describe the normal Spin protocol briefly here. Spin is a round-robin token-passing protocol used to schedule transmission of nodes in a manner which prevents packet collisions while still maintaining high data collection rate. When one node transmits, all other nodes receive the packet and make the RSS measurements. These RSS measurements

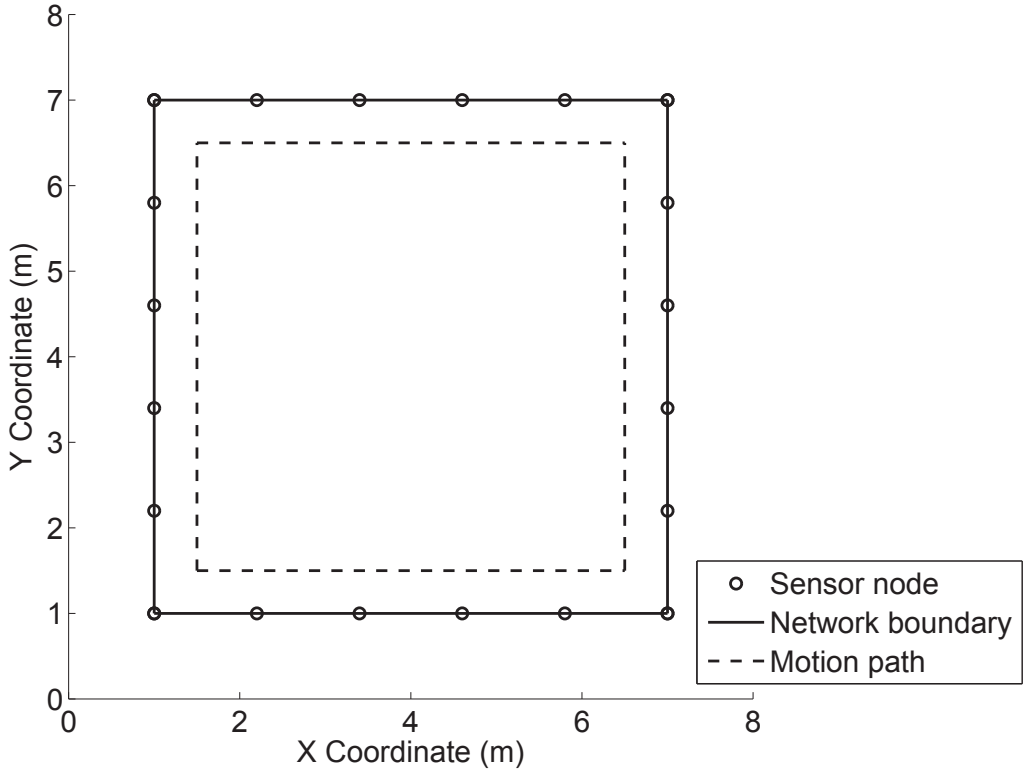


Figure 4.1. Set up for In-room environment setup

are transmitted to a base station along with the node's unique ID. The base station collects all RSS measurements and forwards the data to a laptop for storage and later processing. We define a *Spin cycle* as one round of the token passing scheduling protocol Spin. Each spin cycle consists of RSS data with at most one transmission from every sensor node.

4.2.2 Experiment description

We perform two experiments in the In-room environment.

1. No-attack: This experiment is a standard VRTI localization experiment. During this experiment, all nodes are normal (nonadversarial). Spin is used as the data collection protocol. A subject walks on a known path with constant speed shown by a dotted line in Figure 4.1. A metronome is used to ensure that the subject maintains the constant speed. Data are collected for a period of 4 minutes.
2. Attack: This experiment is used to create a power attack scenario. During

this experiment, some nodes are made adversarial by programming them with a modified version Spin protocol in which the transmit power is changed by a_k with an attack interval n of 32. The complete experiment is conducted in 8 different phases. We start with one adversarial node in phase 1. After completion of a phase, the number of adversaries is increased by one. Nodes are picked randomly, from the normal nodes, to be programmed as adversarial node. Ids of nodes made adversarial are in the order 5, 11, 17, 3, 8, 13, 1 and 14. Each phase further consist of two rounds of 4 minute each. For each phase, round 1 involves adversarial nodes changing their transmit power by 7 dB and round 2 involves the same action with a change of 15 dB in transmit power.

4.2.3 Calculating localization error

We use the data collected from the No-attack experiment to obtain baseline error in localization in DFL. The Attack experiment is performed to measure the increase in localization error with increasing power attack amplitude and increasing number of adversaries.

We calculate localization error using a set of N_r reference points on the known path walked by the subject. The reference points are labeled as (x_i, y_i), $i \in \{0, ..., N_r - 1\}$ and are placed such that the subject walks moves from one reference point to the next in one time unit, starting at (x_0, y_0). At time i, we calculate the closest reference point (x_i, y_i) to the actual position of the subject. Let the reference point closest to the estimated position using VRTI at time i be (x'_i, y'_i). Then, the error in localization is calculated as:

$$\text{RMS localization error} = \sqrt{\frac{\sum_{i}^{N_r}\{(x_i - x'_i)^2 + (y_i - y'_i)^2\}}{N_r}} \tag{4.5}$$

4.3 Results

Figure 4.2 plots the root mean squared (RMS) error between the estimated and actual position for the attack experiments in the *In-room* environment.

From Figure 4.2, we make the following observations:

- Localization error increases rapidly with the increase in the number of adversary nodes. RMS localization error of VRTI when there is no adversary present is about 0.65m. For power attack amplitude of 7 dB, the RMS error increases by almost 100% in presence of a single adversarial node. When number of adversaries increases to 8, a 7 dB power attack results in a 2.5 fold increase in the RMS error of localization in VRTI.
- Localization error is lower for power attacks of small amplitude (7dB) than power attacks of larger amplitude (15 dB). In presence of 8 adversarial nodes, the RMS error of VRTI is almost 4.5 times that of the baseline (no adversary present in network) for a power attack of 15 dB.

4.4 Conclusion

In this chapter, we experimentally demonstrate the affect of adversarial nodes in DFL using VRTI. We show unexpected transmit power variations can result in increased localization error. The localization error increases with an increase in power attack amplitude and the number of adversaries.

In the next two chapters, we present methods which can be used to detect and identify adversarial nodes in DFL.

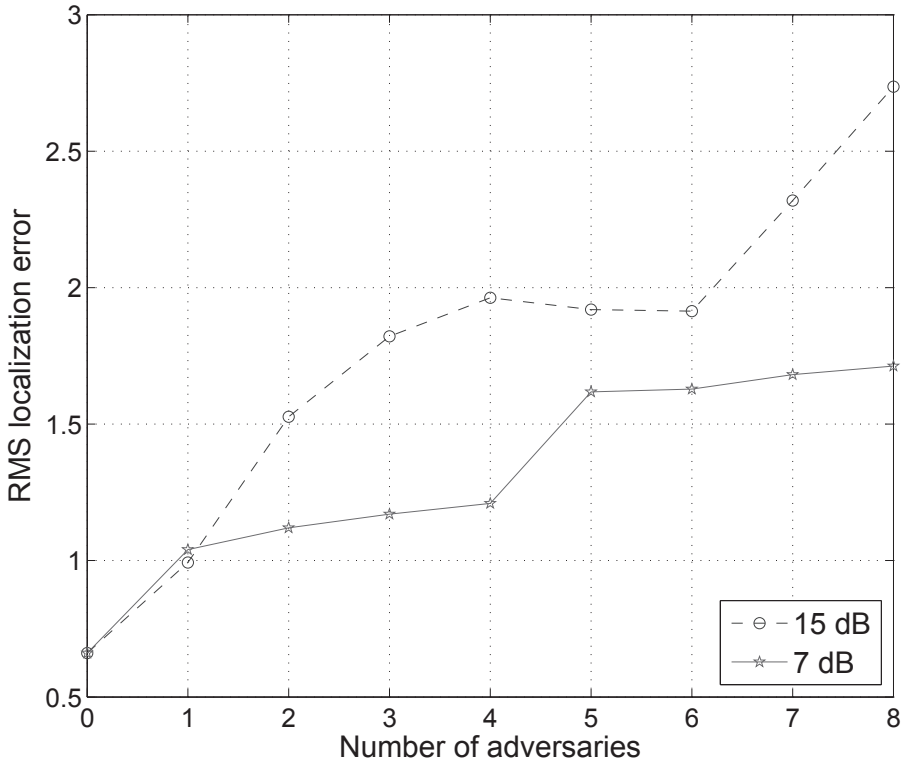


Figure 4.2. RMS error for 7dB and 15 dB with number of adversaries.

CHAPTER 5

DETECTION USING TEMPORAL CORRELATION IN RSS MEASUREMENTS

The last chapter discussed the affect of adversarial nodes on localization error in DFL. In this chapter, we will discuss our first method, hereafter referred to as M1, to detect the presence of adversarial nodes which takes advantage of the temporal correlation in RSS variations. We first present here a basic intuition into the method and then formalize this intuition in Section 5.2.

When there is no movement in the network area, the changes in RSS measurement on a wireless link are determined by the wireless channel noise. For most cases, these changes can be approximated as Gaussian. As the changes are random, no two links show a significant temporal correlation in the RSS measurements on them.

In addition to noise, the RSS measurements on multiple links can change simultaneously in two cases: 1) a movement in the network or 2) a power attack by an adversary. This simultaneous change results in a temporal correlation either positive or negative. However, the two cases are not similar in terms of the number of link pairs which show this effect. When there is some channel perturbation due to a movement, the RSS measurements on the links change; increasing or decreasing depending on the fade-level of the links [42]. However, a subject's movement only perturbs the wireless channel for links passing through a region of finite volume around him. This finite region is much smaller than the total volume of the room and hence, the affected links are only a small fraction of the total links present in the network. Thus, the temporal correlation observed due to the movement will only be limited to pairs in that small fraction of total links.

On the other hand, when an adversarial node k changes its transmit power, it results in a change in RSS measurements on all the links $L_{k,j}$ s.t. $j \in \mathcal{H}_k$. Since the change affects every link originating from k simultaneously, a high temporal correlation in the RSS measurements is observed among all link pairs with k as the transmitter.

By using the fraction, of all link pairs in $\mathcal{H}_k$, which show a high temporal correlation, we can determine whether the observed variations in RSS are due to normal movement or due to a power attack; a lower fraction indicating a normal movement whereas a higher fraction indicating a power attack.

In Section 5.1, we present a brief theory on Pearson product-moment correlation coefficient. We present our method M1 in Section 5.2, our experiments and evaluation results in Section 5.3, and finally the conclusion in Section 5.4.

5.1 Pearson product-moment correlation coefficient

We use Pearson product-moment correlation coefficient to determine the temporal correlation between RSS measurements on a pair of links.

Pearson correlation coefficient of two random variables X and Y is defined as the covariance of two variables divided by the product of their variances. Its value ranges from -1 to 1 and it is not defined when the variance of either X or Y is zero.

$$\rho_{X,Y} = \frac{Cov(X,Y)}{\sigma_X \sigma_Y} = \frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sqrt{E(X^2)-(E(X))^2}\sqrt{E(Y^2)-(E(Y))^2}} \tag{5.1}$$

where $E(X)$ is the expected value of X.

The interpretation used for the Pearson correlation coefficient is shown in Table 5.1.

5.2 Model

In this section, we formulate our model for detecting power attack using the temporal correlation between the RSS measurements. The method discussed could be used independently for each adversary in the network where multiple adversaries are present. We consider deciding between the following two hypotheses:

Table 5.1. Correlation coefficient interpretation

0-0.09	None
0.1-0.29	Small
0.3-0.49	Medium
>0.5	High

- H_0: No power attack from transmitter k is present at time i.
- H_1: A power attack from transmitter k is present at time i.

We define the neighborhood of k by $\mathcal{H}_k = \{n_0, n_1, ...n_{M-1}\}$ consisting of $M \subset N$ receivers capable of communicating with k. RSS measurements are made on every link in the network and $r_{k,j}(i)$ is defined as the RSS measurement at receiver j from transmitter k at time i.

To determine the temporal correlation between RSS measurements, we define a detection window $\mathbf{S}_{k,j}(i)$ consisting of RSS measurements at receiver j from transmitter k during previous p time units, ending at time i as:

$$\mathbf{S}_{k,j}(i) = [r_{k,j}(i-p+1),\ r_{k,j}(i-p+2),\ \ldots\ ,\ r_{k,j}(i)]^{\mathsf{T}} \tag{5.2}$$

where $k \in \{1, ..., N\}$ and $j \in \mathcal{H}_k$.

Next we calculate the temporal correlation between vectors $\mathbf{S}_{k,a}$ and $\mathbf{S}_{k,b}$, for receivers a and b respectively, given by $\rho_{\mathbf{s}_{k,a}\mathbf{s}_{k,b}}$ using Equation (5.1).

Then, we define a indicator random variable as:

$$I_{k,a,b} = \begin{cases} 1, & \rho_{\mathbf{s}_{k,a}\mathbf{s}_{k,b}} > 0.5 \\ 0, & \rho_{\mathbf{s}_{k,a}\mathbf{s}_{k,b}} < 0.5 \end{cases} \tag{5.3}$$

A value of 1 for $I_{k,a,b}$ indicates a high temporal correlation between $\mathbf{S}_{k,a}$ and $\mathbf{S}_{k,b}$ and a value of 0 indicates otherwise.

Then, we determine the fraction f_k of total link pairs originating from k which have a value of 1 for $I_{k,a,b}$ using:

$$f_k = \frac{1}{C_k} \sum_{\substack{a,b \in \mathcal{H}_k \\ a \neq b}} I_{k,a,b} \tag{5.4}$$

where $C_k = \binom{|\mathcal{H}_k|}{2}$, the total number of link pairs originating from k.

Now, we can choose between the two hypotheses using:

$$f_k \underset{H_0}{\overset{H_1}{\gtrless}} \theta \tag{5.5}$$

Here, θ is a suitable threshold.

5.3 Evaluation

In this section, we evaluate the method M1 developed in the previous section. First, we give a brief description of the experiments performed and then present the results obtained. We set the value of θ to 0.75 and p to 100 in our experiments.

In our model, we have assumed that the neighbor set $\mathcal{H}_k$ of each transceiver is always known. In practical deployments, a node's transmission range can vary due to changes in the environment resulting in a change in $\mathcal{H}_k$. Ensuring instant availability of neighborhood information is not trivial and may require a lot of network communication to pass the changing neighborhood information. Hence, to keep our experiments simple and reliable, we use a fully connected network. This is a special case for the network considered in the previous section with $|\mathcal{H}_k| = N, \forall\ k$.

5.3.1 Experimental environments

We use the data set from two different environments for our evaluation:

1. *Simulated attack environment*: In this approach, we use a publicly available RTI data set [43] collected in an outdoor experiment. The original experiment of this data set consisted of 28 *TelosB* nodes deployed in a square layout of area 21 X 21 feet. The data collection protocol used was Spin [33], which is explained in Section 4.2.1. The data set is in the form of rows of RSS measurements, each row consisting of readings made by a receiver node during a spin cycle. The rows are ordered by the receiver ID and time of measurement. We use the file

empty.csv from the data set. During this experiment, there was no movement in the deployment area.

We simulate power attacks from two nodes, 12 and 23. To simulate power attack, we subtract a constant value, a_k, from RSS measurements measured by every receiver corresponding to transmissions from nodes 12 and 23. This is done once for every n transmission from 12 and 23 where n is the power attack interval.

2. *In-room* environment: This environment is explained in detail in Section 4.2.1. We perform two experiments, No-attack and Attack, for our evaluation. The primary objective of these experiments is to analyze the performance of M1 with variations in the power attack amplitude in an experimental environment. Spin is used as the data collection protocol.

   The No-attack experiment is described in Section 4.2.2. In the Attack experiment, a single transmitter is chosen randomly to act as an adversary and programmed with a modified Spin code which reduces the transmit power by a_k. We consider five values for a_k – 6, 9, 12, 15 and 18 dB. We use a fixed attack interval of 16. By collecting data from a large set of experimental data, we evaluate the probability of missed detection P_{MD} and probability of false alarm P_{FA} defined as:

   - P_{MD}: Failure to detect a power attack by an adversarial node in the network.
   - P_{FA}: A detection event for any of the normal nodes in the network.

5.3.2 Detection results

In this section, we present the results obtained with M1 in the simulated power attack and In-room experimental environment.

5.3.2.1 With simulated data

In this set of experiments, we simulate the attack by subtracting a_k from RSS for transmitter k at all receivers in the network. We also control the interval of attack n

by making one change every n spin cycles. Using the attack interval and total spin cycles present in the data set, we can calculate actual number of power changes as

$$\text{Total power changes, } S_{mal} = \frac{\text{total spin cycles}}{n} * 2 \tag{5.6}$$

We use S_{mal} to calculate the detection rate as

$$\text{Detection rate} = \frac{\text{number of detections}}{S_{mal}} * 100 \tag{5.7}$$

Since the detection of an adversarial node in M1 is independent of other adversarial nodes present in the network, we present our results by averaging over all the adversaries. The detection results can be applied independently for each adversary where multiple adversaries are present.

Table 5.2 gives the variations in detection count for malicious nodes as the attack interval is changed for constant $a_k = 18$ dB . Figure 5.1 plots the variation in average detection rate for $a_k = 3$ dB and 18 dB.

From Figure 5.1 we can conclude that M1 can detect adversarial nodes with nearly 90 % success rate for attack intervals less than 4. However, as the attack interval increases, i.e., as the adversary becomes less active, the number of successful detections decreases.

Table 5.3 and Figure 5.2 show the M1's performance with varying power attack amplitude for known attack intervals n.

Table 5.2. Number of detections with $a_k = 18$ dB for simulated data.

n	S_{mal}	# detections for node 12	# detections for node 23
2	138	130	123
4	69	61	58
8	34	18	20
16	17	8	6
32	8	4	3

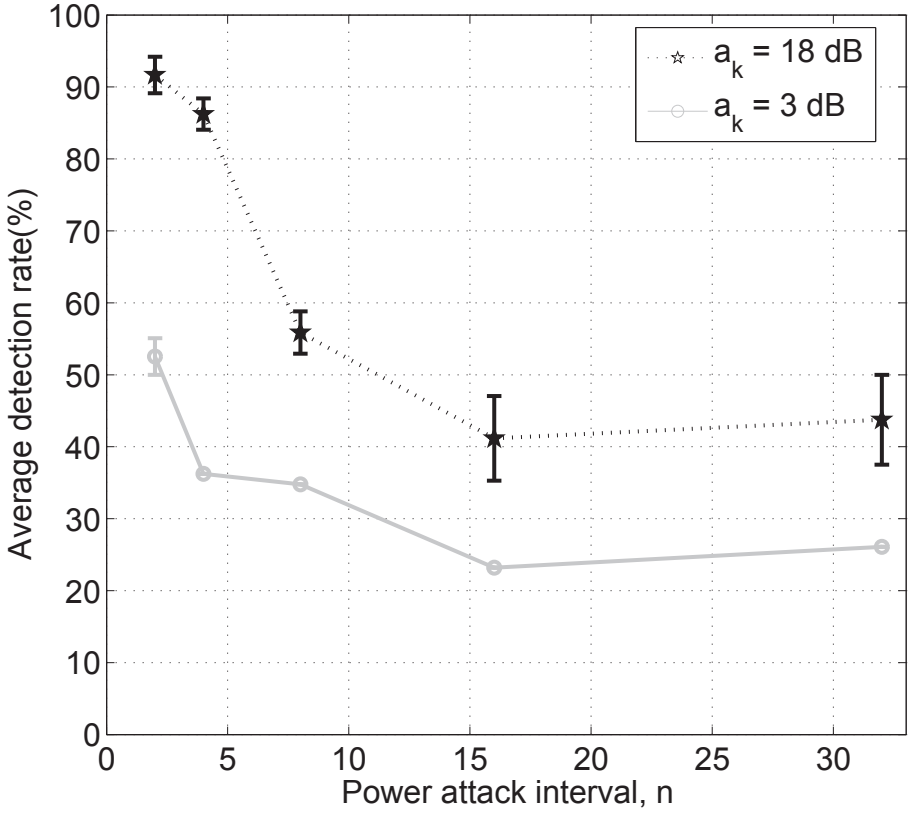


Figure 5.1. Variation in average detection rate with n for simulated data.

The results in Table 5.3 and Figure 5.2 show that with increasing values of a_k, we get better detection performance with M1. The performance reaches its peak at $a_k = 18$ dB and does not improve further with an increase in power attack amplitude.

We obtain zero false alarms for all the simulation results presented in this section.

5.3.2.2 With experimental data

Using simulation data, we showed that M1 can be used to detect adversarial nodes with acceptable detection rate, especially for small attack intervals. To test our method in a more realistic environment, we conduct experiments in a classroom as described in Section 5.3.1. For this experiment, n was set to 16.

Figure 5.3 plots P_{MD} and P_{FA} for the experimental data. We observe a similar trend with experimental data as observed with the simulation data. Detection rate of M1 increases (P_{MD} decreases) with increasing value of a_k. The best performance

Table 5.3. Number of detections with $n = 16$ for simulated data.

a_k	# detections for node 12	# detections for node 23
3	4	4
5	5	5
7	5	5
10	5	5
12	6	6
15	8	6
18	8	6

with M1 is obtained for power attack amplitude of 18 dB, which is a detection rate of 0.48 which is close to and slightly better than the results obtained with simulation data (a detection rate of 0.4).

5.4 Conclusion

In this chapter, we presented the first of our two methods to detect adversarial nodes in WSN. We provided a mathematical formulation for our method M1 which uses Pearson product-moment correlation to determine temporal correlation in RSS measurements observed on link pairs in the neighborhood of a transmitter. We evaluate our method using simulated power attack scenarios as well as experimental data. Our results show that M1 can detect adversarial nodes with acceptable detection rate, especially for smaller attack intervals, achieving more than 80 % detection rate for $n = 2$ and $a_k = 18$.

However, we observe that for larger attack intervals, the performance of M1 is mediocre. For $n = 16$, M1 achieves 40 % percent success rate in simulations and 48 % percent in experiments. On the other hand, in Section 4.3, we show that an adversary changing its transmit power with an interval of $n = 32$ can introduce significant localization error in DFL. The localization error doubles for a power attack amplitude of 7 dB and is four times in the worst case with multiple adversaries. Hence, M1 will not provide robust detection for many applications when the power attack

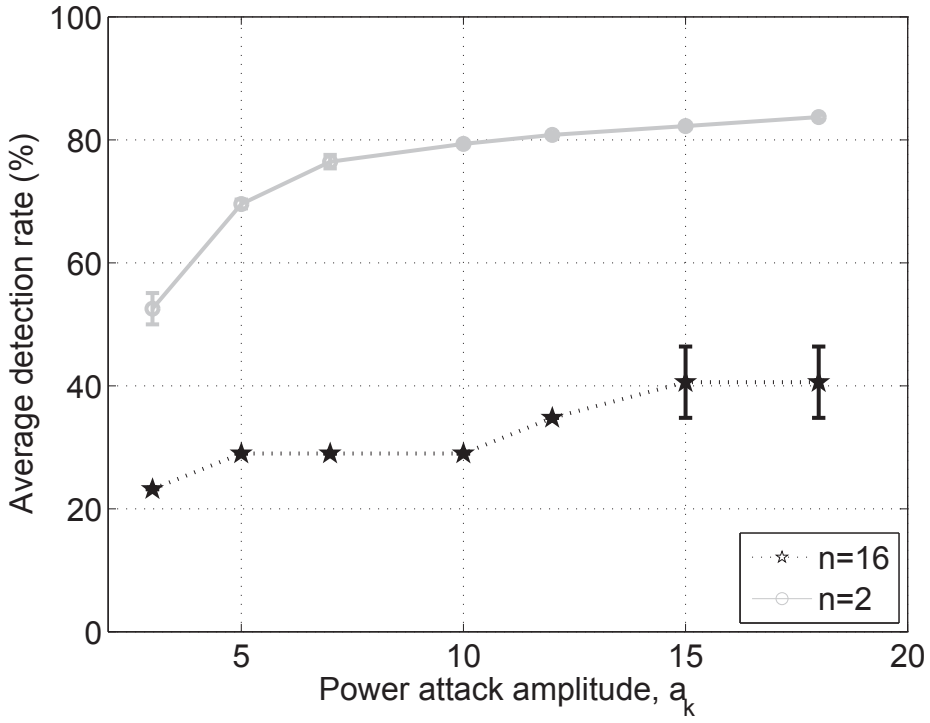


Figure 5.2. Variations in average detection rate with a_k for simulated data.

interval is large. M1 would also not perform well in scenarios where a single adversary is not very active but multiple adversaries acting simultaneously can create significant performance degradation in DFL.

In the next chapter, we present our second method which shows a substantial performance gain over M1. Our next method is able to detect less active adversaries with high success rate.

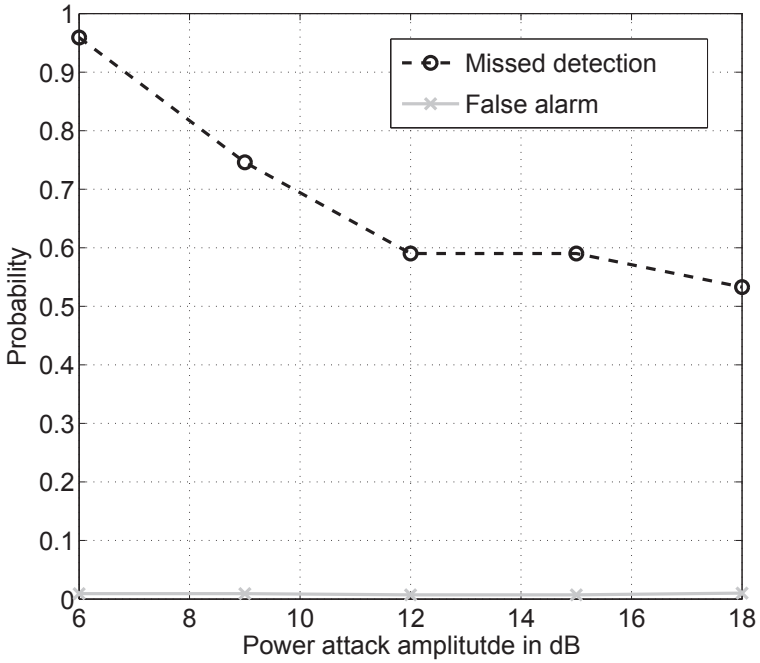


Figure 5.3. P_{MD} and P_{FA} with power attack amplitude for $n = 16$.

CHAPTER 6

DETECTION USING DISTANCES IN RSS VECTOR SPACE

In this chapter, we present our second approach to detect power attacks in WSN. The method is based upon the same basic intuition discussed in Chapter 5. We refer to this method as M2. In M2, we use the changes in RSS measurement instead of the RSS measurement itself. The RSS changes are calculated for each receiver in the neighborhood $\mathcal{H}_k$ of transmitter k and plotted in a multidimensional space where each dimension corresponds to a receiver belonging to $\mathcal{H}_k$. We then use these RSS changes to formulate a statistical hypotheses test which acts as the basis of detection.

In this method, we incorporate the factor a_{min} in our model to ignore attacks with amplitude less than a_{min}. This reduces the number of false alarms and makes the detection process more robust. We also discuss a heuristic-based method to choose the threshold parameter γ used in the hypotheses test for detection.

The evaluation for M2 consists of extensive experiments conducted in a classroom environment. We first present results to demonstrate an example detection with M2. Then, ROC curves are presented which can be used to determine an appropriate operating threshold for the detector, based on the constraints on false alarms and missed detections. We then present results for evaluation of our heuristic-based operating threshold. With the threshold fixed heuristically, we vary size of the detection window to tune the performance of the detector and provide a trade-off analysis between performance accuracy and latency of detection process. Finally, we evaluate our detection method for through-wall localization applications which is a distinguishing feature of DFL.

6.1 Hypotheses formulation

Let $\mathbf{r}_k(i)$ be the RSS vector defined as:

$$\mathbf{r}_k(i) = [r_{k,n_0}(i), ..., r_{k,n_{M-1}}(i)]^\mathsf{T} \tag{6.1}$$

where $r_{k,j}(i), j \in \mathcal{H}_k$, denote the RSS measurement at receiver j from transmitter k at time i and mean RSS vector over a window of time T as:

$$\bar{\mathbf{r}}_k(i) = \frac{1}{T}\sum_{t=1}^{T} \mathbf{r}_k(i-t) \tag{6.2}$$

Using (6.1) and (6.2), we can define the change in RSS for a transmission of node k at time i as

$$\Delta\mathbf{r}_k(i) = \mathbf{r}_k(i) - \bar{\mathbf{r}}_k(i) \tag{6.3}$$

Next, we consider two cases for $\Delta\mathbf{r}_k(i)$:

1. *No attack*: When a power attack is not present, changes in RSS can be caused by many reasons. However, these changes are equally likely to increase or decrease the RSS measurement. For example, noise and quantization error are likely to be zero mean. Movement of people and objects in the environment will similarly tend to increase RSS on some links and decrease RSS on others [42]. Thus for generality, we model $\Delta\mathbf{r}_k(i)$ as

   $$\Delta\mathbf{r}_k(i) = \boldsymbol{\epsilon} \tag{6.4}$$

   where $\boldsymbol{\epsilon}$ is a vector of zero mean random variables. We do not make any assumptions about the distribution or the correlation between elements of $\boldsymbol{\epsilon}$.
2. Attack: When there is a power attack from k, $\Delta\mathbf{r}_k(i)$ can no longer be modeled as a vector of zero mean random variables. For this case, we model $\Delta\mathbf{r}_k(i)$ as

   $$\Delta\mathbf{r}_k(i) = a_k\mathbf{1} + \boldsymbol{\epsilon} \tag{6.5}$$

   where a_k is the transmit power variation by k and $\mathbf{1} = [1, ..., 1]^\mathsf{T}$.

Corresponding to the two cases above, we formulate the two hypotheses:

- H_0: No power attack from transmitter k is present.
- H_1: A power attack from transmitter k is present.

6.1.1 Estimating a_k

The main difficulty of the detection problem considered is that, under H_1, we do not know the amplitude, a_k, of the power attack *a priori*. In order to judge the likelihood that H_1 is occurring, we first need to estimate a_k.

Since we are estimating a_k given H_1, we know that the amplitude of our estimate must be greater than a_{min}, which is the minimum attack amplitude parameter.

We first define $\bar{a}$ as

$$\bar{a} = \frac{1}{M} \sum_{j=0}^{M-1} \Delta \mathbf{r}_{k,n_j}(i) \tag{6.6}$$

where M is the size of $\mathcal{H}_k$ and $\Delta \mathbf{r}_{k,n_j}(i)$ represents the j^{th} element of $\Delta \mathbf{r}_k(i)$.

Then, we define $\hat{a}_k$ to be an estimate of the attack amplitude as

$$\hat{a}_k = \begin{cases} \max\ (\ \bar{a},\ +a_{min}\ ), & \bar{a} > 0 \\ \min\ (\ \bar{a},\ \text{-}a_{min}\ ), & \bar{a} \leq 0 \end{cases} \tag{6.7}$$

6.1.2 Detecting power attack

Next, we consider the problem of detecting a power attack. We define a *detection window*, $\mathbf{Q}_k(i)$, of p transmissions for transmitter k ending at time i as

$$\mathbf{Q}_k(i) = [\Delta \mathbf{r}_k(i-p+1),\ \Delta \mathbf{r}_k(i-p+2),\ ...,\ \Delta \mathbf{r}_k(i)\ ]^{\mathsf{T}} \tag{6.8}$$

Also define a line in space $\mathbb{R}^{|\mathcal{H}_k|}$, with slope 1, as:

$$\mathcal{L}:\ \Delta \mathbf{r}_{k,n_0} = \Delta \mathbf{r}_{k,n_1} = \cdots\ = \Delta \mathbf{r}_{k,n_{M-1}} = \hat{a}_k \tag{6.9}$$

Next, we define the distance of $\Delta \mathbf{r}_k(i)$ from $\mathcal{L}$ using the estimated parameter $\hat{a}_k$ as

$$d_k(i) = ||\Delta \mathbf{r}_k(i) - \hat{a}_k \mathbf{1}|| \tag{6.10}$$

Finally, to choose between H_0 and H_1 for the detection window $\mathbf{Q}_k(i)$, we use the distances $d_k(i-j)$, $\forall\ j \in [0,p)$ as

$$\min_{j\in[0,p)} \left(d_k(i-j)\right) \underset{H_1}{\overset{H_0}{\gtrless}} \gamma \tag{6.11}$$

where γ is an appropriately chosen distance threshold. Like (5.5), (6.11) is independent of the number of adversaries in the network. (6.11) can be applied independently to each node to test for multiple adversaries.

If there is a power attack at time j such that $\Delta\mathbf{r}_k(j) \in \mathbf{Q}_k(i)$, we can model $\Delta\mathbf{r}_k(j)$ as (6.5). This lies in a region of constant diameter around $\mathcal{L}$ and hence, $d_k(j)$ is smaller than the threshold value γ. Thus, we choose H_1 for $\mathbf{Q}_k(i)$.

When there is no attack, $\Delta\mathbf{r}_k(j)$ can lie randomly at any point in space. In this case, $\min(d_k(i-j))$, $j \in [0,p)$, has a low probability of lying in a region of constant radius around $\mathcal{L}$. This probability is further decreased as the number of receivers and thus the number of dimensions increase, the region of constant diameter around $\mathcal{L}$ occupies an increasingly smaller percentage of total volume in space. Effectively, $\min(d_k(i-j))$, $j \in [0,p)$ is greater than γ when there is no attack and hence, we choose H_0 for $\mathbf{Q}_k(i)$.

Further, the definition of $\hat{a}_k$ ensures that the distance $d_k(i)$ is not close to zero for power variations less than a_{min}. This reduces the probability of choosing H_1 for a normal node due to noise (a false alarm) or an adversarial node with power attack amplitude less than a_{min} (not significant).

Figure 6.1 illustrates attack detection in $\mathbb{R}^3$ where $\mathcal{H}_k = \{n_0, n_1, n_2\}$. The cylinder around $\mathcal{L}$ is the detection region. The cube around the origin is excluded out of the attack detection region.

6.2 A heuristic-based method to choose γ

To successfully detect a power attack, we need to set the threshold appropriately. Since the value of γ can change with the experimental environment , we provide a

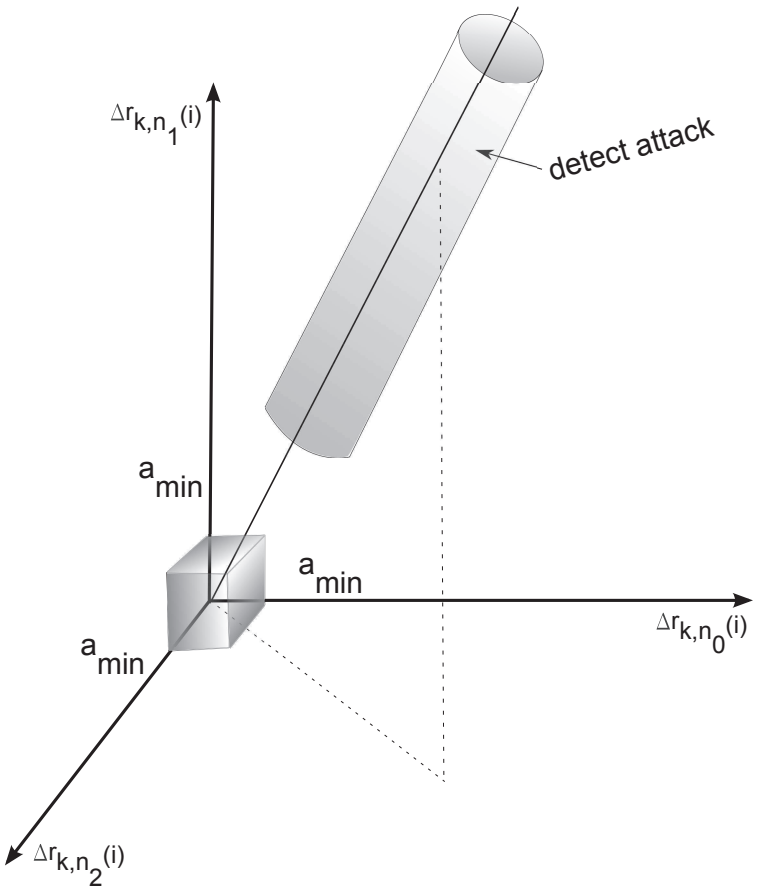


Figure 6.1. Attack detection in $\mathbb{R}^3$ space

method to find the optimal γ automatically. The method leverages the fact that the minimum distance measured for a normal transmitter is usually determined by the environment noise, whereas for an adversarial node, it is determined by the power attack amplitude a_k. In presence of an attack, the minimum distance measured for an adversarial node is relatively much smaller than the distance measured for normal nodes and hence, an optimal value of γ can be chosen by picking an outlier from the distribution of minimum distances of the transmitters. The method is based on the assumption that the adversarial nodes are never present in majority in the network.

6.2.1 Method

For a transmitter k, $\mathbf{Q}_k(i)$ represents a detection window of size p ending at time i. In this section, we consider identical detection windows for every transmitter in the

network and use (6.10) to get p distances from $\mathcal{L}$ for each window. Let $\mathbf{d}_{min}$ denote the vector giving minimum distance points recorded for each window such that

$$\mathbf{d}_{min}[k] = \min_{l \in [0,p)} (d_k(i-l)) \tag{6.12}$$

where $\mathbf{d}_{min}[k]$ is the k^{th} element of $\mathbf{d}_{min}$ which also corresponds to transmitter k. Let's define the mean of $\mathbf{d}_{min}$ as

$$m_d = \frac{1}{M} \sum_{k=0}^{M-1} \mathbf{d}_{min}[k] \tag{6.13}$$

and the standard deviation of $\mathbf{d}_{min}$ as

$$s_d = \sqrt{\frac{1}{M} \sum_{k=0}^{M-1} (\mathbf{d}_{min}[k] - m_d)^2} \tag{6.14}$$

Then we define $\gamma_h(i)$ as:

$$\gamma_h(i) = m_d - h * s_d \tag{6.15}$$

The $\gamma_h(i)$ defined above can be used as threshold for (6.11). We provide detailed experimental evaluation of using $\gamma_h(i)$ in Section 6.3.2.3. A qualitative analysis of performance using $\gamma_h(i)$ is given here.

If there is no adversary transmitter, $\mathbf{d}_{min}$ is determined only by the environment noise. All elements of $\mathbf{d}_{min}$ lie close to each other and hence s_d is small. For such cases, the calculated $\gamma_h(i)$ lies well below $\mathbf{d}_{min}[k]\ \forall\ k$. If k is an adversary node, $\mathbf{d}_{min}[k]$ would be close to zero. Since majority of nodes are assumed to be normal, the calculated $\gamma_h(i)$ lies below all $\mathbf{d}_{min}[j]$, $j \in [0, |\mathcal{H}_j|],\ j \neq k$ and lies above $\mathbf{d}_{min}[k]$. Hence, k can be identified using (6.11).

6.2.2 Evaluation criteria

The heuristic discussed in the previous section sets the threshold γ for (6.11) automatically. We now vary another parameter, the detection window size p, to

tune the performance of the detection method. Increasing p increases the latency of detection. Thus, we provide a trade-off analysis between detection accuracy, measured in P_{MD} and P_{FA} as defined in Section 5.3.1, and the latency of detection, measured in window size p.

Further, by setting the threshold γ relative to distances measured for all nodes, the detection process for an adversary is no longer independent of other adversaries in the network. With a large number of adversaries, $\gamma_h(i)$ would not be effective as the mean of $\mathbf{d}_{min}$, m_d, could now be controlled by the adversaries. Hence, we also evaluate the robustness of our heuristic-based detection method with increasing number of adversaries.

6.3 Evaluation

In this section, we evaluate the performance of M2 with extensive experimental data. To keep the evaluation simple and reliable, we assume a fully connected network for reasons discussed in Section 5.3.

6.3.1 Experiments

We evaluate the performance of M2 under two different experimental scenarios. The primary objectives of the experiments are manifold:

1. To validate the working of detection method M2.
2. To obtain ROC curves which can be used to determine a suitable operating threshold based on the constraints of P_{MD} and P_{FA}.
3. To perform a trade-off analysis between detection accuracy and latency of detection using heuristically chosen threshold, $\gamma_h(i)$.
4. To determine the robustness of M2 while using $\gamma_h(i)$ as the number of adversaries are increased.
5. To analyze the performance of M2 for through-wall localization.

We present results which meet the above experimental objectives in Sections 6.3.2 and 6.3.3. Next we describe the experimental environments and the experiments performed.

6.3.1.1 Experimental environment

We perform experiments in two different environments.

1. In-room environment: This is as described in Section 4.2.1.
2. *Through-wall*: The through-wall environment consists of a typical office room with access to all four walls of the room from outside. The walls are made of drywall and wood. Nodes are deployed on stands 3 feet high placed close to the outer boundary of the room. The node arrangement in the through-wall experiment is shown in Figure 6.2. The solid line rectangle drawn is the wall location. Twenty-six TelosB nodes are deployed in the network in a rectangular area of dimensions 7m X 6m.

6.3.1.2 Experiment description

For the In-room environment, we perform two experiments, *No-attack* and *Attack*, which are explained in detail in Section 4.2.2. We briefly revise the experiments here.

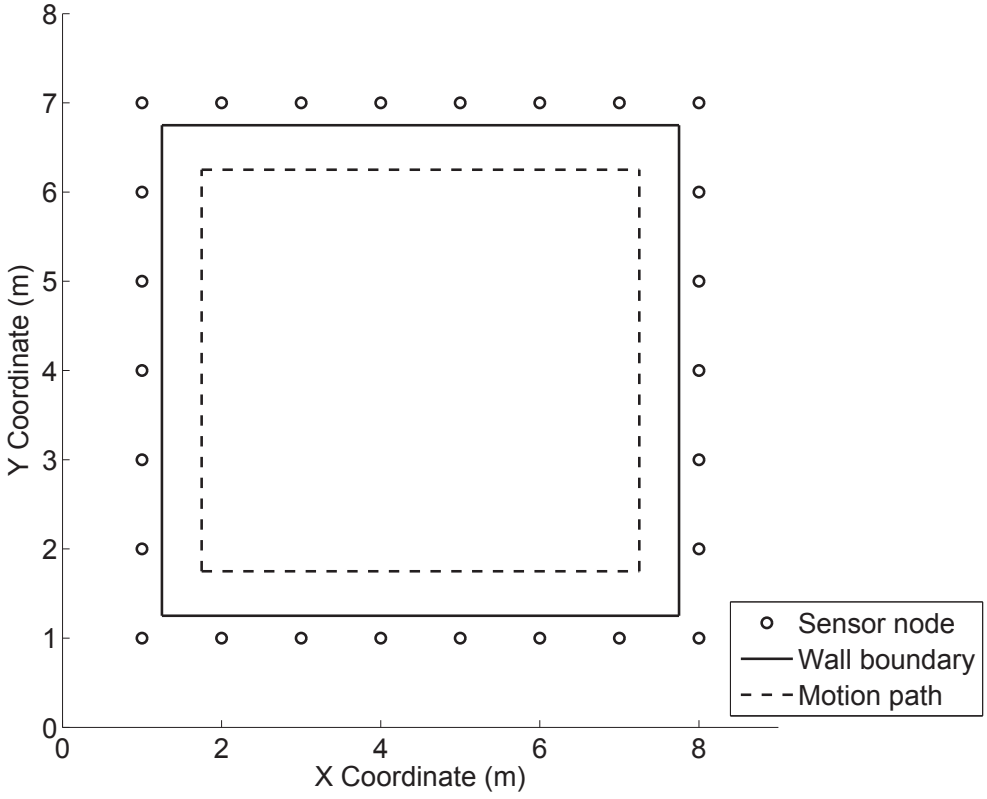


Figure 6.2. Setup for Through-wall experimental environment.

The experiments are performed on a testbed of 20 wireless sensor nodes. The No-attack experiment consists of all normal nodes. The data from this experiment is used to validate the working of M2 and to calculate P_{FA}. In the Attack experiment, nodes are picked randomly, from the normal nodes, to be programmed as adversarial node. Ids of nodes made adversarial are in the order 5, 11, 17, 3, 8, 13, 1 and 14. Two power attack amplitudes are considered, 7dB and 15 dB. Power attack interval n is set to 32.

For the through-wall environment, we perform the same set of experiments No-attack and Attack. However, the attack experiment only consist of power change of 15 dB and with a single adversarial node of ID 22. n is 16 for this environment. The data are collected for a period of 4 minutes.

During both the experiments, a subject is walking in the deployment area on a known path with a fixed velocity. The path and velocity are not relevant for this analysis but are recorded for the purpose of completeness and future work. For all the experiments, no one other than the subject is present in the network.

6.3.2 In-room detection results

In this section, we evaluate our method and present the experimental results. First, we validate the working of our method using sample data collected from No-attack and Attack experiments. Next, we present the ROC curves for the detector and finally results for our heuristic-based method for choosing the threshold γ.

6.3.2.1 Method validation

We validate our method by comparing results obtained from No-attack and Attack experiments and confirm that the measured distance from line $\mathcal{L}$ measured using (6.10) is indeed a suitable metric for detecting power attacks. We consider a sample window of 50 consecutive spin cycles. Each spin cycle gives us one data point $\Delta\mathbf{r}_k(i)$ in $\mathbb{R}^{|\mathcal{H}_k|}$ space for each node. The distance of this data point from $\mathcal{L}$, $d_k(i)$, is calculated using (6.10) and plotted in Figure 6.3.

From Figures 6.3 (b) and 6.3 (c), we observe that the distances measured for adversarial nodes are considerably lower than those measured for normal nodes.

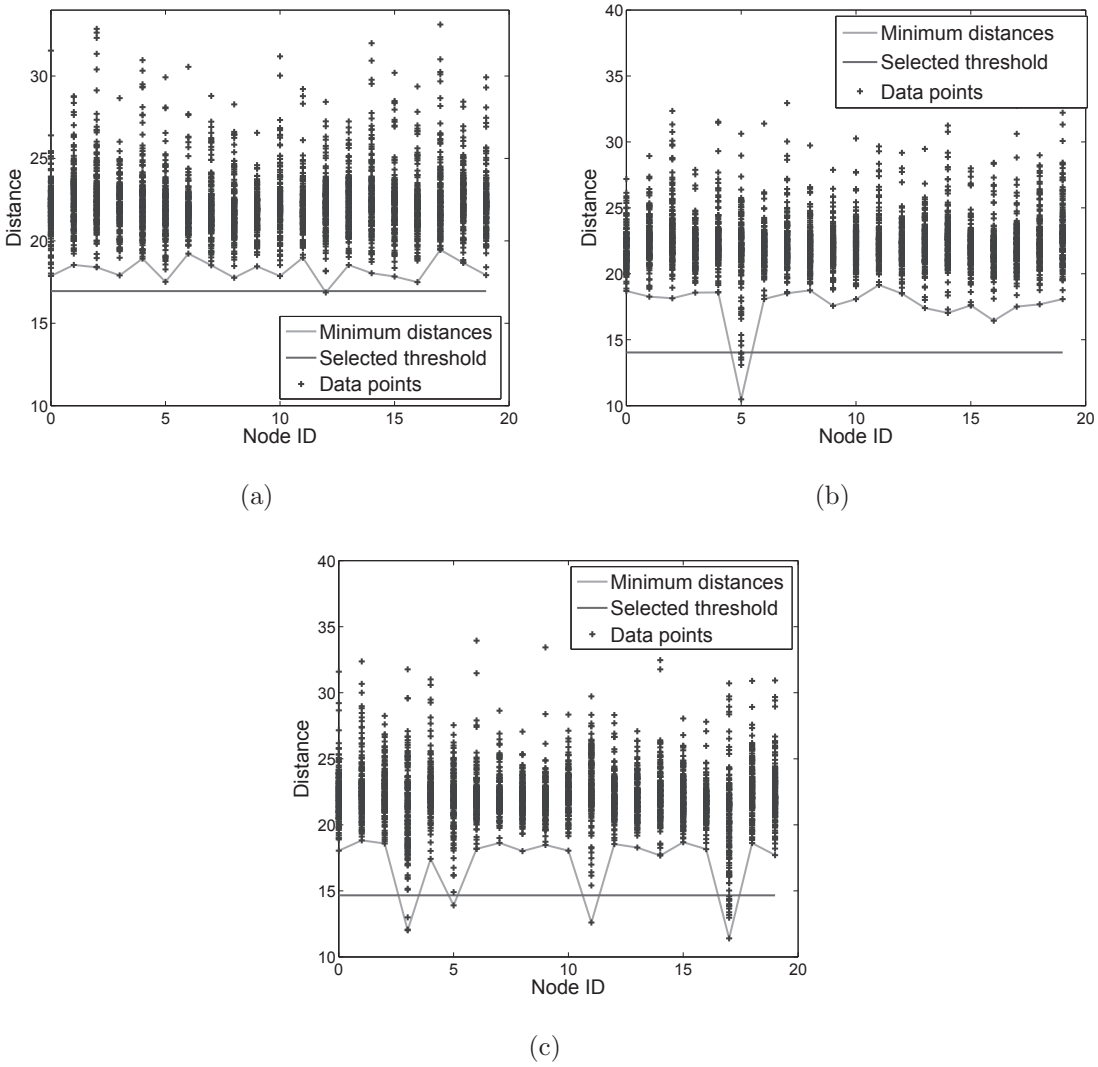


Figure 6.3. Distances from slope 1 Line $\mathcal{L}$ for In-room environment. The figure shows three cases with (a) no-attack, (b) attack with one adversary (node 5), and (c) attack with 4 adversaries (nodes 3, 5, 11, and 17). A appropriate value of threshold γ is selected which separates adversarial nodes from normal nodes.

The distance from $\mathcal{L}$ for normal nodes is determined by the environment. As the power attack amplitude increases from 0, the distance of adversarial nodes from $\mathcal{L}$ decreases while the distance for normal nodes remain almost the same. The increased separation between adversarial nodes and normal nodes helps us to detect power attacks using 6.11 by choosing a suitable threshold γ.

The choice of threshold plays an important role in determining the number of

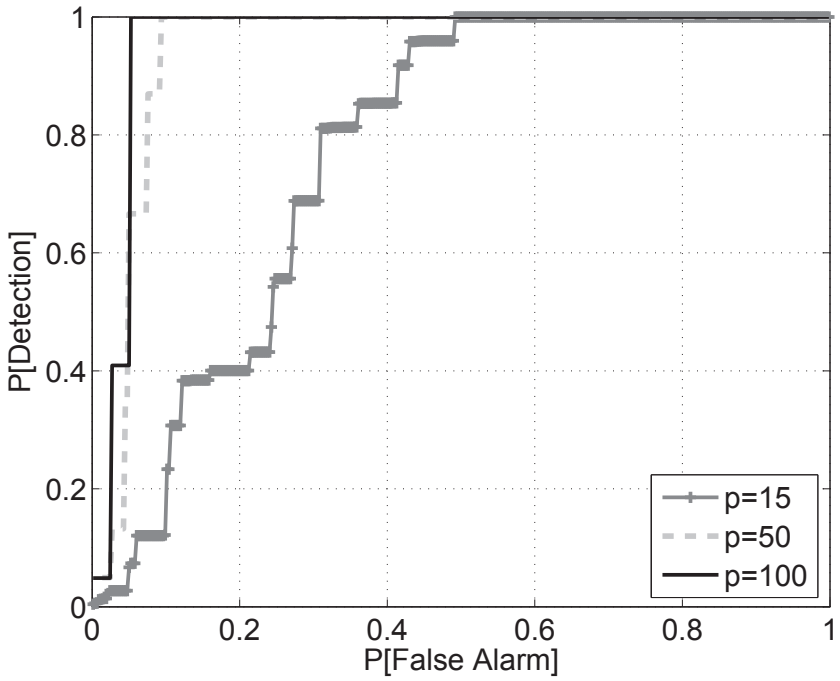
missed detections and false alarms. As an example, we have 4 adversarial nodes for the experiment of Figure 6.3 (c). By setting the threshold at distance 12, we see that some of the distances for nodes 3, 11 and 17 lie below the threshold and hence, nodes 3, 11 and 17 can be detected as adversarial. But with this threshold, we cannot detect node 5 which is also an adversarial node. Choosing a higher distance threshold of 18 increases the detection rate (all adversarial nodes are detected) but it also increases the rate of false positives (node 4 is detected as an adversary). Depending on the deployment conditions, the desired level of threshold can be chosen. An appropriate threshold which results in 100 % detection and 0 % false alarms is also shown in Figure 6.3.

6.3.2.2 ROC curves

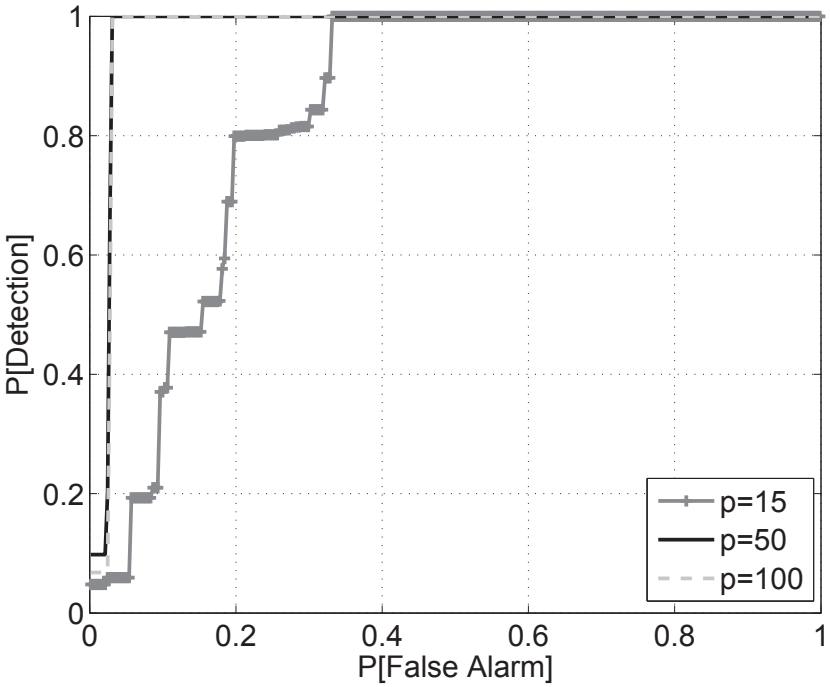
In this section, we present ROC curves for our detection method which are a classical way of representing a detector's performance. We use ROC curves to display the trade-off between probability of detection P_D ($1 - P_{MD}$) and probability of false alarm P_{FA} for M2. These ROC curves can be used to determine a suitable threshold γ for the detection of an adversarial node based on the constraints on P_D and P_{FA}. We plot ROC curves for three values of detection window size p and for 2 different power attack amplitudes, a_k in Figure 6.4.

From Figure 6.4, we make the following observations:

1. We achieve higher detection percentage for a given percentage of false alarms as the size of the detection window increases. The reason for this is that as we increase the size of the detection window, more numbers of malicious transmissions would be present in the detection window which increases the probability of detection.
2. As the power attack amplitude increases, we achieve higher detection rates and a lesser number of false alarms. This is because an increase in power attack amplitude decreases the distance of $\Delta\mathbf{r}_k(i)$ from $\mathcal{L}$, thereby increasing the separation between normal and adversarial nodes. The increased separation results in better detection and fewer false alarms.



(a)



(b)

Figure 6.4. ROC curves for two different power attack amplitudes (a) 7 dB and (b) 15 dB in In-room environment.

6.3.2.3 Performance using heuristic for threshold, $\gamma_h(i)$

6.3.2.3.1 P_{MD} and P_{FA}

In this section, we use the data from *Attack* experiment in In-room environment and calculate P_{MD} and P_{FA} as a function of detection window size p. We also calculate P_{MD} and P_{FA} as a function of number of adversaries N_a. The method is able to detect simultaneous activity for up to 7 adversarial nodes out of 20 in the best case with $h = 1$ in (6.15). The performance is tuned for low false alarms while using $h = 1$. We do not plot results for more than 7 adversarial nodes. The results are plotted in Figures 6.5 and 6.6. The results convey the following information:

- Variation of P_{MD} and P_{FA} with p for constant N_a. This gives the trade-off between accuracy and latency of detection.
- Variation of P_{MD} and P_{FA} with N_a for constant p. This gives a measure of robustness of M2 with increasing number of adversaries.

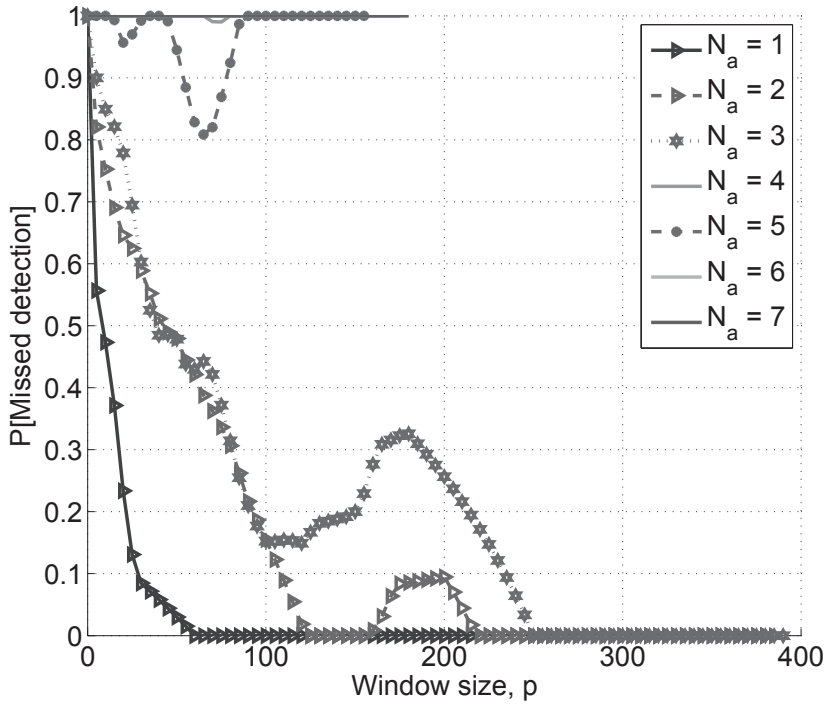
Further, we plot P_{MD} and P_{FA} for two power attack amplitudes – 7 dB and 15 dB. There are a total of 20 nodes in this experiment.

From Figures 6.5 and 6.6, we make the following observations:

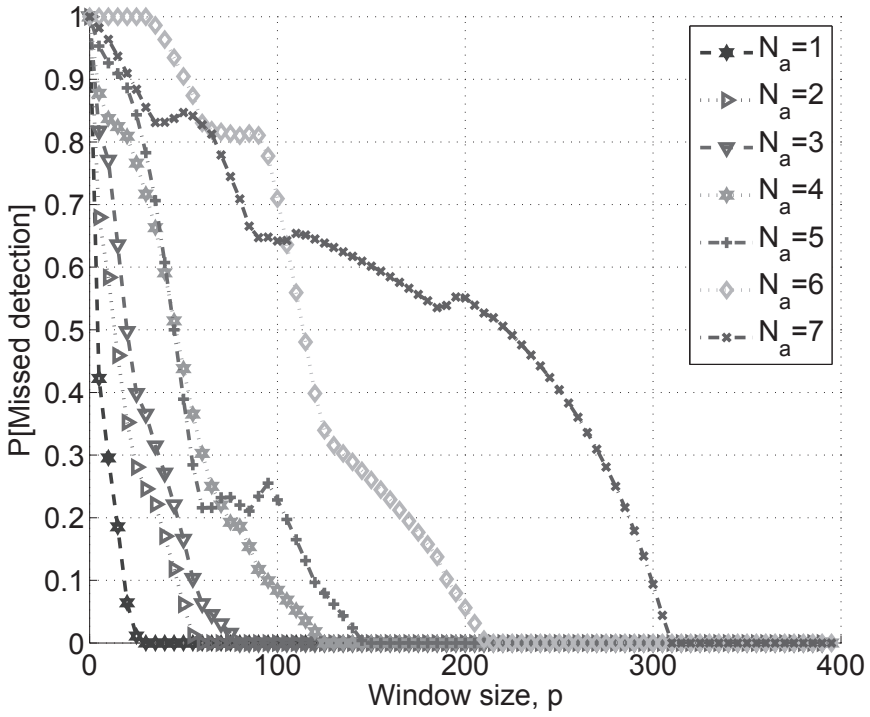
1. The performance of the detector improves with increasing amplitude of power attack and decreases with increasing number of adversarial nodes.
2. For 7 dB of power attack, we can achieve 100 % detection rate for up to 3 adversarial nodes. For 15 dB power attack, 100 % detection is possible for a maximum of 7 adversarial nodes (one third of the total number of nodes).
3. 0 % false alarm rate is achievable for a maximum of 7 adversarial nodes. We do not plot the results for more than 7 adversarial nodes but the trend is likely to continue with increasingly larger window size required.

6.3.2.3.2 Accuracy vs timeliness of detection

In Figure 4.2, we observed that the localization error increases as the number of adversaries are increased. From Figure 6.5, we observe that even with increasing number of adversaries, we can identify all adversarial nodes by increasing the detection window size p.

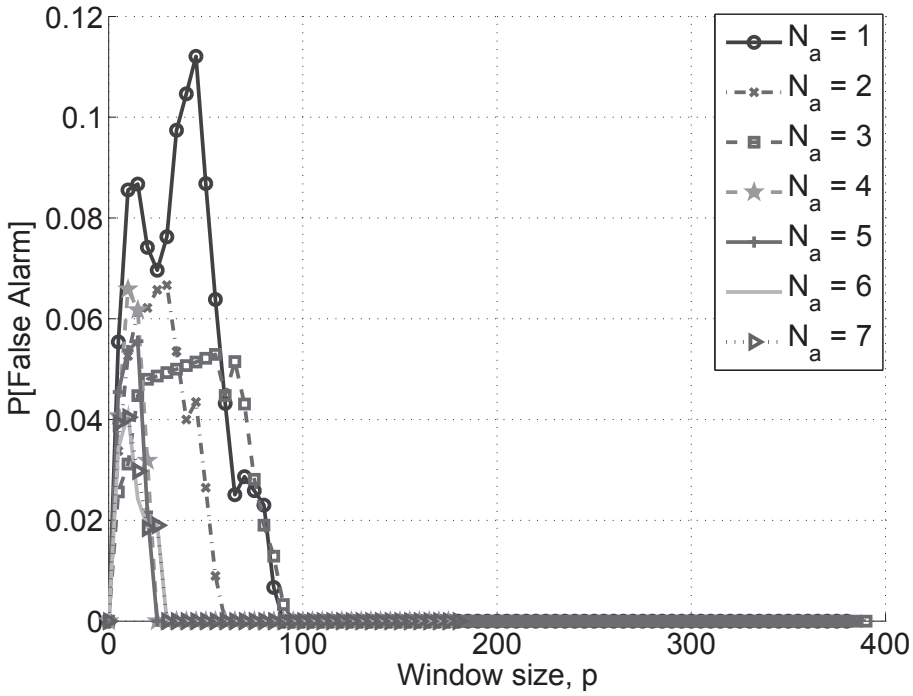


(a)

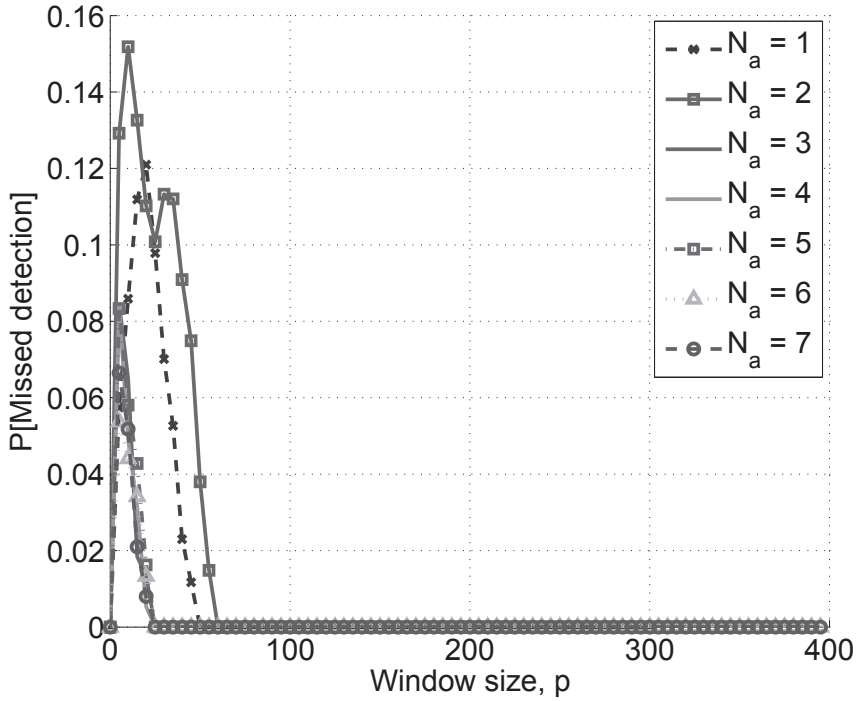


(b)

Figure 6.5. Plot for P_{MD} for (a) 7dB and (b) 15 dB



(a)



(b)

Figure 6.6. Plot for P_{FA} for (a) 7dB and (b) 15 dB

This holds true up to a certain number of adversaries (3 in case of 7dB and 7 in case of 15 dB) beyond which the detection method breaks down and no adversaries are detected. Thus, we conclude that the accuracy of the system in detecting the adversary reliably, i.e., with 0 % missed detection rate, does not degrade as the number of adversaries increase. This, however, comes at the cost of increased time of detection resulting from the large detection window size required.

6.3.3 Through-wall detection results

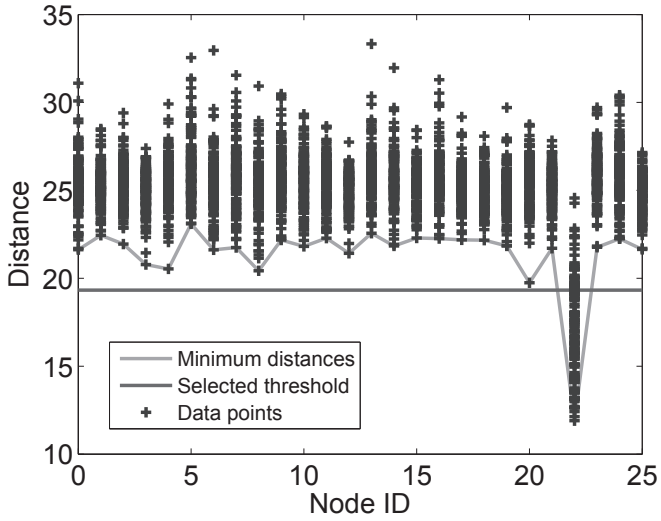
This experiment is performed to check the applicability of M2 for through-wall localization techniques. We test our method for one adversarial node which varies its power by 15 dB every 16 cycles. The results obtained from our through-wall experiments are shown in Figure 6.7.

The results obtained from this experiment are quite encouraging and confirm the efficiency of our detection method in case of through-wall localization techniques. Detailed analysis of performance for different power attack amplitudes and the affect of increasing number of adversaries is to be considered in future research.

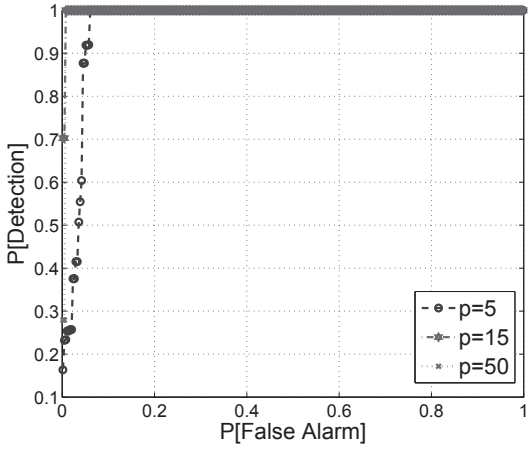
6.4 Conclusion

In this chapter, we presented a novel approach which used distances in RSS vector space to detect adversarial nodes in WSN. We showed through extensive experimentation that during power attack, the distances measured from slope 1 line $\mathcal{L}$ are considerably lower for adversarial nodes in comparison to distances measured for normal nodes. This separation allows us to effectively identify adversarial nodes from normal nodes.

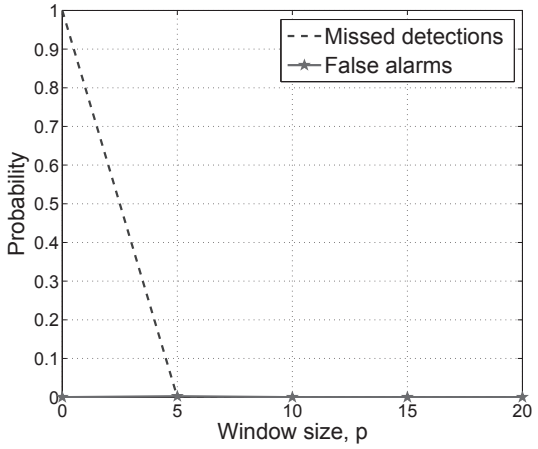
We present ROC curves for the detector and observe that the performance of the detector gets closer to the ideal detector as the window size is increased to 100. Better performance is also achieved for a higher power attack amplitude. Similar observations are made for the heuristic-based method to calculate γ with near ideal performance achievable with sufficiently large window size. With $\gamma_h(i)$, we observe that M2 is robust against up to 7 adversaries, a third of the total nodes, for a power



(a)



(b)



(c)

Figure 6.7. Through-wall detection of adversarial nodes. (a) Distance from slope 1 Line $\mathcal{L}$ while under power attack from node 22. (b) ROC curve for performance of detector in through-wall environment. (b) P_{MD} and P_{FA} for detector when using $\gamma_h(i)$ with one adversary.

attack amplitude of 15 dB. Finally, we evaluate M2 for through-wall localization environment with one adversary and find that the method also performs equally well in that scenario.

CHAPTER 7

ISOLATION OF ADVERSARIAL NODES

The previous two chapters discussed methods to detect adversarial nodes which can introduce significant errors in localization in DFL by varying their transmit powers. These methods, especially M2, are shown to be efficient in the detection process. Next, in this chapter, we propose a simple yet robust enhancement to the token passing protocol Spin which can be used to isolate the detected adversarial nodes efficiently from the token ring. We call this protocol *Enhanced-Spin* or *eSpin*. Assuming that the detection algorithm is executed at the basestation, eSpin allows basestation to issue commands which would adjust the token ring such that the detected adversarial node is no longer a part of the schedule. Note that, in case of adversarial nodes, it may not be possible to make them stop transmitting or varying their transmit powers by issuing instructions from the basestation. However, taking them off the token ring allows us to free up the transmission slot which may be used again for a replacement node. In such cases, the adversarial node may compete with the replacement node for the same transmission slot. The basestation then needs to ignore measurements received from the adversarial node until it is turned off manually.

In addition to isolation of adversarial nodes, eSpin can, in general, be used to handle any failed node in the network. Node failures are common in WSN resulting from exhausted batteries or damaged components. While using Spin, failed nodes not only decrease the coverage area but also slow down the Spin protocol as other nodes in the token ring start timing out while waiting for the failed node to transmit.

The protocol also allows us to add replacement nodes in place of the removed nodes by automatically assigning transmission slots to the new nodes. In the following sections, we discuss the protocol in detail.

7.1 Protocol design

In this section, we discuss the design of the eSpin protocol. This protocol assumes a single hop network and has been designed with the following objectives in sight:

- Removal of detected adversarial nodes or failed nodes from the network.
- Allowing replacement nodes to join the sensor network on-the-fly.
- Have as less overhead as possible while maintaining reliability and stability.

In eSpin every node is given a node ID and a transmission slot. The node IDs are static and are assigned at the time of programming. Transmission slots are dynamic and assigned by the basestation when a node joins the protocol. Basestation keeps a map of the allotted transmission slots along with the associated node IDs.

eSpin follows a token ring protocol. At any time, the token ring consists of a number of sensor nodes and the basestation. The transmission schedule can be explained with the help of a virtual transmission token where only the node with the transmission token is allowed to transmit. When a node transmits, all other nodes receive the packet and make the RSS measurements. These RSS measurements are then transmitted to a base station along with the node's unique ID.

A token ring schedule in eSpin consist of two beacons, a control slot and transmission slots for nodes in the token ring. The control slot is bounded by two marker packets (beacon A and beacon B). Beacon A marks the start of the control slot whereas beacon B marks the end. Beacon B is followed by transmission slots for nodes in the token ring. An example eSpin schedule with a control slot is shown in Figure 7.1 .

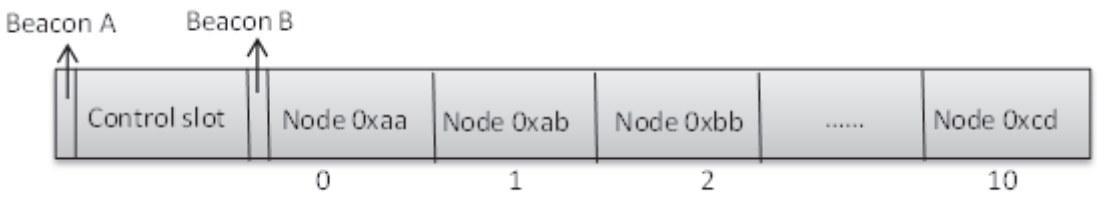


Figure 7.1. A token ring schedule with 1 control slot, 2 beacon frames and 11 transmission slots. Node Ids are shown in the boxes.

Basestation initiates the control slot by transmitting beacon A. The control slot is like an unallocated transmission slot in which any node can transmit/receive commands to/from the basestation. Duration of the control slot is usually determined by the basestation and can be changed from one cycle to another. After the control slot is over, basestation transmits beacon B to pass the transmission token to the node in slot 0. Nodes in later slots follow node 0 in the same manner as in Spin. After the last node in the token ring transmits, the transmission token comes back to the basestation. Basestation now has the three options

- Start a new token ring cycle with control slot by transmitting beacon A.
- Start a new token ring cycle without control slot by directly transmitting beacon B.
- Stop the token ring cycle by not transmitting at all.

To avoid stalls in the token ring protocol, each node implements a timeout. If a node having the transmission token does not transmit for a specified period of time or its transmission is missed by the node next in the token ring, the next node times out and grabs the token from it and continues the cycle. Each cycle of token ring is identified by a sequence number which is incremented by basestation and repeated by every other node. If any of the nodes miss beacon B, it can identify start of a new cycle by observing a new sequence number in transmissions from nodes in slots earlier than it.

7.2 Removal of nodes

Nodes may need to be removed from the token ring either because they are detected adversarial or they may have failed.

To explain the node removal steps, we use the sample token ring of Figure 7.1. Let us assume that node 0xab is identified adversarial or is nonresponsive due to failure.

- When node 0xab is identified as adversarial or observed to be nonresponsive for a timeout T1, its slot is swapped with the last node (0xcd) in the token ring. To swap the slots, basestation sends out a new slot information packet to both the nodes.

- The token ring is now observed for a timeout T2. If slot 1 now becomes responsive, it means that the node (0xcd) has successfully moved to slot 1. This would imply that slot 10 is now nonresponsive (node 0xab may or may not have moved to slot 10). Now the basestation can discard the last slot and start a new cycle as soon as slot 9 is over. The new token ring schedule looks like as shown in Figure 7.2.

Timeout T2 is required to ensure that node 0xcd has successfully moved to the new slot. It might be possible that the new slot information from basestation does not go through successfully to node 0xcd. If after timeout T2, basestation still identifies slot 1 to be nonresponsive (and slot 10 to be responsive), it would imply that the node did not receive the new slot information packet. Basestation can then re-initiate the process from step 1. This 2 step approach eliminates the need for any acknowledgment packets from the nodes during the removal process and hence creates less overhead messages.

7.3 Addition of new nodes

New nodes may be added to the token ring in Spin to replace the adversarial nodes or to just increase the range of the network. eSpin provides a mechanism to add new nodes by allowing them to request a slot in the schedule from basestation during the control slot. The steps involved in the joining process are:

- When a new node, ready to enter the token ring, hears beacon A, it sends out a join request to the basestation.

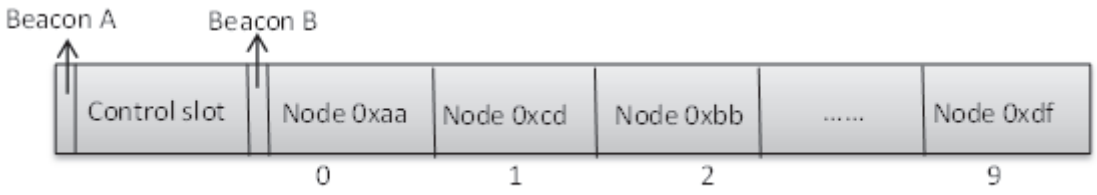


Figure 7.2. Example token ring schedule after removing the node 0xab.

- Upon receiving a join request, basestation looks for the next free slot and responds to the new node in the control slot (current or next).
- Once the new node receives the new slot information from the basestation, it can start transmitting in the allotted slot.

In the meantime, nodes already on the token passing ring wait for beacon B to start the next cycle. All communications from basestation to the new node take place within the control slot.

CHAPTER 8

CONCLUSION AND FUTURE WORK

8.1 Conclusion

In this thesis, we consider the problem of power attacks in DFL. During a power attack, an adversary can vary transmit power of a transmitter node and introduce significant error in localization. Several nonadversarial circumstances like faults developed due to physical damage or depleting power levels and use of power control algorithms also results in change in transmit power. Such changes, if not conveyed to the receiver nodes in the WSN, can result in an increase in localization error.

To detect such unanticipated power changes, we present two detection methods, M1 and M2, that use a statistical hypothesis test of choosing between attack and no-attack hypotheses. Our methods do not depend on the training data and hence, are very robust in environments where the wireless channel characteristics can change frequently. The results obtained during our extensive experiments show the efficiency of our detection methods in in-door settings. In particular, we found M1 to be sufficiently successful in scenarios where the adversary is highly active. However, as the adversary becomes less active, the efficiency of M1 decreases. On the other hand, M2 was found to be highly successful in most adversarial circumstances considered. In addition, we also give a heuristic-based approach to choose the distance threshold γ automatically for M2 by considering data collected in the detection window. We present the performance of this heuristic by giving a trade-off analysis between the accuracy and latency of detection method. Zero missed detection and zero false positive rates are achievable using this heuristic method with very few transmissions from the adversary in cases when only one adversary is present. In the presence of multiple adversaries, our method scales well and can detect all adversaries as long as two-thirds of the nodes are normal.

We also test our method for through-wall device free localization method and the results obtained are highly encouraging, confirming the wide application of our method.

We finally provide a simple enhancement to the Spin protocol, called eSPin, which can be used to remove detected adversarial nodes from the network. eSpin can also be used, in general, to remove any failed node in the network and add in new replacement nodes.

8.2 Future work

In this thesis, we made some assumptions about the adversary and the network to formulate a simple, yet powerful analysis. Some of these assumptions may not be true always and thus, several avenues for future research need to be explored further:

- *Smarter colluding adversaries*: We assumed that the malicious nodes do not collude with each other to perform a more sophisticated power attack by varying their power in a coordinated manner. Addressing these RSS-based attacks is an interesting and important area of future research.
- *Faking RSS values:* We considered here a malicious node capable of varying its transmit power. A malicious node can also report false RSS values received from other transmitters in order to create similar effects. Our preliminary experiments indicate that such actions are less significant than varying transmit power. However, an adversary can combine both type of effects to perform advanced attacks.
- *Power variation patterns*: We only conducted experiments with periodic power variations. Though the methods developed do not make any assumption about the power variation patterns, experimental evaluation of different patterns of varying power variation needs to be performed.

REFERENCES

[1] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location-support system," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, (New York, NY, USA), pp. 32–43, ACM, 2000.

[2] J. Hightower and G. Borriello, "Location systems for ubiquitous computing," *Computer*, vol. 34, no. 8, pp. 57–66, 2001.

[3] D. Quercia, N. Lathia, F. Calabrese, G. Di Lorenzo, and J. Crowcroft, "Recommending Social Events from Mobile Phone Location Data," in *2010 IEEE International Conference on Data Mining*, pp. 971–976, IEEE, 2010.

[4] S. Steiniger, M. Neun, and A. Edwardes, "Foundations of location based services," *CartouCHe Lecture Notes on LBS, version*, vol. 1.

[5] B. Parkinson, J. Spilker, P. Axelrad, and P. Enge, "Global Positioning System: Theory and Applications Volume II," *Progress in astronautics and aeronautics*, vol. 163, 1996.

[6] G. Lachapelle, H. Kuusniemi, D. Dao, G. MacGougan, and M. Cannon, "HSGPS signal analysis and performance under various indoor conditions," *Navigation*, vol. 51, no. 1, pp. 29–43, 2004.

[7] M. Chansarkar and L. Garin, "Acquisition of GPS signals at very low signal to noise ratio," in *2000 Navigating into the New Millennium Proceedings of the Institute of Navigation National Technical Meeting*, no. January, pp. 731–737, 2000.

[8] O. Mezentsev, J. Collin, and G. Lachapelle, "Pedestrian Dead Reckoning–A Solution to Navigation in GPS Signal Degraded Areas?," *Geomatica*, vol. 59, no. 2, pp. 175–182, 2005.

[9] X. Wang, O. Bischoff, R. Laur, and S. Paul, "Localization in Wireless Ad-hoc Sensor Networks using Multilateration with RSSI for Logistic Applications," *Procedia Chemistry*, vol. 1, no. 1, pp. 461–464, 2009.

[10] P. Bahl and V. Padmanabhan, "Radar: an in-building rf-based user location and tracking system," in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2, pp. 775 –784 vol.2, 2000.

[11] M. Brunato and R. Battiti, "Statistical learning theory for location fingerprinting in wireless LANs," *Computer Networks*, vol. 47, no. 6, pp. 825–845, 2005.

[12] T. Roos, P. Myllymaki, and H. Tirri, "A statistical modeling approach to location estimation," *IEEE Transactions on Mobile Computing*, pp. 59–69, 2002.

[13] R. Battiti, A. Villani, R. Villani, and T. L. Nhat, "Neural network models for intelligent networks: Deriving the location from signal patterns," in *in Proceedings of AINS2002, (UCLA*, 2002.

[14] J. Hightower, R. Want, and G. Borriello, "SpotON: An indoor 3D location sensing technology based on RF signal strength," *UW CSE 00-02-02, University of Washington, Department of Computer Science and Engineering, Seattle, WA*, 2000.

[15] K. Woyach, D. Puccinelli, and M. Haenggi, "Sensorless sensing in wireless networks: Implementation and measurements," in *WiNMee 2006*, April 2006.

[16] M. Youssef, M. Mah, and A. Agrawala, "Challenges: device-free passive localization for wireless environments," in *MobiCom '07: ACM Int'l Conf. Mobile Computing and Networking*, pp. 222–229, 2007.

[17] D. Zhang, J. Ma, Q. Chen, and L. M. Ni, "An RF-based system for tracking transceiver-free objects," in *IEEE PerCom'07*, pp. 135–144, 2007.

[18] M. Moussa and M. Youssef, "Smart services for smart environments: Device-free passive detection in real environments," in *IEEE PerCom-09*, pp. 1–6, 2009.

[19] D. Zhang, J. Ma, Q. Chen, and L. M. Ni, "Dynamic clustering for tracking multiple transceiver-free objects," in *IEEE PerCom'09*, pp. 1–8, 2009.

[20] M. Youssef, A. Agrawala, 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, 2003. (PerCom 2003)*, pp. 143 – 150, march 2003.

[21] J. Wilson and N. Patwari, "Radio tomographic imaging with wireless networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 5, pp. 621–632, 2010.

[22] J. Wilson and N. Patwari, "See Through Walls: Motion Tracking Using Variance-Based Radio Tomography Networks," *IEEE Transactions on Mobile Computing*, 2010.

[23] A. Mishra and W. Arbaugh, *An initial security analysis of the IEEE 802.1 X standard*. Citeseer, 2002.

[24] Y. Chen, W. Trappe, and R. Martin, "Detecting and localizing wireless spoofing attacks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*, pp. 193–202, IEEE, 2007.

[25] S. Jana and S. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pp. 104–115, ACM, 2008.

[26] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: The need for secure systems," tech. rep., 2005.

[27] P. Tague and R. Poovendran, "Modeling adaptive node capture attacks in multi-hop wireless networks," *Ad Hoc Netw.*, vol. 5, pp. 801–814, August 2007.

[28] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker, "The directional attack on wireless localization: how to spoof your location with a tin can," in *Proceedings of the 28th IEEE conference on Global telecommunications*, GLOBECOM'09, (Piscataway, NJ, USA), pp. 4125–4130, IEEE Press, 2009.

[29] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. Martin, "The robustness of localization algorithms to signal strength attacks: a comparative study," *Distributed Computing in Sensor Systems*, pp. 546–563, 2006.

[30] S. Blom, C. Bellettini, A. Sinigalliesi, L. Stabellini, M. Rossi, and G. Mazzini, "Transmission power measurements for wireless sensor nodes and their relationship to the battery level," in *2nd International Symposium on Wireless Communication Systems, 2005*, (Siena, Italy), pp. 342–345, IEEE, 2005.

[31] B. Z. Ares, P. G. Park, C. Fischione, A. Speranzon, and K. H. Johansson, "On power control for wireless sensor networks: System model, middleware component and experimental evaluation," in *European Control Conference*, 2007.

[32] H. Tan and W. Seah, "Dynamic topology control to reduce interference in MANETs," in *Proc. of the 2nd International Conference on Mobile Computing and Ubiquitous Networking*, pp. 117039–1, Citeseer, 2005.

[33] J. Wilson and N. Patwari, "Spin: A token ring protocol for rss collection, "http://span.ece.utah.edu/spin","

[34] K. Jamshaid and L. Schwiebert, "Seken (secure and efficient key exchange for sensor networks)," in *IEEE International Conference on Performance, Computing, and Communications*, pp. 415–422, 2004.

[35] A. Khalili, J. Katz, and W. Arbaugh, "Toward secure key distribution in truly ad-

hoc networks," in *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, pp. 342 – 346, january 2003.

[36] K. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *Proceedings of IEEE SECURECOMM*, 2007.

[37] S. Capkun and J. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 3, pp. 1917–1928, IEEE, 2005.

[38] L. Lazos, R. Poovendran, and S. **C**apkun, "ROPE: robust position estimation in wireless sensor networks," in *Proceedings of the 4th international symposium on Information processing in sensor networks*, p. 43, IEEE Press, 2005.

[39] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for wireless sensor networks," in *Proceedings of the 3rd ACM workshop on Wireless security*, pp. 21–30, ACM, 2004.

[40] L. Lazos and R. Poovendran, "HiRLoc: High-resolution robust localization for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 233–246, 2006.

[41] Y. Chen, W. Trappe, and R. Martin, "Attack detection in wireless localization," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pp. 1964–1972, IEEE, 2007.

[42] A. Wilson, *Device-free localization with received signal strength measurements in wireless networks*. PhD thesis, The University of Utah, 2010.

[43] *RTI dataset*. http://span.ece.utah.edu/rti-data-set.