UNIVERSITY OF CINCINNATI

Date: _____

I, _____,
hereby submit this work as part of the requirements for the degree of:

in:

It is entitled:

This work and its defense approved by:

Chair: _____

DCLAD: Distributed Cluster Based Localization Anomaly Detection in Wireless Sensor Networks using Single Mobile Beacon

A thesis submitted to the
Division of Research and Advanced Studies
Of the University of Cincinnati

In partial fulfillment of the
Requirements for the degree of

MASTER OF SCIENCE

In the department of
Electrical and Computer Engineering
Of the College of Engineering
2007

By

Karthika Paladugu

B.E. (Hons) Electrical and Electronics Engineering
Birla Institute of Technology & Science,
Pilani, Rajasthan, India, July 2005

Thesis Advisor and Committee Chair:

Dr. Dharma P. Agrawal

Abstract

In the last few years, Wireless Sensor Networks (WSNs) have emerged as a disrupting technology for myriad military and civilian applications. They demand an accurate location of the event detected and is done by using a mobile beacon node to provide accurate location and assume a benign environment. However, in a hostile environment, such a node can be easily tampered by an adversary. In this paper, we propose a distributed cluster based anomaly detection scheme by assigning few randomly chosen cluster heads a critical task of estimating the reliability of the mobile beacon node. As localization of remaining sensors is cautiously performed only after verifying the authenticity of the mobile beacon node, a considerable overhead is saved in the incorrect localization of the entire network. We perform extensive simulation for different attacks and observe our scheme to have a high detection rate of 99% and a low false positive rate of 20 %.

Acknowledgements

I would like to express my sincere gratitude to my thesis advisor Dr. Dharma P Agrawal for his valuable suggestions and guidance during my research work. I am grateful that he always encouraged us to work in areas that personally interested us and found time to discuss and review our work. I would also like to thank Dr. Wen-Ben Jone and Dr. Yiming Hu for being a part of my defense committee.

I would like to thank my fellow lab members at the Center for Distributed and Mobile Computing (CDMC) for their helpful suggestions and feedback throughout my research. I specially thank Lakshmi Santhanam and Bin Xie for their constant help, patience and valuable research ideas.

I cannot find words to thank my parents for loving me so much and supporting me in all my decisions. Also, I am very grateful to my brother and relatives for giving me enough strength during my ups and downs without which I would be no where. I am deeply indebted to my best friend Murali Krishna Gudibandi who cared for me a lot and stood as a strong support every time I was down.

Many thanks to my closest friend at University of Cincinnati, Sushma Musunuru. I cannot think of a day when Sushma was not there to give me support and encouragement when I most needed it. I also thank all my other friends Anoosha,

Kashmira, Srinivas, Suman, Murali, Disha, Torsha and Damanjit who made my stay at UC so much more pleasurable, enjoyable and memorable.

Last but not least, I would like to thank University of Cincinnati for granting me University Graduate Scholarship and providing me a platform to excel professionally and otherwise.

Contents

List of Figures	ix
------------------------------	-----------

1 Introduction.....	1
----------------------------	----------

1.1 Mobile Wireless Sensor Networks	3
1.1.1 Improvement of coverage.....	3
1.1.2 Enhancement of Lifetime	4
1.2 Applications of MWSN	6
1.2.1 Static sensors and mobile sink	6
1.2.2 Mobile sensors and static sink.....	8
1.2.3 Mobile sensors and Mobile sink.....	8
1.3 Localization in WSN	9
1.4 Security issues in MWSN	10
1.4.1 Security Attacks in MWSN.....	11
1.5 Motivation for our work	12
1.6 Organization of thesis	14

2 Related Work	15
-----------------------------	-----------

2.1 Localization Basics	16
2.2 Mobility Model	20
2.3 Localization techniques for MWSN	21
2.4 Localization Anomaly Detection techniques for MWSN	22

3 System Model and Design Goals.....	24
---	-----------

3.1 Network Deployment Model	25
3.2 Mobility Model of Mobile Sink.....	26
3.3 Localization Model	28
3.4 Security Model.....	29

3.5	Design Goals.....	30
4	DCLAD Scheme	31
4.1	STAGE I: Localization Phase.....	32
4.2	STAGE II: Cluster Head Election Phase.....	32
4.3	STAGE III: Anomaly Detection Phase	35
4.4	STAGE IV: Backend Calculations at the Base Station	36
5	Performance Analysis.....	39
5.1	Performance Metrics.....	40
5.2	Attack Patterns	41
5.3	Simulation Results	42
5.3.1	TPR and FPR variation with Compromised Sensors	42
5.3.2	TPR and FPR variation with Aggregation Instant	44
5.3.3	TPR and FPR variation with Node Density	45
5.3.4	ROC Curves	47
6	Conclusions and Future Work	48
	Bibliography	50

List of Figures

Figure 1-1 Bottle Neck Node problem in Static WSN.....	5
Figure 1-2 WSN with Mobile Sink and Static sensors	7
Figure 1-3 Forest Fire Detection Example	13
Figure 2-1 Factors differentiating the various localization techniques	16
Figure 2-2 Triangulation	19
Figure 2-3 Trilateration	20
Figure 3-1 WSN with grid based deployment points.....	25
Figure 3-2 Movement path of MB node in one Grid	27
Figure 4-1 Parsing by Base Station.....	37
Figure 5-1 TPR vs. % of compromised sensor nodes	43
Figure 5-2 FPR vs. % of compromised sensor nodes	44
Figure 5-3 TPR & FPR at 18 th vs. 36 th instant (Attack 5).....	45
Figure 5-4 TPR and FPR vs Node density for Attack 2 and Attack 5	46
Figure 5-5 ROC Curve for Attack 2 and Attack 4	47

Chapter 1

1 Introduction

In the last few years, wireless networks like cellular networks, MANET (Mobile Adhoc network), WMN (Wireless Mesh Networks), etc. have gained popularity due to usage of devices like PDAs, cell phones, Laptops, etc., by a vast majority of people. Sensors are another popular devices being explored for numerous applications of WSN (Wireless Sensor Networks). Each one of these networks differs from the other

based on the technology used, associated characteristics and underlying infrastructure. A Wireless Sensor Network (WSN) is a highly distributed wireless network of small sensors, deployed in large numbers to monitor the environment. The sensors have the capabilities of sensing the environment, processing the sensed data, and wirelessly transmitting the data to the “Base Station”, which acts as a gateway to a backbone network. Due to the availability of sensors with different sensing capabilities, computing and communication technology the applications where WSNs can be used, is very wide.

Some of the important applications of WSN are environmental monitoring – which involves monitoring air, soil and water, Physiological monitoring, condition based maintenance, habitat monitoring (determining the plant and animal species population and behavior), seismic detection, military surveillance, inventory tracking, smart spaces, etc. In most of the cases, the environments in which sensors are deployed are inaccessible and hostile such as dense jungles (for habitat monitoring applications), battlefields (for enemy troop movement monitoring), etc. Since these environments are not easily accessible, physical placement of sensors at any specified location is not possible. Therefore, they are dropped randomly from a low flying airplane in an area to be monitored. These sensors are equipped with Locomotion Capability to be able to self-deploy; that is, starting from some initial random configuration, the sensors can move to intended or desired locations. Also, recent works in WSNs [1] [2] [3] [4] [5] [6] [7] have demonstrated an enhancement in the coverage and lifetime of the WSN if mobile sensors are employed. The next section discusses the advantages of WSN with

mobile nodes. WSN consisting of mobile sensors is called a Mobile WSN (MWSN). One or more sensors can be configured with mobility as needed by the underlying application of MWSN and optimization could be done either in terms of the lifetime or the coverage of the network. This thesis concentrates on developing a protocol for detecting a compromised mobile sink which causes incorrect localization of the sensors in a WSN and hence, we concentrate more on WSN with mobile nodes, their applications and technical challenges.

1.1 Mobile Wireless Sensor Networks

The MWSN provides several benefits over static WSN and a brief discussion is given below.

1.1.1 Improvement of coverage

When the environment in which sensors are to be deployed, is adequately known and under control and the area to be monitored is relatively small, placements of sensors can be predetermined to cover the total area efficiently and sensors can be manually placed at those points. In such cases, even if the sensors are mobile, they will be of a very little use in enhancing the coverage of the network. However, when the environment is hostile and the area to be monitored is very large, then the manual placement of sensors may not be possible and are usually dropped from an aircraft at a predetermined deployment point. Due to presence of obstacles and wind pressure, sensors may not drop at exactly predetermined locations. By providing mobility,

sensors can be programmed to move to exact locations from their dropped point and hence could improve the coverage. A lot of research work has been done in this area. The algorithms described in [8] [9] use potential- fields between sensors such that each sensor is repelled by both obstacles and by other sensors, thereby forcing the network to spread itself equally throughout the environment. But, the algorithm in [9] discusses the case when there is a constraint on the deployed network, like connectivity of sensors. The centralized and the distributed approaches for deployment of Mobile sensors are discussed in [10] [1] . Voronoi diagram is used in [1] to find coverage holes in the WSN, and discusses the algorithms to guide sensor movement toward these holes. All the algorithms in [8] [9] [10] [1] differ from each other only in the way the desired positions of sensors are computed, while all aim to improve the coverage of the WSN by exploiting the mobility of sensors. Thus, MWSN provides better coverage than the static WSN. Also, in a MWSN, an intruder is more likely to be detected as the moving sensors can better patrol the field. This can significantly improve the intrusion detection capability of a WSN.

1.1.2 Enhancement of Lifetime

Lifetime of any WSN depends on the initial energy of deployed sensors, as once sensors are deployed in the environment; it may be impractical to replace their batteries. Energy in sensors is consumed in sensing, data processing and communicating the sensor readings (in raw or processed form) to a central station called as Base Station (BS). In a static WSN as shown in Figure 1-1 data from sensors is relayed to BS in a multi-hop manner. Due to this forwarding, sensors close to the BS become bottleneck nodes since they relay traffic for all the other sensors in the

network. They consume battery energy at a much faster rate than the remaining sensors in the network, leading to a nonuniform depletion of energy and eventually leading to a disconnected network. Thus, the remaining sensors which have these bottleneck nodes in their multihop path to the BS will have no route to pass the packets to the BS and drop their packets resulting, in loss of data.

Figure 1-1 Bottle Neck Node problem in Static WSN

However, in case of MWSN, special sensors called “Sinks” are used to collect the data. Use of Sinks in the network avoids any multihop relaying and reduces the energy overhead at sensors near the BS, enabling the network to last longer. Existing approaches utilizing Sinks for data collection differ on whether a mobile sink and static sensors are used; or static sink and mobile sensors relays the data packets. The works in [2] and [3] assume that the sink moves through out the network following a predefined path and collects data from sensors by sending a wakeup signal to sensors when within its sensing range. These kinds of schemes may be efficient in terms of

energy consumption and network lifetime. But, latency of data transfer is increased, since a sensor need to wait for the mobile sink to be within its communication range. They are acceptable in delay tolerant applications. Other methods [5] [6] focus on minimizing the delay in data transfer by considering multi-hop communication to the mobile sink. The work in [2] discusses how mobile sensors can be used as relays to improve the Lifetime and reduce the energy consumption. Thus, whether it is a mobile sink or a mobile sensor, the energy consumed by MWSN is less than a typical Static WSN and hence the lifetime achieved by MWSN is more than the Static WSN.

1.2 Applications of MWSN

MWSN could be used for a wide range of real life applications, ranging from military applications to civil applications. They can be primarily classified into three different network models based on the characteristics (mobility, data collection, energy) of the sink, the sensors in the network and associated characteristics of underlying applications.

1.2.1 Static sensors and mobile sink

In this kind of network model, the sink is mobile and it moves through the network in a predefined or a random manner. The sensors are static and are deployed randomly through out the network. There can be one or more sinks in the network, depending on the requirements of the application in hand. Figure 1-2 shows a WSN with static sensors and a sink moving in a predefined path. This is the most widely used model

due to the inherent advantages, like extended network lifetime and coverage due to the data collection by a mobile sink. Some of the applications using this kind of network model are given below:

- Habitat monitoring where static sensors are deployed in the environment and sink attached to the animals or an airplane can collect the monitored data from sensors without engaging in intrusive and disruptive monitoring of sensitive wildlife and habitats.

Figure 1-2 WSN with Mobile Sink and Static sensors

- Environmental monitoring where sensors are used to monitor the environmental data like the temperature, humidity, chemical or gas leakage in an area and report the data to the mobile sink. The data can be used to detect and characterize Chemical, Biological, Radiological, Nuclear, and Explosive attacks.

- Surveillance in battlefields by deploying static sensors in the enemy's territory and collecting the data from an airplane. This kind of technique is also used in parking lots and shopping malls to provide security.

1.2.2 Mobile sensors and static sink

In this case, the sensors are moving with respect to each other and static sink in the network. There can be one or more sinks in the network. As the sinks are static, it is better to place multiple sinks through out the network to increase the network lifetime and decrease the latency of data transfer. For example, traffic monitoring by attaching sensors to taxis is a typical example of this scenario. As the taxis move, the attached sensors continuously move and provide information about the traffic to the static sink through a transceiver. Another example is the deployment of sensors in the river water. The sensors become mobile as they float in the current along a river and sinks at fixed locations on the river banks can be used to collect the data.

1.2.3 Mobile sensors and Mobile sink

This kind of model is seen in all those applications where the sensors and mobile sinks move either because of the environment they are in (wind, currents, etc.) or by attaching them on robots or any other motion actuators.

In this thesis, we consider the network model with static sensors and mobile sink for developing an anomaly detector because it is the most widely used model in many applications and also offers better benefits than the remaining models.

1.3 Localization in WSN

In most of the applications discussed above, it is of at most importance to know location of the sensors. The data reported by the sensors makes sense only if the position information at which the data is collected is reported. For example, in a rescue operation or in a military surveillance application, the personnel can take a proper action only if the location of the event is known. Also, the location information is important for self deployment protocols where the sensors determine their next move based on current location and geographic routing protocols, in which such information (in the form of coordinates) is used to select the next forwarding host among the sender's neighbors.

The problem of determining the location of sensors is called localization problem. Usually a large number of sensors are required to be deployed in a given area due to the small sensing range and limited capabilities of sensors. As equipping all the sensors with GPS becomes costly due to the cost of each GPS unit, a number of localization protocols [11][12] - [16] for WSN which do not entirely depend on GPS have been proposed in the past. These schemes mostly rely on few sensors which know their location either manually or through GPS, called Beacon nodes, deployed through out the network. The remaining sensors estimate their location using the location information provided by the beacon nodes. The localization schemes can be classified

into two main categories based on whether static Beacon nodes or a “*Mobile Beacon*” [17] - [25] (MB) node is used. The localization schemes using Mobile beacon nodes offer several benefits over the schemes using static beacon nodes. A more detailed discussion about the different localization algorithms is done in the next chapter of this thesis. We consider WSN using a Single MB node for Localization. The MB node broadcasts its beacon messages as it traverses through the network along a pre-determined or a random path. Using the location information carried by the beacon messages, other static sensors can estimate their own location with reference to the coordinates of the MB node.

1.4 Security issues in MWSN

Similar to any kind of wireless network, basic security requirements like authentication, confidentiality, integrity, non-repudiation and availability remain the same for MWSNs. However, the resource constrained nature of the sensors imposes additional requirements like survivability and degradation of security services on MWSN. The network should be able to provide a minimum level of service, even in the presence of outage of power of certain sensors and the security level should be changed as the resource availability changes. Achieving these security requirements is a major problem in MWSN due to the wireless nature of communication, lack of infrastructure and uncontrolled environment. The radio channel in WSN is broadcast in nature and is shared by all the sensors within the direct transmission range of

another sensor. So, a malicious node could easily obtain access to the data being transmitted in the network. Also, the lack of central authority that monitors the sensors in MWSN makes it more susceptible to adversary attacks. Possible types of attacks that the attacker can undertake in a MWSN are discussed below.

1.4.1 Security Attacks in MWSN

Security attacks in MWSNs can be widely classified into Active attacks and Passive attacks depending upon the capabilities of the adversary.

Active Attacks: In an active attack, the adversary can intercept the message being sent over the wireless medium in a MWSN and try to modify, corrupt or use the intercepted data in other ways and disrupt the normal functionality of the MWSN. The adversary can either be a part of the network or a part of another network. If the adversary belongs to a different network and tries to forge the identity of a valid sensor in the MWSN and introduce malicious data into the network, then it is called an External attack. These attacks can be prevented using standard security mechanisms such as a strong encryption technique and a firewall. On the other hand, internal attacks are those attacks caused by sensors that are a part of the network. These attacks occur when the authorized sensors which are already a part of the network are compromised by the adversary. When they are compromised, the adversary gets hold of the entire secret key information needed for authentication and encryption and makes them behave as normal sensors. Hence, they are difficult to detect and prevent and are more prevalent in MWSN due to their deployment in hostile terrains.

Passive Attacks: In these kinds of attacks, the adversary silently listens to the wireless medium and will not try to modify the data in the network. The adversary tries to intercept the data and capture the security information and derive passwords in the MWSN. Hence, security requirement of confidentiality is violated if the adversary is able to interpret the captured data. Sinks are usually trust centers and store information such as security credentials, sensor readings, routing tables and location information. Thus, compromise of one or more of them can render the entire network useless.

1.5 Motivation for our work

Major applications of MWSN require monitoring of surrounding environment and providing valuable inputs about any undesirable events like the location of the event to the Sink. To get the location of the event, Sensors use localization algorithms. The sensors are usually predeployed with sensitive key information for establishing a secure communication channel through authentication and thus preventing rogue nodes from joining the network. However, MWSN can be susceptible to the active or passive attacks as described in the previous section and the adversary can capture sensitive key information. The adversary can even capture the beacon nodes and tamper the GPS of beacon node to send incorrect location to the static sensors. If the compromised beacon node sends a wrong location, all the sensors get incorrectly localized and report wrong location information to the base station. This kind of attack

on beacon node can introduce severe impact in critical applications like Forest Fire Detection as shown in Figure 1-3.

Figure 1-3 Forest Fire Detection Example

This figure shows the scenario where sensors are deployed in a forest to detect the forest fires and a mobile beacon node patrolling the area to help the sensors determine their locations. Assuming the mobile beacon node to be compromised by the adversary, all the sensors in the network will have wrong location information. The sensor which detects a forest fire at location A, i.e., (X, Y) computes a wrong location of the event as (X', Y') and reports this information to the base station. The base station will send the rescue vehicle to the location (X', Y') where there is no fire and will not be able to stop the fire at the actual location (X, Y). Thus, the authentication mechanism alone is incapable of protecting the sensors from being physically

compromised and it is very critical to enforce a security scheme that can detect the compromised beacon node in a WSN.

In this thesis, we propose a novel cluster based anomaly detection scheme to detect this compromised MB node that causes localization errors. We take into consideration the constraints of the WSN and propose this security scheme which uses the information only from the sensors and also minimizes the Bandwidth and energy consumption by assigning the reporting task only to a few sensors called the cluster heads. We perform concurrent localization and anomaly detection to reduce the latency of attack detection.

1.6 Organization of thesis

The thesis is organized into six chapters. Chapter 2 provides an overview of various localization algorithms for WSN and the localization anomaly detection approaches. Chapter 3 describes the system model and design goals for our proposed scheme. Our proposed algorithm for detecting a compromised MB node in WSN is discussed in Chapter 4. In Chapter 5, we present the results of the simulation of the algorithm. Chapter 6 includes the conclusions we derive from our work and outline a few extensions that can be made to the mechanisms proposed in this thesis.

Chapter 2

2 Related Work

In this chapter, we discuss the background for our work, including a survey of the various localization techniques and localization anomaly detection techniques proposed in the past.

2.1 Localization Basics

The process of determining the location of sensors is called Localization. A number of localization algorithms [11] - [25] have been proposed in the past. Each one of them differs from the other based on the assumptions taken about the network model like the operational environment(Indoor or outdoor), beacon based or non beacon based, the mobility model of the beacon nodes and sensors, signal characteristics used for distance estimation, the density of beacon nodes in the network, computational model and the method of computation. Figure 2-1 illustrates the different factors effecting the classification of localization techniques and a brief description is given below.

Figure 2-1 Factors differentiating the various localization techniques

Beacon based Vs Beacon less

The first factor differentiating the various localization schemes is whether they rely on beacon nodes or not. Beacon based schemes [11] – [25] assume a certain number of special nodes called beacon nodes that know their position either through GPS or manual configuration to be deployed in the network. In such schemes sensors use the beacon nodes location as a reference for computing their own location. On the contrary, beacon less algorithms [26] do not have any special nodes that know their location. All the sensors estimate their location using the deployment knowledge and the neighbor set.

Range based vs. Range Free

Range based schemes use the signal characteristics of the received beacon message to determine their distance relative to the beacon nodes. The various signal characteristics used are Received signal strength indicator (RSSI), Angle of Arrival (AOA), Time of Arrival (TOA) and Time Difference of Arrival (TDOA). RSSI based schemes use the received beacon message signal strength as an indicator to the distance of the sensor from the beacon node. AoA schemes use the relative angles between neighbors to estimate their location. In TOA based schemes the propagation time from the beacon node to the sensor is used to estimate the distance. TDOA schemes use ultrasound to estimate the distance between the sensors and the beacon nodes. Range-free schemes do not use signal characteristics. These schemes are totally based on the contents of the beacon messages, i.e. the coordinates of the

beacon node location for distance estimation. Some schemes use the number of hops from the beacon node as an indication of their distance from the beacon node.

Computation

Localization schemes are also classified based on the location at which the computation takes place. Centralized techniques [12] are the ones in which all the sensors report their estimated distance information from their neighbors or beacon nodes to a central location or the base station. The base station then computes the exact location for each sensor using the information provided by them. Centralized computation is not feasible when the sensors are moving. In such a case the sensors will have frequent distance information updates and by the time base station computes their present location, they might have moved to another location, making the computation results useless. Also, the total computation burden at a single place delays the computation and if the base station fails, the entire network will go down. To overcome this, computation is distributed through out the network. In distributed schemes each sensor computes its own location in a distributed manner without the help of any central location for computation.

Method of computation

Firstly, all the sensors estimate their distance relative to the beacon nodes or neighbor nodes using any of the range based or range free methods. Then, they transmit that information either to a central location for computation or compute themselves. Triangulation, trilateration and multilateration are the three most commonly used

computation methods in the literature. The type of method used for computation depends upon the type of signal characteristics used to estimate the distance to neighbors or beacon nodes. A brief description of each one of them is give below.

Triangulation: In this method, the sensor estimates its coordinates using its received AOA measurements to at least two beacon or neighbor nodes and the law of sines and law of cosines [27]. As shown in Figure 2-2, if the AOA measurements of sensor C to Beacon1 and Beacon2 are a, b respectively then it can compute the third angle c as $c = 180^\circ - (a + b)$. The sensor also has knowledge of the locations A, B of two beacon nodes. It then estimates its coordinates C using Law of sines and cosines.

Figure 2-2 Triangulation

Trilateration: This method of computation is the same as triangulation. But, in this method the measured distances of the sensor using the received signals from at least three beacon nodes are used to calculate its location. Whereas, in triangulation AOA measurements from at least two beacon nodes are sufficient for computation. In Figure 2-3 the sensor finds its distance from the three beacon nodes B1, B2 and B3

using the received beacon signals. It then uses the laws of geometry [28] to find its location.

MultiLateration: In this process the location of sensor is computed by finding the intersection of multiple hyperbolas [29] corresponding to the different TDOA of the received beacon signals.

2.2 Mobility Model

The localization schemes can also be classified based on the mobility model of the sensors and the beacon nodes in the network. Four different scenarios are possible based on the mobility. The first two under the mobility model in Figure 2-1 are the cases where the beacon nodes are static. All the schemes using these models should have multiple beacon nodes deployed in the network to localize the entire network due to the static nature of the beacon nodes. Whereas, the remaining two models where the beacon nodes are mobile, either one or multiple beacon nodes can be used

for localization depending on the delay tolerable by the network. If the application of WSN is delay tolerable a single Mobile beacon node can be used to localize the entire network and reduce the cost of deployment.

In this section, we give the basic details about the localization procedure and the localization schemes. In the next section, we give an overview of the localization schemes using mobile beacon nodes proposed in the past.

2.3 Localization techniques for MWSN

Most of the localization schemes using mobile beacon nodes employ a distributed approach where each node computes its location based on the received beacon information. Further, these schemes are classified along two dimensions as range based vs. range free schemes, depending upon whether they use signal strength, distance or angle estimates in location calculations or they depend only on the contents of the received messages as discussed in the previous section. The range based schemes such as Received Signal Strength Indicator (RSSI) [20], Time of Arrival (TOA) [24] developed for WSN with static sensors and single MB node utilizes range information to estimate the distance. Each sensor using the scheme in [20] uses the estimated distance in the Bayesian rule to determine its location. The sensors using [24] apply the centroidal formula with distance information to estimate their coordinates. Another range based approach discussed in [25], used in WSN with static beacon nodes and mobile sensors uses triangulation method on the measured

range estimates for location estimation. Range free methods, such as [18] and [22] used in WSN with multiple MB nodes use radio connectivity constraints to bound sensor location within the transmission area of MB node for each received beacon to determine its exact location. In Monte Carlo Localization [23], the sensors estimate their location based on their motion and perception with reference to the MB nodes. Though there are several schemes for localization in a WSN using Mobile beacon node, the problem of localization anomaly detection in WSN using a MB node has been largely neglected. Localization by using a MB node than multiple static Beacon nodes offers many benefits like reduces the cost of using multiple GPS receivers, helps to localize the entire network without leaving few nodes uncovered.

2.4 Localization Anomaly Detection techniques for MWSN

Owing to the hostile environment in which sensors are deployed, all localization schemes are prone to be compromised. In the past few years, few schemes have been proposed to detect such localization anomalies. They are primarily based on the principle of anomaly based detection, which classifies any significant deviation from the established normal behaviors as an attack. Echo protocol [30] uses radio frequency and ultra sound to verify the location information broadcasted by a MB node. But, this scheme verifies the region of the sensor and not the exact location. Du et al. [31] propose an operational model of anomaly detection based on certain threshold metrics which reflects deviations between the observed set of neighbors computed by applying the localization scheme and the known set of neighbors derived from a node's

deployment knowledge. Liu et al. [32] propose to detect malicious beacons in the network using redundant information available from other near by beacon nodes. Each beacon node uses multiple non-beacon IDs, called detecting IDs, as a mask to perform validation check using the threshold metrics on other beacon's broadcasted location information. However, such a scheme is inapplicable to a WSN where the entire network is primarily localized based on a single MB node. It is a challenging task to detect malicious mobile beacon in a WSN due to dynamic nature of the MB node. We employ the deployment knowledge based anomaly detection module based on a difference metric [31]. However, this scheme incurs considerable latency in detecting the attack as detection is performed only after the entire network is localized. Therefore, we focus on concurrent localization and detection using randomly chosen CHs.

Chapter 3

3 System Model and Design Goals

In this chapter, we provide details about the network deployment model, localization model and the security model of the system considered for the analysis of our scheme. We also enlist design goals of the proposed anomaly detector.

3.1 Network Deployment Model

We assume a WSN consisting of a Single MB node and thousands of Static sensors deployed in a hostile environment. The responsibility of the MB node equipped with GPS is to broadcast location information and assist the remaining sensors in localization. The Static sensors compute their location information, monitor the environment and report the data and the anomaly information to the base station. Uniform coverage of the entire region is ensured by dividing the area into small square regions $R_i, i = 1, 2, \dots, n$, where $n = \text{Total number of square regions}$ and precomputing the deployment points $d_i = (x_i, y_i); i = 1, 2, \dots, n$, as the centre point of each square grid as shown in Figure 3-1.

All sensors lying inside one region collectively form a group and are assigned a unique sensor ID

$ID_k, k = 1, 2, \dots, m$, where $m = \text{Total number of sensors in the network}$, group ID $G_l, l = 1, 2, \dots, M$, where $M = \text{Number of sensors in each square region}$ and are also preloaded with the deployment point information. Due to hostile environment, the sensors are deployed from a low flying airplane or unmanned Aerial/ground vehicle around the deployment points. The presence of obstacles like wind, trees etc. makes the final resident point of sensors different from the deployment points. They fall around the deployment points with a certain distribution. The Gaussian distribution is the most generally used distribution model and hence we take the resident points of sensors follows a Gaussian distribution in each square region (Figure 3-1) and thus the probability distribution of node k in group G_l is given by :

$$f_k^l(x, y / k \in G_l) = \frac{1}{2\pi\sigma^2} e^{-[(x-x_i)^2 + (y-y_i)^2] / 2\sigma^2}, \sigma - \text{standard deviation.}$$

3.2 Mobility Model of Mobile Sink

We consider a MB node equipped with GPS receiver traversing through out the network along a semi-deterministic path as shown in Figure 3-2, with the

Figure 3-2 Movement path of MB node in one Grid

speed V m/sec and broadcasting location information as beacons at regular intervals of time, i.e., every t sec. This mobility path ensures that each sensor receives more than three non collinear beacon messages. As shown in Figure 3-2, the sensor 'P' is able to receive five beacons at different instances. Each sensor follows the procedure in section 3.3 to estimate their location. We focus on the above specific sensor deployment strategy as it is the mostly widely used [31]. Also, our detection scheme is not affected by the deployment model of sensors and mobility model of the MB node as the sensors, will have the deployment knowledge. Our scheme can be easily extended to the case of a WSN with Multiple MB nodes with some modifications. For example, each MB node can be detected separately by using the proposed scheme.

3.3 Localization Model

Many localization protocols [18] [20] [24] dealing with WSN using MB nodes have been developed. Here, we adopt a range free technique called Received Signal Strength Indicator (RSSI) based localization scheme [20] because it is widely used for localization with a single MB node. Each sensor measures the RSSI for each received beacon. It finds the probability of distribution for the distance corresponding to the received RSSI, i.e. PDF_{RSSI} . It then forms a constraint on its location (x, y) as

$$const(x, y) = PDF_{RSSI}(dist((x, y), (x_B, y_B))),$$

satisfying the distance between MB node location (x_B, y_B) and its location to be in accordance with PDF_{RSSI} . Using this, a sensor estimates its initial location $ILE(x, y)$. For each received beacon it updates its location to a new location $NLE(x, y)$ using the Bayesian rule [20] as mentioned below:

$$NLE(x, y) = \frac{ILE(x, y) \times const(x, y)}{\int_{x_{\min}}^{x_{\max}} \int_{y_{\min}}^{y_{\max}} ILE(x, y) \times const(x, y)}, \forall \begin{pmatrix} x \in (x_{\min}, x_{\max}) \\ y \in (y_{\min}, y_{\max}) \end{pmatrix}$$

After getting all the beacons, it computes its estimated average location using its estimated location $PDF_{Est}(x, y)$, estimates from the computed locations for the received beacons,

$$(\hat{x}, \hat{y}) = \left(\int_{x_{\min}}^{x_{\max}} \int_{y_{\min}}^{y_{\max}} x \times Est(x, y) dx dy, \int_{x_{\min}}^{x_{\max}} \int_{y_{\min}}^{y_{\max}} y \times Est(x, y) dx dy \right).$$

For optimal and accurate localization results, the sensors should receive at least three non-collinear beacons [20] .

3.4 Security Model

As WSN are usually deployed in hostile environments, the adversary can capture and compromise the MB node and the sensors. When the compromised MB node moving in the network broadcasts wrong location information in its beacon messages, all the sensors which use these beacons will compute incorrect location. Due to this, it is a key issue for BS to continuously monitor the behavior of the MB node. We can not assume the moving MB node to be always connected with the BS directly so that it can always be monitored by the BS. In other words, the BS will not be able to directly observe the behavior of the MB node, which is moving in a large WSN. Therefore, we delegate the role of monitoring the beacon broadcasted by the MB node to the sensors and check if it is correct or not. If the MB node is broadcasting wrong location, the sensor in the WSN will be able to report this behavior to the BS. On the other hand, it might also be possible that sensor itself is compromised and report the MB node beacon messages to be incorrect, even if the MB node is broadcasting correct messages. In either case, if the sensor reports this wrong location in critical applications, it may lead to a disaster. For example, in a Forest Fire detection application, if the sensors at a particular location which detect the fire report a different location due to incorrect localization, then the official will not be able to stop the fire. Thus, measures need to be taken to provide security by detecting the MB

node compromise, even in the presence of compromised Sensors using anomaly detection and random cluster head election. We assume a secure framework for securing communication among sensor nodes [33].

3.5 Design Goals

Our main design goal is to develop an efficient and accurate anomaly detector for determining a compromised MB node and prevent incorrect localization of the remaining sensors in WSN. In summary, following are the design objectives:

- The scheme should perform anomaly detection and localization simultaneously to reduce the detection latency.
- The scheme should accurately detect any kind of malicious behavior pattern of the MB node, e.g., continuous vs. alternating misbehavior
- The proposed scheme should accurately raise alarm even in the presence of large number of compromised sensor nodes.

Chapter 4

4 DCLAD Scheme

In this section, we describe various stages of our proposed Distributed Cluster Based Localization Anomaly Detection (DCLAD) scheme which can simultaneously perform localization and anomaly detection. The first stage is the Localization Phase where the sensors in the transmission range of MB node localize using RSSI based localization scheme. It is subsequently followed by a Cluster Head (CH) Election Phase. All sensors which had already localized form clusters based on neighborhood and elect a CH. After this phase, the elected CHs enter into Anomaly Detection Phase to determine the reliability of MB node and report the information to the BS. The last

stage is the Backend Calculations where the BS parses the report gathered from few sensors in every grid and raises timely alarm when a compromised MB node is detected. Other sensor nodes check whether such an alarm signal is raised by the BS and if so, they stop the process of localization. A detailed discussion about the various stages is given below.

4.1 STAGE I: Localization Phase

The MB node moves through the network and it broadcasts its location beacons at each broadcast instant. All sensors which are in the transmission range of the MB node hear this beacon and calculate their location information using the localization scheme described in section 3.3.

4.2 STAGE II: Cluster Head Election Phase

As sensors are energy constrained devices, we try to save their energy by employing cluster based detection. Though multiple sensors listen to the beacon of MB node, we delegate the job of monitoring the MB node to few sensors only. We elect only few sensors as leaders, in order to save the energy in anomaly detection and reduce the communication overhead in submitting report to the BS [34] **Error! Reference source not found..** Unlike the mobile cluster formation discussed in [34], we use a

static and distributed Hash Based Cluster Head election approach [35] for detection where few sensors in the transmission range of the MB node are elected as CHs. Clustering is repeated at regular intervals of time called the “clustering instants” or CI which is different from broadcasting instants. The CI should be carefully chosen to ensure that all the sensors involved in clustering would have received enough beacon messages to compute their location before involving in detection. For our analysis, we have chosen three CI in each square region. Larger value of CI, i.e., the number of CHs elected in the network increases the energy consumption. Thus, there is a tradeoff between the accuracy and the energy used.

At each CI, all sensors which are in the transmission range of the MB node and have received at least three non-collinear beacon messages will be involved in clustering and we refer to such sensors as member sensors. Clustering is performed such that all sensors in the 1-hop of vicinity of each other form a cluster group G_j . We restrict to a 1-hop neighborhood. Hence, multiple cluster groups are formed at each clustering instant. This ensures that every surrounding node is a member of a cluster. In each group, the chosen CH then runs the anomaly detection algorithm and reports any anomaly to the Base Station.

At each CI, CH election involves the following steps:

1. Each member sensor with ID_i in a cluster group generates a random token R_i and broadcast a value $(ID_i, \text{Hash}(ID_i, R_i))$ to its cluster group G_j . Hash represents a collision free hash function.

2. Each sensor builds a list of IDs from which it has received a token and stores it locally.
3. After an interval called election round, they exchange the list of IDs to ensure that all members of a cluster group G_j have consistent ID list. If any sensor has an inconsistent list, request is generated for the respective token from the missing sensor. Mark this as pending a request and set a pending timer.
4. On the expiration of pending timer, each sensor discloses the (ID_i, R_i) by broadcasting to all group members.
5. Each sensor then performs a verification round by comparing the hash of the revealed R_i value obtained in step 4 against the hash value obtained in step 1. Each sensor then stores the verified R_i value locally in its memory.
6. At the end of the verification round, each sensor in group G_j computes a value $CH_j = (XOR (R_1, R_2, \dots, R_n) \bmod n)$, where n is the number of members in each group G_j , and is the ID of the sensor to be chosen as CH.

In order to avoid the possibility of a malicious sensor electing itself as a CH, and misreporting the anomaly information, we randomly choose the CH. As the possibility of a malicious sensor elected as a CH is meager among a group of sensors, we take this chance. Thus, there is a tradeoff between the security and the efficiency.

4.3 STAGE III: Anomaly Detection Phase

In stage III, the process of continuously monitoring the behavior of MB node is implemented. If the MB node broadcasts wrong information, the CH will be able to detect it by using the deployed neighborhood knowledge and the estimated location and uses this information to maintain the reliability of the MB node. Initially, all the sensors broadcast their group IDs to each other as a part of the HELLO messages. Then, the elected CHs use these received HELLO messages to derive $N(observed)$, the number of sensors from each neighboring group. Each CH employs a localization algorithm to compute its location. As all sensors are pre-deployed with deployment point information, each sensor is capable of determining its probability of being in the neighborhood of another sensor. Thus, each elected CHs now derives a new observation vector $N(Calculated)$, the number of sensors from each neighboring group using their estimated location and deployment knowledge. Then, they compare it with the initial set of neighbors to compute the Difference Metric [31]

$$DiffMetric = | N(Observed) - N(Calculated) |$$

$DiffMetric$ indicates the extent to which the estimated location is different from the actual location. This is used to trigger an alarm based on a certain threshold th , which reflects the amount of location error that can be tolerated in a network, i.e., the acceptable difference between the number of observed neighbors and calculated neighbors. The CH updates a flag called the Reliability Index (RI) to indicate the behavior of the MB node. The RI value is set as follows:

$$\begin{aligned} & \text{If } (DiffMetric > th) \quad RI = 1 \\ & \text{else} \quad RI = 0 \end{aligned}$$

The value of ‘1’ indicates that the location is far from its actual location and hence the sensor has computed a wrong location. The wrong location can be due to the incorrect beacon messages from the MB node or due to the sensor compromise. We deal with both the cases in our scheme. ‘0’ indicates vice versa. It then submits this value to the BS. In a similar fashion, all CHs in every region send their RI values to the BS. The transmission of a single bit RI value results in very small energy consumption at each CH and also very less overhead at the BS.

4.4 STAGE IV: Backend Calculations at the Base Station

The BS obtains the knowledge on the MB node behavior through the RI values submitted by the CHs. At each clustering instant, CHs belonging to different group submit multiple RI values to the BS. Figure 4-1 illustrates the parsing of RI values by the BS.

Figure 4-1 Parsing by Base Station

If majority ($> 50\%$) of CHs indicates that the MB node is compromised, the BS assign a value of '1' for the RI value of the MB node at that instant and '0' otherwise. Likewise, the BS determines the RI values at all the clustering instants in a particular grid and then determines the overall behavior of the MB node in that grid from this information. If the MB node broadcasts wrong location for most of the time in a grid, i.e., Two out of three CHs report the RI value as '1', then the BS considers the MB node as malicious in that grid. Thus, after observing the behavior of MB node in few grids till the "Aggregation instant" or (AI), the BS checks if the MB node is behaving maliciously in this time span and correspondingly raises an alarm. All sensors which have not yet performed localization, now stops localization and save valuable network resources. The RI values submitted by the CHs are a useful indicator of localized error as it clearly demarks the grid in which MB node performed incorrect localization. Thus, rather than re-localizing the entire network, corrective action can

be restricted to that particular grid. The ‘AI’ or the time for which MB node behavior is observed affects the accuracy of detection. But increasing ‘AI’ increases the detection latency.

Chapter 5

5 Performance Analysis

In this section, we study the performance of our proposed cluster based localization anomaly detection scheme using simulations in MATLAB. We consider an area of 500 x 500 square meters (sq. m) divided into 25 square regions, each of area 10000 sq. m. The network density is taken as $m = 1250$ nodes with $M = 50$ nodes in each group. The detection threshold th for the difference metric *DiffMetric* is taken as 10.

The speed of the MS is taken as $v=10\text{m/s}$. The location broadcast interval by the mobile sink is taken as 1 sec, i.e., it travels 10m, broadcasts the location information. Clustering Intervals are taken after every 8 broadcast instants, i.e., 9th, 18th to ensure that the sensors would have received at least three beacon messages broadcasted by the MB node in that 8 broadcast instants. We consider three Clustering instants (CI) in each grid and 27 broadcast instants (BI) of MB node in each grid. Larger value of CI, i.e., the number of CHs reporting reliability information of MB node to BS, in a grid can be increased by keeping the Aggregation Instant after 6 grids to increase the accuracy of detection. But this increases the energy consumption of larger nodes and also increases the overhead at the BS. Thus, there is a tradeoff between the accuracy, overhead and energy. In the following sections, we will discuss more about the effect of Aggregation Instants and Density of nodes in each square region on the performance of our scheme.

5.1 Performance Metrics

We analyze the performance of our scheme based on the following detection metrics:

1. TPR (True Positive Rate) = $\frac{TP}{TP + FN}$, is the rate at which a Compromised MB node is detected and reported by CHs to the BS, i.e., if MB node is compromised for n instants then for how many instants is this behavior reported correctly by the CHs.

2. FPR (False Positive Rate) = $\frac{FP}{TN + FP}$, is the rate at which a good MB node is

reported as compromised by the CHs.

- True positives (TP): No. of times a compromised MB node is reported as compromised by the CHs in a grid.
- False negatives (FN): No. of times a compromised MB node is reported as good by the CHs in a grid.
- False positives (FP): No. of times a good MB node is reported as compromised by the CHs in a grid.
- True negatives (TN): No. of times a good MB node behavior is reported as good by the CHs in a grid.

5.2 Attack Patterns

We consider the following different attack cases of the MB node to analyze our scheme. We analyze our scheme for only these cases because all the remaining cases can be categorized into one of these major cases. ‘T’ is taken as the instant at which the MB node broadcasts correct location and ‘F’ for the reverse case. The different types of malicious behavior of MB node are listed as follows:

- Attack 1 (all the time Compromised): The MB node is egregiously bad and broadcasts wrong location information at all time instants ‘FFFFFFFFFFFF.....’

- Alternating malicious behavior: This attack results in right location information for nodes in some grids and wrong location in other grids, thereby causing asymmetric localized errors. This type of behavior can be exhibited by the MB node in various ways like Attack 2, First half compromised ('FFFFFFFFTTTTTTTTTT'), Attack 3, Second Half Compromised ('TTTTTTTTTTTTTTTTTTTT'), and Symmetric pattern Attack 4, ('FFTTTTFFTTTTFFTTTT'), Attack 5, ('FTTFFTTFFTTFFTTFF').

5.3 Simulation Results

We illustrate the performance of our scheme and analyze the effect of different parameters on the performance metrics in this section.

5.3.1 TPR and FPR variation with Compromised Sensors

Figure 5-1 demonstrates the detection ability of our system for different attack cases as the number of compromised sensors is increased. This simulation is done with an Aggregation Instant (AI) at 18th instant, i.e., after 6 grids, 3 clustering instants in each grid and with 50 sensors in each grid. We can see that our scheme is able to detect most of the attack patterns followed by the MB node with an accuracy of 97%. The TPR decreases as the number of Compromised sensors in the network is increased because the probability of a compromised sensor being elected as CH might increase.

Figure 5-1 TPR vs. % of compromised sensor nodes

Similarly, Figure 5-2 shows the FPR for varying number of compromised sensors. It can be seen that the maximum value of FPR is within 30%, for a largely compromised network with 50% compromised sensors. We also note that when compared to other attacks the detection rate of attack 5 is less and its False alarm rate is more. This is because the BS is not able to observe the total symmetric attack pattern until the 18th instant. Thus, ‘AI’ affects the accuracy of detection depending upon whether more or less number of RI values is available to the BS.

Figure 5-2 FPR vs. % of compromised sensor nodes

5.3.2 TPR and FPR variation with Aggregation Instant

We study the effect of ‘AI’ on the accuracy of our algorithm. We see from Figure 5-3 that Attack 5 takes more time to be detected when the aggregation is at 18th instant. It also shows that the performance is better if the ‘AI’ is taken at 36th instant, i.e., the BS will have more sample RI values to detect the behavior. Also increasing ‘AI’ increases the detection time. Thus, there is a tradeoff between the accuracy and detection latency and energy consumption of the sensors. We observe a smaller improvement in performance for other kinds of attacks (at 18th and 36th instant) which are relatively easier to detect. We can also increase the accuracy of detection by increasing the number of sensors or CHs reporting RI values to BS in each grid, i.e., increasing the sensor density in each grid. We will discuss the variation of detection metrics with node density in next section.

Figure 5-3 TPR & FPR at 18th vs. 36th instant (Attack 5)

5.3.3 TPR and FPR variation with Node Density

In this section, we study the effect of the node density in each grid on the detection metrics for the different attack patterns. We consider the ‘AI’ as 18th instant, three CIs in each square region and *th* value of 10. We see from Figure 5-4 that there is an improvement in the True positive Rate and False Positive Rate for Attack 2 and Attack 5 as the node density in each grid, i.e., number of sensors in each grid, increases. This improvement is seen for all other attack patterns even in the presence of 10%, 20% and 30% compromised sensors in the network. This increase in detection rate is due to the increase in number of 1-hop groups at each CI and corresponding increase in CHs reporting RI values to the BS. Thus, even if some of the sensors elected as CHs are compromised there will be more sensors that might

give correct RI value to the BS at that particular instance and improve the accuracy of detection.

Figure 5-4 TPR and FPR vs Node density for Attack 2 and Attack 5

5.3.4 ROC Curves

We study the Receiver Operating Characteristics (ROC) curve (TPR vs. FPR) which reflects the tradeoffs in the sensitivity of the detection algorithm in this section.

Figure 5-5 ROC Curve for Attack 2 and Attack 4

Figure 5-5 shows the ROC curves for Attack 2 and Attack 4 using our detection scheme with aggregation point at 18th instant. We observe that using our scheme very less number of times a correct beacon message of MB node is reported as incorrect by the CHs (as seen by 0 FPR value) and all compromised instances of the MB node are correctly reported by the CHs (as seen by the high TPR value close to 1). Similar kind of low FPR vs. high TPR behavior is observed for the detection of remaining attacks using our scheme.

Chapter 6

6 Conclusions and Future Work

In this thesis, we propose a cluster based anomaly detection scheme for detecting malicious MB node that causes incorrect localization of sensors in a WSN. As localization is performed by a single MB node, it is very time consuming to perform detection after the localization of the whole network. Hence, we perform localization anomaly detection and correction at the earliest in a concurrent fashion. Also, as

sensors are energy constrained in nature, we use an efficient cluster based mechanism, where each CH estimates the reliability of the MB node and submits its feedback to the BS. The BS parses the gathered RI values and detects the malicious behavior of MB node. The BS observes the reliability reports from sensors for a considerable amount of time before raising an alarm to avoid the effect of compromised sensors. The random election of CH results in the design of a secure and energy efficient detection scheme. Our cluster based anomaly detection scheme has a high detection rate and a low false positive rate.

As adversaries can compromise the MB node's GPS and broadcast incorrect location information, they can even change the predefined path followed by the MB node. Due to this change in predicted movement path, the static sensors might buffer packets to be transmitted and as the MB node does not come at the expected time they might drop the packets leading to a degradation of throughput. Also, it causes delay in packet delivery. This delay and degradation in throughput is undesirable in mission critical WSN applications. Hence, as a part of the future work, anomaly detection scheme determining the anomaly in the predefined movement of the MB node can be investigated.

References

Bibliography

- [1] G. Wang, G. Cao and T.La Porta, "Movement-assisted sensor deployment," *INFOCOM*, 2004.
- [2] A. Chakrabarti, A. Sabharwal, and B. Aazhang, "Using predictable observer mobility for power efficient design of sensor networks," *IPSN*, 2003.
- [3] A. Somasundara, A. Kansal, D.C. Jea, M.B. Srivastava, D. Estrin, "Controllably Mobile Infrastructure for Low Energy Embedded Networks," *IEEE TMC*, 2006.

- [4] S. Jain, R. Shah, W. Brunnette, G. Borriello, and S. Roy, "Exploiting mobility for energy efficient data collection in wireless sensor networks," *MONET*, 2006.
- [5] Z. M. Wang, S. Basagni, E. Melachrinoudis, and C. Petrioli, "Exploiting sink mobility for maximizing sensor networks lifetime," *HICSS*, 2005.
- [6] J. Luo and J. P. Hubaux, "Joint mobility and routing for lifetime elongation in wireless sensor networks," *INFOCOM*, 2005.
- [7] W. Wang, V. Srinivasan, and K. C. Chua. "Using mobile relays to prolong the lifetime of wireless sensor networks," *MOBICOM*, 2005.
- [8] A. Howard, M. J. Mataric, and G. S. Sukhatme, "Mobile sensor network deployment using potential fields: A distributed, scalable solution to the area coverage problem," *DSRS02*, 2002.
- [9] S. Poduri and G. S. Sukhatme, "Constrained Coverage for mobile sensor networks," *IEEE ICRA*, 2004.
- [10] Y. Zou and K. Chakrabarty, "Sensor deployment and target localization based on virtual forces," *INFOCOM*, 2003.
- [11] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low cost outdoor localization for very small devices," *IEEE PCM*, 2000.
- [12] L. Doherty, K. S. Pister, and L. E. Ghaoui, "Convex optimization methods for sensor node position estimation," *INFOCOM*, 2001.
- [13] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. F. Abdelzaher, "Range-free localization schemes in large scale sensor networks," *MOBICOM*, 2003.
- [14] A. Nasipuri, and K. Li, "A directionality based location discovery scheme for wireless sensor networks," *WSNA*, 2002.
- [15] D. Niculescu and B. Nath, "DV based positioning in ad hoc networks," In *Journal of Telecommunication Systems*, 2003.

- [16] A. Savvides, C. Han, and M. Srivastava, "Dynamic finegrained localization in ad-hoc networks of sensors," *MOBICOM*, 2001.
- [17] P. Dutta, and S. Bergbreiter, "Mobiloc: Mobility enhanced localization," 2003.
- [18] A. Galstyan, B. Krishnamachari, K. Lerman, and S. Pattem, "Distributed online localization in sensor networks using a moving target," *IPSN*, 2004.
- [19] P. N. Pathirana, N. Bulusu, A. V. Savkin, and S. K. Jha, "Node localization using mobile robots in delay-tolerant sensor networks," *MOBICOM*, 2005.
- [20] R. Peng and M. L. Sichitiu, "Localization of wireless sensor networks with a mobile Beacon," *MASS*, 2004.
- [21] N. B. Priyantha, H. Balakrishnan, E. D. Demaine, and S. Teller, "Mobile-assisted localization in wireless sensor networks," *INFOCOM*, 2005.
- [22] K. F. Ssu, C. H. Ou, and H. C. Jiau, "Localization with mobile anchor points in wireless sensor networks," *IEEE Transactions on Vehicular Technology*, 2005.
- [23] L. Hu, and D. Evans, "Localization for mobile sensor networks," *MOBICOM*, 2004.
- [24] G. L. Sun, and W. Guo, "Comparison of distributed localization algorithms for sensor network with a mobile beacon," *ICNSC*, 2004.
- [25] P. Bergamo, and G. Mazzini, "Localization in Sensor Networks with Fading and Mobility," *PIMRC*, 2002.
- [26] L. Fang, W. Du, and P. Ning, "A beacon-less location discovery scheme for wireless sensor networks," *INFOCOM*, 2005.
- [27] <http://en.wikipedia.org/wiki/Triangulation>
- [28] <http://en.wikipedia.org/wiki/Trilateration>
- [29] <http://en.wikipedia.org/wiki/Multilateration>
- [30] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," *WiSe*, 2003.

- [31] W. Du, L. Fang and P. Ning, "LAD: Localization Anomaly Detection for Wireless Sensor Networks," in *Journal of Parallel and Distributed Computing*, 2006.
- [32] D. Liu, P. Ning, and W. Du, "Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks," *ICDCS*, 2005.
- [33] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *MOBICOM*, 2001.
- [34] Y. A. Huang, and W. Lee, "A cooperative intrusion detection system for ad hoc networks," *SASN*, 2003.
- [35] M. Pirretti, S. Zhu, V. Narayanan, P. McDaniel, M. Kandemir, and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," *ICA DSN*, 2005.