Localization Against Wormhole Attacks in Wireless Sensor Networks

Pradeep Kumar Sharma

(211CS1051)

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela – 769 008, India

Localization Against Wormhole Attacks in Wireless Sensor Networks

Thesis submitted

in partial fulfillment of the requirements

for the degree of

Master of Technology

by

Pradeep Kumar Sharma

(Roll No. 211CS1051)

with the supervision of

Prof. Manmath Narayan Sahoo

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. www.nitrkl.ac.in

Prof. Manmath Narayan Sahoo
Assistant Professor

June 3, 2013

Certificate

This is to certify that the work in the thesis entitled "***Localization Against Wormhole Attacks in Wireless Sensor Networks***" by *Pradeep Kumar Sharma*, bearing roll number *211CS1051*, is a record of an original research work carried out by him with my supervision and guidance of the requirements for the award of the degree of *Master of Technology* in *Department of Computer Science and Engineering* with the specialization *Computer Science*. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Prof. Manmath Narayan Sahoo

Acknowledgment

This dissertation, though an individual work, has benefited in various ways from several people. Whilst it would be simple to name them all, it would not be easy to thank them enough. The enthusiastic guidance and support of Prof. Manmath Narayan Sahoo inspired me to stretch beyond my limits. His profound insight has guided my thinking to improve the final product. My solemnest grateful to him. It further gives me a deep sense of pride to have received the tutelage of Prof. S. K. Rath, Prof. B. Majhi and Prof. A. K. Turuk. Overwhelming thanks to all members of the Department of Computer Science and Engineering, NIT Rourkela for their encouragement and co-operation throughout. Many thanks to my fellow research colleagues and classmates at Advanced Database Engineering Lab. It gives me immense happiness to be graduating with such an energetic batch of students.

Finally, my heartfelt thanks to my family for their unconditional love and support. Words fail me to express my gratitude to my beloved parents, who egged me on every step of the way.

Pradeep Kumar Sharma

Abstract

In the last decade, wireless sensor networks deployed at an accelerated pace in military, industrial, healthcare etc. fields but that were originally developed in the late 1960s and 1970s. Navigation or localization is an intuitive important because it can help in reducing the complexity of energy efficient algorithm, target tracking, routing protocol and data collection/aggregation algorithm in wireless sensor networks (WSNs). Localization has an important role in both network application domains and services; for example geographical routing. Due to self configuring nature of WSNs, it mainly deployed in a hostile environment, and hence it can be easily threatened by internal or external attack. Therefore, localization and security are essential issues in WSNs. We know that 'Wormhole Attack' is a severe security threat where two malicious colluding sensor nodes create a virtual tunnel to WSNs. Detection and prevention of wormhole attacks in WSNs are a considerably challenging task because of its independence of MAC protocols and immunity to cryptology techniques. Around all the existing defenses have required some additional hardware requirements on the network or strong assumptions; that's may not have perfect applicability in real environment. Our main objectives are to find the *location of wormhole attackers* as well as *the location of sensor nodes* in a wireless network system. In our schemes, we consider the three types of nodes : locators, attackers and sensors in the network and makes a conflicting set matrix on the basis of abnormal behavior of message exchanging among neighboring locators, which helps in differentiation between valid locators and dubious locators. We evaluate location estimation results through simulations in our last section.

***Keywords*:** Wireless Sensor Networks, Wormhole Attacks, Localization, Conflicting set, Maximum likelihood estimation (MLE)

Contents

List of Abbreviations

WSN	Wireless Sensor Network
GPS	Global Positioning System
TOA	Time of Arrival
TDOA	Time Difference of Arrival
RSSI	Received Signal Strength Indication
R_L	Transmission range of locator
R_A	Transmission range of attacker
R_S	Transmission range of sensor
D_{R_S} (S)	disk centered at S with radius R_S
L_i	i^{th} locator
L_C	Conflicting set matrix
D_{R_L} (A_1)	Disc centered at A_1 with radius R_L
loc-RREQ	Locator routing request
loc-ACK	Locator acknowledgement
$I_{i,j}$	Identification scheme of Class i^{th} wormhole attack with j^{th} scheme.

List of Figures

List of Tables

List of Algorithms

Chapter 1

Introduction

Chapter 1

Introduction

1.1 Wireless sensor network (WSN)

Wireless sensor network (WSN) is an important and accelerated area of deeply networked systems of low battery powered wireless sensor nodes with small amount of memory and CPU, and useful in various critical domains such as environment, military, industry, healthcare, commercial, science/technology, security, home and process control applications. A sensor node is a tiny light weighted device that collects the sensory data, compute/process the data and can communicate with neighboring nodes in the network [21]. In a large and open environment first time, wireless network was used in the Sound Surveillance System (SOSUS), to detect and track Soviet submarines in the late 1950s by the United States Military. In 1960s and 1970s, echoes made to develop hardware for the internet. In 1980s, United States Defense Advanced Research Projects Agency (DARPA) developed the distributed sensor network (DSN). First time, Carnegie Mellon University and Massachusetts Institute of Technology Lincoln Labs started research work on DSN. IBM and Bell Labs also started industrial applications of WSNs in power distribution and factory automation. Every decade, size of sensor devices becomes smaller and the involvement of people in its control and monitoring requires very less number up to zero. In Figure 1.1, we

can see the accelerated progress in WSNs during last five decades.

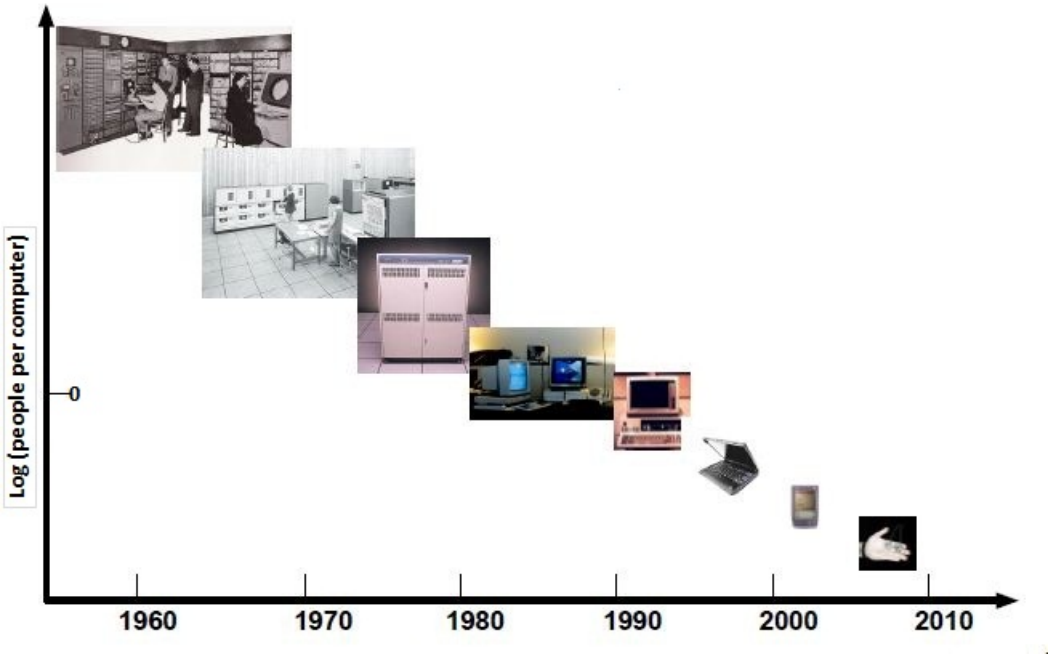

Figure 1.1: Progress of WSNs in last five decades

Wireless sensor networks (WSNs) are built with a very large number of tiny light weighted and inexpensive sensor nodes that have typically resource constrained, limited memory, with low-battery backup sensors, slow embedded processors, and low-bandwidth radios in virtually any environment to solve problems in many fields such as environmental monitoring systems, military field operations and emergency response systems [22]. Sensors are either passive or active in state. Passive sensors are seismic, acoustic and temperature measuring devices. It consumes low energy. Active sensors are included in radar and sonar and these consumes high energy. General features of sensor node in WSNs are following as:

- Sensor nodes are densely deployed even in an open environment.
- Topology of sensor network changes highly frequently.

- Sensor nodes have limited memory, battery power, and computational capacities.
- Sensor nodes may prone to failures because low battery power.
- Sensor nodes may not have a unique identity.

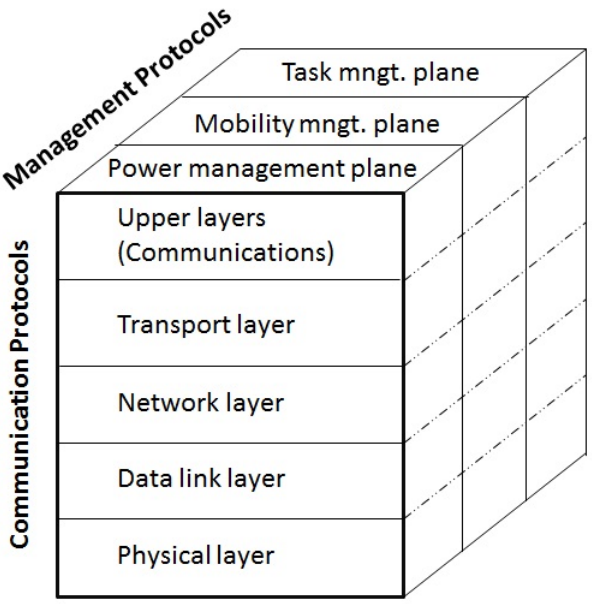

Figure 1.2: Generic protocol structure of sensor networks

Usually, sensor networks are dispersed randomly in a hostile/unfriendly environment and hence the sensor nodes are threatened by various types of attacks. So many attacks in the networks e.g., black-hole, wormhole, Sybil attack Denial-of-Service (DoS) and replay attacks can cause an existing route to be broken or a new route to be prevented from being established. Wormhole attacks are hard to detect and its prevention among these attacks because wormhole attack does not inject abnormal volumes of traffic into the network [1–9].

Upper layers	For network applications and also for data aggregation, external database and external querying query processing
Layer 4	For transport and also for data dissemination and accumulation
Layer 3	For networking and also for adaptive topology management and topological routing
Layer 2	Data link layer: channel sharing (MAC), time SYN/ASYN., data compression and locality
Layer 1	Physical medium: communication channel, sensing, signal processing and actuation

Table 1.1: WSN Protocol Stack [21]

1.2 Applications of sensor networks

Initially sensor nodes were mainly used to detect intrusion in military applications. Now days, we can't grow even a step without WSNs. Sensor networks have been used in accelerated motion in every field. Wireless sensor network applications are following as:

- **Military applications**: Targeting, battlefield surveillance, battle damage assessment, monitoring inimical forces, biological, nuclear and chemical attack detection etc.
- **Environmental applications**: Flood detection, forest fire Detection, micro climates, agriculture etc.
- **Health applications**: Tracking/monitoring patients and doctors, remote monitoring of physiological data, drug administration etc.
- **Commercial applications**: Traffic flow surveillance, vehicle tracking, Environmental control in industries and offices and detection, inventory control.

- **Home applications**: Home/institute automation, automated meter reading, instrumented environment etc.

1.3 Thesis organization

Chapter 1 gives a brief introduction and applications to wireless sensor network. Chapter 2 explores the different types of attacks in the wireless sensor network. It also explores about wormhole attacks, localization and k-means. Chapter 3 it throws light on localization approaches, wormhole attacks and basic terms by survey papers. The proposed scheme has been discussed in Chapter 4. We described the localization scheme on attackers as well as sensor nodes using conflicting set. Chapter 5 described the simulation results and their analysis along our proposed scheme. Finally, Chapter 6 concludes our research work.

Chapter 2

Preliminaries

Chapter 2

Preliminaries

2.1 Attacks and their Classification

It is a very challenging task to secure wireless sensor networks because of its characteristics such as unreliable wireless communication, resource constraints, self organizing, unknown topology prior to deployment, physical tampering and unprotected environment. To secure them, we have to satisfy security goals. Some of the attacks have been explained below :

- **Sybil attack**: Sybil attack was first proposed by J. R. Douceur. In the Sybil attack, an adversary presents multiple identities to other nodes to the network. Geographic routing protocols such as Greedy Perimeter Stateless Routing (GPSR) highly susceptible to Sybil attack.

- **Denial of Service (DoS) attack**: DoS might send so many unnecessary repeated requests to a server so that the server crashes because of heavy load. The attacker may intercept or delete a server's response or client's request and believed that the server is not responding. It slows down the network or interrupt the service of a system.

- **Black hole attack**: An attacker starts dropping all the network packets through its path. If the attacker is also a sink node, the attacker is much more effective.

- **Gray hole attack/Selective forwarding attack**: In this attack [16], malicious nodes behave like black hole and may refuse to forward certain messages and simply drop them without any further propagation. An adversary either suppressed or modified packets originating from a few selected nodes.

- **Wormhole attacks**: It is a severe attack in WSNs where two malicious nodes form a virtual channel between them. Attackers pass the packet through virtual channel and replays them into the network. It can be launched even if the network communication uses the cryptographic technique.

2.2 Wormhole attack

Wormhole attack is a devastating attack where two malicious colluding sensor nodes create a virtual tunnel in the wireless sensor network, which is used to forward message packets between the tunnel edge points [1, 12]. Dezun Dong et al. [3] analyze the inevitable symptom wormhole in the network without using any special hardware and develop a distributed detection with some restriction. An adversary is an outsider, who does not have a valid network identity and also not a part of the network. The attackers have the capability to launch a variety of attacks, such as dropping or corrupting the relayed packets, that significantly harms a lot of network protocols including energy efficient routing, localization, and etc. The basic severe feature of wormhole attack lies in the fact that the attackers can easily launch a virtual wormhole without understanding the protocols or cryptographic mechanisms used in the network.

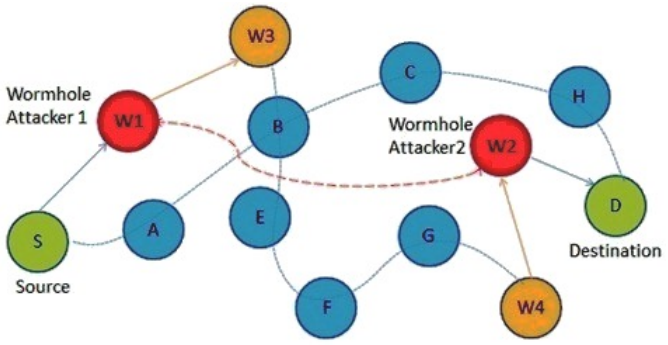

Figure 2.1: Pictorial view of wormhole attack in WSNs

In Figure 2.1, when the source node (S) broadcast the RREQ packet, a malicious node ($W1$) which is closer to the source node (S) receives the RREQ packet. It sniffs that packet to next colluding party ($W2$) which is near to a destination node (D), it rebroadcasts the RREQ. The neighbors of ($W2$) the second colluding party receives the RREQ and drop the further legitimate requests that may arrive later on legitimate multihop paths. Node (D) now has two routes, the first is five hops long ($S - A - B - C - H - D$), and the second is apparently three hops long ($S - W1 - W2 - D$). Node (D) will choose the second route since it appears to be the shortest. Hence there may have a chance of wormhole (tunnel) in the routes of the source (S) and the destination (D).

2.3 Localization

Localization systems are a key part of WSNs, because they not only locate events but it is also useful in the routing protocol, density control, tracking, and a number of other protocols. However, manual configuration of individual nodes with a Global Positioning System (GPS) receiver to obtain its location is expensive and infeasible in large scale. GPS has also affected by heavy trees and buildings because it requires line-of-sight for communication.

2.3.1 Localization process

A localization algorithm runs on different input parameters. The anchor available in the network provides the location as an input [4]. Other inputs e.g. hop counts etc. are connectivity information for range free techniques; distance or angle between node inputs taken from a range based techniques that calculated based on signal modality. Generally, we take the output of the localization algorithm as an absolute coordinate and for anchor free methods as a relative coordinate.

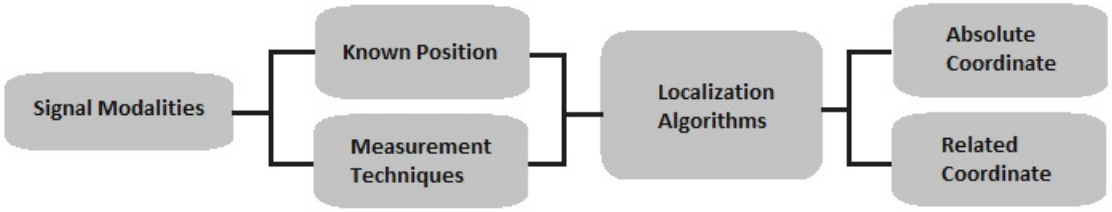

Figure 2.2: Process of a localization algorithm

- **Signal modality**: The accuracy of location estimation based on signal modality. In this modality, we choose a sufficient signal type depends on the various factors such as node hardware, the application and environment like as in temperature, pressure, humidity, acoustic signal, etc.

- **Measurement techniques**: The transmitted signal from each sensor will be processed on the receiving nodes to find out measured transmission ranges or hop counts. Range estimation methods measure the distance or angle between two neighbor nodes. The famous methods of this group are Time-Of-Arrival (TOA), Time Difference of Arrival (TDOA), Angle of Arrival (AOA), or the Received Signal Strength Indication (RSSI). Range-free algorithms are independent of hardware and ranging error. They use only connectivity information and hop counts between nodes as an input parameter.

- **Localization algorithms**: Localization algorithm executed and produced absolute or relative location.
- **Absolute localization**: The absolute location of nodes is defined by position-aware nodes (anchors).
- **Relative location**: Relative location can be found out by absolute localization. We can get the relative location by finding the relationship of distance and angle between network nodes.

2.4 k-means clustering

By Kardi Teknomo, k-means clustering is a mathematical concept by which the objects classify into a particular class and form the cluster. It allows the unsupervised learning of neural network, Classification analysis, Pattern recognitions etc. It has the following steps:

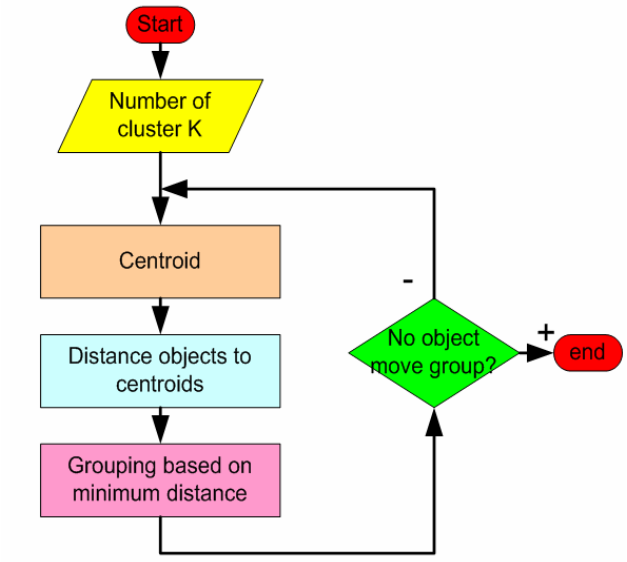

Figure 2.3: Execution flow of k-means

First of all, we have knowledge about the number of clusters of the dataset. Initialize the centroids of each cluster randomly. Calculate the distance of each object to the centroids and group the object based on minimum distance. Iterate these following process until there is no any changing to its centroids.

Chapter 3

Literature review

Chapter 3

Literature review

3.1 Introduction

In many WSNs applications e.g. target tracking, people monitoring, routing, forest fire detecting, vehicle tracking etc. gathered data are not usable without knowing the location of an event. Localization problem refers to the process of estimating and computing the positions of sensor nodes. The location service is a basic service of many emerging computing/networking paradigms. Localization also called positioning or navigation is a technique for determining one's position accurately on the surface of earth [5,17,19]. Localization is a part of the navigational problem that provides orientation and routing information and also about its location.

In general, attackers can use high power antennas or a wired/wireless link, or any other methods and choose the resulting route through the wormhole may have a better metric, i.e., either have a lower hop-count or shorter distance relative to normal routes.

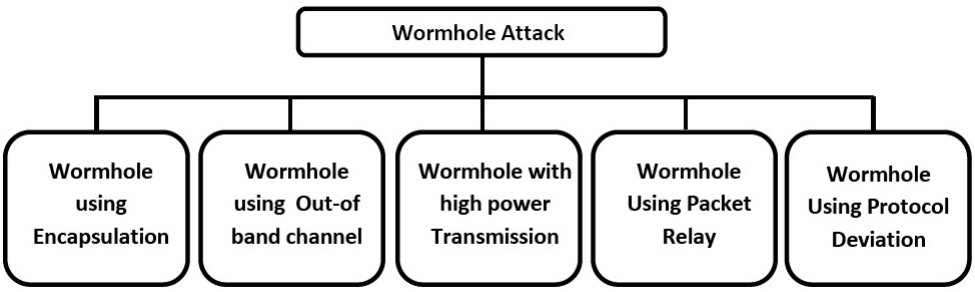

Figure 3.1: Basic approaches of wormhole attacks

3.2 Different approaches of wormhole attacks

Wormhole attack can be achieved by primitive methods [1]. There are five basic types of wormhole attacks.

3.2.1 Wormhole using Encapsulation

In encapsulation-based wormhole attacks, several internal nodes present between two malicious nodes. At one wormhole edge point the data packets are encapsulated and packets forward via wormhole link. Since encapsulated data packets do not increase the actual hop count during the traversal through wormhole link [1]. At the other wormhole edge point, the data packets are decapsulated and broadcast to its neighbors.

In Figure 3.2, source nodes (S) and sink (D) try to determine the shortest path between themselves, when the network threatened by two malicious nodes $M1$ and $M2$. When the source node S broadcasts a RREQ, $M1$ gets the RREQ and encapsulates the data packet forward to $M2$ through the wormhole link exists between $M1$ and $M2$ (E-F-G). Node $M2$ decapsulates the data packet, and rebroadcasts it again. Due to the encapsulation, the hop count does not increase during the traversal through $M1$ and M. At the same time, a copy of the RREQ travels from S to sink D over the path that includes nodes $(A - B - C)$. Now, there are two routes from

S to Sink: the first one is four hops long ($S - A - B - C - Sink$), and the second one appears to be three hops long ($S - M1 - M2 - Sink$), while in reality it is six hops long ($M1 - E - F - G - M2 - Sink$). The sink chooses the second route since it appears to be the shortest path. Its a possible solution is, sensor nodes choose the fastest route reply rather than the one which claims to have the smallest number of hop counts.

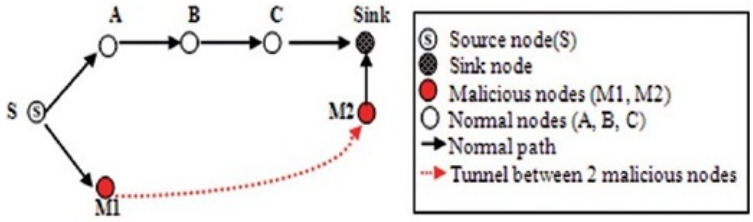

Figure 3.2: Wormhole attack using packet encapsulation

3.2.2 Wormhole Using High-quality/Out-of-band Channel

In this type, the wormhole attack is launched by having a high-quality, single-hop, out-of-band link between the malicious nodes. This type of attack needs specialized hardware capability.

From Figure 3.3, malicious nodes $M1$ and $M2$ linked by out-of-band channel between themselves. Let us assume that source node (S) forward a RREQ to sink node and sink node gets two RREQs: ($S - M1 - M2 - Sink$) and ($S - A - B - C - Sink$); the first route is shorter as well as faster than the second one and hence the sink node chooses the traversal.

3.2.3 Wormhole Using High-power Transmission Capability

In this type of attack, there is only one malicious node with high-power transmission capability in the network. It can communicate with other normal nodes from a long distance. When a malicious node receives a RREQ, it broadcasts the request at a

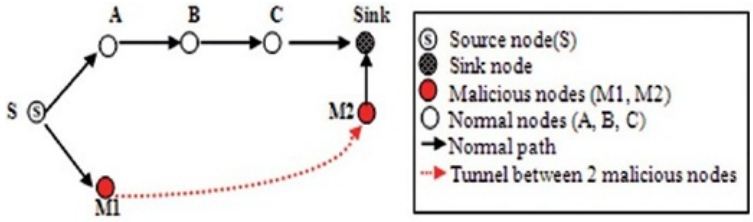

Figure 3.3: Wormhole attack using out-of-band channel

high-power level. Any node that receives the high-power broadcast rebroadcasts the RREQ to its neighbors. It can be mitigated if each sensor node is accurately measure the received signal strength.

3.2.4 Wormhole Using Packet Relay

In this type of attack, a malicious node relays data packets of two distant sensor nodes to convince them that they are neighbors. In Figure 3.4(a), sensor node A and B are actually non-neighboring nodes. Node $M1$ can relay packets between sensor nodes A and B to make them believe that they are neighbors to each other. As shown in Figure 3.4(b), if there are several cooperating malicious sensor nodes, sensor nodes that are multiple hops away from each other can be victims of this attack.

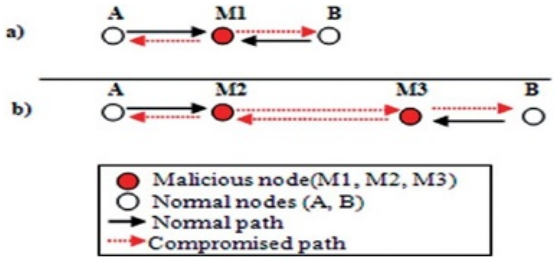

Figure 3.4: Wormhole attack using Packet Relay

3.2.5 Wormhole Using Protocol Distortion

Routing protocols that are based on the 'shortest delay' instead of the 'smallest hop count is at the risk of wormhole attacks by using protocol distortion. In

hop-count-based routing protocols, sensor nodes typically wait for a random back-off time before RREQ forwarding to reduce the number of MAC-layer collisions. In this wormhole mode, a malicious node can create a wormhole by not forwarding RREQs without back-off. The purpose is to let the RREQ packet arrive first at the destination so that the malicious node make a part of path to the destination.

3.3 Localization

Localization systems are a key part of WSNs, because they not only locate events but it is also useful in the routing protocol, density control, tracking, and a number of other protocols. Localization is an active area of research with several surveys [17,19]. Minsu Huang et al. [9] apply the greedy algorithm to localize all the nodes in the network using minimum number of anchors. J. Aspnes et al. [5] provided a network localization solution by constructing grounded graphs to model network localization using graph rigidity theory to test the conditions for unique localizability and to construct uniquely localizable networks. Samira Afzal [8] surveys the localization algorithms and proposes a different taxonomy schemes based on key features like learning, anchor existence, movement in network etc. Ting Zhang et al. [17] divided localization systems into three different components: distance/angle estimation, position computation and localization algorithm.

- **Distance/angle estimation**: This component is responsible for estimating information regarding the distances and/or angles between two nodes. This component include receiving signal strength indicator (RSSI), time [difference] of arrival (ToA/TDoA), number of hops, or angle of arrival (AoA).

- **Position computation**: This component is responsible for computing the position of a node by getting information about the distances/angles and positions of reference nodes. Some techniques used to compute a position include trilateration, multilateration, or triangulation.

- **Localization algorithm**: This is the main component of a localization system. It determines how the available information will be manipulated to enable most or all of the nodes of the WSN to estimate their positions. It is a distributed and usually multi-hop algorithm. Some known algorithms include the Ad Hoc Positioning System (APS) and Directed Position Estimation (DPE).

Recently, novel schemes have been proposed to determine the locations of the nodes in a network where only some special nodes (called beacons) know their locations. In these schemes, network nodes measure the distances to their neighbors and then try to determine their locations. The process of computing the location of the nodes is called network localization. For example, Savvides et al. propose the iterative multilateration scheme to determine the location of nodes that do not know their locations initially. Basically we have two types of nodes: regular nodes and beacons. Regular nodes, also known as unknown, free, or dumb nodes, refer to nodes in the network that have no knowledge of their position and no special hardware to acquire this information. Beacon nodes or locators, are nodes that do not require a localization system to estimate their physical positions.

A localization algorithm localizes sensor nodes based on different input parameters. The anchor available in the network provides the location as an input [4]. Other inputs e.g. hop counts etc. are connectivity information for range free techniques; distance or angle between node inputs taken from a range based techniques that calculated based on signal modality. Generally, we take the output of the localization algorithm as an absolute coordinate and for anchor free methods as a relative coordinate.

3.4 Reviewed papers

Majid Meghdadi et al. 2011 [1], Priya Maidamwar et al. 2012 [12], Murad A. Rassam et al. 2012 [16] described the fundamental types of wormhole attacks and also gave its solution. They discussed wormhole attack detection mechanisms: Distance-bounding/Consistency-based Approaches, Synchronized Clock-based Solutions, Multidimensional Scaling-Visualization-based Solutions, Trust-based Solutions, Localization-based Solutions, Secure Neighbor Discovery Approaches, Connectivity-based Approaches, Radio Fingerprinting Approaches.

Jin Guo et al. 2011 [2] found the characteristics of wormhole attacks and applied wormhole attack defense strategy based on neighbors verification. In this strategy, each normal node received the control packet and monitor the control packet to decide that whether the control packet coming from normal nodes or not to avoid the wormhole attacks. The lacking part of their paper, initially all normal nodes deployed static in the network and determined their neighbors but, they considered, there were no any malicious node at that time.

Dezun Dong et al. 2011 [3] analyzed symptom of wormholes and developed distributed detection methods by making few assumptions. They gave effective distributed detection approach which fully depends on network connectivity information, against wormhole attacks by topological methods without using any extra hardware devices. By detecting non separating loops (pairs), their approach can detect and locate various wormholes and relies solely on the topological information of the network.

Azzedine Boukerche et al. 2008 [4], Ting Zhang et al. 2012 [17], Samira Afzal, 2012 [18], A. Srinivasan et al. 2008 [19] and Amitangshu Pal et al. 2010 [22] define the secure localization schemes in WSNs. They explain the security through cryptography and also non-cryptography in localization. They explain approaches of Liu et al. In their method, the sensor field is quantized into a grid of cells, and each neighboring reference node votes on the cells. Finally, they determine the centroid

of voted cells and set it to the position of the node. Since they used centroid to find out node location but it gives more accurate if the reference nodes deployed densely in the network.

J. Aspnes et al. 2004 [5] provide the localization scheme by some anchor nodes. They construct grounded graphs by connecting the neighbor nodes and apply graph rigidity theory to test the conditions for unique localizability and to construct uniquely localizable networks. They used trilateration method for distance measurement in localization. Mingbo Zhao et al. 2005 [6] gave a maximum likelihood estimation method. MLE method used in finding localization via triangulation, trilateration, and also in Gaussian noise.

Junfeng Wu et al. 2010 [7] proposed a label-based secure localization scheme to defend against the wormhole attack. This approach is a range-free algorithm and anchors in the network find hop-counts. In this scheme, they generate a pseudo neighbor list for each beacon node, use all pseudo neighbor lists received from neighboring beacon nodes to classify all attacked nodes into different groups, and then label all neighboring nodes. According to the labels of neighboring nodes, each node prohibits the communications with its pseudo neighbors, which are attacked by the wormhole attack. But it works well when the network has no packet loss, and the transmission ranges of all nodes are identical.

Xiaomeng Ban et al. 2011 [8] introduce a wormhole detection algorithm based on local connectivity tests. In this approach, there were two sets of neighbors on both sides of wormhole link. Small neighbors of opposite ends of wormhole link are removed one by one, we got a time where the network is free from the wormhole.

Minsu Huang et al. 2010 [9] apply the greedy algorithm using both trilateration and local sweep operations to localize all the nodes in the network using minimum number of anchors. MCLP determines the minimum anchor set to localize the whole network.

TIAN Bin et at. 2012 [10] proposed a scheme based on statistical analysis. In

this scheme, a sensor can detect the fake neighbors by neighbor discovery process, and then apply a k-means clustering method to determine its true neighbors and fake neighbors.

Zorana Bankovic et al. 2012 [11] propose a machine learning solution to detect temporal and spatial inconsistencies in the sequences of sensed values and the routing paths. In the presence of an attacker, produced data considered as outliers and applied clustering techniques for anomaly detection.

H. Chen et al. 2010 [13–15] proposed a localization scheme based on conflicting set. In their scheme, there are three different types of nodes: sensor, locator and attacker. Localization is mainly depending on conflicting set matrix. They consider two classes: Class 1 and Class 2 wormhole attacks. In the first stage, they apply wormhole detect approach in the network. In the second stage, they apply neighboring locators differentiation schemes and in third stage apply the secure localization process using the MLE method. The scheme applies the localization process only for sensor. It is beneficial when the length of wormhole link is less than $2 * R_L$ otherwise, it is common to other approaches.

Loukas Lazos et al .2004 [20] proposed a range independent localization algorithm in an untrusted environment. In SeRLoc, each locator transmits different beacons at each antenna sector with each beacon containing, (a) the locator's co-ordinates, (b) the angles of the antenna boundary lines, with respect to a common global axis. The sensor can identify the region within which they reside by computing the overlap between all the sectors that they hear. Each sensor determines its location as the center of gravity (CoG) of the overlapping region.

Kazem Sohraby et al. 2010 [21] discussed all about the wireless sensor network. They explain WSNs and its application, wireless transmission technology, MAC protocol, routing and TCP protocol in WSNs, network management, performance etc.

3.5 Motivation

Localization is a part of navigation problem to find out one's position accurately on the surface of the earth. The motivation came from the growing need for localization in WSNs because the core function of WSNs collects and processed the sensory data and to detect and report events only if the accurate location of the event is known [19]. The three important metrics associated with localization are energy efficiency, accuracy, and security. Though the first two metrics have been researched extensively, the last i.e. the security metric has drawn the attention of researchers only recently, and as such has not been addressed adequately. The objective of this research work is to find out location information of any sensor node at low cost in the wireless sensor networks even when it is threatened by wormhole attack.

3.6 Problem definition

WSNs are widely deployed in hostile environments and hence it can be easily threatened by so many attacks as, black hole attack, wormhole attacks, gray hole attack etc. WSNs are widely spread in the network, so we can't affix the GPS receiver in each and every sensor node because GPS receivers are costly and also sensor has constraint energy and memory space. Wormhole attack is a severe threat and is immune to MAC protocol and cryptology. So, wormhole attack can easily launch a virtual link and affect the localization scheme in WSNs. Localization is itself information in so many applications. Most authors provided the solutions based on anchors to resolve the localization problem. We are also using anchors to the resolving localization problem but we use conflicting set concept in localization without using any external device.

Chapter 4

Proposed scheme

Chapter 4

Proposed scheme

4.1 Introduction

We considered that the three different types of nodes: *locators*, *sensors* and *attackers* dispersed in the network. Locators are uniformly distributed and have known location and its identification. Sensors are randomly distributed in the network and they estimate their locations by neighboring locators via message exchanges. The attackers launch a wormhole in the network. For simplification, we assume that the transmission range of sensors, locators and attackers are R_S, R_L and R_A respectively and have their relations $R_S \leq R_L \leq R_A$. D_{R_S} (S) represents disc centered at S with radius R_S.

Types of sensor nodes:

- **Neighboring locators** $(N - locators)/L_N$: Those locators that can communicate with the sensor, either via the wormhole link or not, are defined as the (N-locators) of the sensor.
- **Valid locator** $(V - locators)/L_V$: The neighboring locators, which can communicate directly with the sensor, are called (V-locators).

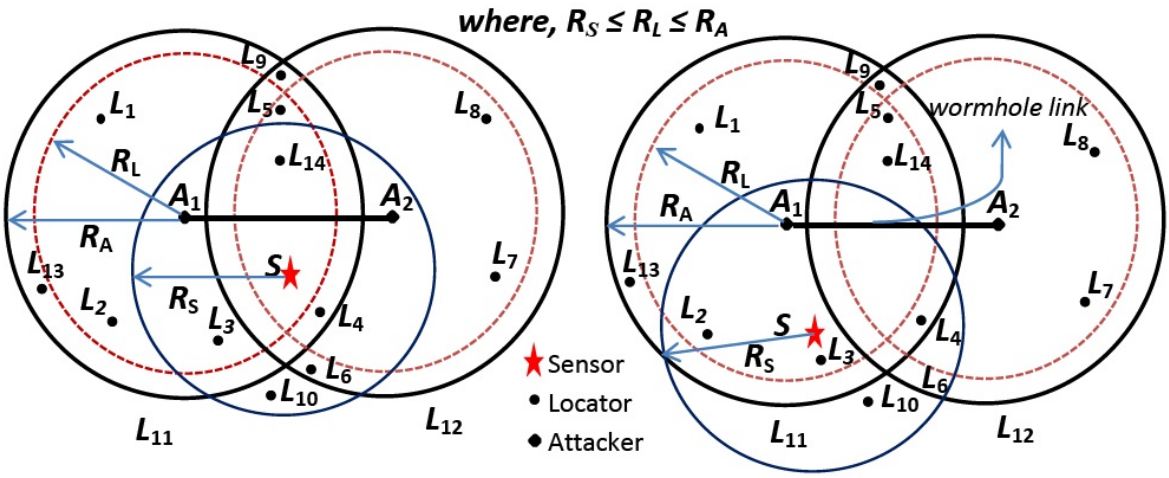

Figure 4.1: (a) Class 1 wormhole attacks, (b) Class 2 wormhole attacks

- **Dubious locator** $(D - locators)/L_D$: The locators, that can communicate with the sensor via the wormhole link, are defined as (D-locators).

In Figure 4.1(a),

Neighboring locators : L_N=$\{L_1, L_2, L_3, L_4, L_5, L_6, L_7, L_8, L_{10}, L_{14}\}$

Valid locators : L_V=$\{L_3, L_4, L_6, L_7, L_8, L_{10}, L_{14}\}$

Dubious locators : L_D=$\{L_1, L_2, L_3, L_4, L_5, L_7, L_8, L_{14}\}$

In Figure 4.1(b),

Neighboring locators : $L_N = \{L_2, L_3, L_4, L_5, L_6, L_7, L_8, L_{14}\}$

Valid locators : $L_V = \{L_2, L_3, L_4, L_6, L_{10}, L_{11}\}$

Dubious locators : $L_D = \{L_4, L_5, L_7, L_8, L_{14}\}$

4.1.1 Wormhole Attack Classification

When the sensor node communicates with the locators via wormhole link then two types of wormhole classification may arise.

- **Class 1 wormhole attack**: The sensor is considered under Class 1 wormhole attack, when the sensor receives the same message transmitted by itself via the

wormhole link. Therefore the measured distance between the sensor and one of the attackers is less than R_S, while measuring the distance between the sensor and the other attacker is less than R_A.

- **Class 2 Wormhole attacks**: The sensor is considered under class 2 wormhole attack, when the sensor can exchange messages in the network via the wormhole link, but can't receive its own message. Therefore, the measured distance between the sensor and one of the attackers is less than R_S, while the measured distance between the sensor and the other attacker is larger than R_A.

4.1.2 Wormhole attack detection

The following four properties can be used to detect the existence of the wormhole attack [13, 14]:

(A) Node's self-exclusion property: A node can't receive a message/messages transmitted by itself in a loop-free path.

(B) Packet unduplication property: A node can receive at most one copy of the same message from one of its neighboring nodes.

(C) Neighboring nodes' spatial constraint property: A node can't receive messages from its two neighboring nodes simultaneously if the measured distance between them is larger than $2*R_S$.

(D) Node's spatial constraint property: The measured distance between two neighboring nodes can't be larger than the transmission range (R_L or R_S).

Now, if it violates any of the above sensor properties then it is threatened by wormhole attack, there we apply Neighboring Locators Differentiation Scheme to find the actual neighbors of the node.

4.2 Conflicting Set

Neighboring locators (L_i) can be determined if every locator builds the conflict sets. Those locators that are not involved in the conflicting sets but its beacon message received by the sensor node, such locators are considered as valid locator (L_V).

Conflicting sets (C (L_i)) create a list of the abnormality of the beacon message exchange among neighboring locators.

Conflicting Set Theorem [13]:

- If L_i lies in D_{R_A} (A_2) but not in $D_{R_A}(A_1)$, all the locators in C (L_i) lie in D_{R_L} (A_1)
- If L_i lies in D_{R_A} (A_1) but not in D_{R_A} (A_2) all the locators in C (L_i) lie in D_{R_L} (A_2)
- If L_i lies in D_{R_A} (A_1) $\cap$ D_{R_A} (A_2) , all the locators in C (L_i) lie in D_{R_L} (A_1) $\cup$ D_{R_L} (A_2).

From Figure 4.1, Conflict sets of L_i:

C(L_1/ L_2/ L_3/ L_{13})=$\{L_4, L_5, L_7, L_8, L_{14}\}$

C(L_4/ L_5/ L_9/ L_{14})=$\{L_1, L_2, L_3, L_4, L_5, L_7, L_8, L_{14}\}$

C(L_6)=$\{L_1, L_2, L_3, L_4, L_5, L_{14}\}$

C(L_7/ L_8)=$\{L_1, L_2, L_3, L_4, L_5, L_{14}\}$

Here we can see that, the locators (L_4, L_5, L_{14}) lie in $D_{R_L}(A_1) \cap D_{R_L}(A_2)$ and also, lie in the C (L_4, L_5, L_{14}). As locators (L_6, L_{13}) do not lie in the conflicting sets C (L_i) hence locators (L_6, L_{13}) are taken as valid locators if they are in the range of $D_{R_S}(S)$ otherwise they are not taken.

Every locator makes a conflicting set matrix (L_C) of those locators that find the abnormal behavior of locators.

$$L_C = \begin{bmatrix} L_{11} & L_{12} & L_{13} & ... & L_{1n} \\ L_{21} & L_{22} & L_{23} & ... & L_{2n} \\ : & : & : & ... & : \\ L_{n1} & L_{n2} & L_{n3} & ... & L_{nn} \end{bmatrix}$$

Here,

$$L_{ij} = \begin{cases} 0, & when\ L_i\ is\ not\ in\ the\ list\ of\ C(L_i)\ i.e.;\ L_j \notin C(L_i) \\ 1, & when\ L_j \in C(L_i) \end{cases}$$

For making the conflicting set C (L_i), locator L_i can use either distance formula or time of arrival (ToA).

Algorithm 1 Conflicting Set Matrix

1: **for** every receiving beacon message as L_i and L_j **do**
2: **if** $((x_i^2 - x_j^2) + (y_i^2 - y_j^2)) > R_L^2$ **then**
3: $L_C[i][j] \leftarrow 1$;
4: **else if** (a locator violates the Node's self-exclusion property) **then**
5: $L_C[i][j] \leftarrow 1$, $\forall$ pairs of locator who receive the $loc - ACK$ message;
6: **else if** distance using TOA $>R_L$ **then**
7: $L_C[i][j] \leftarrow 1$;
8: **else**
9: $L_C[i][j] \leftarrow 0$;
10: **end if**
11: **end for**

The Algorithm 1, helps to decide which locator counted as a dubious or not. Every locator broadcasts a *hello* message in the network. If a locator receives a *hello* message from outside of its transmission range, then the other end of locator counted

as dubious/conflicted locator for that locator and it can be added into the conflicted set matrix. The same process is repeated for all locators.

4.3 Localization on Attackers

In our scheme, we have taken two cases. In first case we have taken simple form by taking only two attackers and in second case we have generalized it into N-number of wormhole attackers in the network.

A. Wormhole with two attackers in the network

From the conflicting list we see that for the locator $L_i \in D_{R_L}$ (A_2) but $L_i \notin C(L_i)$ then all locators of C (L_i) lie in the D_{R_L} (A_1). Similarly, if $L_i \in D_{R_A}$ (A_1) then all the locators in C (L_i) lie in the D_{R_L} (A_2). Also for the locator $L_i \in C(L_i)$ i.e. $L_i \in D_{R_L}$ $(A_1) \cap D_{R_L}$ (A_2); C (L_i) shows all the locators within D_{R_L} $(A_1) \cup D_{R_L}$ (A_2) region.

From Algorithm 2, we get two sets of conflicting set ($CS_1 and CS_2$) and their corresponding number of conflicted nodes i.e., $count_1$ and $count_2$. With the help of conflicting set we can find the position of both attackers A_1 and A_2 using centroid method.

Location of attacker $A_1(X_{A_1}, Y_{A_1})$,

$$X_{A_1} = \frac{\Sigma x_{L_i \in CS_1}}{count_1} = \frac{x_{L_1} + x_{L_2} + x_{L_3} + x_{L_4} + x_{L_5} + x_{L_{14}}}{6} = \frac{\sum x_{C(L_i \in (D_{R_L}(A_2) - D_{R_L}(A_1)))}}{\sum count(C(L_i))} \quad (4.1)$$

$$Y_{A_1} = \frac{\Sigma y_{L_i \in CS_1}}{count_1} = \frac{y_{L_1} + y_{L_2} + y_{L_3} + y_{L_4} + y_{L_5} + y_{L_{14}}}{6} = \frac{\sum y_{C(L_i \in (D_{R_L}(A_2) - D_{R_L}(A_1))}}{\sum count(C(L_i))} \quad (4.2)$$

Similarly, location of attacker $A_2(X_{A_2}, Y_{A_2})$,

$$X_{A_2} = \frac{\Sigma x_{L_i \in CS_2}}{count_2} = \frac{x_{L_4} + x_{L_5} + x_{L_7} + x_{L_8} + x_{L_{14}}}{5} = \frac{\sum x_{C(L_i \in (D_{R_L}(A_1) - D_{R_L}(A_2)))}}{\sum count(C(L_i))} \quad (4.3)$$

Algorithm 2 Wormhole with two attackers

count$_1$=count$_2$ $\leftarrow$ 0; vector <int> CS$_1$=CS$_2$ $\leftarrow$ ϕ; //CS$_i$ $\leftarrow$ new vector conflicting set of i-type
for i **do**=1.. N // N= number of locators; C (L_i) = conflicting lists of L_i
  if ((C(L_i) $\neq$ ϕ) && (L_i $\notin$ C(L_i)) && (L_i $\notin$ CS$_1$)) **then**
    if C (L_i) $\in$ CS$_2$ **then**
      CS$_1$.push_back(L$_i$);
      count$_1$ +$\leftarrow$ 1;
    end if
    if CS$_2$ == ϕ **then**
      CS$_2$.push_back(C(L$_i$));
      CS$_1$.push_back(L$_i$);
      count$_1$ +$\leftarrow$ 1;
    end if
  end if
end for
CS$_2$ $\leftarrow$ ϕ;
for i **do**=1..N
  if L_C [I] [I] ==1 then // L_i $\in$ C (L_i) **then**
    CS$_1$. push _ back (L_i);
    CS$_2$. push _ back (L_i);
    count$_1$ +$\leftarrow$ 1;
    count$_2$ +$\leftarrow$ 1;
  end if
end for
for i **do**=1.. N
  if (C(L_i) $\neq$ ϕ) && (L_i $\notin$ C(L_i)) && (L_i $\notin$ CS$_2$) **then**
    if C (L_i) $\in$ CS$_1$ **then**
      CS$_2$.push_back(L$_i$);
      count$_2$ +$\leftarrow$ 1;
    end if
  end if
end for

$$Y_{A_2} = \frac{\Sigma y_{L_i \in CS_2}}{count_2} = \frac{y_{L_4} + y_{L_5} + y_{L_7} + y_{L_8} + y_{L_{14}}}{5} = \frac{\sum y_{C(L_i \in (D_{R_L}(A_1) - D_{R_L}(A_2)))}}{\sum count(C(L_i))} \tag{4.4}$$

B. Wormhole with N-attackers in the network

Using this conflicting set matrix (L_C), we can find numbers of wormhole attackers in the network.

Algorithm 3 Wormhole with N-attackers

```
1: Initialize counter←0; vector <int> CS←null;      //CS ← new vector conflicting set
2: for i do=1..N          // N= number of locators; C(L_i) = conflicting list of L_i
3:     if  thenL_C [I] [I] ==1 then      // L_i ∈ C (L_i)
4:         CS. push _ back (C (L_i));
5:         counter +← 2;
6:     end if
7: end for
8: for i do=1.. N
9:     if ( then(C(L_i) ≠ φ) && (L_i ∉ C(L_i)) && C(L_i) ∉ CS) then
10:        counter +← 1;
11:        CS. push _ back (C (L_i))
12:    end if
13: end for
```

In Algorithm 3, counter gives the number of attackers which form the wormhole and a set of conflicted set of locators in the network. We can apply k-means (k = counter) property on the conflicted set (CS) of locators. Finally, we get the estimated position of locators by k-means property.

4.4 Localization on sensor

We have taken two classes of sensor position in the network. First one, when it is under Class 1 wormhole attacks and the second one, when it is under Class 2

wormhole attacks. The Identification scheme $I_{i,j}$ represents Identification scheme of Class i^{th} wormhole attack with j^{th} scheme.

A. Class 1 wormhole attack identification scheme

When the sensor node shows Node's self-exclusion property then the sensor node consider under Class 1 wormhole attack. To identify the V-locators the following identification schemes are,

1. **Identification scheme** $I_{1,1}$: When the sensor is under Class 1 wormhole attack and the sensor node receives three $loc - ACK$ messages for a locator L_i and its conflicting set C $(L_i) \neq \Phi$ and $L_i \in$ C (L_i) then that locator L_i considered as V-locator as well as D-locators. From fig 4.1(a) the sensor node (S) receives three times $loc - ACK$ messages of same locator L_{14}. Hence, L_{14} considered as V-locator as well as a D-locator.

2. **Identification scheme** $I_{1,2}$: When the sensor is under Class 1 wormhole attack and the sensor node receives only one $loc-ACK$ message for a locator L_i where C$(L_i) \neq \phi$ and $L_i \notin (D_{R_L}(A_1) \cup D_{R_L}(A_2))$ then that locator L_i considered as a V-locator e.g., (L_6). If C $(L_i) \neq \phi$ and $L_i \in (D_{R_L}(A_1) \cup D_{R_L}(A_2))$ then that locator L_i is considered as a D-locator e.g., (L_1, L_2, L_7, L_8).

3. **Identification scheme** $I_{1,3}$: When the sensor is under Class 1 wormhole attack and the sensor node receives two $loc - ACK$ messages for a locator L_i but at least one of the route distance is in the range of sensor node then that locator L_i considered as a V-locator as well as a D-locator e.g., (L_3, L_4) otherwise, it is considered as D-locator e.g, (L_5).

The above identification schemes help to find out the differentiation between valid and dubious locators. We collect the valid locators and apply the maximum likelihood estimation method to find out its location.

B. Class 2 wormhole attack identification scheme

From Figure 4.1(b), when the sensor is under Class 2 wormhole attack, only those locators in $D_{R_L}(A_2)$ are D-locators. The following identification schemes work in this case:

1. **Identification scheme** $I_{2,1}$ [13]: Similar to $I_{1,3}$, when the sensor is under Class 2 wormhole attacks, those locators, which violate packet unduplication property are considered as V-locators as well as D-locators where its distance corresponding to response time $\leq R_S$ e.g., L_4.

2. **Identification scheme** $I_{2,2}$ [13]: When the sensor is under a Class 2 wormhole attack and, the distance between two neighboring locators of the sensor which is larger than 2^*R_L, one of the two locators having greater response time is a D-locator while the other is a V-locator. From Figure 4.1(b), the distance between L_2 and L_8 is larger than $2R_L$. Therefore, the sensor determines that the shortest response time locator treated as V-locator(e.g., L_2) and the other is treated as a D-locator (L_8).

3. **Identification scheme** $I_{2,3}$ [13]: The valid locators L_i (from $I_{2,2}$) such that C $(L_i) \neq \phi$ and $L_i \notin$ C (L_i), then $\forall L_j \in C(L_i)$ are $L_j \in L_D$. From Figure 4.1(b), here L_2 is a valid locator and C(L_2)=$\{L_4, L_5, L_7, L_8, L_{14}\}$ and $L_2 \notin$C(L_2), hence all elements of C (L_2) are counted as D-locators (L_D).

4. **Identification scheme** $I_{2,4}$: The dubious locators L_i (from $I_{2,2}$, $I_{2,3}$) such that $L_i \notin$ C(L_i) and C(L_i) $\neq \phi$, then $\forall L_j \in C(L_i)$ are considered as valid locators (i.e. $L_j \in L_V$) so as to the sensor node receives a $loc - ACK$ message for locator L_j. From Figure 4.1(b), for a dubious locator L_8, conflicting set C(L_8)=$\{L_1, L_2, L_3, L_4, L_5, L_{14}\}$ where $L_8 \notin C(L_8)$ and hence the locators L_j in C (L_8) are considered as valid locators so as to the sensor node receives a $loc - ACK$ message for that locators e.g., $\{L_2, L_3\} \in L_V$.

5. **Identification scheme** $I_{2,5}$: Similar to $I_{1,2}$, when the sensor node receives only one $loc-ACK$ message for a locator L_i where C(L_i)$\neq \phi$ and $L_i \notin (D_{R_L}(A_1) \cup D_{R_L}(A_2))$ then that locator L_i considered as a V-locator e.g.,(L_6).

Identification scheme I_3: when the sensor node receives only one $loc-ACK$ message for a locator L_i and its C(L_i) $= \phi$ then such locators are considered as V-locators.

From the above all classification schemes as $I_{1,*}$, $I_{2,*}$ and I_3; we separate the L_V and L_D. We are considering those locators $L_i \in L_V$ and also those locators that have no any conflicting list (from I_3), the locators also considered as L_V; with the help V-locators we can find the location of the sensor.

Using wormhole attack detection and neighboring locators differentiation processes, the sensor can identify the valid locator. Now we can apply Maximum Likelihood Estimation (MLE) method for localization.

C. Maximum Likelihood Estimation (MLE) localization

Let the sensor node got valid distance measurements from m locators. The co-ordinates of the m valid locators are as $\{(x_1, y_1), (x_2, y_2), (x_3, y_3), ..., (x_m, y_m)\}$ and its corresponding distance measurements by RSSI/TOA/TDOA method from the m locators to the sensor are $\{d_1, d_2, d_3, ..., d_m\}$. Let the location of the sensor is $S(x, y)$.

Therefore, from distance formula,

$$\left.\begin{array}{ccccc} (x_1-x)^2 & + & (y_1-y)^2 & = & d_1^2 \\ (x_2-x)^2 & + & (y_2-y)^2 & = & d_2^2 \\ (x_3-x)^2 & + & (y_3-y)^2 & = & d_3^2 \\ \vdots & ... & \vdots & ... & \vdots \\ (x_m-x)^2 & + & (y_m-y)^2 & = & d_m^2 \end{array}\right\} \quad (5)$$

Algorithm 4 Neighboring locators scheme

1: Each locator periodically exchanges beacon messages among its neighboring locators and builds its conflicting set based on the received beacon messages.
2: Each locator replies $loc - ACK$ message including its conflicting set when it receives $loc - REQ$ from the sensor node.
3: **if** *the sensor node violates the properties* {*(A),(B),(C) or (D)*} **then**
4: the sensor node is under wormhole attack
5: **if** *sensor node violates property (A)* **then**
6: the sensor is under Class 1 and applies identification schemes $I_{1,1}$, $I_{1,2}$ and $I_{1,3}$.
7: **else**
8: the sensor is under Class 2 and applies identification schemes $I_{2,1}$, $I_{2,2}$, $I_{2,3}$, $I_{2,4}$, $I_{2,5}$
9: **end if**
10: **end if**
11: The sensor node scan the identification scheme I_3.
12: for every locator L_i, separates L_V and L_D.

In equation (5), subtracts the last expression from above every expression.

$$\mathbf{x_1^2 - x_m^2 + y_1^2 - y_m^2 - d_1^2 + d_m^2} = [\mathbf{2x(x_1 - x_m) + 2y(y_1 - y_m)}]$$

$$\mathbf{x_2^2 - x_m^2 + y_2^2 - y_m^2 - d_2^2 + d_m^2} = [\mathbf{2x(x_2 - x_m) + 2y(y_2 - y_m)}]$$

$$\mathbf{x_3^2 - x_m^2 + y_3^2 - y_m^2 - d_3^2 + d_m^2} = [\mathbf{2x(x_3 - x_m) + 2y(y_3 - y_m)}]$$

:

The above equation can be represented as a linear equation $MP = N$. Where,

$$M = \begin{bmatrix} 2(x_1 - x_m) & 2(y_1 - y_m) \\ 2(x_2 - x_m) & 2(y_2 - y_m) \\ 2(x_3 - x_m) & 2(y_3 - y_m) \\ : & : \\ 2(x_{m-1} - x_m) & 2(y_{m-1} - y_m) \end{bmatrix}$$

$$N = \begin{bmatrix} \mathbf{x_1^2 - x_m^2 + y_1^2 - y_m^2 - d_1^2 + d_m^2} \\ \mathbf{x_2^2 - x_m^2 + y_2^2 - y_m^2 - d_2^2 + d_m^2} \\ \mathbf{x_3^2 - x_m^2 + y_3^2 - y_m^2 - d_3^2 + d_m^2} \\ \mathbf{.....} \\ \mathbf{x_{m-1}^2 - x_m^2 + y_{m-1}^2 - y_m^2 - d_{m-1}^2 + d_m^2} \end{bmatrix}$$

$$P = \begin{bmatrix} x \\ y \end{bmatrix}$$

This can be calculated as -

$$P = (M^T M)^{-1} M^T N \tag{6}$$

Finally, we get the location of the sensor node $S(x, y)$ from the equation (6).

4.4.1 Analytical study of proposed scheme

In our proposed scheme, we assume that all types of sensors are static in nature. Each locator broadcasts beacon messages and makes a conflicting set matrix (L_C) and it can be achieve by Algorithm 1. Algorithm 2 separates two sets of conflicted locators, so we can apply centroid formula for finding the location of attackers when the network is threatened by only two attackers. When the network threatened by more than two attackers simultaneously then use Algorithm 3 to find out the number of attackers in the whole networks. After we apply k-means clustering method to find out locations of attackers.

In second stage, we apply sensor identification schemes $I_{1,1}$, $I_{1,2}$, $I_{1,3}$ for Class 1 wormhole attacks and $I_{2,1}$, $I_{2,2}$, $I_{2,3}$, $I_{2,4}$, $I_{2,5}$ and I_3 for Class 2 wormhole attacks. With the help these schemes we separate the valid locators against dubious locators and apply the MLE method to find out the sensor location.

Correctness

An algorithm is correct for a problem if it is correct for all instances of the problem. In our research, locators are uniformly distributed in the wireless sensor networks. Each locators sends the beacon messages to the neighbors and builds a conflict set matrix (L_C). The matrix helps us to decide the attacker's position. Since the conflicting sets of locators uniformly distributed around the attackers in a circular region, we can also say that the attackers are in the central position of the conflicted locators and hence attackers are the centroid of the conflicted locators. Equations (1), (2), (3) and (4) are the coordinate locations of the attackers.

On the other hand, we need at least three valid locators to find out the co-ordinate position of the sensor node in a randomly distributed network and apply equally (6) and the neighboring locators scheme algorithm. Let the coordinates of the N

valid locators are as $\{(x_1, y_1), (x_2, y_2), (x_3, y_3), ..., (x_N, y_N)\}$ and the corresponding measured distance from the sensor node to m locators are $\{d_1, d_2, d_3, ..., d_N\}$. Let the location of the sensor is S(x, y).

The root mean square (RMS) error of the sensor location estimation is,
$\delta^2 = \sum_{i=1}^{N} [d_i - \sqrt{(x - x_i)^2 + (y - y_i)^2}]^2 / N$

Completeness

An algorithm is complete for a problem if it completes all parts of the problem. In our proposed, we consider three types of sensor nodes: locators, sensors and attackers in the wireless sensor networks. We know that locators are already position-aware nodes (anchors). Using Algorithm 1, Algorithm 2 and Algorithm 3 we determine the location of attackers. For sensor node localization, we apply sensor identification schemes $I_{1,1}$, $I_{1,2}$, $I_{1,3}$ for Class 1 wormhole attacks and $I_{2,1}$, $I_{2,2}$, $I_{2,3}$, $I_{2,4}$, $I_{2,5}$ and I_3 for Class 2 wormhole attacks and apply MLE method. So, in our proposed scheme we got the position of all types of sensor nodes in network.

Message Transmission

Each locator broadcasts the beacon messages to the neighbors and builds a conflict set matrix (L_C). Therefore, to find out the attacker's position there are N*(N-1) beacon messages transmitted along the network. Once the conflicting sets matrix L_C created, to find out the sensor node location, sensor node broadcasts $loc - REQ$ message to its neighboring locators. In this scheme, total messages transferred in the network to find out the attacker and sensor node's position are (N*(N-1) + n).

Complexity

Communication cost

In the network each locators broadcasts the beacon messages to each other. Let N be the number of locators in the network. Since each locators broadcasts the beacon messages to each other, therefore at most ${}^{N}C_2$ communication among locators. Therefore, communication cost is $O(N^2)$.

Space complexity

Let N be the number of locators. From Algorithm 1, we got the conflicting set matrix (L_C). Since matrix L_C has a dimension of NxN. So its space complexity is $O(N^2)$.

Chapter 5

Simulation and results

Chapter 5

Simulation and results

There are three different types of sensor nodes : sensors, locators and attackers in the network. The transmission ranges of sensor, locator and attacker are $R_S = 27m$, $R_L = 28.3m$ and $R_A = 30m$ respectively with $-5dBm$ transmission output sensitivity. We deployed 39 sensor nodes in the network of 100x100 m^2 area. We deployed only $N = 36$ locators in grid view structure in the network. Rest *two* attackers and *one* sensor node deployed random in nature in the network. So, for the energy points of view this approach is more efficient than others because the scheme requires only $4 - 5\%$ locators to find the location of the sensor node and the attackers. Let the length of the wormhole link is ($L_{W_{12}}$). It gives more accurate results for localization and it is the most helpful when $\frac{L_{W_{12}}}{R_A} \leq 2$, but for $\frac{L_{W_{12}}}{R_A} > 2$, it is common to other approaches.

In Table 5.1, we gave network simulation environment and in Figure 5.1, we depicted the pictorial view of network structure having 36 locators which arranged in grid structure view; two attackers (nodeID: 36, 37) deployed randomly; one out of 1000 sensors (nodeID: 38) also deployed random.

We get the table of conflicted set matrix (L_C) when the network threatened by A_1 (32, 34) and A_2 (62, 64) from Figure 5.2.

Simulation time	150s
Deployment of network	100x100 m^2
Deployment of locators	6x6 grid structure
Deployment of attackers and sensors	random
Transmission output sensitivity	-5dBm
Initial energy	18720 J
Number of sensors	39

Table 5.1: Simulation parameters in Castalia 3.2

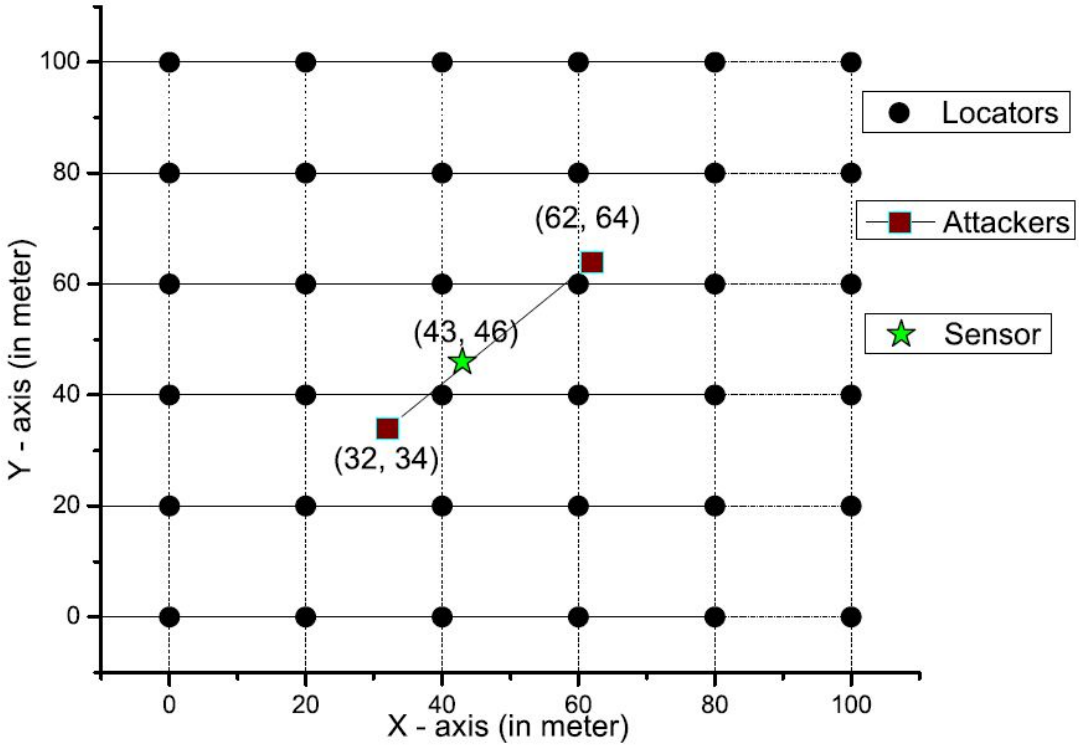

Figure 5.1: Nodes' deployment in grid view structure in the WSNs

In the L_C table,

$$L_C[i][j] = \begin{cases} 1, & \text{nodeID (j) conflicted with nodeID (i) where i, j} = 0..36 \\ 0, & \text{no any confliction} \end{cases}$$

Now, we can find out the position of attackers using Algorithm 2: wormhole with two attackers' position and equations (1), (2), (3), (4).

In Figure 5.3, we can see the position difference of the attacker from its actual position. On an average, we got a relation between actual and estimated position of the attacker to our network deployment. From Figure 5.4,
estimated position of the attacker = actual position of the attacker ± 3.2367 m (approx.)

In Figure 5.5, we can see the position difference of the attacker from its actual position. On an average, we got a relation between actual and estimated position of the sensor to our network deployment. From Figure 5.6,
estimated position of the sensor = actual position of sensor ± 0.2199 m (approx.)

In Figure 5.7, we compare our result to SLAW [13] to find out the probability of wormhole attacks using TOA method. Our result is comparatively beneficial when the length of the wormhole link ≤ 2 otherwise it is common to SLAW approach.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	1	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	1	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 5.2: Tabular form of L_C (36 x 36) when A_1 (32,34) and A_2 (62,64) in the network

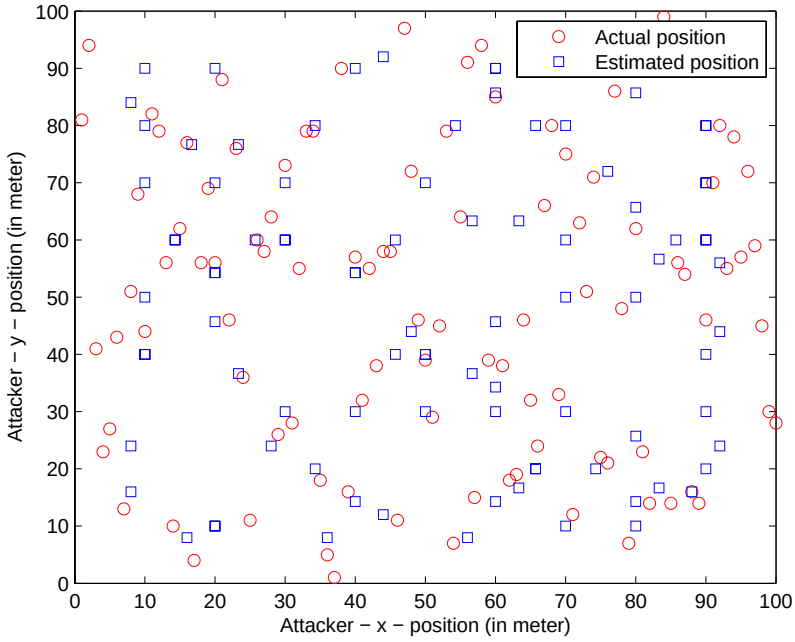

Figure 5.3: Comparisons of actual and estimated position of attackers

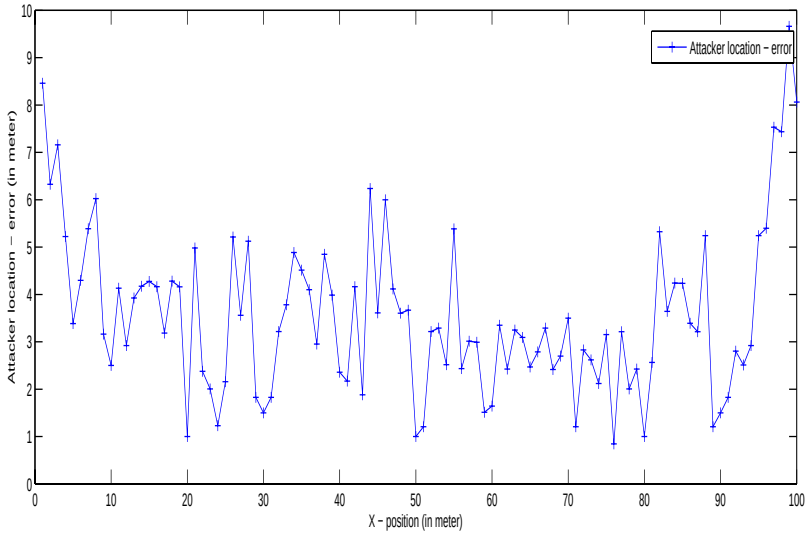

Figure 5.4: Radial error in attacker from its actual position

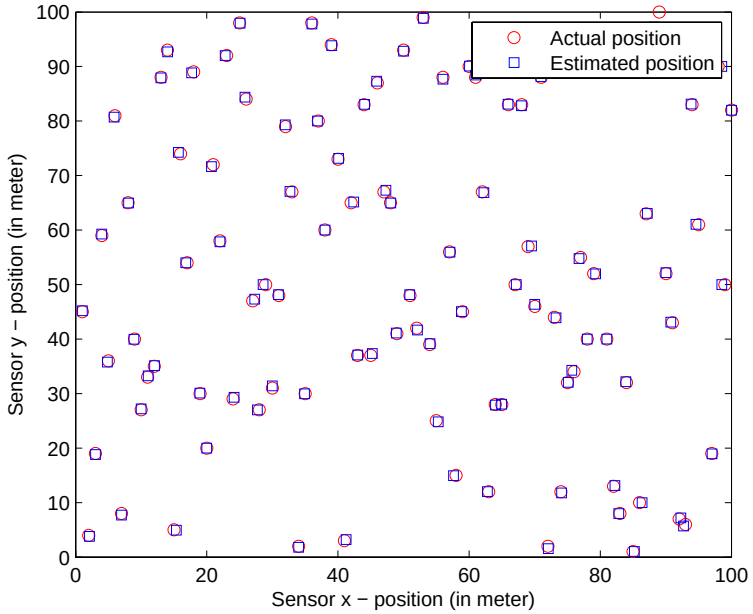

Figure 5.5: Comparisons of actual and estimated position of sensors

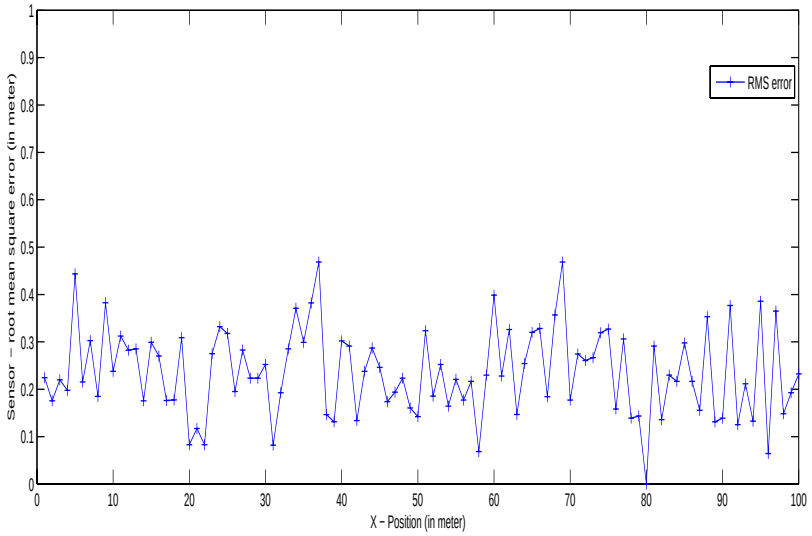

Figure 5.6: Radial error in sensor from its actual position

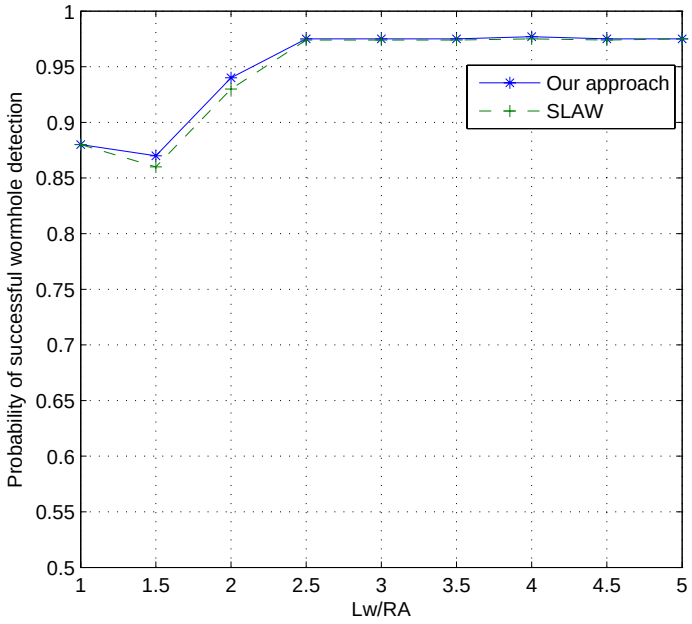

Figure 5.7: TOA method

Chapter 6

Conclusions and future work

Chapter 6

Conclusions and future work

The proposed scheme is a secure and efficient localization technique against wormhole attack in wireless sensor networks. We know that localization is itself an information and it helps in the routing protocol, target tracking etc. Here we applied the conflicting set localization scheme and get the proper position of the sensor node and also, the attacker's position in the references of locators. In this paper, the attacker localization scheme is applicable for any number of attackers in the network. Once we get the location of the attackers we can take a decision to disable/destroy/control the attacker in the network so that it can't harm or misguide the network. Our scheme gives the secure equations in two dimensions networks but, it is also applicable in three dimensional spaces. We consider, all types of nodes in the network are static in nature. If we assume, the nodes in the network are stable during the localization then this scheme is also applicable for the dynamic nature of nodes. A challenging task to apply the localization when the network is attacked by more than two attackers simultaneously. For this problem, we apply the attacker localization scheme to resolve the attackers and then apply neighboring locators differentiation process. The other solution, we can apply wormhole attack detection process and apply separate localization process one by one.

Bibliography

[1] Majid Meghdadi, Suat Ozdemir and Inan Guler; "A Survey of Wormhole-based Attacks and their countermeasures in Wireless Sensor Networks"; IETE tech. reveiw, vol. 28(2), Mar.-Apr., 2011.

[2] Jin Guo; Zhi-Yong Lei; "A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification"; IEEE (3^{rd} conference), pages : 564-568, 2011

[3] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, and Xiangke Liao; "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks"; IEEE/ACM Tranc., 2011

[4] Azzedine Boukerche, Eduardo F. Nakamura et al.; "Secure Localization Algorithms for Wireless Sensor Networks"; IEEE pub., Apr., 2008

[5] J. Aspnes, T. Eren, D.K. Goldenberg, A. S. Morse, Y. R. Yang and B. D. O.; "A Theory of Network Localization";IEEE Tranc. Jul, 2004

[6] Mingbo Zhao, Sergio D. Servetto; "An Analysis of the Maximum Likelihood Estimator for Localization Problems"; IEEE(C), Oct., 2005.

[7] Junfeng Wu, Honglong Chen, Wei Lou, Zhibo Wang, and Zhi Wang; "Label-Based DV-Hop Localization Against Wormhole Attacks in Wireless Sensor Networks"; IEEE (5^{th} conference), 2010

[8] Xiaomeng Ban, R. Sarkar, Jie Gao; "Local Connectivity Tests to Identify Wormholes in Wireless Networks"; ACM New York, USA(C), 2011

[9] Minsu Huang, Siyuan Chena and Yu Wang; "Minimum cost localization problem in wireless sensor networks"; ELSEVIER pub., Aug., 2010

[10] TIAN Bin, LI Qi, YANG Yi-Xian, LI Dong, XIN Yang; "A ranging based scheme for detecting the wormhole attack in wireless sensor networks"; ScienceDirect Journal, vol. 19(1): 6-10, June, 2012.

[11] Zorana Bankovic, David Fraga, Jos M. Moya and Juan Carlos Vallejo; "Detecting Unknown Attacks in Wireless Sensor Networks That Contain Mobile Nodes"; Sensors(Basel, Switzerland) MDPI pub., vol 12(8): 1083410850, Aug, 2012.

[12] Priya Maidamwar and Nekita Chavhan; "A survey on Security issues to detect wormhole attack in wireless sensor network"; IJANS vol. 2(4), Oct., 2012

[13] H. Chen,W. Lou, and Z.Wang; "SLAW: A Secure Localization Aproach Against Wormhole Attacks Using Conflicting Sets"; Technical Report Dept. of Computing, The Hong Kong Polytechnic University, 2010

[14] H. Chen, W. Lou, X. Sun, and Z. Wang; "A Secure Localization Approach Against Wormhole Attacks Using Distance Consistency"; Eurasip Journal on Wireless Communications and Networking, Spacial Issue on Wireless Network Algorithms, Systems and Applications, 2010

[15] H. Chen, W. Lou, and Z. Wang; "Conflicting-Set-Based Wormhole Attack Resistant Localization in Wireless Sensor Networks"; Ubiquitous Intelligence and Computing (UIC), 6^{th} conference, 2009

[16] Murad A. Rassam, M.A. Maarof and Anazida Zainal; "A Survey of Intrusion Detection Schemes in Wireless Sensor Networks"; American Journal of Applied Sciences, vol. 9(10): 1636-1652, 2012

[17] Ting Zhang, Jingsha He and Hong Yu; "Secure Localization in Wireless Sensor Networks with Mobile Beacons"; International Journal of Distributed Sensor Networks, Article ID 732381, 11 pages, 2012

[18] Samira Afzal; "A Review of Localization Techniques for Wireless Sensor Networks"; JBASR vol. 2(8): 7795-7801, 2012

[19] A. Srinivasan and J. Wu; "A Survey on Secure Localization in Wireless Sensor Networks"; Encyclopedia of Wireless and Mobile Communications, B. Furht (Ed.), CRC Press, Taylor and Francis Group, 2008

[20] Loukas Lazos and Radha Poovendran; "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks"; WiSe'04, Oct., 2004

[21] Kazem Sohraby, Daniel Minoli, Taieb Znati; "Wireless Sensor Networks"; Wiley pub. ($2^{nd}ed.$), pages : 01-69, 2010

[22] Amitangshu Pal; "Localization Algorithms in Wireless Sensor Networks: Current Approaches and Future Challenges"; Network Protocols and Algorithms (Macrothink Institute, Las Vegas), vol. 2(1): 1943-3581, 2010