

# **SECURE LOCALIZATION ALGORITHM TO DETECT SYBIL ATTACK IN WIRELESS SENSOR NETWORKS**



By

**Fakiha Khan**

**2019-NUST-MS-IS-317720**

Supervisor

**Dr. Mehdi Hussain**

**Department of Computing**

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science in Information Security (MS IS)

In

School of Electrical Engineering and Computer Science,  
National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(July 2023)

## THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "SECURE LOCALIZATION ALGORITHM TO DETECT SYBIL ATTACK IN WIRELESS SENSOR NETWORKS" written by FAKIHA KHAN, (Registration No 00000317720), of SEECS has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: \_\_\_\_\_  \_\_\_\_\_

Name of Advisor: Dr. Mehdi Hussain

Date: 20-Jul-2023

HoD/Associate Dean: \_\_\_\_\_

Date: \_\_\_\_\_

Signature (Dean/Principal): \_\_\_\_\_

Date: \_\_\_\_\_

## Approval

It is certified that the contents and form of the thesis entitled "SECURE LOCALIZATION ALGORITHM TO DETECT SYBIL ATTACK IN WIRELESS SENSOR NETWORKS" submitted by FAKIHA KHAN have been found satisfactory for the requirement of the degree

Advisor : Dr. Mehdi Hussain

Signature:  \_\_\_\_\_

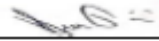
Date: 20-Jul-2023

Committee Member 1:Dr. Muhammad Zeeshan

Signature:  \_\_\_\_\_

21-Jul-2023

Committee Member 2:Dr. Hasan Tahir

Signature:  \_\_\_\_\_

Date: 20-Jul-2023

Signature: \_\_\_\_\_

Date: \_\_\_\_\_


# Dedication

This thesis is dedicated to my mother for her countless prayers and love.

## Certificate of Originality

I hereby declare that this submission titled "SECURE LOCALIZATION ALGORITHM TO DETECT SYBIL ATTACK IN WIRELESS SENSOR NETWORKS" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: FAKIHA KHAN

Student Signature: 

# Acknowledgment

First and foremost, I am thankful to Allah Almighty for continuously bestowing blessings upon me throughout my life.

I would like to express my heartfelt appreciation to my research supervisor, Dr. Mehdi Hussain, for his unwavering guidance and assistance throughout my research journey. He has been instrumental in providing direction whenever I faced challenges.

I am thankful to my parents for their prayers and love.

# Table of Contents

THESIS ACCEPTANCE CERTIFICATE .....	i
APPROVAL .....	ii
Dedication.....	iii
Certificate of Originality.....	iv
Acknowledgment .....	v
Table of Contents.....	vi
List of Abbreviations .....	ix
List of Tables .....	xi
List of Figures.....	xii
Abstract.....	xiii
1. Introduction .....	1
<b>1.1 Background</b> .....	1
<b>1.2 Localization</b> .....	4
<b>1.3 Motivation</b> .....	5
<b>1.4 Problem Statement</b> .....	6
<b>1.5 Thesis Contribution</b> .....	7
<b>1.6 Thesis Organization</b> .....	8
<b>1.7 Summary</b> .....	9
2. Literature Review .....	10
<b>2.1 Introduction</b> .....	10
<b>2.2 Localization Algorithms</b> .....	11
<b>2.3 Secure Localization Algorithms</b> .....	17

2.4	<b>Summary</b> .....	29
3.	<b>Methodology</b> .....	30
3.1	<b>Problem Identification</b> .....	30
3.2	<b>Proposed Methodology</b> .....	33
3.2.1	<b>Pre-detection Assessment of Network</b> .....	34
3.2.2	<b>Detection of Sybil Nodes</b> .....	36
3.2.3	<b>Unknown Node Localization by Robust Maximum Likelihood</b> .....	40
4.	<b>Experimental Setup</b> .....	44
4.1	<b>Experimental Setup</b> .....	44
4.1.1	<b>System Model</b> .....	44
4.2	<b>Evaluation Metrics</b> .....	49
4.2.1	<b>RMSE</b> .....	49
4.2.2	<b>Probability of Detection</b> .....	50
4.2.3	<b>Probability of Correct Detection</b> .....	51
4.2.4	<b>Probability of False Detection</b> .....	51
4.2.5	<b>Probability of No Detection</b> .....	52
4.2.6	<b>Convergence Rate</b> .....	52
5.	<b>Analysis and Discussion</b> .....	53
5.1	<b>Comparative Analysis</b> .....	53
5.1.1	<b>RMSE Analysis for Attacker Model 1</b> .....	54
5.1.2	<b>Probability of Detection Analysis for Attacker Model 1</b> .....	56
5.1.3	<b>RMSE Analysis for Attacker Model 2</b> .....	60
5.1.4	<b>Probability of Detection Analysis for Attacker Model 2</b> .....	61
5.1.5	<b>RMSE Analysis for Failed Detection to Check Robustness</b> .....	64
5.1.6	<b>Convergence Rate Comparison</b> .....	64



<b>5.1.7 Summary</b> .....	66
<b>6. Conclusion</b> .....	67
<b>6.1 Key Findings</b> .....	67
<b>6.2 Limitations</b> .....	68
<b>6.3 Future Directions</b> .....	68
<b>Bibliography</b> .....	70

# List of Abbreviations

WSN	Wireless Sensor Networks
IoT	Internet Of Things
DDOS	Distributed Denial-Of-Service
SYN	Synchronization
UDP	User Datagram Protocol
GPS	Global Positioning System
TOA	Time Of Arrival
TDOA	Time Difference Of Arrival
AOA	Angle Of Arrival
RSS	Received Signal Strength
RFID	Radio Frequency Identification
DV	Distance Vector
GTRS	Generalized Trust Region Subproblem
ML	Maximum Likelihood
CRLB	Cramer Rao Lower Bound
NLOS	Non-Line Of Sight
LOS	Line of Sight
VBL	Variational Bayesian Localization
MCB	Monte Carlo Boxed Localization

MCL	Monte Carlo Localization
RSSI	Received Signal Strength Indicator
WCM	Weighted Central Mass
IP	Intersection Points
GLRT	Generalized Likelihood Ratio Test
NLWLS	Non-Linear Weighted Least Squares Problem
LOC	Law of Cosines
AWGN	Additive White Gaussian Noise
MDS	Multi-Dimensional Similarity
ADMM	Alternating Direction Method of Multipliers
EVD	Eigen Value Decomposition
SR-IRLS	Squared Range Iterative Reweighted Least Squares

# List of Tables

Table 1: Experiment Tool .....	44
Table 2: Environment Parameters.....	48
Table 3: Performance Complexity Comparison .....	65

# List of Figures

Figure 1: Sybil Attack.....	3
Figure 2: Multilateration.....	13
Figure 3: Trilateration.....	14
Figure 4: Enlargement Attack.....	31
Figure 5: Reduction Attack.....	32
Figure 6: Proposed System Flowchart.....	33
Figure 7: Desired Network.....	45
Figure 8: Attacker Model 1 Reduction Attack.....	46
Figure 9: Inaccurate unknown node position in the presence of attackers.....	47
Figure 10: Accurate Estimate by Robust Localization.....	48
Figure 11: RMSE Comparison 2 Attackers.....	54
Figure 12: RMSE Comparison with LOC_GTRS for 2 Attackers.....	55
Figure 13: RMSE Comparison with LOC_GTRS for 3 Attackers.....	56
Figure 14: Probability of Detection Bar Chart with 2 Attackers and 4 Honest Nodes.....	57
Figure 15: Probability of Detection Bar Chart with 2 Attackers and 5 Honest Nodes.....	57
Figure 16: Probability of Detection Bar Chart with 2 Attackers and 6 Honest Nodes.....	58
Figure 17: Probability of Detection Bar Chart with 3 Attackers and 4 Honest Nodes.....	59
Figure 18: Probability of Detection Bar Chart with 3 Attackers and 5 Honest Nodes.....	59
Figure 19: RMSE Comparison for 3 Attackers.....	60
Figure 20: RMSE Comparison with LOC_GTRS for 2 Attackers.....	60
Figure 21: RMSE Comparison with LOC_GTRS for 3 Attackers.....	61
Figure 22: Probability of Detection Bar Chart with 2 Attackers and 4 Honest Nodes.....	62
Figure 23: Probability of Detection Bar Chart with 3 Attackers and 6 Honest Nodes.....	62
Figure 24: Probability of Detection Bar Chart with 2 Attackers and 8 Honest Nodes.....	63
Figure 25: Robustness Check of Estimation.....	64

# Abstract

Wireless sensor networks (WSNs) have revolutionized surveillance and monitoring applications by offering remote control and regulation capabilities. In most applications, networks utilize mobile nodes and rely on localization techniques to track the nodes' positions and movements. However, ensuring the security of the entire network poses a critical challenge. A single malicious node pretending to be another can wreak havoc and compromise the entire system.

To tackle the presence of malicious nodes, this research presents a novel secure localization algorithm designed to estimate the positions of unknown mobile sensors in the presence of multiple coordinated Sybil nodes, while also detecting these malicious nodes. The research aims to provide a robust system that can withstand the rigors of real-world applications. The algorithm accomplishes this by initially evaluating the network's geometric characteristics and unknown node location by time of arrival (TOA) measurements, followed by iterative detection employing the Generalized Likelihood Ratio Test as a mathematical framework. Next, infectious nodes are eliminated from the network, and estimation is performed utilizing the Geman McClure cost function. The final estimation guarantees resilience, facilitating precise localization even in noisy environments and in scenarios where not all malicious nodes are detected.

The algorithm's performance is assessed by analyzing Root Mean Square Error (RMSE) and the probability of correct detections for different network states and considering two types of attacker models, those capable of exclusively performing enlargement or reduction attacks, as well as attackers capable of executing both attacks. The algorithm demonstrates a high probability of detection, surpassing 0.95, for attack intensities greater than 15m, while achieving a lower Root Mean Square Error (RMSE) compared to localization systems reported in the literature. The proposed algorithm's convergence is assessed by comparing it with existing literature, thereby affirming its practicality in WSN environments. The system can be improved by extending the capability to detect and prevent attacks other than enlargement and reduction attacks and improving the detection rate at low attack intensity.

Keywords: localization, Wireless Sensor Networks, attacker detection

# 1. Introduction

## 1.1 Background

Wireless Sensor Network (WSN) is an indispensable part of the Internet of Things (IoT) [1] that has attracted a significant number of IoT applications in military, commercial, and healthcare industries due to its affordability, scalability, and versatility. WSN is a network composed of small-sized devices called sensor nodes which are self-configured and spatially distributed. The network is designed to be cost-effective, low-power, and capable of collecting and transmitting data wirelessly.

In the healthcare sector, WSNs are utilized for remote examination of patients, allowing real-time monitoring of patients' vitals' conditions like sugar level, blood pressure, and heart rate. By equipping objects with wireless sensors, engineers and IT professionals can monitor the location, condition, and usage patterns of equipment and supplies in real time. This helps streamline operations, optimize inventory levels, and prevent loss or theft. In industrial settings, WSNs are used in asset tracking and inventory management that optimize operations. The versatility and flexibility of WSNs make them essential tools for engineers and IT professionals, empowering them to optimize processes, make informed decisions, and enhance performance and security in their respective fields. All the applications above require that the WSN be secure i.e., it should ensure confidentiality, integrity, and availability. Security is a key consideration in contemporary wireless network environments.

Attacks on WSNs can be classified as active and passive [2], protocol-stack-based attacks[3], or attacks compromising a specific aspect of security. Classifying attacks based on the layer in the protocol stack is a holistic approach as it is a relatively technical classification. Mentioned below are attacks on WSNs specific to each protocol stack layer.

At the physical layer, WSNs are susceptible to jamming attacks [4], compromised node attacks [5], and replication attacks [6]. Jamming attacks aim to target the availability of legitimate nodes by interfering with the communication channel. A Compromised Node Attack is when an attacker gains unauthorized access to a legitimate node or device within a network to exploit it for control, gathering sensitive information, further attacks, or disruption of network operations. The attacker can gain access to the node through various means such as exploiting vulnerabilities, password cracking, social engineering, or malware. A Replication Attack involves the unauthorized duplication or cloning of a legitimate node within a network. The attacker copies the characteristics and behavior of a legitimate node, including its identifiers, credentials, or cryptographic keys, to create replicas, which are then used to carry out malicious activities such as distributed denial-of-service (DDoS) attacks, identity theft, or network flooding.

At the data link layer, WSN is susceptible to denial of sleep attack [7]. An attacker in a Denial-of-sleep attack prevents sensor nodes from entering a sleep state and attempts to rapidly deplete the power supply of the nodes. This can decrease the lifespan of the nodes and even damage network communications. While other attacks, such as Jamming and flooding attacks, can also consume the energy of the nodes, Denial-of-sleep is a particularly devious attack that continuously keeps the node in an active state, thus draining the battery more quickly.



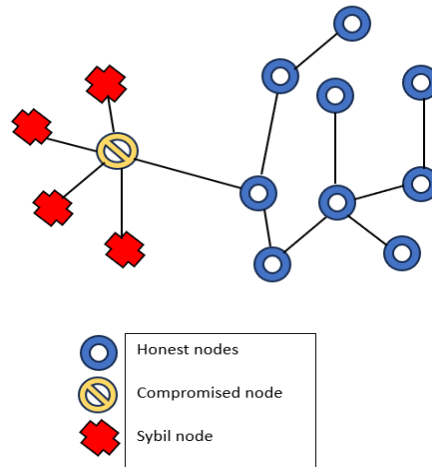


Figure 1: Sybil Attack

Network layer attacks on WSNs include Sybil attack [8], selective forwarding attack [9], wormhole attack [10], and sinkhole attack [11]. In a Sybil attack as illustrated in Figure 1, an adversary generates several fake identities or nodes to gain control over the system or alter its operations. The attacker aims to exploit the trust in a network by generating multiple fraudulent identities.

In a selective forwarding attack, nodes do not fulfill their responsibility of forwarding traffic for other nodes and drop some packets. This makes it harder to detect. If the compromised node is presently receiving dense traffic packets, the attack causes a lot of harm as compared to the compromised node receiving a very limited number of packets. In a Wormhole attack, the attacker sets up two malicious systems that communicate with each other via covert communication point-to-point channel. This enables the attacker to receive the data faster and by effectively bypassing the network.

A sinkhole attack is where the attacker changes the course of the network traffic from its intended destination to a malicious end, known as the sinkhole. The attacker takes advantage of a vulnerability in the routing protocol to redirect the traffic.

The transport layer is exposed to desynchronization attacks & Transmission Control Protocol (TCP) Synchronization SYN flooding and User Datagram Protocol (UDP) flooding attacks. An attacker forges the transport layer datagrams with unnecessary sequence numbers or flags in the de-synchronization attack. The receiver cannot reassemble the datagrams at its end and requests retransmission. When the sensor node receives these datagrams, it will retransmit the lost packets. This will result in retransmission timeouts and increased latency. In a TCP SYN flooding attack, the attacker floods the victim with numerous connection establishment requests i.e., TCP SYN messages. Upon receiving these requests' messages, the victim sends acknowledgment packets and waits for the connection thus occupying network resources inefficiently.

At the Application layer, WSNs are exposed to remote code execution. The attacker inserts a malicious code which may result in a compromise of the network.

## **1.2 Localization**

Localization is a technique to calculate the position of an unknown target. Localization algorithms are employed to estimate the positions of unknown target nodes based on measurements of various parameters such as signal strength, time of flight, angle of arrival, or time difference of arrival or hop count.

It involves estimating the spatial coordinates of sensor nodes in each environment without relying on external infrastructure like GPS. Localization can be performed by angle of arrival, time of arrival, signal strength, etc.

## 1.3 Motivation

Most Wireless sensor applications involve monitoring and tracking where it is crucial to know the geographic position of the nodes. Although each sensor has limited capabilities, when a big WSN is implemented, it can carry out many complex tasks in a range of applications like management and regulation in environmental, agricultural, and industrial settings. An example of this is in agriculture where WSNs can reduce costs and environmental impact by only irrigating and fertilizing where necessary [12]. In recent years, there has been research to minimize the damage that is caused by natural disasters such as volcanic eruptions [13], floods, earthquakes, landslides, forest fires, cyclones, and tsunamis by using sensor networks [14].

Having the ability to recognize the precise positions of the nodes allows the collected sensor data to be associated with specific areas, resulting in more accurate analysis and better decision-making.

Moreover, localization is necessary for network management tasks. With knowledge of the node locations, network administrators can allocate resources more efficiently, plan node deployments, and configure communication parameters. This helps with routing, data aggregation, and energy management, ultimately improving the performance and longevity of the network.

Localization plays a role in finding the exact positions of the nodes to ensure adequate coverage and connectivity within the network. By doing this, it becomes possible to design a deployment plan that meets the sensing coverage needs. Localization data can also be used to spot any coverage holes and relocate or add additional nodes to improve the network's connectivity and performance. Localization can also help to detect and localize any faults or errors within the network. Knowing the exact positions of the nodes lets us recognize any malicious activity.

The utilization of localization algorithms in wireless sensor networks is hindered by a variety of difficulties. Notable among these are: limited resources, communication impediments, precision and accuracy issues, scalability troubles, dynamic topology challenges, harsh environment complications, and security and privacy considerations. To overcome these obstructions, a localization algorithm that is both robust and energy efficient must be developed to address the resource limitations, accuracy requirements, scalability, dynamic network environment, and security needs of wireless sensor networks.

## **1.4 Problem Statement**

Sybil attack ravages Wireless Sensor Networks (WSNs), leaving chaos and destruction in their wake. By creating a network of counterfeit personas, the attacker gains the power to manipulate data aggregation, manipulate routing paths, and exploit valuable network resources. The consequences of such attacks are profound. Legitimate nodes face communication disruptions as the imposter interferes with data exchange. The integrity of transmitted data is compromised and tainted by the injection of falsified information. The attacker consumes network resources, leading to resource depletion and degradation of network performance.

Moreover, the imposter evades authentication and authorization mechanisms, compromising the overall security of the network. The resilience and trustworthiness of the WSN are severely jeopardized. To combat the Sybil menace, it is imperative to implement effective mitigation strategies and detection mechanisms to safeguard the network from these malicious attacks.

While there exist, numerous techniques aimed at securing WSNs from a Sybil attack, they often come at a price, the need for additional hardware, and computationally demanding authentication

and integrity schemes. These formidable defenses, while effective in traditional settings, prove to be impractical within the resource-constrained realm of WSNs. Given the vast array of applications for Wireless Sensor Networks (WSNs) in critical and disastrous scenarios, it is crucial to develop robust mechanisms for detecting and mitigating a Sybil attack. This research aims to formulate a secure and robust localization system that ensures WSN security in mobile adversarial environments in the presence of coordinated attacks such as the Sybil attack keeping in view the computational capacity and limitations of WSN nodes.

## **1.5 Thesis Contribution**

Based on the problem statement, a novel solution to secure the WSN has been proposed that detects the attacker nodes in the network and localizes unknown nodes in a noisy environment. The contribution of the thesis is as follows:

- Formulation of a localization system that estimates the position of an unknown node in a noisy environment.
- A Sybil node detection system to detect the malicious or compromised node performing coordinated enlargement or reduction attack.
- A realistic WSN-based solution that does not make unrealistic assumptions about the network and aims for light-weighted calculation.

## 1.6 Thesis Organization

The first chapter provides the research introduction provides an overview that encompasses the necessary insights into the concepts and terminologies essential for comprehending the research, the motivation behind the research, the problem statement, and the objectives of the research.

Chapter 2 provides a comprehensive exploration of the literature regarding defense mechanisms against attacks in WSNs and localization techniques to calculate the position of an unknown node in WSNs. This includes an in-depth study of the merits and limitations of different localization techniques that lay the foundation for the proposed research.

Chapter 3 elucidates the methodology employed in this study. It delineates the approach taken to design, develop, and evaluate the proposed localization technique. The chapter provides the frameworks utilized to ensure a robust localization system suitable for WSNs.

In Chapter 4 and chapter 5, the experimental setup and the analysis is presented. This encompasses a detailed explanation of the assumptions made and the security analysis of the system. Furthermore, a comparative analysis is conducted to underscore the profound significance of the research about the prevailing literature. By juxtaposing the proposed work with existing studies, a comprehensive evaluation is presented, highlighting the novel contributions and advancements made by this research. This comparative analysis serves to emphasize the unique value and relevance of the proposed research in the broader academic landscape.

Finally, the last chapter summarizes the main contributions, findings, and insights derived from the study. Moreover, within this chapter, attention is directed towards potential avenues for future work, providing valuable recommendations to further enhance the proposed scheme and

effectively mitigate any identified limitations. These recommendations serve as a guide for future researchers and practitioners to explore new possibilities, refine the existing framework, and expand upon its capabilities.

## **1.7 Summary**

This chapter provides a comprehensive overview of Wireless Sensor Networks (WSNs), attacks in WSNs, and the field of localization. It begins by establishing the research motivation and highlighting the problem within WSN-based localization. Throughout this chapter, we delve into the domain of WSNs and localization, examining the array of attacks that pose significant security challenges and understanding the different localization algorithms.

The thesis explains the underlying motivation, centered on bolstering the security and efficacy of WSNs. Furthermore, it highlights the notable contributions of the devised technique, showcasing its capacity to adapt to evolving system requirements. To provide a coherent structure, the organization of the thesis is outlined, delineating the subsequent chapters. The forthcoming chapter offers a comprehensive literature review.

Later in the chapters, a detailed exposition of the technique follows explaining every aspect of the technique and analyzing its performance in comparison to the literature.

## 2. Literature Review

### 2.1 Introduction

The current chapter is dedicated to the in-depth examination of localization algorithms, providing insights into the rationale behind the necessity of localization specific to WSN. Additionally, an extensive review of existing literature is conducted to identify the weaknesses of localization algorithms that can be applied to WSNs to determine the location of an unidentified node in the presence of malicious nodes.

Due to the energy constraint and limited power, Wireless Sensor Networks (WSNs) are susceptible to various types of attacks that compromise the confidentiality, integrity, or availability of the network. Strong encryption and authentication algorithms, secure key management and trust management solutions, effective localization algorithms, and machine learning-based solutions can be employed to reduce the vulnerability of WSNs to attacks.

While designing algorithms to secure WSNs, it must be taken into consideration that they are limited in power and computation capability. Performing complex and lengthy computations of encryption and key management will deteriorate the energy of WSN nodes. As a result, the lifetime of the WSN will decrease. Sending numerous communication packets to ensure secure and reliable communication will lead to network congestion and result in delayed communication.

Key establishment algorithms may work in coordinated Wireless sensor networks but in adversarial networks where all nodes have limited resources, it is challenging to have a centralized entity to perform key establishment. In a dense environment, a considerable amount of energy will



be utilized by each node to exchange keys with all neighboring nodes thus adversely impacting the channel.

Due to the distributed and power-constrained nature of WSNs, security protocols do not need to be universal at the finest level of granularity. Instead, it needs to ensure that it does not drain the power of nodes for unessential tasks. For instance, signal jamming directed against a proportion of nodes can be tolerated due to the implicit redundancy of the system, and data aggregation allows for only necessary information to be protected.

## **2.2 Localization Algorithms**

Global Positioning System (GPS) can satisfy some requirements for localization, but not only is it an expensive solution, but it is also imprecise for nodes deployed in indoor environments due to position error. Moreover, the GPS location may be inaccessible as the GPS can be jammed by climatic conditions.

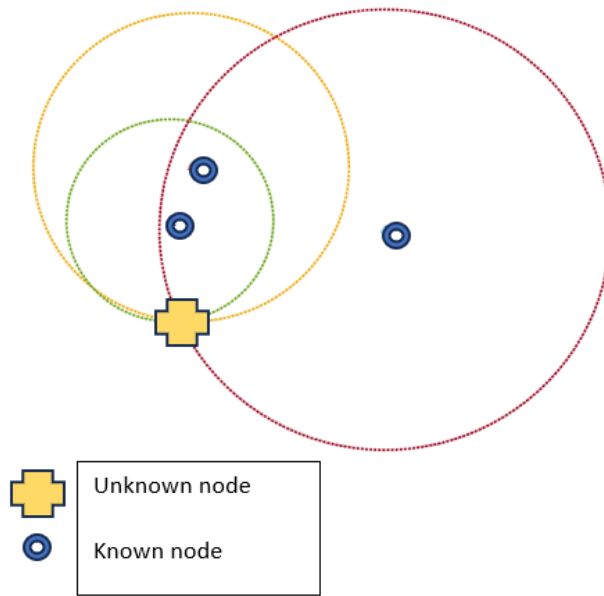
A positioning algorithm must fulfill the following criteria.

- The system needs to be distributed, as a network with low memory and limited bandwidth would be unable to cope with the demands of shuttling the entire topology to a server.
- The communication between the nodes and processing power must be utilized efficiently.
- the positioning system should be able to function even when the network is disconnected.[15]

Some common techniques used for estimating the position of an unknown target are the following:

- Multilateration
- Trilateration
- Received signal strength (RSS) based localization
- Proximity-based localization
- Centroid-based localization
- Gradient-based range localization
- Monte Carlo-based Localization

Multilateration is a technique that relies on either the received signal's time of arrival (TOA) or the time difference of arrival (TDOA). TOA requires synchronization between the receiver and transmitter and calculates the distance between the receiver and the transmitter from the absolute value of the signal's time of flight from the transmitter to the receiver using the TOA and the propagation speed. On the other hand, TDOA requires only synchronization of the receivers. This method involves the anchor nodes receiving the signal transmitted by the tracked node and using the difference in the signal arrival times at the two anchor nodes to calculate the difference in the distances. Figure 2 illustrates Multilateration for 2-dimensional position estimation. Blue nodes are identified by their known positions, while the yellow node represents a position that is sought after. The circles symbolize the distance between the known node and the unknown node. The measurement of distance is determined by calculating the time difference of arrival. For 3-dimensional position estimation, at least 4 known nodes are required.

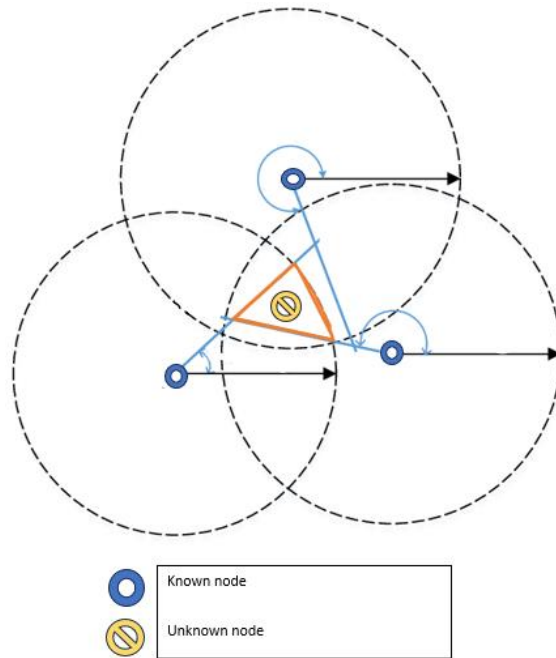


*Figure 2: Multilateration*

Trilateration estimates the position of an unknown target by the angle of arrival measurements. Angle of Arrival (AOA) measurement techniques are also referred to as bearing measurements or direction of arrival measurements. There are two main categories of AOA measurement techniques:

- The amplitude response of the receiver antennae
- Phase response of the receiver antennae

They both calculate the angle from which a signal from an anchor node arrives at an unknown sensor node. The region in which the unknown sensor is located can then be determined from the angle of the line formed between the anchor node and the unknown sensor as illustrated in Figure 3. To accurately calculate the position of the unknown sensor, at least two anchor nodes are needed.



*Figure 3: Trilateration*

Received signal strength (RSS) based localization is a technique that utilizes the attenuation of wireless signals to calculate the position of a device or object. The strength of the signal is measured at various points and the distance between the device and the transmitter is estimated. This information, combined with the known positions of the transmitters, is then used to determine where the device is located.

RSS-based localization can be achieved using wireless communication protocols, for example, Radio Frequency IDentification (RFID) Wi-Fi, Bluetooth, or Zigbee. The accuracy and reliability of estimating the unknown target position depend on the communication protocol's characteristics and signal propagation properties. Advantages of RSS-based localization include cost-effectiveness, ease of deployment, and compatibility with existing wireless infrastructure. Limitations of RSS-based localization include sensitivity to signal interference, multipath effects, and environmental changes.

Proximity-based localization does not calculate the exact position but rather the relative position of the unknown node relative to an anchor node. In Distance vector (DV) hop-based localization, the sensors estimate the distance between each other based on hop count. The anchor nodes broadcast their position coordinates to their neighboring nodes, incrementing the hop number and sending it to their neighboring nodes. Based on the number of hops it takes to reach the unlocalized node, the unlocalized node sets a value of the distance from anchor nodes.

Hop Terrain is a distance estimating technique that is similar to the DV hop method. It calculates the position of unknown nodes by evaluating the average hop distance of the unlocalized node from the anchor node. Then the initial estimated position and distance information is broadcasted to the neighboring nodes. The previously unlocalized node refines its position using the least square method.

Centroid-based localization calculates the position based on connectivity information between sensors. Unlike other range-free algorithms, centroid-based localization depends on the relative positions of neighboring nodes rather than the actual distances between them. Sensors calculate their locations based on the centroid of their neighboring nodes. The centroid is determined through the connectivity or signal strength readings. The algorithm assumes that the sensors are distributed uniformly across the network.

Gradient-based range localization estimates the positions of sensors in WSN based on an iterative method that initially has a guess position and performs gradient descent on signal strength or connectivity-based attributes to update the position. The gradient value determines the direction to reach the position of an unknown node. The magnitude of gradient descent is regulated by the

learning rate parameter. The process of calculation of estimates continues until the difference between the consecutive estimates becomes less than the threshold defined for convergence.

Monte Carlo-based Localization is an iterative probabilistic technique that calculates the target position by network communication and particle filtering.

During a phase of network communications, the essential data for updating location information is obtained. In this process, anchor nodes transmit their locations, which are then received by unknown nodes. Upon receiving the information, these unknown nodes rebroadcast it to other nodes. Regardless of the type of broadcast received, nodes store both the location data and the corresponding node IDs. At regular intervals, nodes utilize this accumulated information to update their location estimates through the utilization of a particle filter. Particle filtering involves estimating the target location by defining a motion model and performing prediction and estimation. The previous position of the sensor is used to assign weights to the measurement and these weights are resampled after each iteration to improve the accuracy of the position calculated.

While most range and range-less localization algorithms can fulfill the following criterion, each has its own merits and limitations. A concise overview of localization techniques designed for non-adversarial environments is provided [16-20].

[16] is based on least squares approaches i.e., range-difference measurements (RD-LS), squared range observations (SR-LS), and squared range-difference measurements (SRD-LS) for localizing the node. Even though the outcome of the optimization problems is not convex, the position is calculated accurately by solving the Generalized Trust Region Subproblem (GTRS).[17] on the other hand, performs maximum likelihood (ML) estimation and converts a non-convex problem to a convex problem. An algebraic approach is presented in [18] to localize an object in three-

dimensional space using Angle of Arrival (AOA) measurements, which can handle the impact of sensor position errors. It achieves the theoretical lower limit defined by Cramer Rao Lower Bound (CRLB) and keeps a bias low. It assumes that the position lies within the convex hull. [19] performs localization with a hybrid approach using both TOA and RSS-based localization techniques. Keeping in view the power constraints of WSN, the algorithm does not perform iterative calculation, rather it uses Maximum likelihood estimation which is closed form and thus an efficient way to localize nodes in WSN.

The conventional localization algorithms mentioned above are formulated to be used in harmless environments. As a result, they become vulnerable to a variety of security risks that could arise from interference and attacks.

## **2.3 Secure Localization Algorithms**

The failure of conventional localization algorithms in the presence of an adversary calls for a secure localization scheme that estimates the correct position of the unknown node when attackers are trying to manipulate the calculation.

SeRLoc [20] is a secure range-independent localization system designed for wireless sensor networks (WSNs), employing two types of nodes, mobile nodes, and Locator nodes. The position of the unknown node is estimated by locators who transmit different beacons to the omnidirectional antennas and collect the information from each sensor in its neighborhood. The locator then performs a search to specify the search region where the sensor lies and then employs a grid scoring system to choose the region that is specified by the overlapping region of all the

locators in its vicinity. The algorithms can defend against impersonation, Sybil, and wormhole attacks.

HiRLoc [21], an enhancement to the SeRLoc model, enables nodes to passively detect their location without increasing the number of sensors. It achieves this by intersecting beacon frames in the coverage area with multiple reference points. HiRLoc effectively addresses security concerns such as a Sybil attack, wormhole attack, false beaconing, and impersonation by utilizing properties like antenna orientation and communication range. It employs cryptographic primitives like GSK (Global symmetric key) to secure beacon frames.

While HiRLoc offers improved accuracy compared to SeRLoc, it does introduce higher computation and communication overhead due to the reception of multiple beaconing frames from different locators. It is worth noting that SeRLoc requires additional hardware, specifically a locator node with a directional antenna, which may limit its suitability in adversarial WSN scenarios.

In the range-based localization, Verifiable Multilateration, location authentication with mobile base stations, and distance bounding protocols were proposed to withstand attacks. In [22], a distance reduction attack was countered with a distance-bounding protocol and authentication attacks were countered with a simple challenge-response protocol. [23] proposed a modulation scheme-based distance commitment-verification protocol that assumes that the attacker can perform a replay attack. The process of correct estimation of unknown nodes involves a 2-step procedure, data distance commitment, and distance verification. In the distance commitment phase, the device upper bounds the distance measurements by modulation. An adversary enlarging distance by more than the communication range is also exposed.



After distance bounding, the committed distance is verified by round-trip time-of-flight measurement. In this exchange, the sender initiates the distance verification phase by transmitting a verification code; the receiver tries to detect the presence of that code, or traces thereof, in the transmission, despite the adversary's efforts to trail-hide its existence from the channel. The model is limited to localizing securely only when an enlargement attack occurs and provides no security in case of reduction attacks. The [22] and [24] guarantee a high level of security when the target and anchor node topology is such that the location estimation is a convex problem.

[25] proposed three forms of Attack-Resistant Minimum Mean Square Estimation Schemes that were brute force based, greedy, and enhanced greedy-based algorithms. The brute force is the most computationally expensive approach among the proposed approaches. Greedy and enhanced greedy decrease the computational load of the algorithm by identifying the attackers efficiently. The position of the target sensor node is calculated by determining the target field. The reference sensor nodes identify the region of a rectangle with the minimum area that covers all the locations that are declared by references. The extended rectangle is formed by keeping in view the maximum transmission range of the signal. The extended rectangle is declared as the target field. The extended rectangle is divided into sub-regions which are assigned a vote which is incremented based on the rings formed by reference sensors. Finally, the location of the unknown node is calculated by centroid-based localization. It verifies whether the location references are suspicious or not based on a degree of consistency metric. If the consistency metric is less than a threshold, the nodes are suspicious. The algorithm checks for all nodes and removes the suspicious node and performs localization. A greedy approach reduces the computations by a voting-based system, wherein the localization area was divided into a grid and the vote count of each grid point was increased if the distance from the reference point matched the distance measurement from the

reference point. To overcome resource constraints and achieve higher accuracy in location estimation, an iterative refinement algorithm is proposed. The number of cells is determined based on memory limitations. After the initial round of voting, the algorithm identifies the smallest rectangle enclosing cells with the highest vote and repeats the voting process. This iterative refinement allows for a smaller quantization area and finer precision. Malicious location references are likely discarded as their candidate rings do not overlap with benign references. The refinement process terminates when the desired precision or the limit of refinement is reached. The algorithm outputs the estimated location obtained in the final iteration. By setting a desired precision threshold, the algorithm ensures termination.

In [26], localization based on Geometric dilution of precision is proposed that considers the distance measurements of unknown nodes and known nodes. Weights are assigned to the estimates that are calculated by the GDOP value. These weights reflect the respective significance of each location estimate. The position of unknown nodes is calculated accurately irrespective of the node's visibility or lack thereof. It is scalable as it utilizes a distributed architecture, enabling each node to independently compute its location. However, its computational complexity increases as it relies on the number of anchors needed to localize randomly deployed nodes within the network. To mitigate this problem, one solution is to limit the number of anchors required within a specific communication range of each node.

[27] addresses the challenge of localizing a target in challenging environments where direct line-of-sight links may not be available. It performs localization based on the network topology information and received signal strengths of reference nodes. By combining measurements of received signal strength (RSS) and time of arrival (TOA), the system estimates the azimuth angle

between a reference point and the target. These estimated azimuth angle observations are then employed to linearize the measurement models, facilitating the derivation of a new estimator. The technique can calculate the azimuth angle without the requirement of additional hardware while assuming that the nodes are fixed and form a topology that can calculate the azimuth. The assumption that the position of known nodes is fixed and limited to a certain geometry supports the calculation of azimuth angle but limits the usage of the technique with randomly deployed WSN architecture.

A novel strategy using Variational Bayesian Localization (VBL) was used for localization in [28], where imperfect knowledge about the anchors' locations is taken into consideration. The technique claimed to perform accurate localization with mobile anchor nodes in dense environments where the nodes are at NLOS, and their exact position is not known. The approach incorporated a mixture of Gaussian distribution to model noise. Since the direct estimation of the likelihood function for the target node's position is challenging when the node position has an uncertainty factor, variational distributions were used to approximate the posterior distributions by minimizing the divergence that can result from the calculation of non-convex geometry. Importance sampling was employed to handle nonlinearities and node uncertainties.

Conversely, the available secure localization solutions rely on specific assumptions about the network topology, communication channel, or malicious intent of nodes, which limits their practicality.

Recently, several wireless localization techniques have been used in the Monte Carlo approach e.g. SA-MCL [29], RESA-MCL [30], IMCB [31], and MCB-PSO [32].

SA-MCL [29] introduced a notable improvement to the MCL algorithm [33] by utilizing dead reckoning to update node locations when anchor nodes are not within communication range. This enhancement enhances the localization accuracy during the time intervals between encounters with anchor nodes. The MCL approach had limitations, however. It outperformed the MCL approach only when the anchor nodes are not present in the communication range of the targeted node. Therefore, in dense networks where anchor nodes are more readily available, the SA-MCL was improved to the conventional MCL approach only in the network where anchor nodes are scarce.

RESA-MCL [30] enhances the conventional MCL algorithm by implementing modifications that enhance accuracy and resilience to attackers. Initially, particle positions are updated through dead reckoning. The received anchor lists undergo a positional plausibility check and update the distrusted points. To prevent a single malicious node from significantly impacting the position estimate, RESA-MCL selectively applies anchor node information to a subset of particles and allows motion-based updates. It provides security against biased position attacks, random position attacks, and fixed position attacks.

Monte Carlo Boxed Localization (MCB) is an adaptation of Monte Carlo Localization (MCL) that involves establishing individual one-hop and two-hop anchor sets for each unknown node through listening, effectively limiting impossible samples. MCB goes a step further by utilizing anchor set information to restrict the sample space, leading to significant energy savings for sensor nodes and enhanced sampling accuracy.

Improved Monte Carlo Localization Boxed (IMCB) incorporates historical anchor node and RSSI ranging data. It leverages historical anchor nodes and RSSI-ranging information to narrow down the sampling range for unknown nodes. This approach improves node position sampling efficiency

and addresses the anchor node density issue. Secondly, it optimizes the weight allocation based on RSSI, effectively distinguishing the importance of different sampling points. This optimization contributes to reducing localization errors in node positioning. Thirdly, the motion model is improved, enhancing the direction prediction for nodes, and thereby reducing the sampling range for position prediction. These improvements lead to increased efficiency and accuracy in node localization. However, IMCB cannot capture discriminatory factors that lead to malicious user detection. The approach has a high dependency on measurements, if measurements are fraudulent, the position will not be estimated correctly. It also requires a database to store historical Received Signal Strength Indicator (RSSI) and node position which can be a challenge in dense environments.

Monte Carlo-based (MCB) algorithms have certain drawbacks. One of the limitations is the absence of a specific search direction since candidate positions are randomly generated within an anchor box. As a result, the time required for localization is high and the overall efficiency is low. Additionally, MCB algorithms may not be suitable for scenarios with high mobility demands. In extreme cases, a significant number of candidate nodes within the anchor box may fall outside the coverage area of their corresponding anchors, leading to low localization accuracy upon completion of the iteration.

MCB-PSO [32] aims at overcoming the flaws in traditional Monte Carlo-based localization by incorporating an algorithm for optimization. It is an MCB approach designed for an environment where both anchor and unknown nodes are mobile. Initially, the nodes transmit packets containing position information and hop counts to the entire network. The unknown node receives these packets and establishes its neighbors based on the hop counts. Subsequently, the anchor box is

constructed using the neighboring nodes connected to the unknown node. To optimize the localization process, the Particle Swarm Optimization algorithm is employed. The adaptive anchor node selection parameter is utilized to evaluate the cost of each particle, and the position and velocity of the particles are updated accordingly based on the cost value. It achieves convergence efficiency by adaptively varying the anchor selection operator. It also overcomes the particle degeneracy problem that the conventional MCB techniques faced.

A unique cube-based multitarget three-dimensional localization solution was proposed in [34] which uses time-difference-of-arrival (TDOA) measurements of sensors. Turbo expectation propagation (EP)-based decoding algorithm (TED) is formulated to perform localization successfully in asynchronous networks. The approach proposed does not require synchronization among TDOA-based sensor arrays. The cube-based 3D location system proposed was designed for WSNs that use narrowband signal transmission.

In contrast to most existing schemes that assume prior knowledge of model parameters to reduce the dimensionality of cost functions in the location estimation process, the approach presented in [35] takes a different approach. In contrast to the existing techniques that assume a model with fixed parameters, [35] proposed an adaptive estimation of model parameters. The localization equation is an open-form solution and depends on how the parameters are set. The proposed algorithm is a 2-step calculation that utilizes TOA and RSS measurements and calculates the position iteratively by the Least square approach. It is assumed that even if a very simple LOS communication is performed, the calculation by TOA and RSS is nonlinear and thus cannot be modeled by a closed form. Initially, calibration is performed to calculate the nuisance parameters as the reference node locations and signal strengths are known. Afterward, the position of the

unknown node is estimated by taking advantage of both TOA and RSS measurements, and an iterative least square is carried out to estimate the position of the node.

CFFLS [36] proposed three closed-form least squares (LS) algorithms for three-dimensional localization using time difference of arrival (TDOA) measurements. Two of these algorithms were specifically designed to leverage knowledge about nuisance parameters to achieve accurate localization. The algorithms utilized different sets of TDOA measurements, including a single set, an extended single set, and a full set. To evaluate the performance of the algorithms, simulations, and real-world measurements were conducted. The experiments involved placing transmitters in a quasi-coplanar configuration within a wireless system. The results obtained from both simulations and real-world measurements were compared, demonstrating consistent outcomes. The study concluded that when TDOA measurements were contaminated by noise, the CFSSLS provided better estimation as compared to CFExSSLS and CFFSLS algorithms at different signal-to-noise ratio (SNR) levels. Moreover, the CFFSLS algorithm did not show drastic estimation performance differences due to changes in the signal power or noise.

[37] devised a novel technique for estimating the position of the unknown target with Multi-Dimensional Similarity (MDS) analysis for the environment with the NLOS propagation model. The position approximation was formulated Alternating Direction Method of Multipliers (ADMM) to solve the constrained minimization problem. Initially, ADMM was used to create a low-rank matrix for a complex propagation model that contained both Gaussian and non-gaussian noise and biases. TOA measurements were used for range calculation in matrices. Next, the generalized subspace method was used to separate the signals from noise by Eigen Value

Decomposition (EVD). The impact of outlier measurements is mitigated by using ADMM and the approach is made robust by using  $\ell_2$  norm.

Recently, the concept of Generalized Trust Region Sub-Problem (GTRS) has been used to solve the localization problem efficiently. [38] calculates the unknown target node position Weighted Central Mass (WCM) for the sensors that have a direct link with the nodes whose positions are known. It is accompanied by forming triangles using the law of cosines between the sensors. The triangles between sensors are created by adopting multi-hopping, which simplifies the problem into a GTRS. It is assumed that all sensors possess the ability to obtain RSS measurements, but only anchors nodes possess the ability to measure AOA.

SR-MCC [39] focused on calculating the position of an unknown node in the NLOS environment using only TOA measurements. It proposed a mixture model with 2 types of noise, gaussian noise for thermal disturbances in the sensor and non-gaussian noise for NLOS and biases. Using GTRS and half quadratic theory, the severely non convex problem is solved via bisection. Half quadratic theory is adopted with alternating optimization to set the value of Kernel, a variable that assigns weights to the outlier measurements. The use of half-quadratic theory, coupled with an alternating optimization technique, effectively handles the nonlinearity of the problem, enhancing the robustness of SR-MCC against NLOS effects.

The localization approach proposed in [40] calculated the position of unknown nodes assuming that there may be malicious nodes in the network as well. The malicious nodes can corrupt the network with a distance enlargement attack. The initial position is calculated using WCM including malicious nodes as well. Initially, the methodology utilizes TOA measurements from known nodes to create range circles. These circles are centered on the known anchor nodes'



location and have radii equal to the distance between the known node and the unknown node being localized. These range circles are employed to determine the intersection points between each circle and other circles in the network. Based on the resulting intersection points, the nodes are categorized as potential nodes. A node is considered potential if its range circle either does not intersect with other circles or has fewer intersections. If all nodes are classified as potential, this may indicate interference in communication channels, such as Non-Line-of-Sight (NLOS) or a noisy channel. The mode is calculated for all the potential nodes and after removing the node, the position is calculated again by GTRS. The honest, malicious nodes and the nodes in a noisy channel are differentiated based on a threshold defined to differentiate between the attacker and the noisy channel. If the range circle of a particular node does not intersect with any other node, the line is extended from the node to check if it will intersect in case it is extended. If the line intersects, the node is not considered malicious as the network assumes only an enlargement attack can be performed by the nodes.

A novel attacker detection scheme is proposed in [41] that combines a geometric approach for obtaining the estimate of the location of an unknown node with the Generalized Likelihood Ratio Test (GLRT) in an environment where nodes are present and capable of performing distance reduction and distance enlargement attacks. The initial position is calculated as in [40] by using WCM. The malicious node is detected by calculating the noise standard deviation and tuning the false alarm probability. The problem of detecting attackers involves the task of differentiating between two hypotheses.  $H_0$  is the hypothesis that distance measurement is the result of the distance of each sensor from the unknown sensor with an additive noise value whereas  $H_1$  is the hypothesis that distance measurement is the result of the distance of each sensor from the unknown sensor with an additive noise value and a deviation value  $\sigma$ . Under the assumption that  $H_0$  is

true, the distance measurement indicates that node  $a_i$  is honest, although it may contain some noise attributed to the channel. On the other hand, if  $H_1$  is true, it signifies that the node  $a_i$  is an attacker engaging in an enlargement attack when the value of  $\sigma$  is positive, or a reduction attack when the value of  $\sigma$  is negative. After detecting the malicious identities, they are excluded from the localization process which is converted into a GTRS using the law of cosines (LOC) and solved efficiently with the bisection principle.

[42] aimed to estimate both the position and orientation of the source accurately in the NLOS environment. propose an iterative algorithm that effectively utilizes RSS and TOA measurements. The algorithm performs iteratively utilizing RSS and TOA measurements. The localization problem solves the non-convex arrangements of nodes and transforms the non-convex problem into GTRS. Considering that the RSS measurements of the target can vary significantly depending on its directionality, initially, the location of the target is estimated using only the TOA measurements. The limitation of this approach is that it assumes prior knowledge of the transmission power and transmission time of the target for the anchors.

A novel iterative approach is used to address the challenge of localizing a target node in wireless sensor networks utilizing the TOA and RSS when dealing with NLOS conditions [43]. It does not necessitate the knowledge of NLOS bias distribution. To solve the localization problem, a Non-Linear Weighted Least Squares (NLWLS) problem is formulated and solved using a majorization-minimization (MM) algorithm. The MM algorithm uses a series of simple update steps to decrease the NLWLS objective until it converges to a stationary point.

From the aforementioned approaches, most localization algorithms that claim high accuracy are either not able to detect the case an attacker is present or make unrealistic assumptions about the

network or detect only a specific kind of attacker. In the case of adversarial networks, localization is a challenge, and a technique must be devised that not only calculates the accurate position of the unknown target but can detect a wide variety of attackers. Traditional systems used for localizing sensors in WSN often assume Gaussian noise due to its approximation capabilities in real-life situations. However, this assumption may not hold in environments with signal-blocking obstacles and reflecting surfaces, such as in IoT applications. To address the challenges posed by noise and interference, a non-linear system model is formulated. Since solving this problem directly is difficult, convex relaxation techniques are employed to tackle the non-linear least squares problem. Convex optimization solvers based on the interior-point method are iterative and computationally expensive rendering them unsuitable for WSNs. As an alternative, the problem can be transformed into the framework of a GTRS or approached using the maximum likelihood method. These approaches help mitigate the impact of adverse environmental conditions by reducing computational complexity, trimming out outlier-sensitive losses, and achieving resistance to biased measurements. By employing these techniques, the algorithm becomes more suitable for adverse environmental cases.

## **2.4 Summary**

This chapter covered the literature review regarding localization algorithms specifically for WSN. Further, identify the weaknesses of localization algorithms that can be applied to WSNs to determine the location of an unidentified node in the presence of malicious nodes.

In the next chapter, we propose a secure localization technique that can detect attackers and calculate the position of unknown nodes accurately.

## 3. Methodology

In this section, the proposed methodology to achieve secure localization is explained. The chapter is divided into two parts:

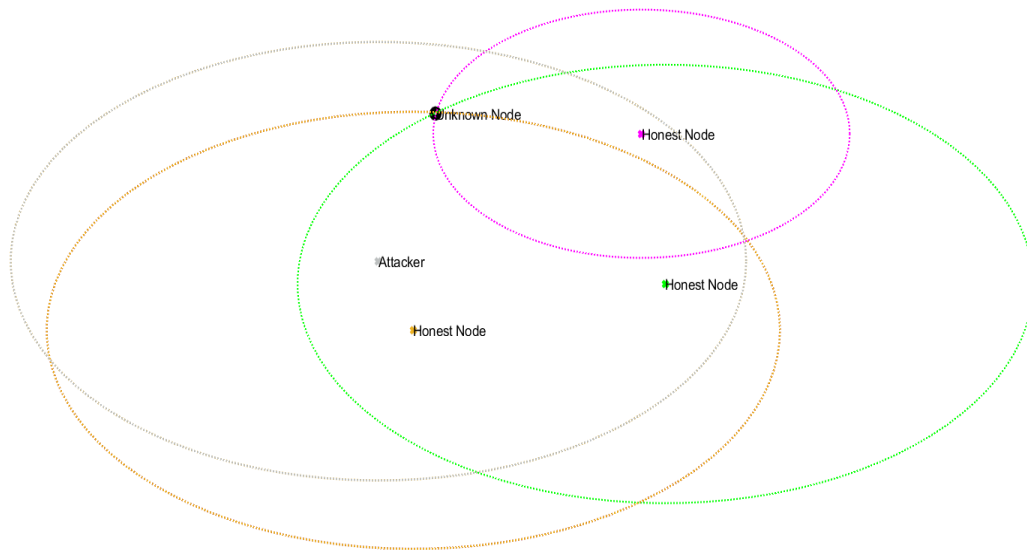
- Problem identification
- Proposed methodology

### 3.1 Problem Identification

Based on the literature review, the focus of this research is to achieve a secure localization system that not only calculates the accurate position of the unknown node in a WSN but can detect the attackers when the system has coordinated attackers such as a Sybil attack.

In a Sybil attack, the attacker employs a strategic approach to establish multiple fraudulent nodes. These fabricated nodes are designed to engage in communication and collaboration with one another, thereby amplifying their collective influence or deceiving other participants within the targeted system. By orchestrating the operation of multiple fake identities in a coordinated manner, the attacker can significantly impact the system, potentially leading to disruptive consequences. The coordinated nature of a Sybil attack enables the attacker to exploit the system's decision-making processes, effectively undermining the system's reliability and compromising its overall functionality. A Sybil attack leverages the presence of multiple fake identities or nodes, known as Sybil nodes, to carry out various forms of manipulation within a network. One such manipulation

technique involves distance enlargement and reduction attacks, which impact the measurements of distance or similarity between entities.



*Figure 4: Enlargement Attack*

In a distance enlargement attack depicted in Figure 4, the attacker illustrated by a grey range circle, strategically connects the Sybil nodes to specific entities and provides misleading information, thus inflating the perceived distance between these entities.

Conversely, a distance reduction attack exploits Sybil nodes to establish fraudulent connections or relationships in a way that the distance between the nodes is perceived to be less than it is. In Figure 5, the node with grey colored range circle is performing a reduction attack.

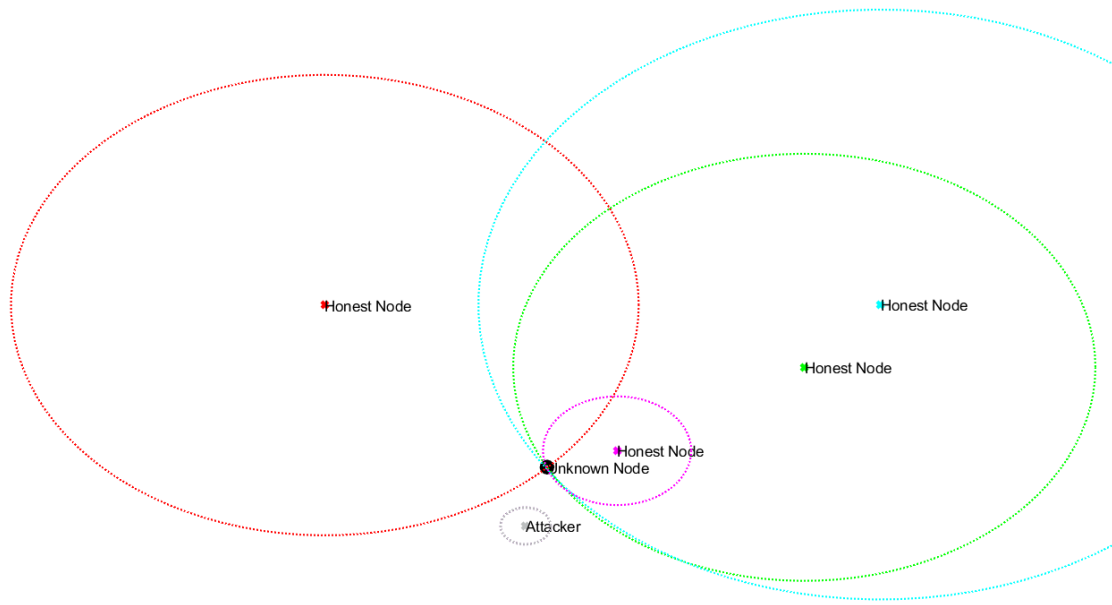


Figure 5: Reduction Attack

The impact of these distance manipulation techniques can be amplified by employing multiple Sybil nodes, enabling the attacker to exert greater influence on algorithms or systems reliant on distance or similarity measurements.

The objectives of both distance enlargement attacks and distance reduction attacks revolve around undermining the accuracy and dependability of the localization system by manipulating the perceived distances among nodes. Such attacks pose significant risks to localization-based applications, including location-based services and tracking systems, as they can result in erroneous positioning data and potentially facilitate malicious endeavors.

Previous research has focused on identifying and detecting distance enlargement attacks and distance reduction attacks. However, an important aspect that has been overlooked is the investigation of coordinated attacks, where attacker nodes engage in both enlargement and reduction attacks simultaneously, posing a significant threat to system integrity.

## 3.2 Proposed Methodology

This section provides an overview of the methodology employed to detect a Sybil attack and ensure secure localization. The methodology is an amalgamation of localization technique and attacker detection technique.

The estimation of the position of the unknown mobile node is achieved by using both TOA and RSS measurements. The acquisition of estimates using TOA and RSS is an improvement on localization using a single set of measurements in terms of localization accuracy as it takes advantage of relatively inexpensive realization by RSS measurements while reaping the benefits of time resolution and higher accuracy by TOA measurements.

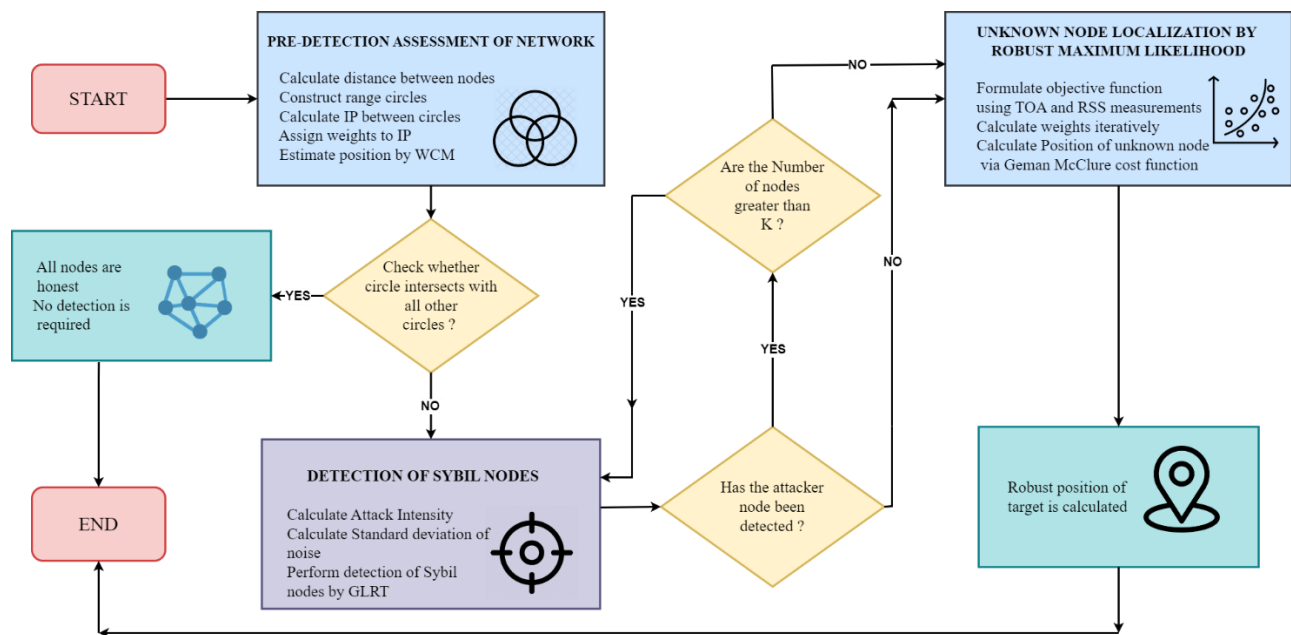


Figure 6: Proposed System Flowchart

The procedure involves three steps:

- Pre-detection assessment of the network
- Detection of Sybil nodes

- Unknown node localization by robust maximum likelihood

### **3.2.1 Pre-detection Assessment of Network**

Initial assessment of the network utilizes TOA or RSS measurements from known nodes to create range circles. These circles are centered on the known node's location and have a radius equal to the distance between the known node and the unknown node being localized.

Next, these range circles are employed to determine the intersection points (IP) between each circle and other circles in the network.

Based on the IP of circles, the mean distance of each circle with range circles of other nodes is calculated.

The distance distinguishes two cases:

- The circles do not intersect because either one is an attacker
- The circles do not intersect due to noise or environmental bias

It does so by setting a potential intersection point and assuming an imaginary line. If the node's measurements are corrupted due to environment the intersection points will lie on the line.

The distance will be used to assign weights to the IP and based on these weights position of the unknown node is calculated geometrically. Weighted Central Mass (WCM) serves as the foundation for the mathematical methodology employed to allocate weights to IP.

WCM is a concept used for estimating a value by assigning a priority parameter to the components involved in the estimation process. In the context of localization in WSNs, WCM can be applied



to calculate the weighted center of mass using neighboring anchor nodes, eliminating the requirement for explicit range or distance measurements. In WCM, each anchor node is assigned a weight, which is determined based on factors like signal strength or connectivity to the target node. These weights reflect the significance or trustworthiness of each anchor node in the position estimation process.

The primary goal is to identify any potential IP between these circles, which can be achieved by calculating the point of intersection. Subsequently, the computed IP of interest  $I_{ij}$ , are derived as the mean value between the two intersection points,  $I_i$ , and  $I_j$ . This approach is based on the rationale that in scenarios where the two anchors are solely affected by noise, the closest pair of points on their respective circles will align precisely along the line passing through the anchors. In other words, these points would have intersected in proximity if it were not for the presence of noise.

The IP of range circles are calculated as follows:

$$I_{ij} = I_0 \pm t$$

$$i = 1, \dots, N - 1$$

$$j = i + 1, \dots, N$$

$$I_0 = \frac{a_j + a_i}{2} + \frac{d_i^2 - d_j^2}{2 \|a_j - a_i\|^2} \times (a_j - a_i)$$

$$S = \frac{\sqrt{S} \times M \times}{2 \|a_j - a_i\|^2} (a_j - a_i)$$

$$S = [ ((d_j + d_i)^2 - \|a_j - a_i\|^2) (2 \|a_j - a_i\|^2 - (d_j - d_i)^2) ]$$

The selection of weights is intentionally designed in such a way that smaller weights are assigned to pairs of the largest (on average) distance measurements. This deliberate weighting technique aims to minimize the impact of a corrupted anchor node, especially when the corrupted node has not been identified or exposed yet. By assigning smaller weights to these larger distance measurements, the influence of a potentially corrupted anchor node is mitigated.

By calculating the weighted center of mass, which involves averaging the positions of anchor nodes weighted by their respective the target node's position is obtained from WCM is calculated as follows:

$$P_{xy} = \sum_{i,j=1}^N w_{ij} I_{ij}$$

$$i = 1, \dots, N - 1$$

$$j = i + 1, \dots, N$$

$P_{xy}$  is the position of the unknown node,  $I_{ij}$  are the IP of circles such that for node 1,  $I_{12}$  is the point that intersects node 2 and  $I_{13}$  is the point that intersects node 3, and so on. The points,  $I_{ij}$  are utilized to create clusters based on their close physical proximity, aiming to select the cluster with the smallest convex hull. This is accomplished by assigning weights and determining the clusters accordingly.

### 3.2.2 Detection of Sybil Nodes

Based on the resulting intersection points and weights assigned to the points, the nodes are categorized as potential attackers or intruders. A node is considered a potential attacker if its' range circle does not intersect with other circles, or the imaginary line extrapolated to intersect the points.

If all nodes are classified as potential attackers, this may imply interference in communication channels, such as Non-Line-of-Sight (NLOS) or a noisy channel.

To effectively address this situation, additional filtering is applied to the potential nodes based on their intersection points with other nodes. This filtering process aims to identify nodes that exhibit characteristics indicating a higher likelihood of being associated with an attacker. To evaluate the potential nodes, the average distance between pairs of intersection points is calculated. This average distance plays a key role in determining the weights assigned to the nodes.

By focusing on these specific nodes, the methodology can prioritize the detection and mitigation of potential malicious nodes, enhancing the overall robustness of the system. Filtering is an iterative process and depends on the number of nodes that are assigned as potential attackers and the dimensionality of the system. The process of detection is carried out sequentially for potential attackers until the node under scrutiny is identified as honest or until the number of nodes reaches the specified threshold. For a two-dimensional network, the threshold (K) is set at four nodes, while for a three-dimensional network, it is set at five nodes.

The problem of detecting attackers involves the task of differentiating between two hypotheses. Under the assumption that  $P_n$  is true, the distance measurement indicates that the node  $a_i$  is honest, although it may contain some noise attributed to the channel. On the other hand, if  $P_A$  is true, it implies that the node  $a_i$  is an attacker engaging in an enlargement attack when the value of  $\delta_i$  is positive, or a reduction attack when the value of  $\delta_i$  is negative.

The node is honest node if it satisfies the hypothesis  $P_n$ .

$$P_n : d_{i,k} = ||P_{xy} - a_i|| + n_{i,k}$$

The node is the attacker if it satisfies the hypothesis  $P_A$ .

$$P_A : d_{i,k} = \|P_{xy} - a_i\| + n_{i,k} + \delta_i$$

$$\delta_i \neq 0$$

These hypothesis conditions can be translated into probabilistic terms.

$$P(d_i | P_n) = c \times \exp \left\{ \frac{1}{2\sigma^2} \sum_{k=1}^k (d_{i,j} - \|P_{xy} - a_i\|^2) \right\}$$

$$P(d_i | P_A) = c \times \exp \left\{ \frac{1}{2\sigma^2} \sum_{k=1}^k (d_{i,j} - \delta_i^2 - \|P_{xy} - a_i\|^2) \right\}$$

Once the potential attacker is assessed to determine if it is indeed an attacker, it is subsequently classified as either an attacker or not. If it is identified as an attacker, the node is excluded from further calculations. Following this exclusion, the detection process is carried out on the remaining potential attackers, one by one. The generalized Likelihood Ratio Test is used for this purpose.

GLRT is a statistical hypothesis test that compares two competing hypotheses using their likelihood functions. It is applicable when the likelihood functions are either known or can be modeled. By computing the likelihood ratio, which is the ratio of the likelihood of the observed data under one hypothesis to the likelihood under the other hypothesis, the GLRT quantifies the relative support for each hypothesis. The resulting test statistic is then compared to a predetermined threshold or critical value, enabling the decision-making process to choose between the hypotheses.

One of the key advantages of the GLRT is its suitability for scenarios where the likelihood functions deviate from Gaussian distributions or when the underlying statistical distributions are

not well-established. This flexibility allows for rigorous statistical analysis and inference, facilitating accurate and informed decision-making in a diverse range of practical applications.

The GLRT detection process involves calculating the attack intensity for each link, as well as estimating the noise standard deviation based on the Maximum Likelihood principle. Given the presence of multiple potential attackers, the GLRT test is performed iteratively, considering the number of potential attackers and the honest nodes within the network.

The GLRT involves comparing the likelihood ratio between two models: the null hypothesis model also known as the restricted model and the alternative hypothesis model also known as the unrestricted model. The null hypothesis assumes certain constraints or simplifications, while the alternative hypothesis relaxes those constraints, providing a more flexible representation of the data. The formula to calculate the standard deviation is:

$$\sigma_{estimated} = \sqrt{\frac{1}{k-1} \sum_{i=1}^N \sum_{k=1}^N (d_{i,k} - \delta_i - \|P_{xy} - a_i\|)^2}$$

The attack intensity against each communication link:

$$\delta_i = \frac{1}{k} \sum_{k=1}^k (d_{i,k} - \|P_{xy} - a_i\|)^1$$

For hypothesis  $P_A$ , the estimated attacker intensity must satisfy the following condition:

$$|\delta_{iestimated}| > \sqrt{\frac{2}{k} (\sigma_{estimated})^2 \ln(\tau)}$$

For hypothesis  $P_n$ , the estimated attacker intensity must satisfy the following condition:

$$|\delta_{iestimated}| < \sqrt{\frac{2}{k} (\sigma_{estimated})^2 \ln(\tau)}$$

In the equations above,  $\tau$  is the threshold that defines a false alarm.

### **3.2.3 Unknown Node Localization by Robust Maximum Likelihood**

Upon successful detection of the attackers, they are eliminated from the system. The remaining honest nodes are then utilized to calculate a more accurate position estimation. This refined position estimation is achieved by employing the Received Signal Strength (RSS) measurements and applying a Geman-McClure cost function.

By removing the detected attackers and focusing solely on the honest nodes, the methodology aims to improve the accuracy of the final position calculation. This helps mitigate the impact of potential attackers on the localization process, ensuring a more reliable and precise position estimation for the unknown node.

In the upcoming section, a concise overview of the mathematical concepts employed in the proposed methodology is presented, outlining their implementation and integration within the system. The next chapter will offer detailed insights into how these techniques are implemented and applied.

The Geman McClure likelihood function belongs to the class of M-estimators. M estimators are generalizations of Maximum Likelihood estimators[44] that claim robustness in the presence of outliers. Robust Maximum Likelihood Estimators (MLEs) are statistical estimation techniques designed to enhance the reliability and resilience of parameter estimates when faced with outliers or violations of underlying assumptions. Traditional MLE assumes that data conform to a specific

distribution with known parameters. However, real-world data often diverge from these assumptions, resulting in biased or inefficient parameter estimates.

Robust MLE acknowledges the possible existence of outliers and strives to produce more dependable and consistent estimates in the presence of outliers and noisy measurements. It accomplishes this by employing robust estimation techniques, including robust loss functions, or weighting schemes, which diminish the impact of outliers or assign them reduced weights during the estimation procedure. Robust MLEs integrate robustness measures into the estimation process. These estimators seek to minimize the impact of outliers or heavy-tailed distributions, which can significantly influence estimation obtained through conventional MLE methods.

The challenge lies in the accurate yet efficient computation of unknown nodes for realistic scenarios where assumptions regarding channel are as minimal as possible to make the solution applicable for diverse scenarios. One of the key advantages of robust maximum likelihood estimation is its suitability in dealing with anomalous data or measurements containing outliers.

After identifying the intruder or multiple intruders in the network, the position of the unknown mobile node is calculated excluding the intruders. The calculation utilizes the RSS range measurements that are extracted from the received signal modeled as:

$$P_i = P_0 - 10\gamma \log_{10} \| P_{xy} - a_i \| + n_g - n_{ng}$$

$P_i$  is the RSS of the  $i$ th sensor,  $P_0$  is the RSS for the sensor at a 1m distance and  $\gamma$  is the path loss exponent,  $n_g$  is the noise that is modeled as zero-mean Gaussian and  $n_{ng}$  is non gaussian noise.

By arithmetic simplification and Taylor expansion, the RSS range-based model is transformed as:

$$\beta_i = 10^{\frac{PDIFF}{-(10\gamma)}}$$

$$PDIFF = -P_i + P_0$$

TOA range-based measurements are modeled as:

$$r_i = \| P_{xy} - a_i \| + nt_g - nt_{ng}$$

In the equation above,  $r_i$  is the distance between the target  $P_{xy}$  and anchor node  $a_i$ ,  $nt_g$  is the zero mean gaussian noise in TOA measurements and  $nt_{ng}$  is the non-gaussian noise in TOA measurements.

With the help of the TOA range measurement model, the robust solution becomes:

$$\min \sum_{i=1}^{2L} \zeta e_i$$

$$e_i = 10 \gamma(1 - \beta_i \|P_{xy} - a_i\|_2) / \ln 10$$

$$e_{i+l} = r_i - \|P_{xy} - a_i\|_2$$

$\zeta$  represents the outlier-resistant loss function.  $\zeta$  will become Geman McClure loss with a tunable parameter  $\epsilon$  which is set to 1 as in [44]. Next, the weights are assigned by squared range iterative reweighted least squares (SR-IRLS) [45].

$$w_i = \frac{1}{e_i^2 + \epsilon^2}$$

After determining the weights iteratively using the alternating minimization (AM) approach, the final estimate is calculated by using a similar approach as used in [46] wherein the estimation was performed using an iterative message passing algorithm. The estimation of position



leverages the concept of M-estimators and AM by recursively approximating the objective function.

$$S_1 = \sum_{i=1}^L \eta_i \eta_i^T q$$

$$S_2 = \sum_{i=1}^L \eta_i q \left[ q^{-1} \cdot \frac{200\beta_i^2 \gamma^2 w_i}{\ln^2(10) + 2w_{i+L}r_i} - \varphi_i \right]$$

$$q = \left[ \frac{200\beta_i^2 \gamma^2 w_i}{\ln^2(10) + 2w_{i+L}r_i} \right]$$

$$\varphi_i = \|P_{xy} - a_i\|_2 - \eta_i^T P_{xy}$$

$$\eta_i^T = \frac{P_{xy} - a_i}{\|P_{xy} - a_i\|_2}$$

The position estimate from WCM is fed to the robust estimator. This enables fast convergence as the algorithm is open form and calculates the position estimate iteratively. The iterations are controlled by an error threshold and maximum iteration parameter.

# 4. Experimental Setup

In this section, the experimental setup and the results are provided. The chapter is divided into two parts:

- Experimental setup
- Evaluation metrics

## 4.1 Experimental Setup

The hardware and software used in the experiment are as follows:

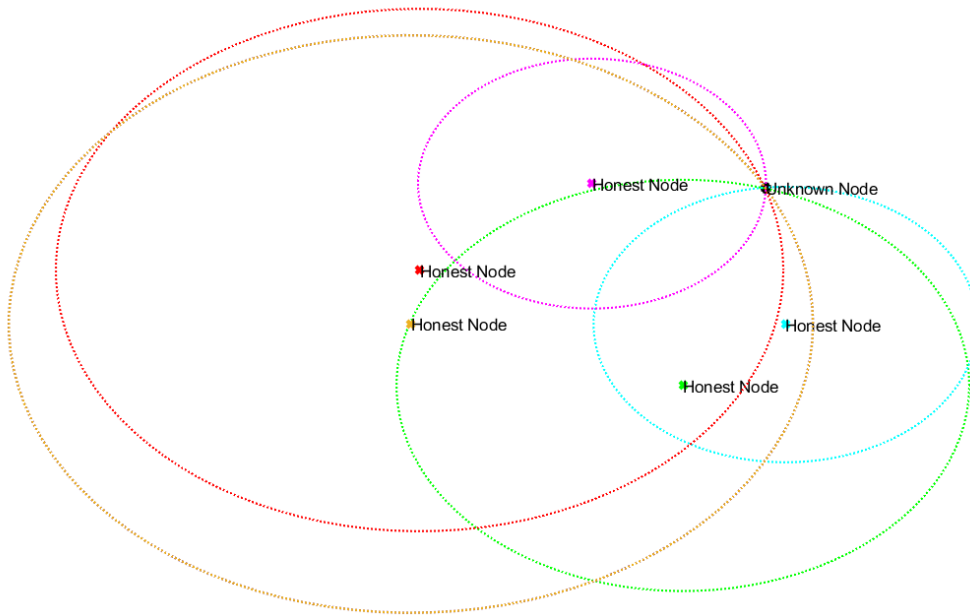
*Table 1: Experiment Tool*

Hardware Tool	Laptop Core i7
System type	64-bit operating system
Operating system	Windows
Programming tool	MATLAB 2023a (student licensed)

### 4.1.1 System Model

The WSN designed for the experiment consists of an  $N$  number of anchor nodes and an unknown node. The nodes are mobile, and their motion is not predetermined. The nodes can transmit and receive packets within their communication range. This implies that the anchor node can perform TOA, TDOA, or RSS distance calculations. Any anchor node can be compromised by an attacker

and converted into a Sybil node capable of performing both distance enlargement attack and distance reduction attack. To determine the two-dimensional position of the target node, we need the two-dimensional position of the anchor nodes. Similarly, if we aim to determine the three-dimensional position of the target node, we require the three-dimensional position of the anchor nodes. The system can calculate both the two-dimensional and three-dimensional positions of the unknown node. However, when determining the three-dimensional position of the unknown node, an additional anchor node is needed compared to determining the two-dimensional position. In an ideal case with 5 anchor nodes, the localization in the network can be visualized as in the figure below.



*Figure 7: Desired Network*

Figure 7 assumes that the noise is low enough that it does not impact the distance calculation of the nodes. However, this is not the case in realistic scenarios. The communication channel adds noise which in ideal cases may be Additive White Gaussian Noise (AWGN) and in non-ideal cases can be complex distribution e.g., Nakagami or log-normal distribution.

The system has 2 types of attacker models:

- Attacker model with multiple attackers operating with the same attack intensity exclusively performing either enlargement attack or reduction attack. This attacker model is referred to as attacker model 1.
- Attacker model with multiple attackers operating with the same attack intensity performing both enlargement attack and reduction attack. This attacker model is referred to as attacker model 2.

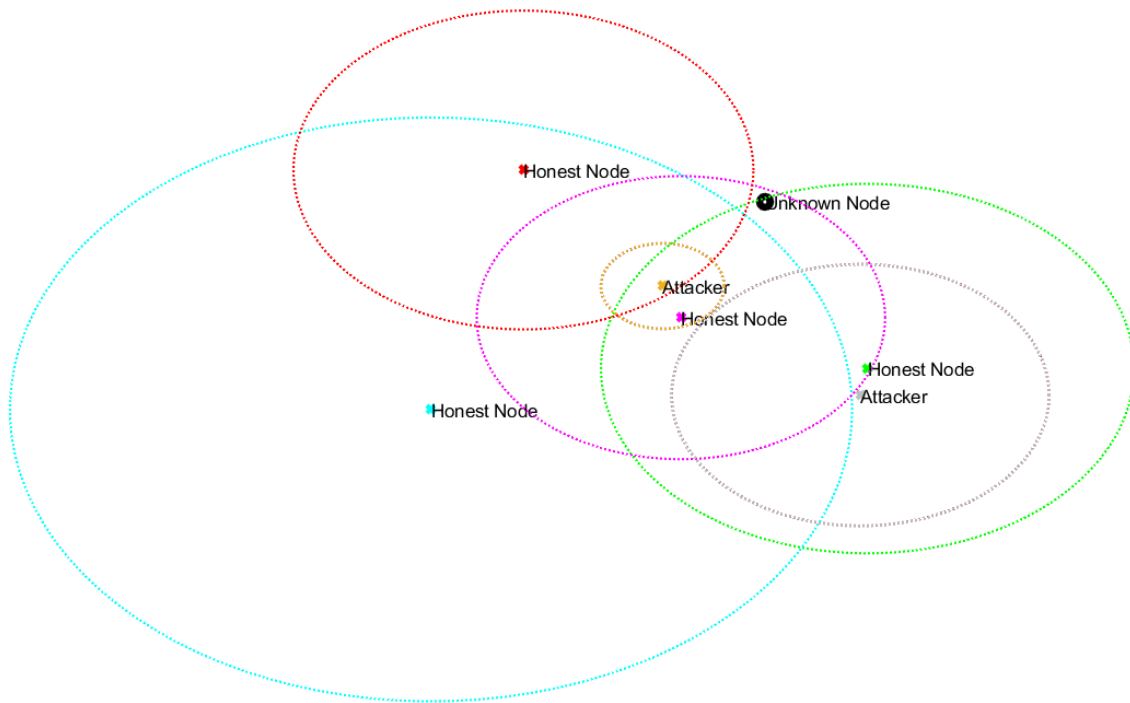


Figure 8: Attacker Model 1 Reduction Attack

Figure 8 showcases a network consisting of four honest nodes and two attacker nodes. The honest nodes are represented by red, cyan, green, and pink crosses, and their range circles are depicted using corresponding colors. The attacker nodes, on the other hand, are depicted by grey and yellow

crosses, and their range circles are also shown using respective colors. In this scenario, both attacker nodes are engaged in a reduction attack, as the target lies outside the range circles of both attackers. In the presence of the attackers, the position will not be calculated accurately as depicted in Figure 9. The blue circle shows the position calculated when all the nodes are taken into consideration and the position is calculated by WCM. The position is not precisely close to the black circle, the actual position of the unknown node.

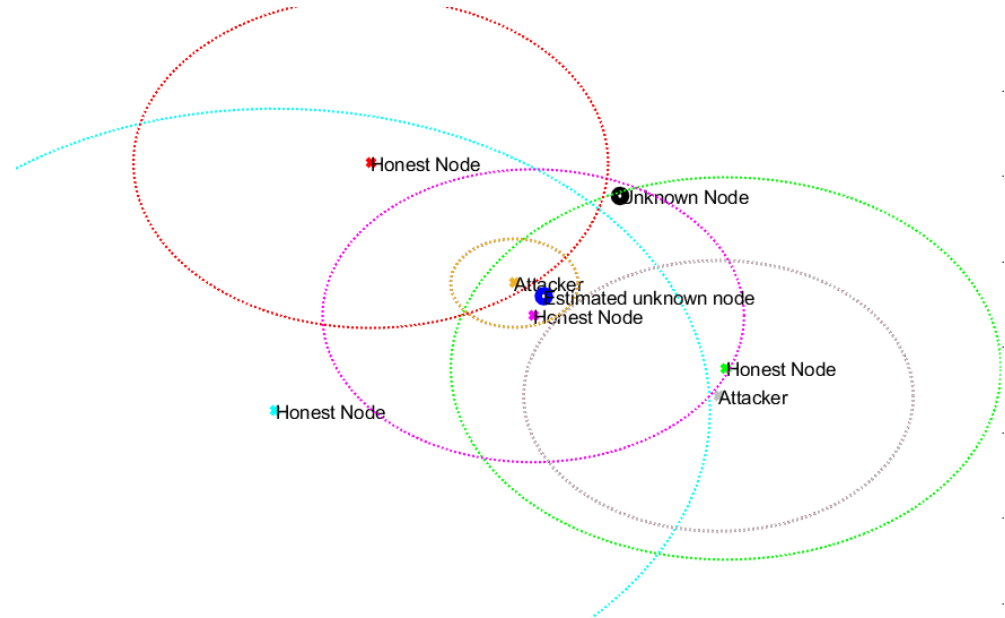


Figure 9: Inaccurate unknown node position in the presence of attackers

After detecting the attackers and calculating the position by the robust Maximum likelihood estimator the resultant position has a minimum error.

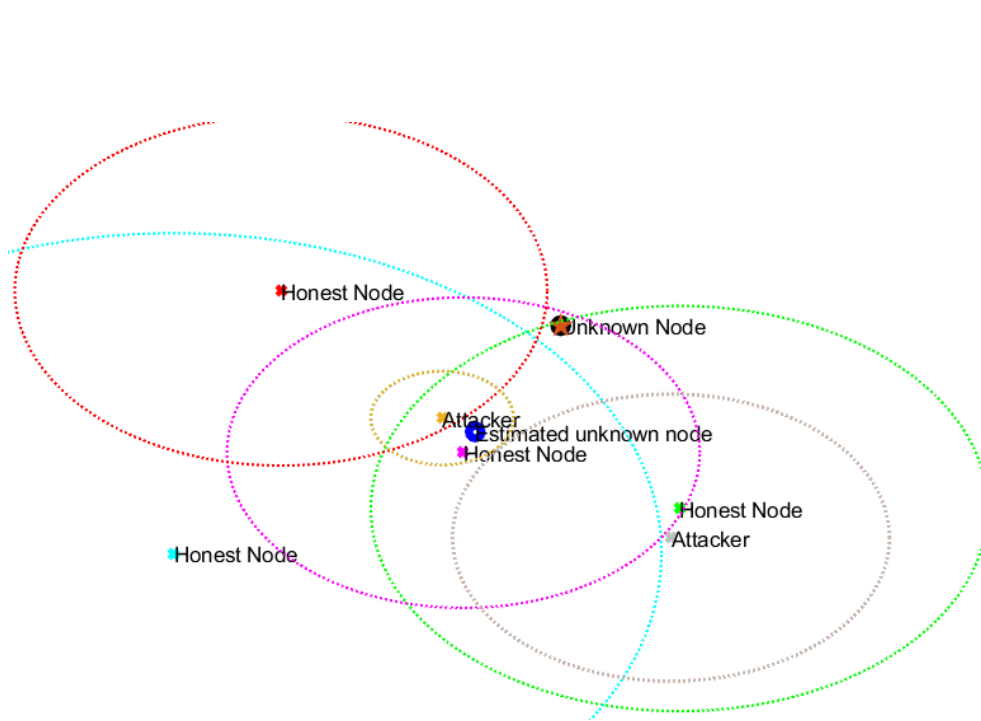


Figure 10: Accurate Estimate by Robust Localization

Figure 10 illustrates the same network as in Figures 8 and 9. The estimate after detecting attackers and removing them from the network is shown by an orange star symbol.

Table 2: Environment Parameters

<i>Parameter</i>	<i>Value</i>
Dimensionality	2 or 3
Communication Range	25 x 25 m <sup>2</sup>
Path loss { $\gamma$ }	3
Reference RSS { $P_0$ }	20 dBm
Desired probability of false alarm	0.1
Monte-Carlo Runs	500 Runs
Standard deviation in RSS { $\sigma_{RSS}$ }	3
Standard deviation in TOA { $\sigma_{TOA}$ }	3

## 4.2 Evaluation Metrics

The evaluation metrics to analyze the performance of the system are:

- RMSE
- Probability of detection
- Convergence Rate

### 4.2.1 RMSE

Root Mean Square Error (RMSE) is a commonly used metric to measure the accuracy or the average difference between predicted values and actual values in various fields, including statistics, machine learning, and regression analysis. It is a measure of the dispersion or the spread of errors.

Mathematically, RMSE is calculated by taking the square root of the mean of the squared differences between predicted values and actual values.

$$RMSE_x = \sqrt{\frac{\Sigma(\hat{x} - x)^2}{n}}$$

$$RMSE_y = \sqrt{\frac{\Sigma(\hat{y} - y)^2}{n}}$$

$$RMSE_r = \sqrt{RMSE_x^2 + RMSE_y^2}$$

$\hat{x}$  and  $\hat{y}$  represent the position coordinates calculated by the system and  $x$  and  $y$  represents the actual position coordinates, and  $n$  is the total number of samples.

RMSE is a measure of the deviation between predicted and actual values, and it is expressed in the same unit as the variable being measured. It provides a single numerical value that represents the overall error or accuracy of a predictive model or estimation technique.

The lower values of RMSE indicate better accuracy and less dispersion of errors. A value of zero indicates a perfect match between predicted and actual values. However, it's important to note that RMSE is sensitive to outliers and large errors, as it squares the differences before calculating the mean.

### **4.2.2 Probability of Detection**

The probability of Detection (POD) is a vital statistical measure used to assess the effectiveness of detection systems and algorithms. It gauges the likelihood of successfully detecting a target or desired signal within the system.

In detection systems, POD is commonly defined as the ratio of correctly detected instances to the total number of actual instances present. It offers insights into how well the system identifies and detects the desired targets while minimizing false negatives, which are instances that go undetected.

POD is typically expressed as a probability value ranging from 0 to 1 or as a percentage from 0% to 100%. A higher POD indicates a greater chance of successfully detecting targets, while a lower POD suggests a higher probability of missed detections.



Calculating POD depends on the specific detection scenario and the availability of ground truth information. In many cases, it involves comparing the detection system's outputs with a known set of ground truth labels or annotations.

The probability of detection is assessed through the following 3 key measures:

- Probability of Correct Detection
- Probability of False Detection
- Probability of No Detection

### **4.2.3 Probability of Correct Detection**

The Probability of Correct Detection refers to the likelihood that a detection system correctly identifies or detects the presence of a target or event when it is indeed present. It represents the probability that the system makes an accurate positive detection or correctly recognizes the occurrence of the target or event of interest.

$$P_{Correct\ detection} = \frac{attack\_det\_tot}{attack\_det\_tot + false\_det\_tot + no\_attack\_det\_tot}$$

### **4.2.4 Probability of False Detection**

The Probability of False Detection is the probability that a detection system erroneously indicates the presence of a target or event when it is not present. It measures the likelihood of false positive detection, where the system incorrectly identifies the occurrence of the target or event.

$$P_{False\ detection} = \frac{false\_attack\_det\_tot}{attack\_det\_tot + false\_det\_tot + no\_attack\_det\_tot}$$

### 4.2.5 Probability of No Detection

The Probability of No Detection represents the probability that a detection system fails to identify or detect the presence of a target or event when it is present. It indicates the likelihood of a false negative, where the system fails to recognize the occurrence of the target or event of interest.

$$P_{No\ detection} = \frac{No\_attack\_det\_tot}{attack\_det\_tot + false\_det\_tot + no\_attack\_det\_tot}$$

### 4.2.6 Convergence Rate

The convergence rate refers to the number of iterations required to achieve a certain error value in a process to attain an optimal solution. It serves as a metric in optimization and numerical analysis to gauge the performance of the algorithm with which it assures accuracy. The system is time intensive and computationally inefficient if convergence is slow.

## 5. Analysis and Discussion

This chapter presents a thorough examination of the proposed scheme. The analysis encompasses the system's performance under various attack models and different configurations of nodes in the system and attacker nodes. Furthermore, a comparison with existing literature is included.

### 5.1 Comparative Analysis

The experiment is conducted through 500 Monte Carlo runs to accurately observe and analyze trends. Initially, the number of attackers remains constant while the total number of anchor nodes increases. This allows for the observation of the response of additional honest nodes within the network.

In terms of minimum requirements for estimation, the number of honest nodes needed is determined by adding one additional node to the dimension of the node positions. For example, in a 2-dimensional position scenario, a minimum of 3 nodes must be honest, while in a 3-dimensional position scenario, at least 4 nodes should be honest.

The performance is evaluated based on detection accuracy and localization error. Attacker intensity is set to be in the range -of 20:5:20 to understand the impact of attacker intensity on RMSE.

The algorithm's performance is evaluated by comparing the root mean square error (RMSE) and the probability of detection. Two different simulation scenarios are used to model the attack.

- In the first scenario, multiple attackers are either all conducting enlargement attacks or all performing reduction attacks. This attacker model is referred to as attacker model 1.
- In the second scenario, the attackers perform both enlargement and reduction attacks simultaneously, but with a specific attack intensity. For example, if there are two attackers, one performs an enlargement attack while the other conducts a reduction attack of the same attack intensity. In the case of three attackers, two perform reduction attacks, and one performs an enlargement attack during half of the Monte Carlo runs. For the remaining half, one attacker conducts a reduction attack, while the other two perform enlargement attacks. This attacker model is referred to as attacker model 2.

### 5.1.1 RMSE Analysis for Attacker Model 1

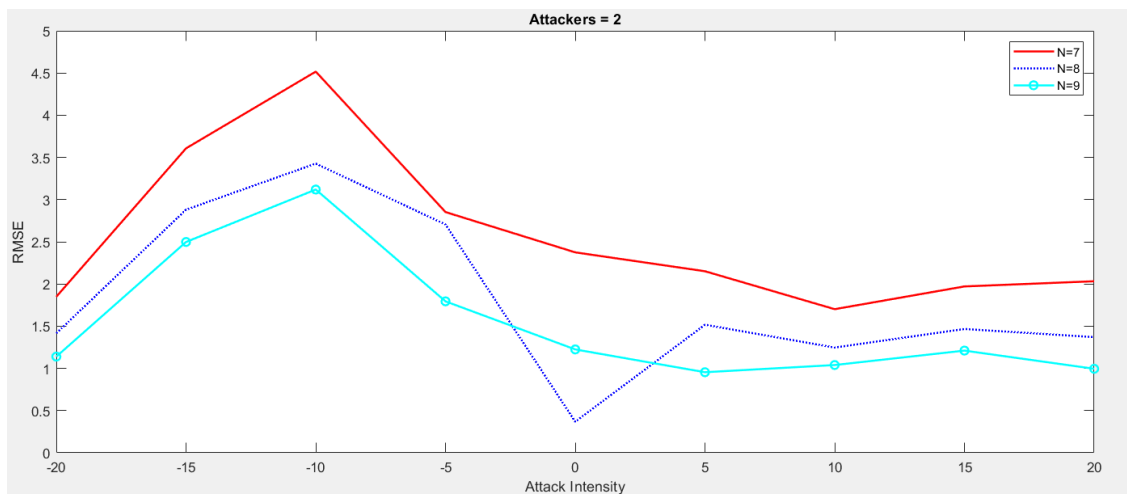


Figure 11: RMSE Comparison 2 Attackers

Figure 11 illustrates the impact of RMSE on the number of nodes against a range of attack intensity values. When the total number of nodes is 7 and 2 of them are attackers, the error is

greater as compared to the case when the total number of nodes is 8 and 9 against the same value of attack intensity.

To assess the performance of the proposed algorithm in comparison to existing literature, the LOC-GTRS-based localization [41] is used as a benchmark as it considered both enlargement and reduction attacks. However, it should be noted that LOC-GTRS does not include a detection mechanism for coordinated attacker models. Therefore, the comparison between the proposed algorithm and LOC-GTRS is made solely based on the RMSE of the estimate after the detection of attackers. Figure 12 and 13 depicts the localization error comparison of the proposed technique and LOC-GTRS for attacker model 1. Figure 12 shows the RMSE performance of attacker model 1 with 2 attackers for a network with 7 nodes represented by red and cyan lines and 8 nodes represented by pink dotted and green dashed lines.

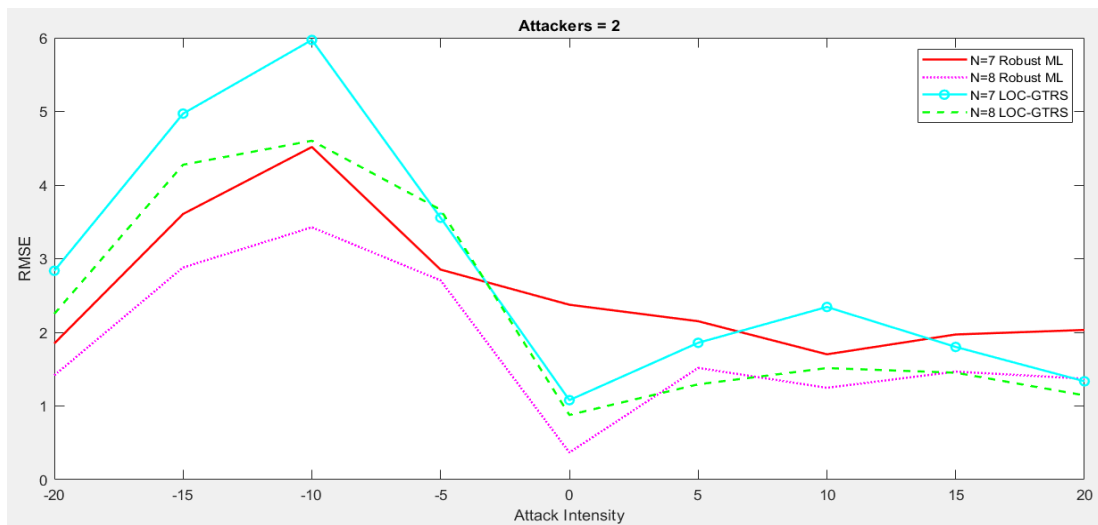


Figure 12: RMSE Comparison with LOC\_GTRS for 2 Attackers

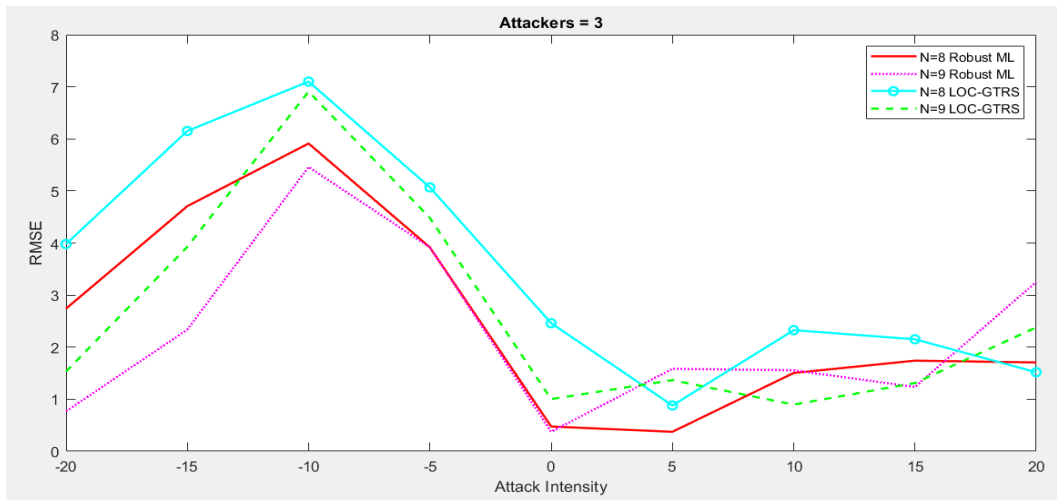


Figure 13: RMSE Comparison with LOC\_GTRS for 3 Attackers

Figure 13 shows the localization error performance of attacker model 1 with 3 attackers for a network with 8 nodes represented by red and cyan lines and 9 nodes represented by pink dotted and green dashed lines.

### 5.1.2 Probability of Detection Analysis for Attacker Model 1

The proposed secure localization algorithm's performance is evaluated by analyzing Attacker Model 1. In this model, the probability of detection is compared for scenarios involving 2 attackers, with a total number of nodes set at 6, 7, and 8 in Figures 14, 15, and 16, respectively.

It can be observed from Figures 14, 15, and 16 that when the attacker intensity is greater, the detection is accurate and when the attacker intensity is less, the malicious nodes are hard to detect resulting in false detections. Enlargement attacks are easily detected as compared to reduction attacks. When the attacker intensity is zero, there is no change in the distance measurement of the attacker so there is no detection.

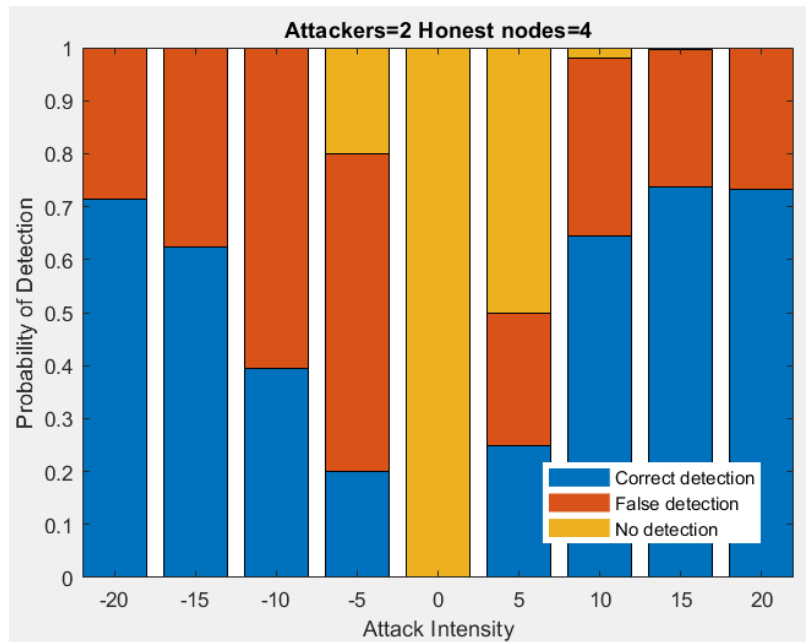


Figure 14: Probability of Detection Bar Chart with 2 Attackers and 4 Honest Nodes

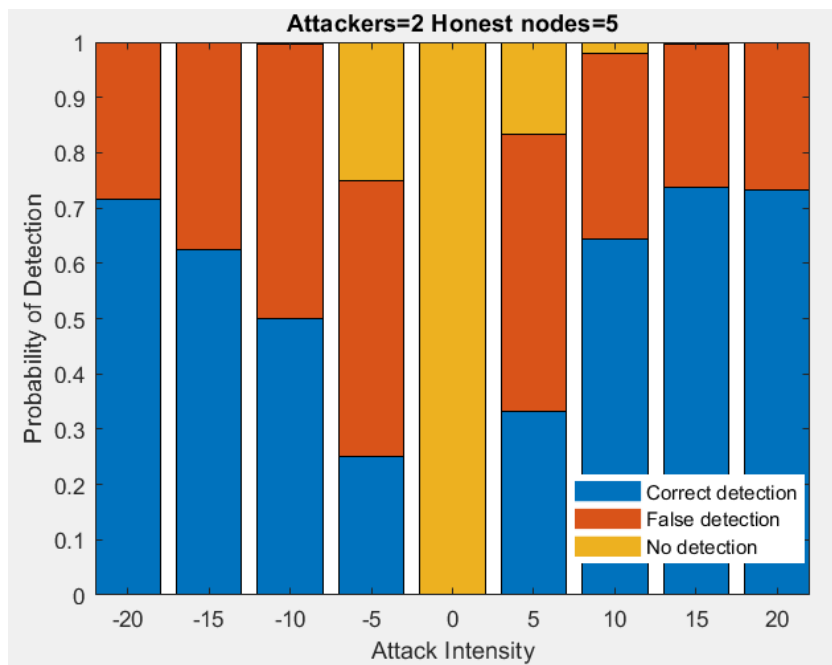


Figure 15: Probability of Detection Bar Chart with 2 Attackers and 5 Honest Nodes

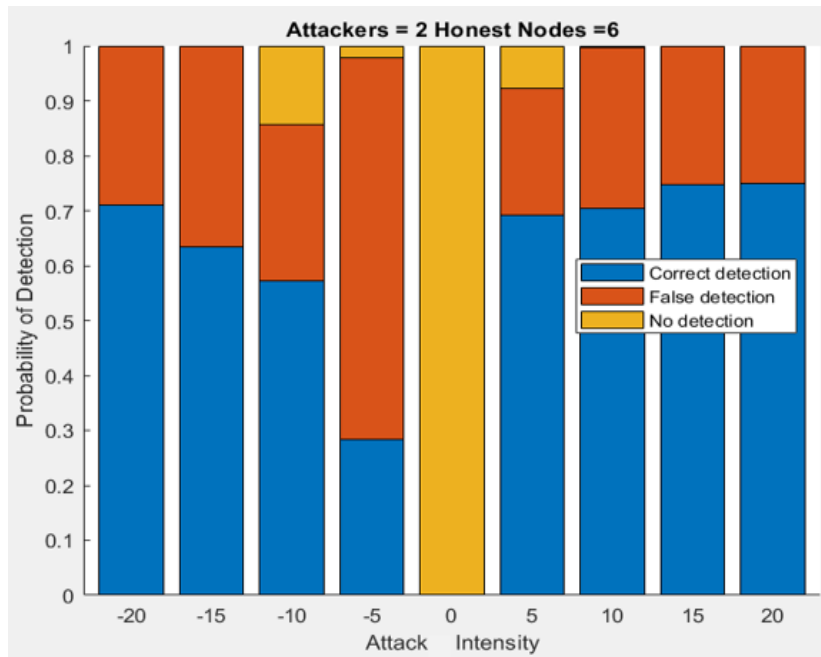


Figure 16: Probability of Detection Bar Chart with 2 Attackers and 6 Honest Nodes

Based on these observations, it can be concluded that the system performs well in both dense and sparse node environments. This suggests that the system is robust and can effectively detect attacks regardless of the density of the network nodes.

Figures 17 and 18 present scenarios with 7 and 8 nodes with 3 attackers. Comparative analysis of the figures deduces that there is a relatively smaller difference in the detection rates at higher attack intensities. As the number of honest nodes increases, the system becomes better equipped for accurate detection. The performance of detection is better for coordinated enlargement attacks as compared to coordinated reduction attacks.

Based on these observations, it can be concluded that the system performs well in both dense and sparse node environments. This suggests that the system is robust and can effectively detect attacks regardless of the density of the network nodes.



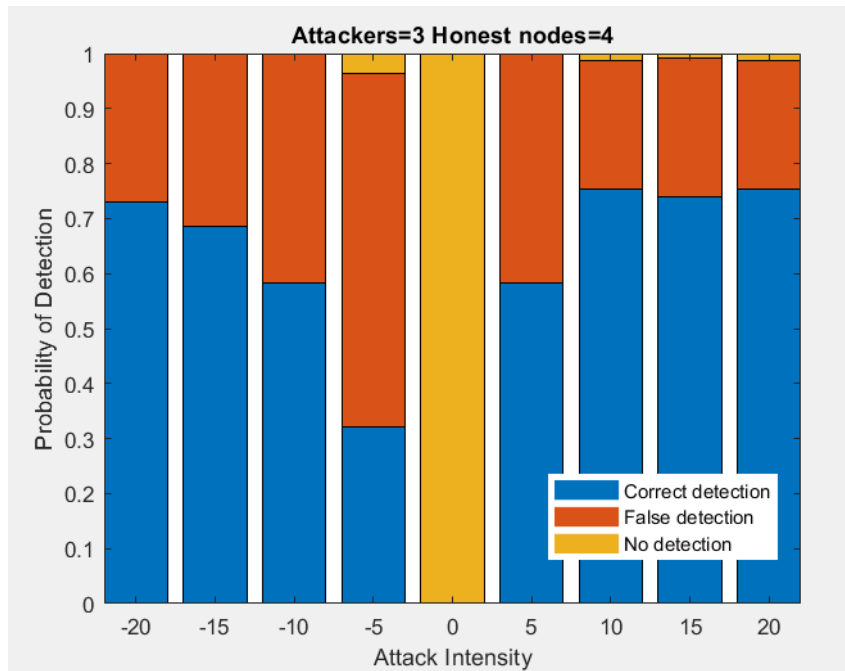


Figure 17: Probability of Detection Bar Chart with 3 Attackers and 4 Honest Nodes

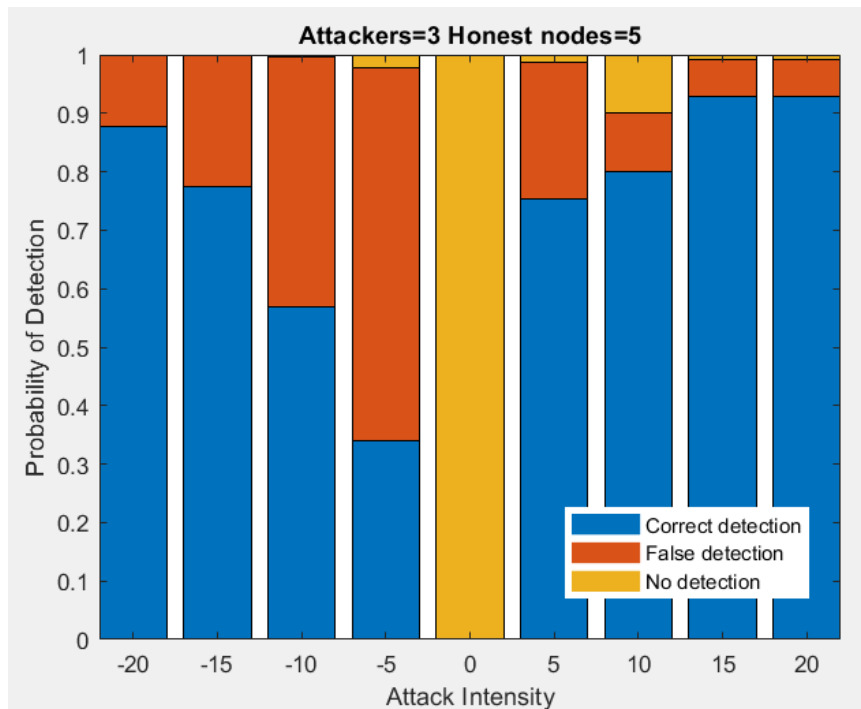


Figure 18: Probability of Detection Bar Chart with 3 Attackers and 5 Honest Nodes

### 5.1.3 RMSE Analysis for Attacker Model 2

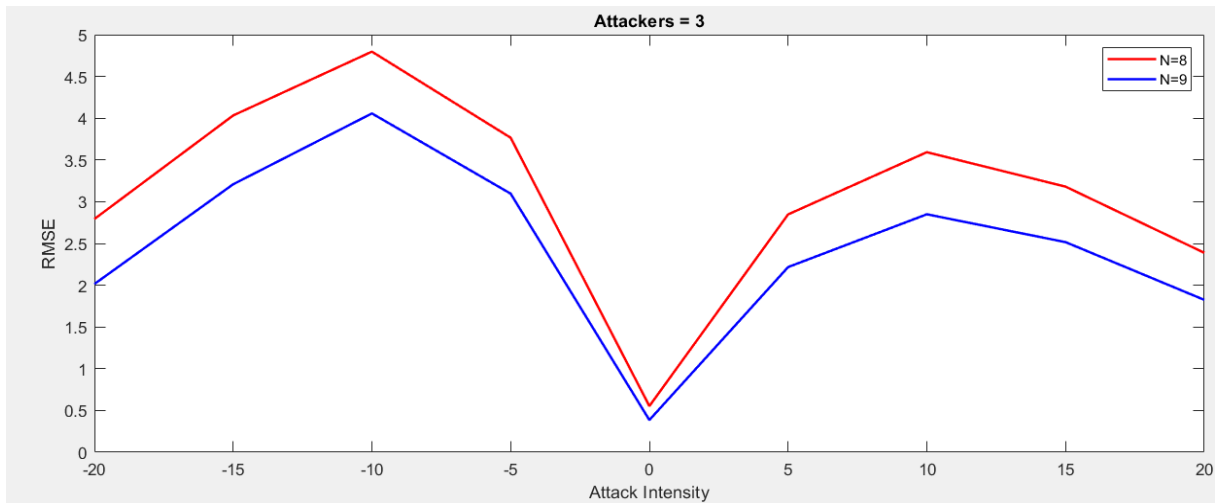


Figure 19: RMSE Comparison for 3 Attackers

Figures 19, 20, and 21 display the RMSE for attacker model 2. In comparison to Attacker Model 1, the RMSE demonstrates symmetry, and the error is similar to coordinated enlargement attacks, which performed better than coordinated reduction attacks. Additionally, the algorithm's performance surpasses that of the LOC-GTRS for Attack Model 2 as well.

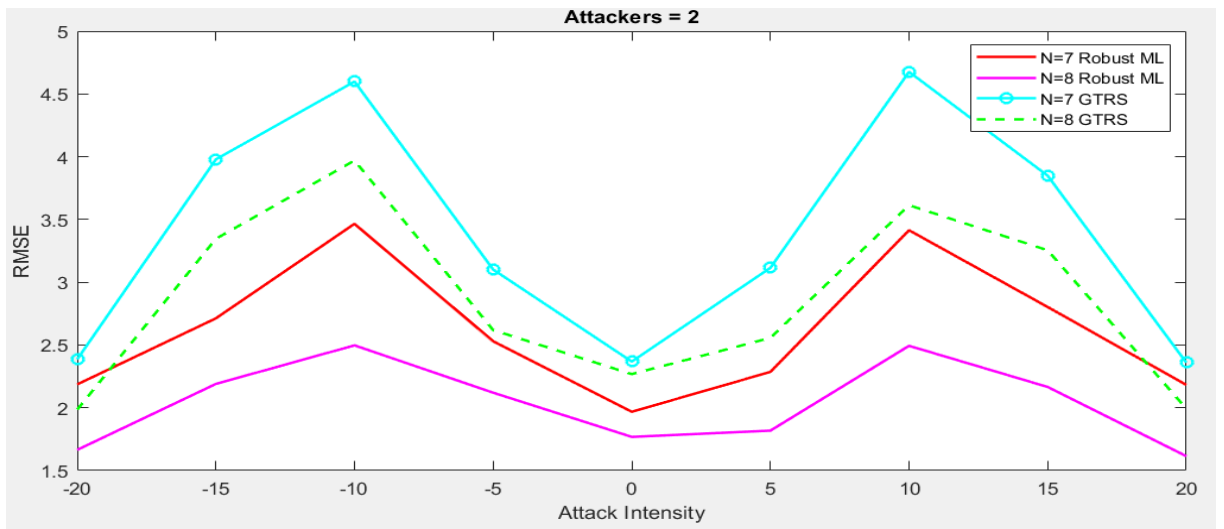


Figure 20: RMSE Comparison with LOC\_GTRS for 2 Attackers

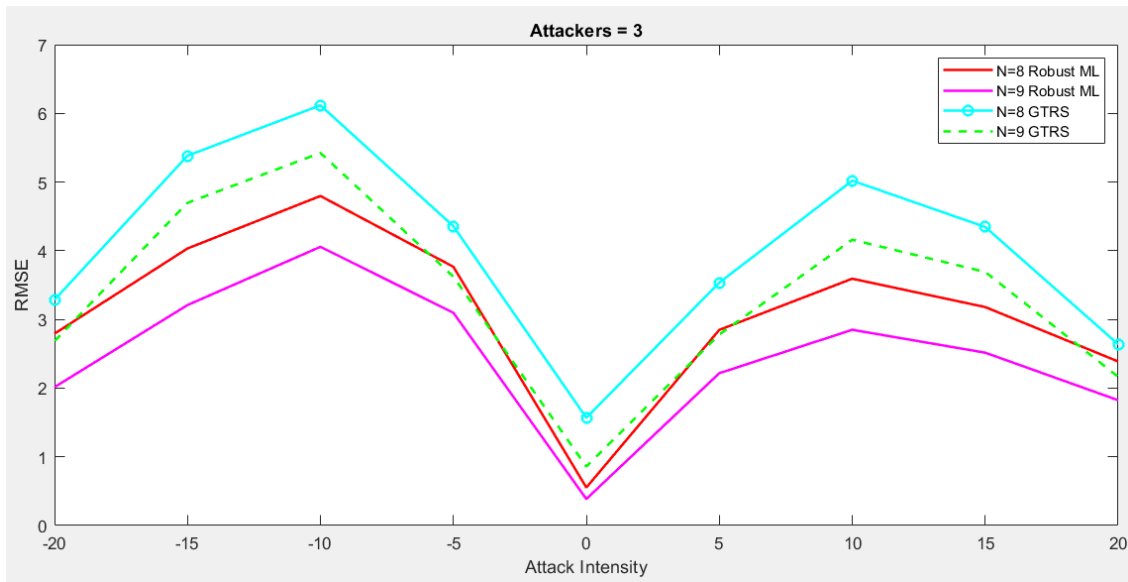


Figure 21: RMSE Comparison with LOC\_GTRS for 3 Attackers

### 5.1.4 Probability of Detection Analysis for Attacker Model 2

Figures 22, 23, and 24 illustrate the Probability of Detection Bar Chart for Attacker Model 2. When 33.33% of the nodes in a network are attackers, the probability of correct detection is higher when the attackers have a high intensity. This is supported by Figures 22 and 23 representing 2 and 3 attackers respectively where the detection probability remains consistent for higher intensities. Additionally, the probability of correct detection increases for low attack intensities when the total number of nodes increases, while keeping the attackers' percentage the same.

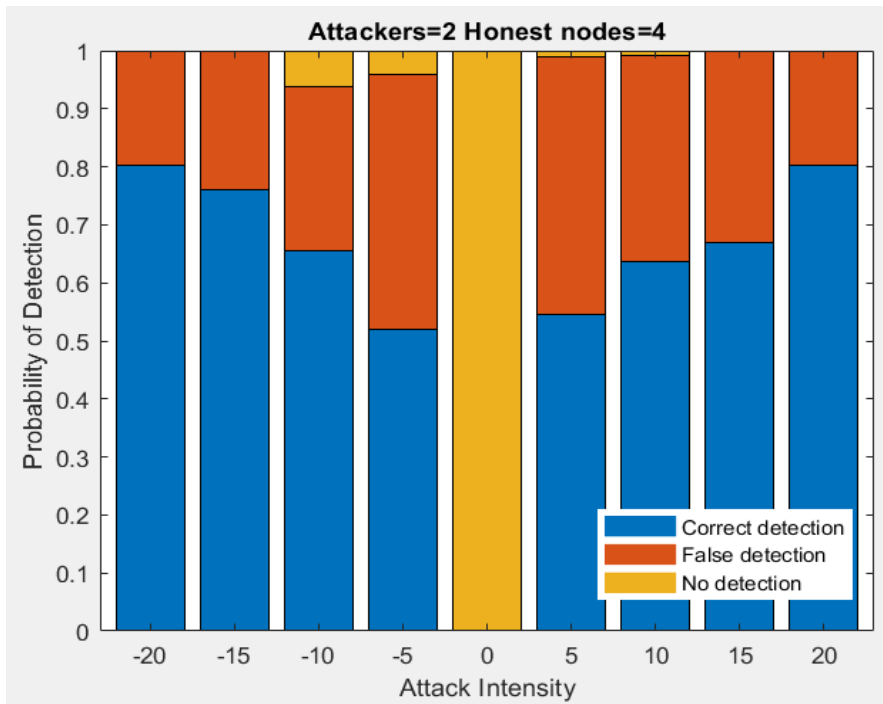


Figure 22: Probability of Detection Bar Chart with 2 Attackers and 4 Honest Nodes

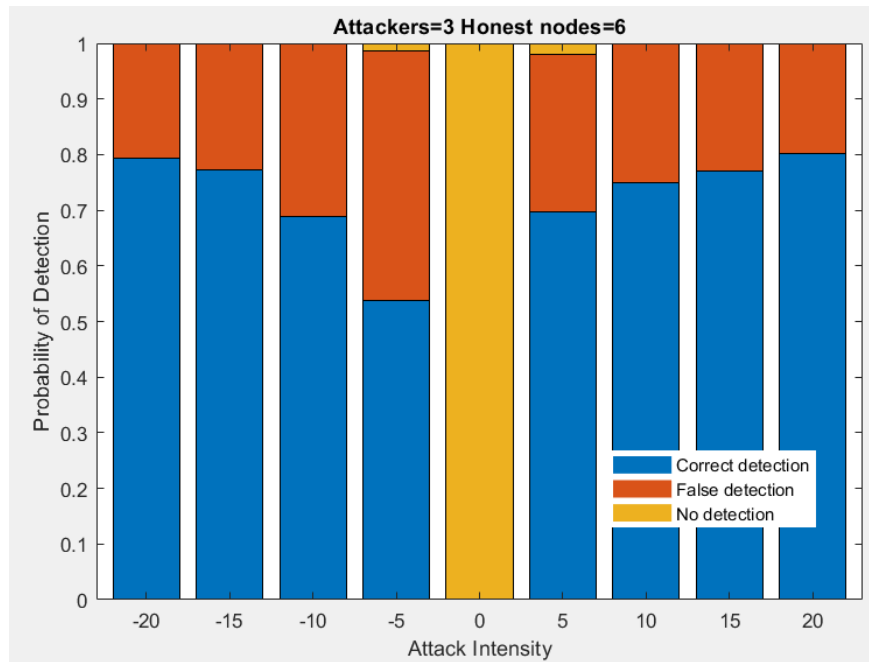


Figure 23: Probability of Detection Bar Chart with 3 Attackers and 6 Honest Nodes

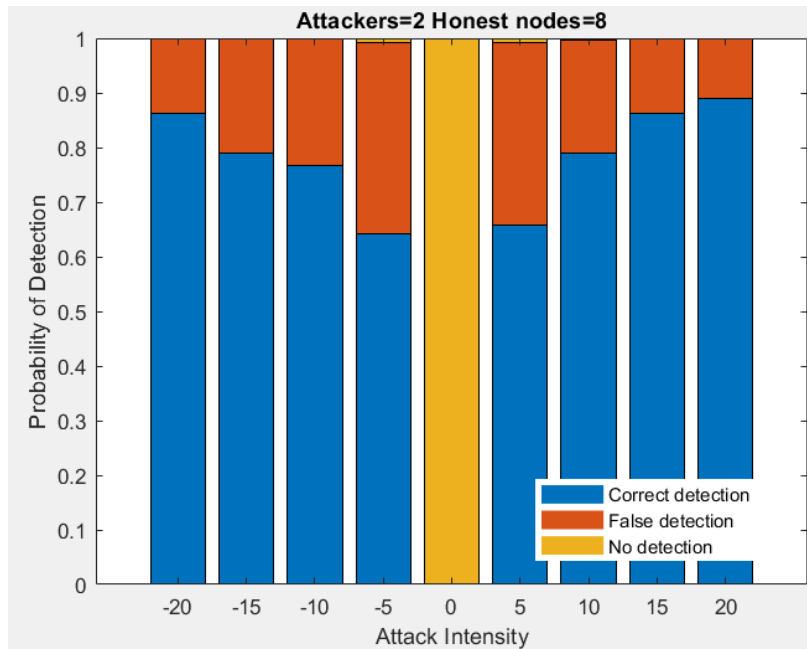


Figure 24: Probability of Detection Bar Chart with 2 Attackers and 8 Honest Nodes

Furthermore, when the percentage of attackers is reduced to 20% of the total nodes in the network, the probability of detection improves significantly compared to when 33.33% of the nodes are attackers as illustrated in Figure 24. Figure 24 depicts the network's detection probability when there are 2 attackers and 10 honest nodes, representing a 20% attacker ratio. Based on figures 22, 23, and 24, it can be deduced that the probability of detecting attackers in a network is influenced by both the percentage of attackers and their attack intensity. Decreasing the percentage of attackers or increasing their attack intensity leads to higher detection probabilities.

Nevertheless, when compared to Attack Model 1, Attack Model 2 falls short in achieving a high probability of detection, especially when compared to the exclusive enlargement attack. Therefore, the system demonstrates its optimal performance in terms of detection probability when facing enlargement attacks.

### 5.1.5 RMSE Analysis for Failed Detection to Check Robustness

To evaluate the algorithm's robustness, the position estimate is scrutinized by deliberately manipulating the detection model to exclude specific attackers. The resulting estimate is then compared with the estimation obtained through the LOC-GTRS approach, using the same missed attack detection model. Even in cases where the detection fails, the RMSE performance outperforms that of LOC-GTRS. In Figure 25, the total number of nodes is 8 out of which 3 are attackers and the detection model is manipulated to detect only 2 attackers. The attacker detected are excluded from the measurement model and both proposed Robust ML-based estimation and LOC\_GTRS estimation is performed. The RMSE graph illustrates that the proposed technique outperforms the LOC-GTRS approach.

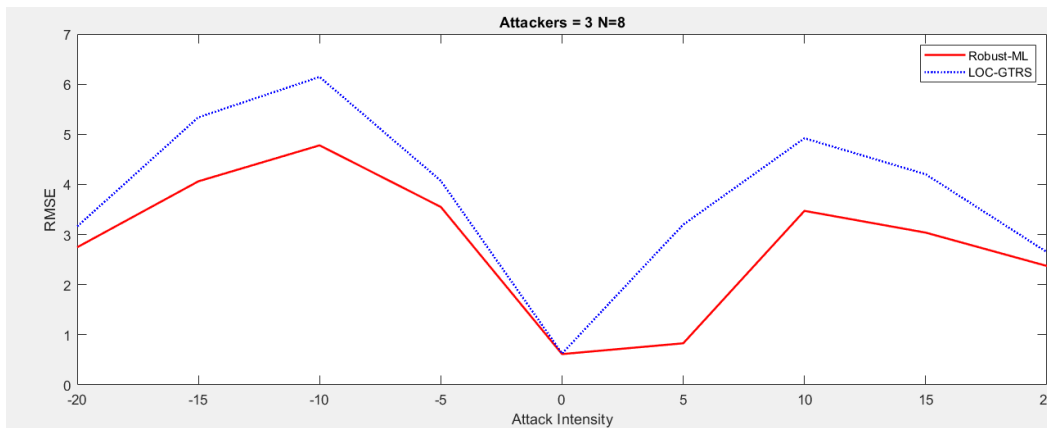


Figure 25: Robustness Check of Estimation

### 5.1.6 Convergence Rate Comparison

While aiming for accuracy in secure localization schemes, certain limitations on network topology and the presence of noise are often encountered. These schemes typically assume that the problem can be represented by a convex hull, which simplifies calculations due to the availability of closed-

form solutions. However, non-line-of-sight (NLOS) conditions, environmental biases, and the specific topology of the nodes can render localization a non-convex problem.

A comparison with recent literature that provides localization solutions addressed for non-convex scenarios is presented in Table 3.

$N$  represents the total number of nodes,  $\mathcal{E}$  denotes the number of iterations required for VMP[47] to converge,  $N_p$  denotes the number of particles drawn by sampling in VBL[28],  $\eta$  is the number of iterations required for VBL to converge,  $B_{max}$  is the number of bisection steps and  $CF_{max}$  denotes the number of iterations required by the proposed algorithm estimation to converge. Among the localization schemes documented in the literature, enlargement\_attack\_GTRS and LOC\_GTRS provide the best convergence rate.

Table 3: Performance Complexity Comparison

<b>ALGORITHM</b>	<b>COMPLEXITY</b>
VBL [28]	$\sigma(NN_p\eta)$
Enlargement_attack_GTRS [40]	$\sigma(NB_{max})$
LOC-GTRS [41]	$\sigma(NB_{max})$
MM-NLWLS [43]	$\sigma(kN)$
VMP [47]	$\sigma(8(N+1)\mathcal{E})$
WLS [48]	$\sigma(N)$
Proposed scheme	$\sigma(NCF_{max})$

The proposed algorithm is compared against LOC-GTRS. In the proposed algorithm, the maximum iteration counter is fixed at 10, while the LOC-GTRS approach sets it to 30. The

performance evaluation demonstrates that the proposed algorithm achieves faster convergence compared to LOC-GTRS. In contrast, the proposed scheme achieves precise position calculation and exhibits rapid convergence.

### **5.1.7 Summary**

In this chapter a detailed comparative analysis is presented, illustrating the comparison between two localization approaches: the proposed Robust Maximum Likelihood-based approach and the Generalized Trust Region Subproblem law of cosines (GTRS-LOC) based approach discussed in [41]. The localization approach described in [41] utilizes the law of cosines to transform the quadratic objective function into a GTRS problem. On the other hand, the Robust Maximum Likelihood approach utilizes RSS measurements. Upon conducting an analysis based on the evaluation metrics, the following are inferred:

- The robust Maximum Likelihood approach yields lower localization errors compared to the method in LOC-GTRS.
- The proposed system can detect coordinated attacks, unlike LOC-GTRS.
- The robust Maximum Likelihood approach applies to a variety of network environments. This versatility allows the RML approach to be deployed and adapted in diverse scenarios, accommodating different network structures and characteristics.
- The proposed approach exhibits faster convergence compared to the method presented in [41]. This means that the Robust Maximum Likelihood approach can efficiently achieve low localization error.



## 6. Conclusion

This chapter serves as the conclusion of the research, presenting a comprehensive summary of the research findings, limitations, and potential future work. It provides an overview of the proposed work, and how it will impact the domain of WSN security. Furthermore, this chapter addresses the limitations of the proposed work and suggests avenues for future research.

### 6.1 Key Findings

This thesis addresses the research conducted in response to the high demand for location-aware wireless sensor networks (WSNs). WSNs possess unique characteristics that give rise to various challenges concerning localization and communication. Within this thesis, we tackle two key challenges which are accurate location information and detection of malicious entities. We propose a computationally efficient and robust scheme to achieve the challenges.

To achieve this, we utilize the distance measurement and received signal strength measurement while catering to both Line of sight and non-line-of-sight scenarios. The adoption of the scheme results in distinct advantages in terms of ranging and reliable communication. This scheme can be used in diverse environments as it does not impose plenty of conditions on the network noise, topology, or communication protocol.

In the domain of environmental monitoring, secure localization in WSN will ensure precise spatial information acquisition of environmental parameters, including temperature, humidity, and pollution levels. Surveillance and monitoring systems will benefit from secure localization,

enabling reliable and secure positioning of valuable assets in real-time. Healthcare systems will leverage secure localization for precise localization of wearable or implantable medical devices, enhancing patient monitoring and emergency response. The military and air defense industry will leverage secure localization systems to identify the enemy target, thereby improving situational awareness and threat detection capabilities.

## **6.2 Limitations**

As localization requires a minimum of 3 sensors for 2-dimensional position estimation and 4 sensors for 3-dimensional position estimation if Sybil nodes can penetrate the network such that they overpower honest nodes, the position will not be calculated accurately. Moreover, since the algorithm focuses on enlargement and reduction attacks, any attacker that performs a passive attack will not be detected.

## **6.3 Future Directions**

The presented work can make a significant contribution toward secure localization in WSN. However, there is room for further research as follows:

- Improving the detection of malicious identity when the attack intensity is low.
- Reducing the computational cost of the localization algorithm by devising a more robust yet lightweight localization scheme.

- Extending the secure localization to detect and prevent other attacks as well other than enlargement and reduction attacks e.g., passive attacks, and jamming attacks.

# Bibliography

- [1] M. Amarlingam, P. K. Mishra, K. V. V Durga Prasad, and P. Rajalakshmi, “Compressed sensing for different sensors: A real scenario for WSN and IoT,” in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016, pp. 289–294. doi 10.1109/WF-IoT.2016.7845487.
- [2] M. Keerthika and D. Shanmugapriya, “Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures,” *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362–367, 2021, doi: <https://doi.org/10.1016/j.gltp.2021.08.045>.
- [3] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, “Data Collection for Security Measurement in Wireless Sensor Networks: A Survey,” *IEEE Internet Things J*, vol. 6, no. 2, pp. 2205–2224, 2019, doi 10.1109/JIOT.2018.2883403.
- [4] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: attack and defense strategies,” *IEEE Netw*, vol. 20, no. 3, pp. 41–47, 2006, doi: 10.1109/MNET.2006.1637931.
- [5] M. Smache, N. El Mrabet, J.-J. Gilquijano, A. Tria, E. Riou, and C. Gregory, “Modeling a node capture attack in a secure wireless sensor network,” in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016, pp. 188–193. doi 10.1109/WF-IoT.2016.7845447.
- [6] M. Conti, R. Di Pietro, L. Mancini, and A. Mei, “Distributed Detection of Clone Attacks in Wireless Sensor Networks,” *IEEE Trans Dependable Secure Comput*, vol. 8, no. 5, pp. 685–698, 2011, doi: 10.1109/TDSC.2010.25.
- [7] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, “A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks,” *IEEE Sens J*, vol. 15, no. 6, pp. 3590–3602, 2015, doi: 10.1109/JSEN.2015.2395442.
- [8] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: analysis & defenses,” in *Third International Symposium on Information Processing in Sensor Networks, 2004. IPSN 2004*, 2004, pp. 259–268.
- [9] N. M. Alajmi and K. Elleithy, “A New Approach for Detecting and Monitoring of Selective Forwarding Attack in Wireless Sensor Networks.”

- [10] Z. Zhao, B. Wei, X. Dong, L. Yao, and F. Gao, "Detecting wormhole attacks in wireless sensor networks with statistical analysis," in *Proceedings - 2010 WASE International Conference on Information Engineering, ICIE 2010*, 2010, pp. 251–254. doi: 10.1109/ICIE.2010.66.
- [11] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a sinkhole attack in wireless sensor networks; the intruder side," in *Proceedings - 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communication, WiMob 2008*, 2008, pp. 526–531. doi: 10.1109/WiMob.2008.83.
- [12] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming," *IEEE Access*, vol. 7. Institute of Electrical and Electronics Engineers Inc., pp. 156237–156271, 2019. doi: 10.1109/ACCESS.2019.2949703.
- [13] S. Awadallah, D. Moure, and P. Torres-González, "An internet of things (IoT) application on volcano monitoring," *Sensors (Switzerland)*, vol. 19, no. 21, Nov. 2019, doi: 10.3390/s19214651.
- [14] K. Sharma, D. Anand, M. Sabharwal, P. K. Tiwari, O. Cheikhrouhou, and T. Frikha, "A Disaster Management Framework Using Internet of Things-Based Interconnected Devices," *Math Probl Eng*, vol. 2021, 2021, doi: 10.1155/2021/9916440.
- [15] D. Niculescu and B. Nath, "Ad hoc positioning system (APS)," in *Conference Record / IEEE Global Telecommunications Conference*, 2001, pp. 2926–2931. doi: 10.1109/glocom.2001.965964.
- [16] A. Beck, P. Stoica, and J. Li, "Exact and approximate solutions of source localization problems," *IEEE Transactions on Signal Processing*, vol. 56, no. 5, pp. 1770–1778, 2008, doi: 10.1109/TSP.2007.909342.
- [17] S. Tomic, M. Beko, and R. Dinis, "RSS-based localization in wireless sensor networks using convex relaxation: Noncooperative and cooperative schemes," *IEEE Trans Veh Technol*, vol. 64, no. 5, pp. 2037–2050, May 2015, doi: 10.1109/TVT.2014.2334397.
- [18] Y. Wang and K. C. Ho, "An Asymptotically Efficient Estimator in Closed-Form for 3-D AOA Localization Using a Sensor Network," *IEEE Trans Wirel Commun*, vol. 14, no. 12, pp. 6524–6535, Dec. 2015, doi: 10.1109/TWC.2015.2456057.

- [19] A. Coluccia and A. Fascista, “On the Hybrid TOA/RSS Range Estimation in Wireless Sensor Networks,” *IEEE Trans Wirel Commun*, vol. 17, no. 1, pp. 361–371, Jan. 2018, doi: 10.1109/TWC.2017.2766628.
- [20] L. Lazos and R. Poovendran, “SeRLoc: Robust Localization for Wireless Sensor Networks.”
- [21] L. Lazos and R. Poovendran, “HiRLoc: High-resolution robust localization for wireless sensor networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 233–246, Feb. 2006, doi: 10.1109/JSAC.2005.861381.
- [22] S. Čapkun, “Secure positioning in wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, Feb. 2006, doi: 10.1109/JSAC.2005.861380.
- [23] M. Singh, P. Leu, A. Abdou, and S. Capkun, “UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband,” in *28th USENIX Security Symposium (USENIX Security 19)*, Santa Clara, CA: USENIX Association, Aug. 2019, pp. 73–88. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity19/presentation/singh>
- [24] M. Singh, P. Leu, A. Abdou, S. Capkun, and E. Zurich, *UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband*. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity19/presentation/singh>
- [25] D. Liu, P. Ning, A. Liu, C. Wang, and W. K. Du, “Attack-Resistant Location Estimation in Wireless Sensor Networks,” *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 4, Jul. 2008, doi: 10.1145/1380564.1380570.
- [26] S. Kumar and R. M. Hegde, “Indoor node localization using geometric dilution of precision in ad-hoc sensor networks,” in *Conference Record - Asilomar Conference on Signals, Systems and Computers*, IEEE Computer Society, Apr. 2015, pp. 1525–1529. doi: 10.1109/ACSSC.2014.7094718.
- [27] S. Tomic, M. Beko, and M. Tuba, “Exploiting Orientation Information to Improve Range-Based Localization Accuracy,” *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2978298.
- [28] Y. Li, S. Ma, G. Yang, and K. K. Wong, “Robust Localization for Mixed LOS/NLOS Environments with Anchor Uncertainties,” *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4507–4521, Jul. 2020, doi: 10.1109/TCOMM.2020.2982633.

- [29] S. Hartung, A. Bochem, A. Zdziarstek, and D. Hogrefe, "Applied Sensor-Assisted Monte Carlo Localization for Mobile Wireless Sensor Networks," in *Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks*, in EWSN '16. USA: Junction Publishing, 2016, pp. 181–192.
- [30] A. Bochem and H. Zhang, "Robustness Enhanced Sensor Assisted Monte Carlo Localization for Wireless Sensor Networks and the Internet of Things," *IEEE Access*, vol. 10, pp. 33408–33420, 2022, doi: 10.1109/ACCESS.2022.3162288.
- [31] C. Zhou, H. Tian, and B. Zhong, "An improved MCB localization algorithm based on weighted rssi and motion prediction," *Computer Science and Information Systems*, vol. 17, no. 3, pp. 779–794, Oct. 2020, doi: 10.2298/CSIS200204020Z.
- [32] H. Wu, H. Wu, J. Liu, Z. Dong, Y. Liu, and Y. Liu, "A Hybrid Mobile Node Localization Algorithm Based on Adaptive MCB-PSO Approach in Wireless Sensor Networks," *Wirel Commun Mob Comput*, vol. 2020, 2020, doi: 10.1155/2020/3845407.
- [33] L. Hu and D. Evans, "Localization for Mobile Sensor Networks," 2004.
- [34] C. Y. Wei and C. C. Chen, "Cube-Based Multitarget 3D Localization Using Bayesian Learning-Based Turbo Decoding in Wireless Sensor Networks," *IEEE Sens J*, vol. 22, no. 17, pp. 17291–17306, Sep. 2022, doi: 10.1109/JSEN.2022.3193021.
- [35] A. Coluccia and A. Fascista, "Hybrid TOA/RSS Range-Based Localization with Self-Calibration in Asynchronous Wireless Networks," *Journal of Sensor and Actuator Networks*, vol. 8, no. 2, 2019, doi 10.3390/jsan8020031.
- [36] M. Khalaf-Allah, "Performance Comparison of Closed-Form Least Squares Algorithms for Hyperbolic 3-D Positioning," *Journal of Sensor and Actuator Networks*, vol. 9, no. 1, 2020, doi: 10.3390/jsan9010002.
- [37] W. Xiong and H. C. So, "TOA-Based Localization With NLOS Mitigation via Robust Multidimensional Similarity Analysis," *IEEE Signal Process Lett*, vol. 26, no. 9, pp. 1334–1338, 2019, doi: 10.1109/LSP.2019.2929860.
- [38] S. Tomic and M. Beko, "A geometric approach for distributed multi-hop target localization in cooperative networks," *IEEE Trans Veh Technol*, vol. 69, no. 1, pp. 914–919, Jan. 2020, doi: 10.1109/TVT.2019.2952715.

- [39] W. Xiong, C. Schindelhauer, H. C. So, and Z. Wang, "Maximum Correntropy Criterion for Robust TOA-Based Localization in NLOS Environments," *Circuits Syst Signal Process*, vol. 40, no. 12, pp. 6325–6339, 2021, doi: 10.1007/s00034-021-01800-y.
- [40] M. Beko and S. Tomic, "Toward Secure Localization in Randomly Deployed Wireless Networks," *IEEE Internet Things J*, vol. 8, no. 24, pp. 17436–17448, Dec. 2021, doi: 10.1109/JIOT.2021.3078216.
- [41] S. Tomic and M. Beko, "Detecting Distance-Spoofing Attacks in Arbitrarily-Deployed Wireless Networks," *IEEE Trans Veh Technol*, vol. 71, no. 4, pp. 4383–4395, Apr. 2022, doi: 10.1109/TVT.2022.3148199.
- [42] P. Zuo, H. Zhang, C. Wang, H. Jiang, and B. Pan, "Directional target localization in NLOS environments using RSS-TOA combined measurements," *IEEE Wireless Communications Letters*, vol. 10, no. 11, pp. 2602–2606, Nov. 2021, doi: 10.1109/LWC.2021.3109787.
- [43] K. Panwar, M. Katwe, P. Babu, P. Ghare, and K. Singh, "A Majorization-Minimization Algorithm for Hybrid TOA-RSS Based Localization in NLOS Environment," *IEEE Communications Letters*, vol. 26, no. 5, pp. 1017–1021, May 2022, doi: 10.1109/LCOMM.2022.3155685.
- [44] D. Q. F. de Menezes, D. M. Prata, A. R. Secchi, and J. C. Pinto, "A review on robust M-estimators for regression analysis," *Comput Chem Eng*, vol. 147, p. 107254, 2021, doi: <https://doi.org/10.1016/j.compchemeng.2021.107254>.
- [45] A. Zaeemzadeh, M. Joneidi, B. Shahrabi, and N. Rahnavard, "Robust Target Localization Based on Squared Range Iterative Reweighted Least Squares," Feb. 2018, doi: 10.1109/MASS.2017.50.
- [46] W. Xiong, S. Mohanty, and C. Schindelhauer, "A Low-Complexity Iterative Message Passing Algorithm for Robust RSS-TOA IoT Localization," *IEEE Internet Things J*, p. 1, 2023, doi: 10.1109/JIOT.2023.3267100.
- [47] Y. Li, S. Ma, G. Yang, and K.-K. Wong, "Secure Localization and Velocity Estimation in Mobile IoT Networks With Malicious Attacks," *IEEE Internet Things J*, vol. 8, no. 8, pp. 6878–6892, 2021, doi: 10.1109/JIOT.2020.3036849.



- [48] B. Mukhopadhyay, S. Srirangarajan, and S. Kar, “Robust Range-Based Secure Localization in Wireless Sensor Networks,” in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6. doi: 10.1109/GLOCOM.2018.8647742.

**Certificate for Plagiarism**

It is certified that PhD/M.Phil/MS Thesis Titled "SECURE LOCALIZATION ALGORITHM TO DETECT SYBIL ATTACK IN WIRELESS SENSOR NETWORKS" by FAKIHA KHAN has been examined by us. We undertake the follows:

- a. Thesis has significant new work/knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
- b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.
- c. There is no fabrication of data or results which have been compiled/analyzed.
- d. There is no falsification by manipulating research materials, equipment or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
- e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC plagiarism Policy and instructions issued from time to time.

**Name & Signature of Supervisor**

Dr. Mehdi Hussain

Signature : 