Neighbour-Based Malicious Node Detection in Wireless Sensor network

MINOR PROJECT-1 REPORT

Submitted by

SAKETH. B

VENUMADHAV. CH

URDHVA RAGHAV. B

Under the Guidance of

Dr. K. ANISH PON YAMINI

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

ELECTRONICS & COMMUNICATION ENGINEERING

Vel Tech
Rangarajan Dr. Sagunthala
R&D Institute of Science and Technology
(Deemed to be University Estd. u/s 3 of UGC Act, 1956)

MAY 2024

Vel Tech
Rangarajan Dr. Sagunthala
R&D Institute of Science and Technology
(Deemed to be University Estd. u/s 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this Minor project-1 report entitled **"Neighbour-Based Malicious Node Detection in Wireless Sensor network"** is the bonafide work of **"SAKETH. B(21UEEB0037), VENUMADHAV. CH (21UEEB0007) and URDHVA RAGHAV. B (21UEEB0002)"** who carried out the project work under my supervision.

SUPERVISOR

Dr. K. ANISH PON YAMINI
Assistant Professor
Department of ECE

HEAD OF THE DEPARTMENT

Dr.A. SELWIN MICH PRIYADHARSON
Professor
Department of ECE

Submitted for Minor project-1 work viva-voce examination held on:_____

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We express our deepest gratitude to our Respected Founder President and Chancellor **Col. Prof. Dr. R. Rangarajan**, Foundress President **Dr. R. Sagunthala Rangarajan**, Chairperson and Managing Trustee and Vice President.

We are very thankful to our beloved Vice Chancellor **Prof. Dr. S. Salivahanan** for providing us with an environment to complete the work successfully.

We are obligated to our beloved Registrar **Dr. E. Kannan** for providing immense support in all our endeavours. We are thankful to our esteemed Dean Academics **Dr. A. T. Ravichandran** for providing a wonderful environment to complete our work successfully.

We are extremely thankful and pay my gratitude to our Dean SoEC **Dr. R. S. Valarmathi** for her valuable guidance and support on completion of this project.

It is a great pleasure for us to acknowledge the assistance and contributions of our Head of the Department **Dr. A. Selwin Mich Priyadharson**, Professor for his useful suggestions, which helped us in completing the work in time and we thank him for being instrumental in the completion of third year with his encouragement and unwavering support during the entire course. We are extremely thankful and pay our gratitude to our Minor project -1 coordinator **Dr. Kanimozhi T**, for her valuable guidance and support on completing this project report in a successful manner.

We are grateful to our supervisor **Dr. K. ANISH PON YAMINI**, Associate Professor ECE for providing me the logistic support and her valuable suggestion to carry out our project work successfully.

We thank our department faculty, supporting staffs and our family and friends for encouraging and supporting us throughout the project.

SAKETH. B

VENUMADHAV. CH

URDHVA RAGHAV. B

TABLE OF CONTENTS

ABSTRACT

This project focuses on developing an advanced neighbor-based detection system for Wireless Sensor Networks(WSNs). The system uses sophisticated methods to spot, communicate, and isolate nodes that act strangely or harmfully, and thus enhance the WSN security and reliability. The methods use machine learning, statistics and behavioral patterns to detect abnormal or malicious activity in a node. Extensive simulations across various scenarios will evaluate the performance, such as node density, mobility, and topology, and the effectiveness of the system in different situations can be evaluated.

The effectiveness of the system will be determined using key performance metrics such as detect, avoid, and react to bad nodes, using key performance metrics such as detection rates, false positives, and time-to-detect. Additionally, this project will also consider how to make the system perform in real world, with resources constraints, scalability, and different needs. The project will help improve network security against new threats, and make wireless sensor networks stronger and more reliable, safeguarding critical infrastructures and sensitive data.

The wireless sensor network is an architecture of connected nodes; each node has its main elements such as sensors, computation and communications capabilities. Ad-hoc WSNs restrained energy sources result in a shorter lifetime of the sensor network and inefficient topology. In this paper, a new approach for saving and energy controlling is introduced using quality of service. The main reason is to reduce the node's energy through discovering the best optimum route that meets QoS requirements; QoS technique is used to find the optimum methodology for nodes packets transmission and energy consumption. The primary goals of the research are to discover the best techniques to:

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Wireless sensor network

In a wireless sensor network, operating in a harsh and unattended environment, sensor nodes may generate incorrect sensor readings and wrong reports to their neighbors, causing incorrect decisions or energy depletion. The potential sources of incorrect readings and reports include noise, faults, and malicious nodes in the network. Unlike noise and faults, malicious nodes can arbitrarily modify the sensed data and intentionally generate wrong reports. To ensure a reliable event detection in the presence of such wrong data and reports, it is necessary to detect and isolate malicious nodes, greatly reducing their impact on decision-making. Several fault detection schemes for wireless sensor networks have been proposed in the literature . They use centralized, distributed, or hierarchical models. Due to the communication overhead most schemes employ a distributed model, using either neighbor coordination or clustering. As the fault or error models for detection, noise and a few types of faults, such as transient and permanent faults, are typically used. Malicious nodes, however, can generate arbitrary sensor readings which do not conform to the typically used fault models. In that case, the resulting malicious node detection rate becomes much poorer than the estimated one. Rajasegarar et al. presented an overview of existing outlier detection schemes for wireless sensor networks . Sensor readings that appear to be inconsistent with the remainder of the data set are the main target of the detection. Curiacetal. proposed a detection scheme using autoregression technique. Signal strength is used to detect malicious nodes in , where a message transmission is considered suspicious if the strength is incompatible with the originator's geographical position. Xiaoetal. developed a mechanism for rating sensors in terms of correlation by exploring Markov Chain . A network voting algorithm is proposed to determine faulty sensor readings. Atakli et al.presented a malicious node detection scheme using weighted trust evaluation for a three-layer hierarchical network architecture. Trust values are employed to identify malicious nodes behaving opposite to the sensor readings. They are updated depending on the distribution of neighboring nodes. An improved intrusion detection scheme based on weighted trust evaluation was proposed . The mistaken ratio of each individual sensor node is used in updating the trust values. Trust management schemes have been proposed in routing and

communications . Some efforts are also being mad to combine communication and data trusts. However, malicious node detection in the presence of various types of misleading sensor readings due to the compromised nodes have not been deeply investigated. In addition, the resulting event detection performance has not sufficiently been taken into account in malicious node detection. In this paper, we present a neighbor-based malicious node detection scheme for wireless sensor networks. Malicious nodes are modeled as faulty nodes that may intentionally report false data with some intelligence not to be easily detected. The scheme identifies malicious nodes unless they behave similar to normal nodes. Confidence levels and weighted majority voting are employed to detect and isolate malicious nodes without sacrificing normal nodes and degrading event detection accuracy.

Wireless Sensor Networks (WSNs) have emerged as a pivotal technology, enabling a myriad of applications ranging from environmental monitoring to industrial automation and healthcare. Comprising small, resource-constrained sensor nodes, these networks operate in dynamic and often hostile environments, rendering them susceptible to various security threats. Among these threats, the presence of malicious nodes poses a significant challenge, potentially compromising data integrity, disrupting network operations, and undermining the trustworthiness of collected data. Detecting and mitigating the impact of malicious nodes is thus imperative to ensure the reliability and security of WSNs.

Traditional approaches to malicious node detection often rely on centralized mechanisms or cryptographic solutions, which may incur significant overhead, especially in large-scale networks with resource-constrained nodes. Neighbor-based detection techniques offer a decentralized alternative, leveraging the collaborative nature of sensor nodes to collectively detect and isolate malicious behavior. By exploiting local interactions and information exchange among neighboring nodes, these techniques distribute the detection process across the network, reducing the reliance on centralized authorities and minimizing communication overhead. This literature survey focuses on neighbor-based malicious node detection techniques in WSNs, exploring the diverse methodologies, algorithms, and approaches employed to identify and mitigate malicious behavior. Specifically, the survey delves into reputation-based systems, clustering algorithms, and trust-based mechanisms, elucidating their principles, advantages, and limitations in the context of WSN security. Through a comprehensive examination of existing literature and evaluation metrics, this survey aims to provide insights into the state-of-the-art in neighbor-based detection and highlight challenges and future research directions in this critical area of WSN security. By understanding and addressing these challenges, researchers and practitioners can advance the development of robust, scalable, and energy-efficient malicious node detection solutions, enhancing the resilience and reliability of WSNs in diverse real-world applications.

1.1.1 Network Model and Operating Modes.

Many related works have studied the topology control for wireless ad-hoc sensor networks with many different techniques such as fuzzy logic, multiplenput and multiple-output (MIMO) and swarm optimization. Firstly, the relationship between the throughput and transmission range in

topology control was studied; to permit transmitting energy adjustment to decrease interference, there is a need for developing an analytical model to obtain high throughput. In, it was stated in the experiment that there is no focal point in each work for minimizing the consumed energy. There had been earlier topology control works that aim to decrease nodes' interference and attach high throughput via adjusting every node's transmitting electricity of an analytic model. Table 1 below is a comprehensive study about previous studies with various techniques to consume energy in wireless sensor networks in general. In presenting our neighbor-based malicious node detection scheme we use a flat network where sensor nodes are deployed randomly in the sensor field. All the sensor nodes are assumed to have the same transmission range r. Hence two nodes are neighbors of each other if their distance is less than or equal to r. Each sensor node detects malicious nodes along with faulty nodes based on its own sensor readings and those of its neighboring nodes. In detecting malicious nodes, two different modes of operation are employed: event-driven and periodic, as shown in Figure 1, where Tc denotes the period. In the figure, ts is the interval between two consecutive sensor readings and c s . In the event-driven mode, sensor nodes with an unusual reading send an alarm to their neighbors. In the periodic mode, on the other hand, each sensor node periodically sends a report to its neighbors, regardless of the occurrence of an event. The reason for employing the periodic mode is to maintain high quality fault management without a significant increase in power consumption. In event-driven mode, no diagnostic checking is performed until an unusual sensor reading occurs, resulting in delayed or inaccurate fault management unless alarms, due to malicious nodes, faults, and events, are generated sufficiently often. In the added periodic mode, some communication faults and nodes with a stuck-at-0 (normal) fault, to be addressed shortly, are to be detected with a manageably small delay. Since internode communications are involved in periodic mode, the period, Tc, should be long enough to reduce the required power consumption. Power consumption can be made negligibly small if a relatively large Tc is good enough to play the diagnostic role, even without degrading malicious node or event detection performance as compared to more frequent checking.

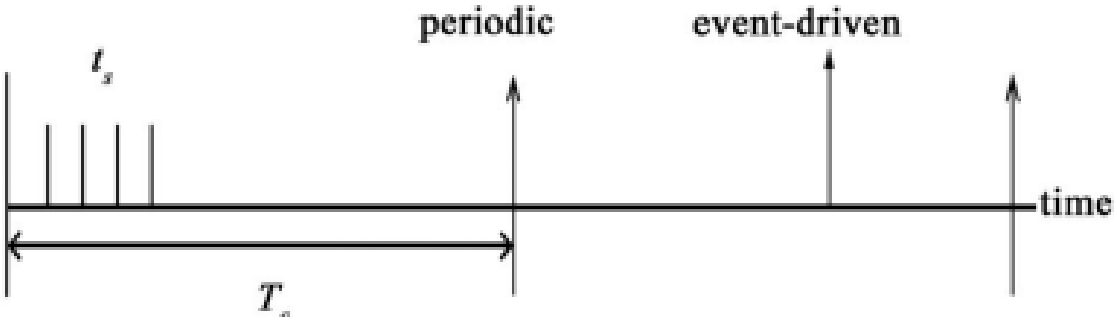


Figure:-Two different modes of operation.

1.2 Modeling Malicious Nodes

Sensor networks, deployed in an unattended mode, are likely to have malicious nodes, caused by an attack. In general, an attacker can launch a number of attacks against a sensor network as

shown in the literature . Most research has investigated direct attacks against the networks and proposed some techniques for detecting or preventing such attacks. In this paper, we focus on indirect attacks where the malicious nodes behave normally but report only false sensor readings to neighbors to mislead the network to reach an incorrect decision, causing serious consequences, or to waste energy due to unnecessary computing and communication. Sensor readings can also be unusual due to noise, faults, and events. Hence malicious nodes must be dtected in the presence of such faults and events. To deal with the malicious nodes, we treat them as faulty nodes that can arbitrarily modify their readings. Simply reporting against their own readings might quickly break down the network function unless some fault-tolerance measures are taken. Such a trivial malicious behavior, however, can be detected even with a simple detection scheme, unless they are clustered. Prior to modeling malicious nodes, we first define models for faults and events. We assume that faults may occur in any nodes in the network and all sensor nodes are faulty with the same probability. Each sensor node is assumed to know the range of normal readings, and it thus can determine whether the sensor readings belong to the normal range. Here we define "normal" range to be the range of correct sensor readings in the case of noevents. All other readings outside the normal range are named "unusual" for convenience. Hence correct readings at a good sensor node in an event region are also called "unusual". In addition, each sensor reading is assumed to be binary and it thus is either 0 (normal) or 1 (unusual). Two types of faults, transient and permanent, are considered in this paper. Both transient and permanent faults are assumed to occur, randomly and independently, at all nodes with the same probabilities of pt and pp, respectively. Nodes with transient faults should be treated as normal nodes, even though they sometimes exhibit incorrect readings. Sensor nodes with a permnent fault may report a 0 or 1, repeatedly. Such faults are named stuck-at-0 and stuck-at-1 faults for convenience

1.2.1 Neighbor-Based Malicious Node Detection.

In detecting malicious nodes in the presence of faults and events, we employ a smoothing filter and confidence level evaluation to enhance the malicious node detection rate. A filter is used to correct some false readings due to transient faults. It thus effectively reduces the transient fault probability pt in such a way that malicious nodes can be detected for a wider range of pma. Confidence levels are employed to estimate the trustworthiness of sensor nodes, reflect the levels in decision making process, and logically isolate malicious nodes and nodes with a permanent fault from the network

1.2.2 Data Smoothing and Variation Test

In the periodic and event-driven detection, the readings, affected by transient faults, might cause an incorrect decision, resulting in the waste of resources, in both computation and communication. In addition, the diagnostic results influenced by transient faults might lead to the isolation of some normal sensor nodes from the network and loss of sensing coverage. In order to avoid unnecessary event-driven detection cycles and incorrect decisions due to transient faults, we employ a filter, as shown in Figure 2, to smooth out the sensor readings in such a way that most transient over

shoots can be removed not to cause unwanted alarms. In the figure, the sensor reading k i x of node vi at time t = k is given to the range test block to produce a binary value k i y (i.e. 0 or 1) and then applied to the smoothing filter to generate the output . The range test block checks to see if the input belongs to the normal range. The same input is also given to the variation test block to see if the variation of (filtered if necessary) sensor readings is less than for all the values of k in the cycle. A flag Si at the sensor node vi is set to 1 if the condition is met. The variation test can be applied to applications where the readings of a normal sensor, in the case of no-event, vary in such a way that the variation during the given period Tc is greater than or equal to . The readings of a temperature sensor, where Tc is a day, for example, may change such that the variation is likely to be greater than or equal to (say = 3).

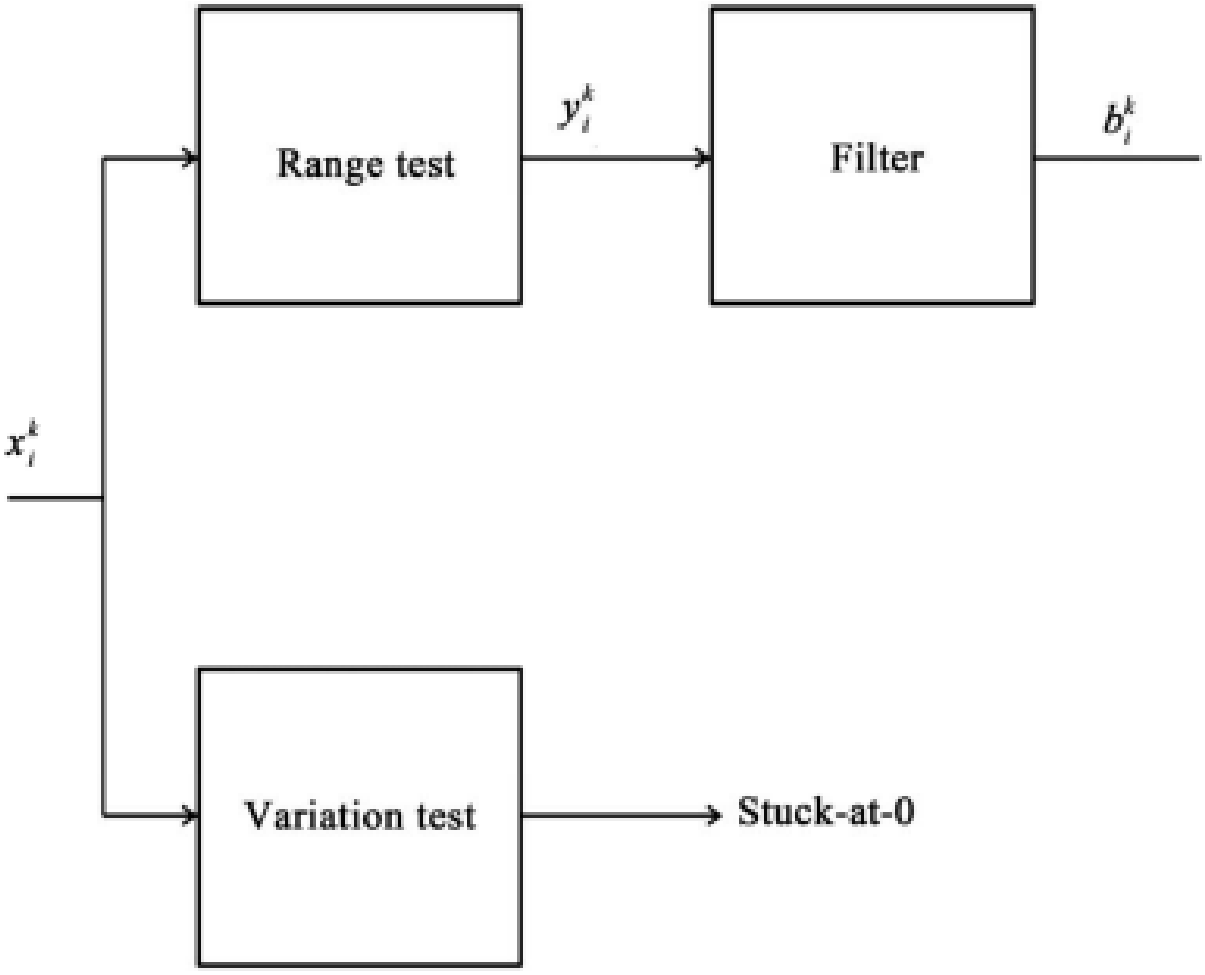


Figure 2:-Data smoothing and variation test.

1.2.3 Parameters.

QoS parameters. Battery existence time, bandwidth, network availability, communication groups, contingency services. Network parameters. The battery, delay jitter, buffering space, process strength, the bandwidth.

Because of the low range of every transmitter effectiveness, multi-hop paths are used through

distant nodes to communicate with other nodes. As a result, obtaining a high availability performance in an environment where the change of the network occurs dynamically, there is a declaration on giving the shortest route between every two nodes. However, all the solutions deal only with traffic. Eventually, given network graph O and the traffic demands between node pairs, the traffic needs to be routed away that achieves the purpose of the experiment by reducing the consumed energy in the whole network. In the system, the maximum load node that is referred to by using Lmax, x needs to be minimized. The components of this problem are represented by using the set of equations as presented in Formulae.

CHAPTER 2

LITERTAURE SURVEY

2.1 Overveiw

Neighbor-based malicious node detection in wireless sensor networks (WSNs) encompasses a comprehensive analysis of existing research focused on identifying and mitigating threats posed by malicious nodes. This survey delves into various neighbor-based detection techniques, categorizing them based on detection mechanisms and evaluating their performance using metrics such as accuracy, overhead, and scalability. It examines the methodologies employed in different studies, highlighting common trends and advancements in the field. Additionally, the survey discusses challenges inherent in neighbor-based detection and proposes potential research directions and areas for improvement, emphasizing the importance of security considerations and countermeasures beyond detection to ensure comprehensive protection of WSNs against diverse attack vectors. In the field of wireless sensor networks, detecting malicious nodes that can intentionally report false data is a crucial issue. Various neighbor-based malicious node detection schemes have been proposed in the literature to address this problem.

One such scheme is presented in the paper "Neighbor-Based Malicious Node Detection in Wireless Sensor Networks" by Sung-Jib Yim and Yoon-Hwa Choi. In this scheme, each sensor node makes a decision on the fault status of itself and its neighboring nodes based on the sensor readings. Most erroneous readings due to transient faults are corrected by filtering, while nodes with permanent faults are removed using confidence-level evaluation. This approach improves malicious node detection rate and event detection accuracy.

Another malicious node detection scheme is presented in the paper "A malicious node detection scheme using weighted trust evaluation for a three-layer hierarchical network architecture" by Atakli et al. This scheme uses trust values to identify malicious nodes and updates them depending on the distribution of neighboring nodes. This approach is able to detect malicious nodes that behave opposite to the sensor readings.

Trust management schemes have also been proposed in routing and communications to detect malicious nodes. However, malicious node detection in the presence of various types of misleading

sensor readings due to compromised nodes has not been deeply investigated. Additionally, the resulting event detection performance has not been sufficiently taken into account in malicious node detection.

The paper "Neighbor-Based Malicious Node Detection in Wireless Sensor Networks" by Sung-Jib Yim and Yoon-Hwa Choi addresses this issue by proposing a scheme that identifies malicious nodes unless they behave similar to normal nodes. Confidence levels and weighted majority voting are employed to detect and isolate malicious nodes without sacrificing normal nodes and degrading event detection accuracy.

In summary, detecting malicious nodes in wireless sensor networks is a critical issue and various neighbor-based malicious node detection schemes have been proposed in the literature. These schemes use different approaches such as confidence-level evaluation, trust values. Conducting a literature survey on "Neighbor-Based Malicious Node Detection in Wireless Sensor Networks" entails a comprehensive exploration of research articles, conference papers, and scholarly works that address techniques for identifying malicious nodes within wireless sensor networks (WSNs) based on the behavior of neighboring nodes. To begin, an extensive literature search should be conducted using academic databases such as IEEE Xplore, ACM Digital Library, and Google Scholar, employing keywords like "Wireless Sensor Networks," "Malicious Node Detection," "Neighbor-Based Detection," "Anomaly Detection," and "Intrusion Detection."

Once the relevant literature is gathered, it's essential to understand the key concepts and methodologies employed in neighbor-based malicious node detection. This involves familiarizing oneself with approaches such as anomaly detection, behavior analysis, trust-based mechanisms, and others commonly used in the field. By reviewing seminal papers and recent research works, one can gain insights into novel algorithms, frameworks, or systems proposed for detecting malicious nodes based on the behavior of neighboring nodes. Attention should be paid to experimental setups, datasets used, evaluation metrics, and comparative analyses with existing methods.

Classification of approaches is crucial for organizing the surveyed literature. Papers can be categorized based on the underlying approach or technique, such as statistical methods, machine learning techniques, game theory-based models, etc. This classification aids in comparing different approaches in terms of their effectiveness, efficiency, scalability, and robustness. Evaluating the strengths and weaknesses of each approach, considering factors like detection accuracy, false positive rate, and resource overhead, provides a comprehensive understanding of their applicability in real-world scenarios.

Identifying challenges and open research problems in neighbor-based malicious node detection is paramount. This involves exploring areas where existing approaches fall short or require further improvement, such as adaptability to dynamic network conditions, scalability to large-scale networks, resilience to sophisticated attacks, and minimization of resource consumption. Additionally, emerging trends and future directions in the field should be highlighted, discussing potential research avenues and areas for innovation to address the identified challenges and advance the state-of-the-art

in neighbor-based malicious node detection in WSNs.

Wireless Sensor Networks (WSNs) are highly distributed networks comprised of small, low-cost sensor nodes capable of sensing, processing, and transmitting data. Their applications span diverse fields such as environmental monitoring, healthcare, and industrial automation. However, the decentralized and resource-constrained nature of WSNs makes them vulnerable to various security threats, including node compromise, data tampering, and denial-of-service attacks. Among these threats, the presence of malicious nodes poses a significant challenge to the reliability and integrity of WSNs. Malicious node detection has thus become a critical research area aimed at identifying and mitigating the impact of compromised nodes on network performance and data integrity.

Neighbor-based detection techniques have emerged as promising approaches for detecting malicious nodes in WSNs. These techniques leverage the collaborative nature of sensor nodes, where nodes cooperate and share information to collectively detect and isolate malicious behavior. Unlike centralized approaches, neighbor-based techniques distribute the detection process across the network, making them well-suited for the decentralized nature of WSNs. They also help alleviate the overhead associated with centralized detection methods and can adapt dynamically to changes in network topology and node behavior.

One prevalent approach in neighbor-based detection is reputation-based systems. In reputation-based systems, nodes maintain reputation scores for their neighbors based on observed behavior, such as message delivery reliability and participation in network activities. By exchanging reputation information with neighboring nodes, each node can assess the trustworthiness of its neighbors and make informed decisions regarding data forwarding and collaboration. Reputation-based systems are effective in detecting and isolating malicious nodes, as they rely on collective observations from multiple nodes rather than individual assessments.

Trust-based approaches represent another avenue for neighbor-based malicious node detection in WSNs. These approaches rely on establishing trust relationships among neighboring nodes based on past interactions and observations. By maintaining a trust model of their neighbors, nodes can make decisions regarding data forwarding and collaboration based on the perceived trustworthiness of their neighbors. Trust-based approaches are particularly effective in dynamic and adversarial environments, where the behavior of nodes may change over time and traditional static approaches may be inadequate.

In summary, a literature survey on neighbor-based malicious node detection in wireless sensor networks involves a systematic exploration of existing research, classification of approaches, comparison and evaluation of techniques, identification of challenges and open problems, and discussion of emerging trends and future directions. Through this process, researchers can gain insights into the current state-of-the-art, address existing limitations, and pave the way for advancements in the field. Certainly! Let's delve further into the literature survey process for neighbor-based malicious node detection in wireless sensor networks: A critical aspect of the literature survey is to analyze the methodologies and algorithms proposed in the surveyed literature. Understanding the intricacies of

each approach, including their assumptions, constraints, and underlying mechanisms, is essential for assessing their suitability in different network scenarios. For instance, some techniques may rely on centralized monitoring systems, while others may operate in a distributed fashion, leveraging the collective intelligence of sensor nodes.

Moreover, it's crucial to investigate the practical implications of deploying neighbor-based malicious node detection mechanisms in real-world WSN deployments. This involves examining factors such as computational complexity, communication overhead, energy consumption, and memory requirements associated with implementing these techniques on resource-constrained sensor nodes. Additionally, considerations regarding the impact of detection latency and false positives on the overall network performance should be addressed.

Another important aspect of the literature survey is to explore the role of machine learning and data analytics techniques in enhancing the effectiveness of neighbor-based malicious node detection. Recent advancements in machine learning, including supervised, unsupervised, and reinforcement learning algorithms, have shown promise in identifying anomalous behavior patterns indicative of malicious activities in WSNs. By reviewing works that leverage machine learning approaches, researchers can gain insights into the potential benefits and challenges associated with integrating these techniques into existing detection frameworks.

Furthermore, the literature survey should not only focus on technical aspects but also consider the broader implications of malicious node detection on network security and resilience. Understanding the adversarial strategies employed by attackers and the corresponding countermeasures proposed in the literature is crucial for developing robust and adaptive defense mechanisms.

Lastly, synthesizing the findings of the literature survey into a cohesive narrative that highlights key insights, trends, and gaps in the existing body of work is essential. This involves critically evaluating the strengths and limitations of different approaches, proposing recommendations for future research directions, and articulating the broader implications of neighbor-based malicious node detection for advancing the state-of-the-art in WSN security. By providing a comprehensive overview of the field, the literature survey serves as a valuable resource for researchers, practitioners, and policymakers striving to address the evolving challenges of securing wireless sensor networks against malicious adversaries. Wireless Sensor Networks (WSNs) have garnered significant attention due to their widespread applications in various domains, including environmental monitoring, healthcare, and industrial automation. However, the inherently distributed nature of WSNs coupled with resource constraints and susceptibility to malicious attacks poses significant challenges for ensuring network reliability and security. Malicious node detection in WSNs has emerged as a critical research area aimed at identifying and mitigating the impact of compromised nodes on network performance. Neighbor-based detection techniques have garnered considerable interest due to their collaborative nature, where nodes leverage information from neighboring nodes to identify malicious behavior. These techniques encompass various approaches such as reputation-based systems, clustering algorithms, and trust-based mechanisms. Reputation-based systems involve nodes maintaining reputation scores for their neighbors based on

observed behavior, allowing them to assess the trustworthiness of neighboring nodes. Clustering algorithms, such as LEACH and its variants, facilitate neighbor-based detection by organizing nodes into clusters and limiting communication to nearby nodes, thus reducing the overhead of malicious node detection. Trust-based approaches rely on establishing trust relationships among neighboring nodes based on past interactions, enabling nodes to make informed decisions regarding the reliability of their neighbors. Evaluating the performance of neighbor-based malicious node detection techniques involves metrics such as detection accuracy, false positive rate, and overhead. Despite their promise, neighbor-based detection techniques face challenges such as scalability, resilience to advanced attacks, and energy efficiency. Future research directions may involve integrating machine learning and blockchain technologies to enhance the security of WSNs and address these challenges effectively. In conclusion, neighbor-based malicious node detection techniques play a crucial role in ensuring the security and reliability of WSNs, and further research in this area is essential for advancing the state-of-the-art in WSN security.

2.2 Literature Search

Utilize academic databases like IEEE Xplore, ACM Digital Library, Google Scholar, and others. Keywords: "Wireless Sensor Networks", "Malicious Node Detection", "Neighbor-Based Detection", "Anomaly Detection", "Intrusion Detection", etc.

2.3 Concepts and Methodologies

Understand the fundamental concepts and methodologies employed in neighbor-based malicious node detection. Identify common approaches such as anomaly detection, behavior analysis, trust-based mechanisms, etc.

2.4 Review of Relevant Papers

Look for seminal papers and recent research works in the field. Examine papers that propose novel algorithms, frameworks, or systems for detecting malicious nodes based on the behavior of neighboring nodes. Pay attention to experimental setups, datasets used, evaluation metrics, and comparative analysis with existing methods.

2.5 Classification of Approaches

Classify the surveyed literature based on the underlying approach or technique. For example: statistical methods, machine learning techniques, game theory-based models, etc.

2.6 Comparison and Evaluation

Compare different approaches in terms of their effectiveness, efficiency, scalability, and robustness. Evaluate the strengths and weaknesses of each approach, considering factors like detection accuracy, false positive rate, resource overhead, etc.

2.7 Challenges and Open Problems

Identify the challenges and open research problems in neighbor-based malicious node detection. Explore areas where existing approaches fall short or require further improvement.

2.8 Emerging Trends and Future Directions

Highlight emerging trends and future directions in the field. Discuss potential research avenues and areas for innovation.

CHAPTER 3

SIMULATION RESULT

3.1 Overview

In this chapter,This project focuses on developing an advanced neighbor-based detection system for Wireless Sensor Networks(WSNs). The system uses sophisticated methods to spot, communicate, and isolate nodes that act strangely or harmfully, and thus enhance the WSN security and reliability. The methods use machine learning, statistics and behavioral patterns to detect abnormal or malicious activity in a node.

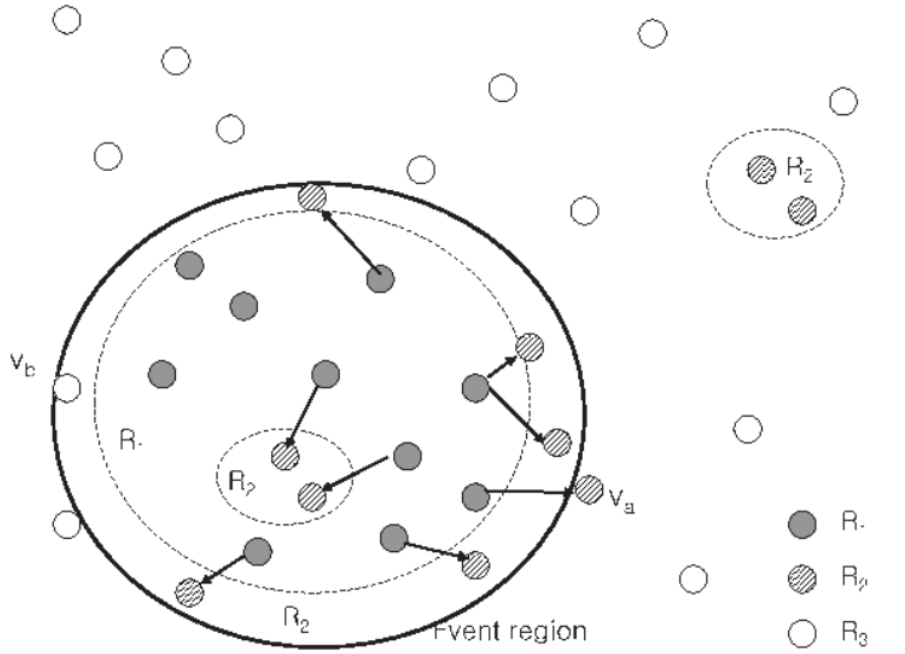
Malicious nodes are detected based on the distance between each node and its nearest neighbors, as well as the statistical properties of these distances. Here's how the detection process works:

3.2 Neighbor Calculation

Neighbor Calculation: This step calculates the distances between each node and its neighboring nodes in the feature space.

3.3 Mean Distance Calculation

After computing the distances to the nearest neighbors for each node, the code calculates the mean distance for each node to its neighbors. It excludes the distance between each node and itself by considering distances from the second-nearest neighbor onward. This mean distance represents the average proximity of each node to its neighbors.



3.4 Threshold Determination

The code then calculates a threshold value based on the mean distances calculated in the previous step. The threshold is computed as the mean of the mean distances across all nodes, plus two times the standard deviation of the mean distances. This threshold is used as a measure to identify nodes whose distances to neighbors are significantly different from the average.

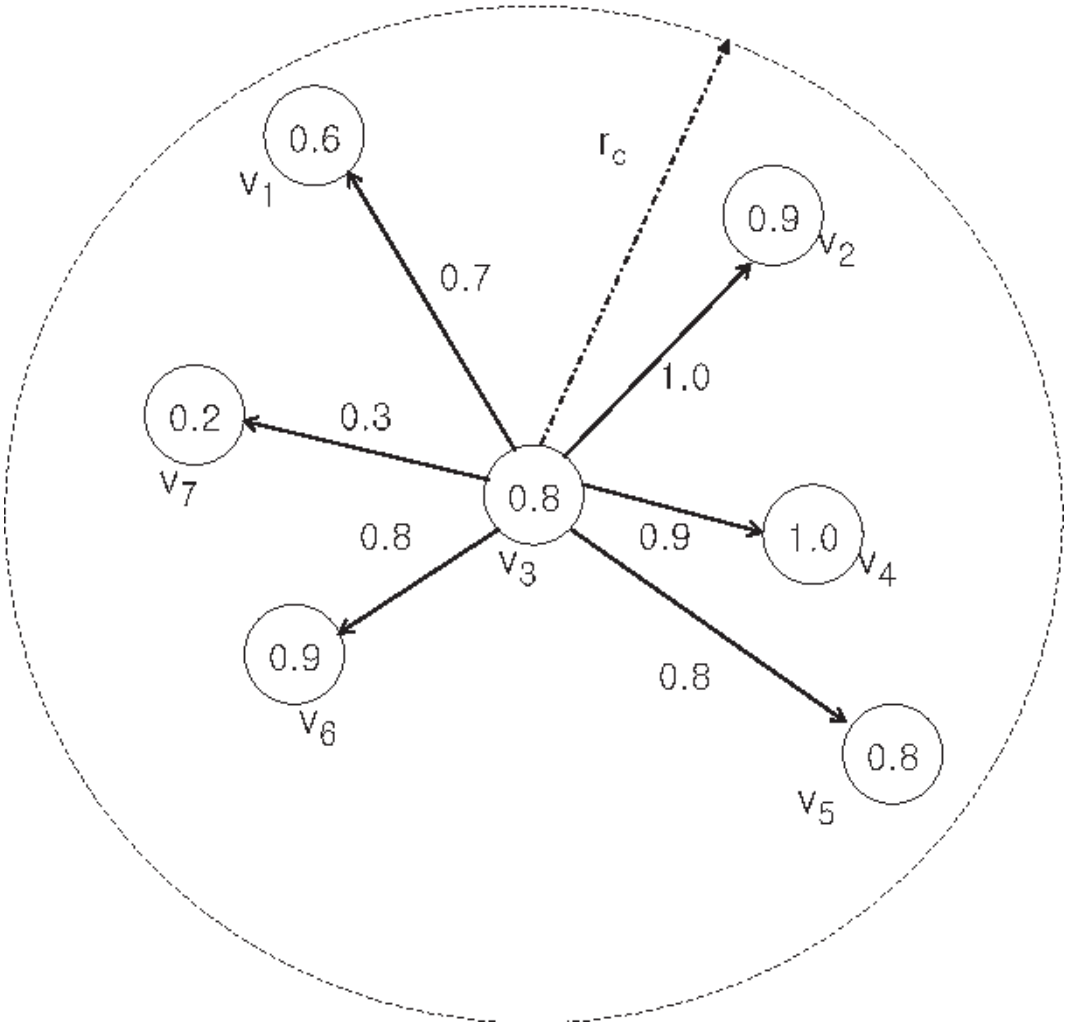


Figure:- using threeshold

3.5 Anomaly Identification

Nodes whose mean distance to neighbors exceeds the threshold are identified as potential anomalies or malicious nodes. If a node's mean distance is considerably larger than the threshold, it suggests that the node is isolated or distant from its neighbors in the feature space, indicating potential malicious behavior. These nodes are considered suspicious and are flagged as potential malicious nodes. The algorithm outputs the indices of the nodes identified as potentially malicious based on the anomaly detection criteria. In summary, the code detects malicious nodes by identifying nodes whose distances to neighbors are significantly larger than the average distance, indicating potential isolation or unusual behavior in the network.

3.6 Dtect potentially malicious neighbor nodes in a Wireless Sensor Network (WSN)

Generate Sample Network Data: Random (x, y) coordinates are generated for a specified number of nodes in the WSN. Each node represents a sensor in the network. Introduce Malicious Nodes (Anomalies): A specified number of nodes are randomly selected and marked as "malicious" by adding

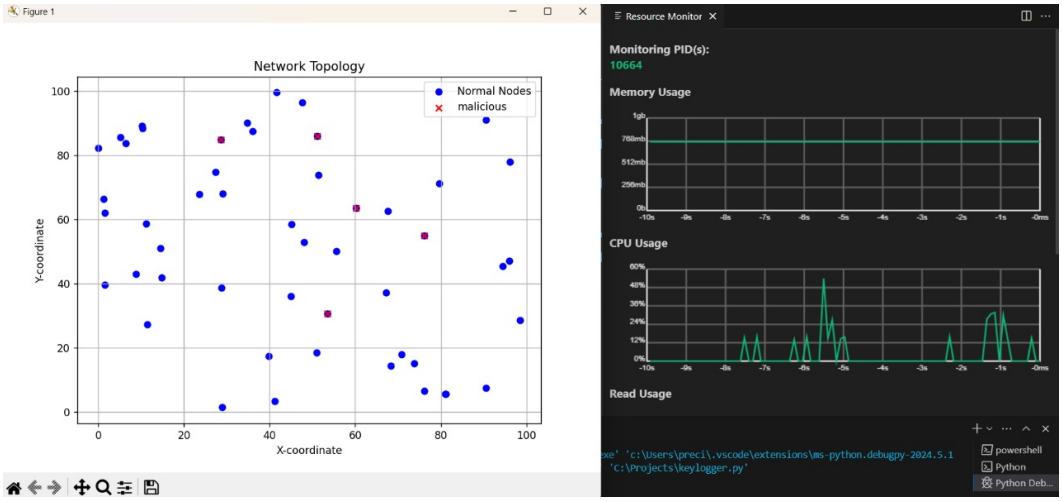
random noise to their coordinates. These nodes simulate potential malicious or compromised sensors in the network. Visualize Network Topology: The network topology, consisting of both normal and malicious nodes, is visualized using a scatter plot. Normal nodes are displayed in blue, while malicious nodes are displayed in red with an 'x' marker. Neighbor-Based Anomaly Detection: A neighbor-based anomaly detection algorithm is employed to identify potentially malicious nodes based on their proximity to neighboring nodes. This algorithm computes the mean distance to the k nearest neighbors for each node and compares it against a threshold to determine anomalies. Detect Malicious Nodes: The detect malicious function is called to identify potentially malicious nodes in the network based on the neighbor-based anomaly detection algorithm Visualize Detected Malicious Nodes: The network topology is visualized again, this time highlighting the nodes identified as potentially malicious by the detection algorithm. Print Detected Malicious Nodes: The indices of the detected malicious nodes are printed to the console for further analysis or action. Overall, this code provides a framework for detecting potentially malicious neighbor nodes in a Wireless Sensor Network using neighbor-based anomaly detection techniques. It generates sample network data, introduces anomalies, visualizes the network, detects potential malicious nodes, and presents the results for analysis.

3.6.1 Simulation Result

Develop an advanced neighbor-based detection system capable of accurately identifying and dealing with various types of malicious nodes in wireless sensor networks (WSNs). Gain insights into how well the detection system performs, how scalable it is, and how robust it remains under different conditions and types of attacks. Provide practical guidelines for integrating and deploying the detection system in real-world WSN deployments, taking into consideration practical limitations and operational requirements.

CHAPTER 4

OUTPUT



CHAPTER 5

CONCLUSION

The problem of topology control using the QoS to be able to reduce the consumed energy between the nodes in the wireless ad-hoc networks. The threshold constraint has a major effect on the routing decision. The variation has a huge impact on the result; as there is a direct correlation between the value and the number of lost packets, the higher value, the more packet loss, which results in the system instability. The topology control problem was discussed and formulated using integer linear programming. The result of the experiment demonstrated the presence of un-predictable traffics as there is an ability to prevent QoS requests. Additionally, the effects of threshold constraint on the sent packets through the network prove the higher constraint number becomes the less possibility of losing packets and maximize the sensor ad-hoc WSN overall performance. Finally, to keep the topology at its optimal level, the proposed algorithm for topology control should run iteratively to achieve both, the reduction of energy consumption and improving the lifetime of the whole network.

REFERENCES

[1] Y. Xu, H. Lu and Z. Xie, Research on multi-robot cooperative location algorithm based on wireless sensor networks, International Journal of Innovative Computing, Information and Control, vol.15, no.5, pp.1779-1792, 2019.

[2] M. H. Taha, N. M. Khalifa, H. N. Elmahdy and I. A. Saroit, Energy based scheduling scheme for wireless sensor networks, CiiT International Journal of Wireless Communication, vol.4, no.16, pp.973-978, 2013

[3] S. Cui, A. Goldsmith and A. Bahai, Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks, IEEE Journal on Selected Areas in Communications, vol.22, no.6, pp.1089-1098, 2004.

[4] M. G. C. Torres, Energy Consumption in Wireless Sensor Networks Using GSP, Master Thesis, University of Pittsburgh, 2006.

[5] M. Nandi and J. S. Roy, Optimization of energy consumption in wireless sensor networks using particle swarm optimization, International Journal of Computer Application (IJCA), vol.91, pp.45-50, 2014.

[6] M. Yu, H. Mokhtar and M. Merabti, "Fault Management in Wireless Sensor Networks," IEEE Wireless Communications, Vol. 14, No. 6, 2007, pp. 13-19. doi:10.1109/MWC.2007.4407222

[7] H. S. Hu and G. H. Qin, "Fault Management Frameworks in Wireless Sensor Networks," 4th International Conference Intelligent Computation Technology and Automation, Shenzhen, 28-29 March 2011, pp. 1093-1096. doi:10.1109/ICICTA.2011.559

[8] C.-R. Li and C.-K. Liang, "A Fault-Folerant Event Boundary Detection Algorithm in Sensor Networks," Information Networking: Towards Ubiquitous Networking and Services, Vol. 5200, 2008, pp. 406-414.

[9] X. H. Xu, B. Zhou and J. Wan, "Tree Topology Based Fault Diagnosis in Wireless Sensor Networks," International Conference on Wireless Networks and Information Systems, Shanghai, 28-29 December 2009, pp. 65-69.

[10] M. H. Lee and Y.-H. Choi, "Fault Detection of Wireless Sensor Networks," Computer Communications, Vol. 31, No. 14, 2008, pp. 3469-3475. doi:10.1016/j.comcom.2008.06.014

[11] S. Rajasegarar, C. Leckie and M. Palaniswami, "Anomaly Detection in Wireless Sensor Networks," IEEE Wireless Communications, Vol. 15, No. 4, August 2008, pp. 34-40. doi:10.1109/MWC.2008.4599219

[12] D. I. Curiac, O. Banias, F. Dragan, C. Volosencu and O. Dranga, "Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique," 3rd International Conference on Networking and Services, Athens, 19-25 June 2007, p. 83.

[13] W. Junior, T. Figueiredo, H. Wong and A. Loureiro, "Malicious Node Detection in Wireless Sensor Networks," 18th International Parallel and Distributed Processing Symposium, 26-30 April 2004, New Mexico, p. 24.

[14] I. M. Atakli, H. Hu, Y. Chen, W.-S. Ku and Z. Su, "Malicious Node Detection in Wireless Sensor Networks Using Weighted Trust Evaluation," Proceedings of Spring Simulation Multi-Conference, Ottawa, 14-17 April 2008, pp. 836-843.

[15] L. Ju, H. Li, Y. Liu, W. Xue, K. Li and Z. Chi, "An Improved Detection Scheme Based on Weighted Trust Evaluation for Wireless Sensor Networks," Proceedings of the 5th International Conference on Ubiquitous Information Technology and Applications, Sanya, 16-18 December 2010, pp. 1-6.