Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 8
August 2023

An Approach on Detecting Malicious Nodes inDistributed Sensor Networks

Pranav Jeevan

Department of Computer science School of Computing, Mysuru CampusAmrita Vishwa Vidyapeetham,
India
Email: pjofficial2000@gmail.com

Pallavi Joshi

Department of Computer science School of Computing, Mysuru CampusAmrita Vishwa Vidyapeetham,
India
Email: pallavijoshi@my.amrita.edu

Abstract—Wireless Sensor Networks (WSN) have become prevalent in various applications, including IoT, monitoring, and surveillance. However, due to their deployment in remote locations, ensuring security is crucial. Security issues may arise due to physical tampering or other types of attacks on the network or nodes. Malicious node detection is an effective approach to prevent security breaches and attacks on WSNs. In this research, a hybrid model is proposed for detecting malicious nodes to enhance the security of WSNs. It utilizes a combination of anomaly-based detection and reputation-based detection techniques to effectively detect malicious nodes in WSNs by using available resources efficiently. Extensive simulations using the COOJA Simulator demonstrate the working of the hybrid model, providing an efficient and effective solution for enhancing the security of WSNs.

Index Terms—security, wireless sensor networks, IoT, mali- cious node detection, decentralised-centralised mechanism, hy- brid model

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are extensively utilized in diverse fields such as the Internet of Things (IoT) and monitoring and surveillance applications. However, security is one of the primary challenges that WSNs encounter [1]–[4]. Since WSNs are typically deployed in remote areas, ensuring the safety and dependable operation of the network becomes crucial, emphasizing the need for security measures.

Wireless Sensor Networks (WSNs) may encounter security challenges in various aspects, including physical tampering of nodes or attacks on the network or nodes. The presence of malicious nodes can pose a significant threat to the normal operation of the network. Different types of attacks, such as DoS attacks, Hello Flood attacks, Sybil attacks, Wormhole attacks, and data and information spoofing, eavesdropping, etc., can lead to security breaches and disrupt the proper functioning of the WSN [5].

To prevent such attacks and security breaches, malicious node detection mechanisms can be employed in WSNs. The existing works in this field can be categorized into two types, prediction models, and signature-based detection models. Pre- diction models, such as Hidden Markov Models (HMMs) and Computational Random Fields (CRFs), use statistical models to detect offsite intrusions. In contrast, signature-based detection models can detect only known attacks [6].

This study aims to address the challenges of detecting malicious nodes in WSNs by proposing a hybrid model that leverages various techniques for enhanced security. The model incorporates the design of attack signature-based rule- sets to identify different types of attacks, allowing for the establishment of guidelines for normal network operation. To efficiently utilize resources, the model includes a fail- safe monitoring mechanism with the usage of decentralised- centralised approach. Furthermore, effective countermeasures and evasive actions are implemented to mitigate the impact of detected malicious nodes. By blacklisting and removing these nodes, the proposed model ensures the network oper- ates securely and reliably, providing an effective solution for malicious node detection in WSNs.

The development of a hybrid model for detecting malicious nodes in WSNs presents a significant advancement in enhanc- ing network security. By effectively and efficiently identifying these nodes, the proposed model contributes to the creation of secure and reliable WSNs. This research has the potential to have a positive impact on various applications, including IoT and surveillance, where the integrity and confidentiality of data transmission are of utmost importance.

II. RELATED WORK

The literature review part of any research work plays an import role in modelling the basic idea of the work. They provide valuable insights into the field of work, existing work, and potential research gaps. This part discusses about various such paper that give a better understanding of malicious node detection. Paper [7] speaks about Intrusion Detection system and their workings. It covers detection system installation mechanisms which include Purely Distributed, Purely Central- ized or Distributed-Centralized mechanisms. And it discusses detection policies which include Misuse Detection, Anomaly Detection or Specification-based detection mechanisms.

Purely distributed IDS works by distributing detection agents in various nodes within the network, which work together to detect attacks. The significant drawback of this method is that it can lead to a high false-positive rate and also consume significant energy and memory resources of the network.

Purely centralized IDS involves the installation of detection agents in a central location, which monitors the network for attacks. This method is easy to manage and has a minimal false-positive rate, but it can be vulnerable to single point failure, and the central agent may be overloaded with a large amount of data.

Distributed-Centralized IDS combines both purely dis- tributed and purely centralized IDS mechanisms. This method uses both a central detection agent and distributed detection agents within the network. The main advantage of this ap- proach is that it provides a balance between the advantages and disadvantages of the other two mechanisms.

Detection policies in IDS include misuse detection, anomaly detection, and specification-based detection [24]–[26]. Misuse detection involves matching network traffic against pre-defined attack patterns, which can be easily circumvented by attack- ers who know these patterns. Anomaly detection involves identifying deviations from normal network behavior, which may result in a high false-positive rate. Specification-based detection involves comparing network traffic to an established specification, which can be difficult to develop and may not detect new types of attacks.

In summary, each IDS installation mechanism and detection policy has its own advantages and disadvantages, and the se- lection of the appropriate method depends on the requirements of the specific network and the types of attacks to be detected. These concepts of installation mechanisms and detection policies helped us to form the base idea of implementation of a malicious node detection system in WSN. In terms of malicious node detection, [8] proposes a machine learning approach for detecting malicious nodes in wireless sensor networks. The proposed approach uses support vector ma- chines (SVM) and features extracted from the network traffic to classify nodes as malicious or legitimate. The performance of the approach is evaluated using both simulated and real- world data, and it is shown to achieve high detection rates while maintaining low false positives. In the literature survey, the authors discuss previous works on intrusion detection in wireless sensor networks, highlighting the limitations of tradi- tional rule-based methods and the need for machine learning

approaches that can adapt to evolving threats.

[9] contributes to the body of research on malicious node detection in wireless sensor networks. It provides a novel approach that combines different trust factors to evaluate the trustworthiness of nodes. Previous research in this area has focused on using a single trust factor, such as reputation or behavior analysis. The paper also compares the proposed scheme with other existing detection schemes, providing insights into the effectiveness and limitations of different approaches. [10] discusses about a novel method based on weighted-trust evaluation to detect malicious nodes in the Wireless Sensor Networks. It uses a three-layer hierarchical network architecture that contains three types of sensor nodes. Malicious nodes are detected on weighted sensor networks and the trust values given to them. Here, blind trust on base stations is applied as it is assumed to be trusted. Each of these papers have its own list of advantages and disadvantages. In this paper the main aim is to investigate the drawbacks of existing works to provide a novel hybrid method to provide security to wireless sensor networks in the form of malicious node detection.

[11] briefly discusses existing approaches for node fault detection in wireless sensor networks, including threshold- based approaches, clustering-based approaches, and machine learning-based approaches. The authors point out the lim- itations of these approaches and argue that their proposed approach overcomes these limitations by using a combination of clustering and fuzzy logic techniques. [12] proposes a threshold-based mechanism to detect and prevent flooding attacks, which are a type of DoS attack that can negatively impact the performance of wireless sensor networks. [13] presents a distributed localization system for WSNs that uses Received Signal Strength Indicator (RSSI) readings to estimate the location of sensor nodes. The proposed system attains greater localization accuracy compared to existing approaches, according to experimental results.

[14] proposes a customized approach to reduce energy consumption in wireless sensor networks by dynamically ad- justing the transmission power of nodes based on their distance from the base station. The proposed approach is compared with other energy-efficient techniques and is found to perform better than them in terms of network lifetime and energy consumption. The study provides insight into how customized approaches can be applied to wireless sensor networks to improve their energy efficiency. [16] presents a contribution to the research on energy-efficient protocols for WSNs by proposing a new protocol that builds on the widely-used cluster-based routing approach.

The existing works on malicious node detection in wireless sensor networks (WSNs) have made significant contributions to the field but still have some limitations and research gaps. One limitation

is the reliance on traditional rule-based methods, which may not effectively adapt to evolving threats in WSNs. Machine learning approaches have shown promise in improving detection rates, but further research is needed to explore their scalability and performance in large-scale WSN deployments. Another research gap lies in the evaluation of trust factors and their combination, where the authors emphasize the necessity for more comprehensive and inte- grated trust evaluation models that consider multiple factors to accurately assess node trustworthiness. Additionally, existing works often focus on specific types of attacks, such as flooding attacks, while neglecting other possible threats, highlighting the requirement for a holistic approach that addresses a wider range of security concerns in WSNs. These limitations and research gaps provide the motivation for our study to propose a novel hybrid method for malicious node detection in WSNs, aiming to overcome these drawbacks and enhance the overall security of WSNs.

III. MALICIOUS NODE DETECTION

The proposed work aims to overcome the limitations of existing works in providing security to Wireless Sensor Net- works (WSN). The existing methods focus on improving the installation and detection policies, but there is still a need for more efficient and effective approaches. The proposed work follows a decentralized-centralized to Decentralized-Centralized detection mechanism and utilizes a specification- based approach. The approach is based on specifications, which provide a framework for defining the expected behavior and characteristics of the network. By incorporating both de- centralized and centralized elements, the proposed mechanism aims to overcome the limitations of existing methods in terms of security provision for WSNs.

The detection mechanism involves monitoring nodes in the cluster-heads and the sink node, as shown in Fig.1. The sink node performs resource-intensive tasks while the cluster-heads perform less intensive detection and monitoring. This approach optimizes the use of available resources in WSNs.

The proposed hybrid system follows a basic flow depicted in the diagram above. The clusters are monitored in real-time, and when an anomaly is detected, it alerts the central node. The central node then takes evasive actions, which may include blacklisting the malicious node or preventing communication of other nodes with the malicious node. After the malicious activity is dealt with, the system goes back to monitoring the WSN.

The proposed system will monitor the WSN for various parameters, including delay, packet drop, high energy con- sumption, traffic jam, and others. These parameters are used to establish a baseline of what is considered normal behavior for the WSN environment. If the system detects a deviation from these baseline thresholds, it can flag the activity as abnormalor malicious.

Delay is the time it takes for a packet to travel from one node to another. If the delay time is higher than usual, it can indicate that there is congestion in the network or that a malicious node is deliberately delaying packet transmission. Similarly, if packets are dropped at a higher rate than usual, it can indicate network congestion or a malicious node droppingpackets.

High energy consumption can indicate that a node is compromised or being used to perform malicious activities. Malicious nodes can consume more energy than regular nodes, leading to the depletion of the battery in a short time. Thus, detecting nodes that consume more energy than usual is essential in identifying potentially malicious nodes.

Traffic jam occurs when multiple nodes try to transmit packets simultaneously, leading to a bottleneck in the network. This can cause delays and packet drops, which are both indications of a potential attack. A sudden increase in traffic jam in a specific area can be an indicator of a Denial of Service(DoS) attack.

Apart from these parameters, there are other parameters, such as packet overhead, packet loss rate, and network con- gestion, which can be used to detect malicious activity. By establishing a baseline of what is considered normal for these parameters, the system can identify any deviations that may indicate an attack.

In summary, by monitoring these parameters, the proposed system can detect anomalies and malicious activities in the WSN environment. This will enable the system to take proac- tive measures to mitigate any security breaches and improve the overall

security of the WSN.

The proposed work thus provides an innovative solution for enhancing the security of WSNs. By incorporating a hybrid detection mechanism that utilizes both decentralized and centralized approaches, it optimizes the use of available resources and ensures the efficient monitoring of WSNs.

IV. PROPOSED SYSTEM

The proposed work aims to overcome the limitations of ex- isting WSN security mechanisms by improving the method of installation and detection policies. The proposed system uses a decentralized-centralized to specification-based approach and a decentralized-centralized detection mechanism.

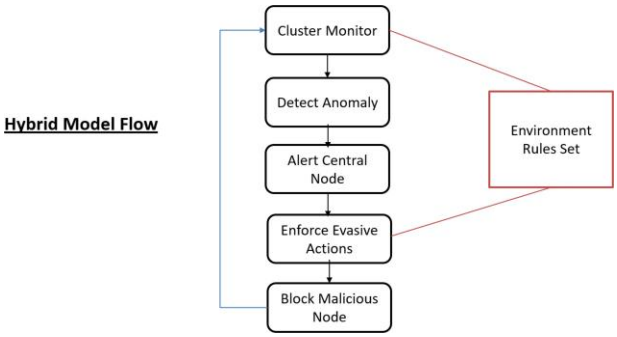


Fig. 1. Main System Architecture.

The detection mechanism involves monitoring nodes in the cluster-heads and the sink node as shown in Fig. 1. The resource-intensive tasks are performed in the sink node, and the less intensive detection and monitoring are done in the cluster-heads. The proposed hybrid system follows the steps outlined in Fig. 2. The clusters are first monitored in real-time, and when an anomaly is detected, it alerts the central node. The central node takes evasive actions, which may include blacklisting the malicious node or preventing communication with the malicious node. Once the malicious activity is dealt with, the system goes back into monitoring the WSN.

The proposed system uses environment rules set to contain the rules and specifications for the normal working of the

WSN environment. If parameters deviate from the thresholds of what is considered normal, then the activity can be flagged as abnormal or malicious. Some of the parameters used for detecting malicious activities include delay, packet drop, high energy consumption, traffic jam, and various other parametersindicating the onset of an attack.

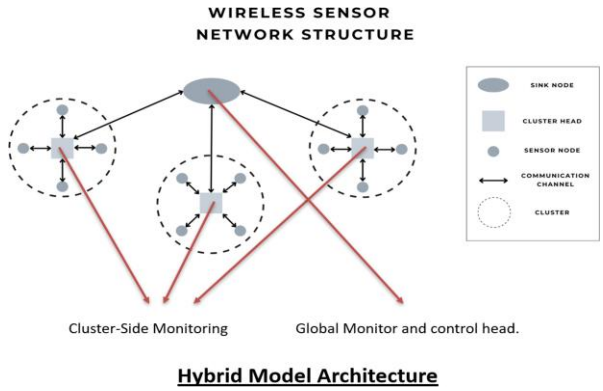


Fig. 2. Decentralized-Centralized detection mechanism Hybrid Model Flow.

The basic flow of the new hybrid system will follow the steps mentioned in Fig. 2. The clusters are monitored in real time first and when an anomaly is detected, it will alert the central node. The central node will take up evasive actions or mechanisms. It may include black listing the malicious node or even preventing communication of other nodes with the malicious node. After the malicious activity is delt with, the system goes back into monitoring the WSN. Here, the environment rules set will contain the rules and specifications for the normal working of the WSN environment. If parame- ters deviate from the thresholds of what is considered normal, then the activity can be flagged as abnormal or malicious. Some of the parameters include- Delay, Packet drop, High energy consumption, Traffic jam and various other parameters indicating the onset of an attack. A step-by-step algorithm for detecting malicious nodes in a wireless sensor network using a decentralized-centralized approach is presented in this paper:

1) Initialize the network with normal nodes and clusterheads.
2) For each cluster head:

a) Send beacon messages and request ACK responsesfrom nodes in its cluster.

b) Monitor the communication behavior of each node and use a distributed reputation system to

deter- mine the trustworthiness of each node.

c) Monitor the anomalous activities of each node and compare it to the expected normal behavior.

d) If a suspicious node is detected, send a report tothe sink node.

3) For the sink node:

a) Maintain a list of all suspicious nodes reported by the cluster heads.

b) Retrieve communication behavior, reputation, and anomalous activity data from the cluster head's.

report.

c) Calculate a spaciousness score for each node basedon the retrieved data.

4) Compare the spaciousness score of each node to athreshold value.

a) If the score is above the threshold, mark the nodeas malicious.

b) If the score is below the threshold, mark the nodeas normal.

5) Use a decentralized-centralized system to investigate a subset of the suspicious nodes and rely on the cluster heads to make local decisions about the remaining nodes.

6) If a node is confirmed as malicious, send a command to all cluster heads to isolate the malicious node.

The aim of this proposed algorithm is to enhance the detection and installation policies of existing mechanisms for identifying malicious nodes in a wireless sensor network (WSN) using a decentralized-centralized approach. This ap- proach is intended to address the limitations of the current detection methods. The algorithm follows a hybrid model that combines both decentralized and centralized approaches for efficient detection of malicious nodes.

The algorithm starts with initializing the WSN with normal nodes and cluster heads. Each cluster head then sends beacon messages and requests ACK responses from nodes in its cluster to monitor their communication behavior. A distributed reputation system is used to determine the trustworthiness of each node based on their behavior.

It also monitors the anomalous activities of each node and compares it to the expected expected normal behaviour to detect any anomalies. If a suspicious node is detected, the cluster head sends a report to the sink node.

The sink node maintains a list of all suspicious nodes reported by the cluster heads and retrieves communication behavior, reputation and anomalous activity data from the cluster head's report. It then calculates a spaciousness score for each node based on the retrieved data. In the proposed detection algorithm for malicious nodes in wireless sensor networks, a score is assigned to each node based on its behavior and activities. This score is then compared to a predefined threshold value to determine whether the node is malicious or normal. Nodes with scores above the threshold are marked as malicious, while those with scores below the threshold are marked as normal.

If a node is confirmed as malicious, the algorithm uses a decentralized-centralized approach to investigate a subset of the suspicious nodes and relies on the cluster heads to make local decisions about the remaining nodes. Once a node is confirmed as malicious, a command is sent to all cluster heads to isolate the malicious node.

In order to detect malicious nodes within a wireless sensor network, various technical specifications are employed. For communication behavior monitoring, beacon messages are sent periodically, such as every 5 seconds, while expecting ACK responses within a specific time frame, like 2 seconds. For instance, if a node fails to respond to more than 3 beacon messages, it can be flagged as suspicious.

A distributed reputation system assigns reputation scores ranging from 0 to 1 to each node based on their past behavior and interactions. This dynamic system allows for accurate assessment over time. Anomalous activity detection involves monitoring parameters such as packet drop rate, delay in message transmission, and energy consumption. For example, a packet drop rate above 5

The spaciousness score, which captures the overall behavior of each node, is calculated using a weighted combination of communication behavior, reputation, and anomalous ac- tivity data. This formula, tailored to the specific network requirements, provides a comprehensive assessment. Nodes are marked as malicious based on a threshold value for the spaciousness score. For

instance, a threshold of 0.6 may be set, indicating nodes with a score above 0.6 as malicious, while those scoring below are considered normal. Any of these thresholds can be employed in the proposed mechanism to detect malicious nodes.

The proposed system relies on a decentralized-centralized approach to investigate a subset of the suspicious nodes and relies on the cluster heads to make local decisions about the remaining nodes. If a node is confirmed as malicious, a command is sent to all cluster heads to isolate the malicious node. Overall, the proposed system provides a more robust and efficient approach to securing wireless sensor networks.

V. RESULTS

This paper introduces a novel decentralized-centralized ap- proach for detecting malicious nodes in WSNs by employ- ing a specification-based approach. The proposed mechanism monitors the WSN in real-time and compares its parameters to expected thresholds. If any deviation from the expected values is detected, the system flags the activity as abnormal or malicious, providing a reliable and efficient approach for detecting malicious nodes in WSNs. The proposed work has been simulated in the COOJA Simulator. A simulation with 2 scenarios with 30 and 60 nodes overall is designed and it included 3 cluster heads in both the scenarios. Two types of nodes are also included in the network: normal nodes and malicious nodes. Both the scenarios were run for 10 mins each and the graphs were recorded. The malicious nodes were detected in both the scenarios and Fig.3 shows the log throwing alert message on detecting the malicious node.

The two implementation scenarios are as follows -

A. Simulation with 30 nodes (1 sink node, 3 cluster heads, 3 edge nodes, 3 malicious nodes, 20 sensor nodes)

Fig.4 represents the network topology of the first scenario with 30 nodes. The Green node represents the sink node, purple nodes represent the edge nodes, dark blue represents the cluster head, sky blue represents the malicious nodes and yellow nodes represent the normal sensor nodes.

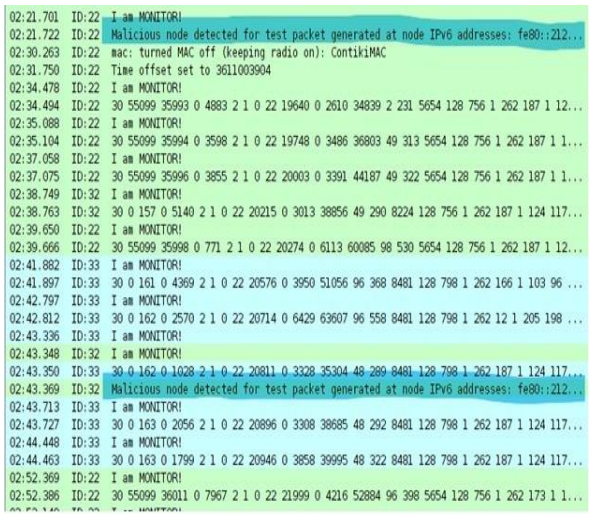
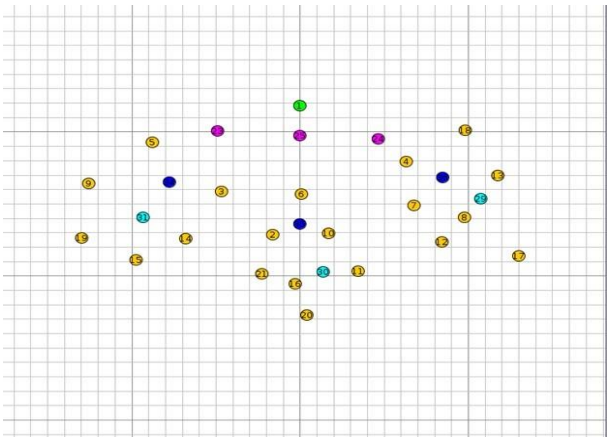


Fig. 3. Malicious Node Detection L

Fig. 4. 30 Node Network Grid

Fig. 5. Scenario 1 Power Consumption Graph



The graph in Fig.5 represents the power consumption trend of the first scenario. The max consumption was clocked at 1.10 mW.

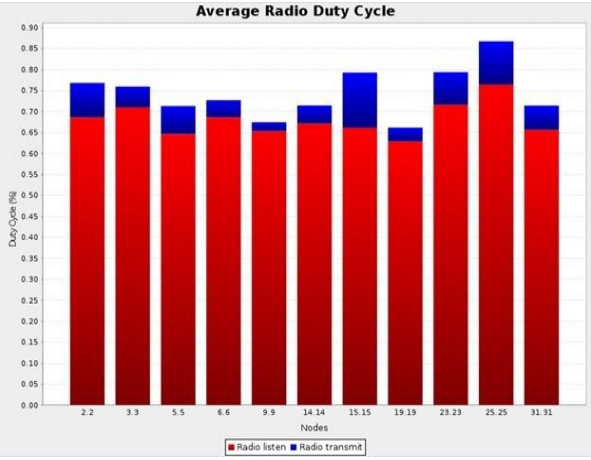


Fig. 6. Scenario 1 Radio Duty Cycle Graph

The graph in Fig.6 represents the Radio duty cycle trend of the first scenario. The major part of the radio duty cycle is occupied by the radio listen cycle.

B. Simulation with 60 nodes (1 sink node, 3 cluster heads, 3 edge nodes, 8 malicious nodes, 44 sensor nodes)

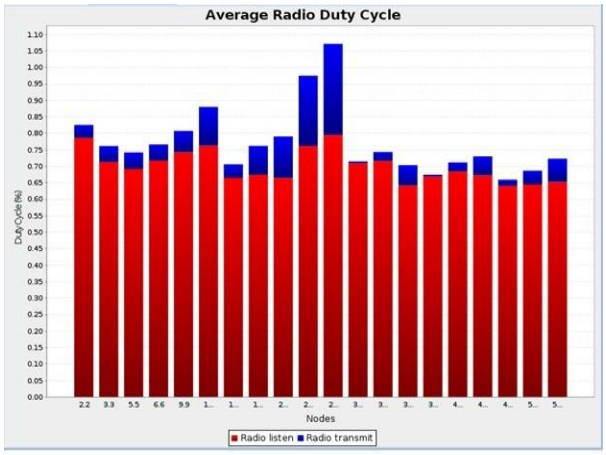


Fig. 7. 60 Node Network Grid

Fig.7 represents the network topology of the first scenario with 30 nodes. The Green node represents the sink node,purple nodes represent the edge nodes, dark blue represents the cluster head, sky blue represents the malicious nodes and yellow nodes represent the normal sensor nodes.

Fig.8 represents the power consumption trend of the first scenario. The max consumption was clocked at 1.25 mW.

The graph in Fig.9 represents the Radio duty cycle trend of the first scenario. The major part of the radio duty cycle is occupied by the radio listen cycle and it is similar to the trend seen in the first scenario.

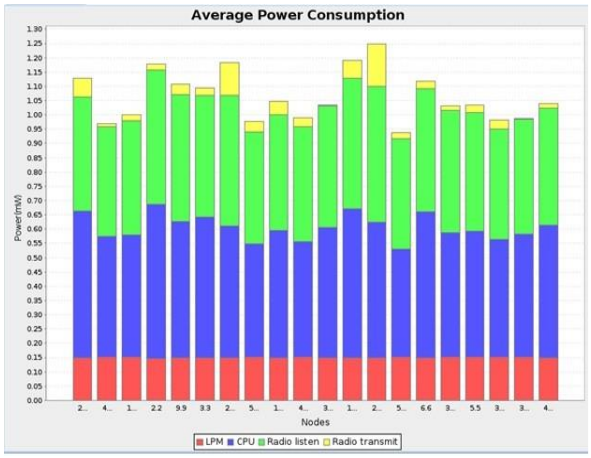


Fig. 8. Scenario 2 Power Consumption Graph

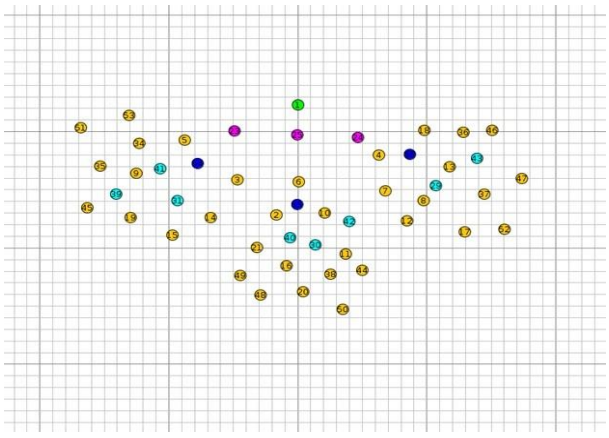


Fig. 9. Scenario 2 Radio Duty Cycle Graph

By comparing the above scenarios, the changes in the power consumption and radio duty cycles are of small proportions fortwice the number of nodes. This

can indicate that the algorithm is working efficiently and is scalable.

The potential advantages of the proposed work:

1) Detection Accuracy: The simulation results demonstrate that the proposed mechanism successfully detects ma- licious nodes in both scenarios. This indicates that the algorithm is effective in identifying and alerting about the presence of malicious nodes in the network. Comparing the detection accuracy of the proposed work with existing solutions would provide more insights intoits superiority.

2)

Scalability: The comparison between the two scenar- ios with different numbers of nodes suggests that the proposed mechanism is scalable. Despite doubling the number of nodes, the changes in power consumption and radio duty cycles are small. This scalability indicates that the proposed algorithm can handle larger networks without significant performance degradation, which can be an advantage over some existing works that may struggle with scalability.

3) Efficiency: The power consumption trend graph shows that the proposed work maintains low power consump- tion in both scenarios. This efficiency is crucial for WSNs, as minimizing power consumption prolongs net- work lifetime and reduces the need for frequent bat- tery replacements or recharging. Compared to existing solutions, the proposed mechanism's efficient resource utilization can be a notable advantage.

4) Decentralized-Centralized Approach: The decentralized- centralized mechanism proposed in this work combines the benefits of both decentralized and centralized ap- proaches. By leveraging a decentralized network of sen- sor nodes to detect abnormal behaviors and then utilizing a centralized fog layer for data analysis and decision-making, the proposed mechanism may offer a robust andefficient solution for malicious node detection.

Overall, our simulations demonstrate that our proposed approach is effective in detecting malicious nodes in a WSN using a specification-based approach.

Our algorithm was able to accurately distinguish between normal and malicious behav- ior. These results suggest that our approach has the potential to be used in real-world WSNs to improve their security and resilience against attacks.

VI. CONCLUSION

In conclusion, the presented algorithm for detecting ma- licious nodes in wireless sensor networks, which employs a decentralized-centralized approach and a specification-based methodology, has yielded promising outcomes. The algo- rithm's performance was assessed through simulations involv- ing scenarios with 30 and 60 nodes, comprising both normal and malicious nodes.

The obtained results revealed a commendable level of detection accuracy, with the algorithm effectively identifying malicious nodes in both scenarios. Furthermore, the algorithm showcased efficient resource utilization as evidenced by the low power consumption trend. Notably, the algorithm demon- strated scalability, as doubling the number of nodes resulted in minimal changes in power consumption and radio duty cycles. These outcomes underscore the merits of the proposed work, which offers an effective solution for detecting malicious nodes and enhancing the security and resilience of wireless sensor networks. The algorithm's decentralized-centralized ap- proach harnesses the advantages of both paradigms, while the

specification-based approach enhances detection precision. The algorithm's capability to monitor communication be-

havior, employ a distributed reputation system, detect anoma- lous activities, and calculate spaciousness scores has proven to be successful in identifying and isolating malicious nodes. By leveraging these techniques, the algorithm significantly bolsters the security of wireless sensor networks.

Overall, the results obtained from this study underscore the potential applicability of the proposed algorithm in real-world wireless sensor networks.

Its effectiveness, scalability, and efficient resource utilization position it as a valuable tool for researchers and practitioners working in the field of wirelesssensor networks and security.

REFERENCES

[1] Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In 2006 8th International Conference Advanced Communication Technology (Vol. 2,pp. 6-pp). IEEE.

[2] Burhanuddin, M. A., Mohammed, A. A. J., Ismail, R., Hameed, M. E., Kareem, A. N., & Basiron, H. (2018). A review on security challenges and features in wireless sensor networks: IoT perspective. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 10(1-7), 17-21.

[3] Tomić, I., & McCann, J. A. (2017). A survey of potential security issues in existing wireless sensor network protocols. IEEE Internet of Things Journal, 4(6), 1910-1923.

[4] Ibrahim, D. S., Mahdi, A. F., & Yas, Q. M. (2021). Challenges and issues for wireless sensor networks: a survey. Journal of Global Scientific Research, 6(1), 1079-1097.

[5] Martins, D., & Guyennet, H. (2010, September). Wireless sensor net- work attacks and security mechanisms: A short survey. In 2010 13th international conference on network-based information systems (pp. 313-320). IEEE.

[6] Farooqi, A. H., & Khan, F. A. (2009, December). Intrusion detection systems for wireless sensor networks: A survey. In International Confer- ence on Future Generation Communication and Networking (pp. 234- 241). Springer, Berlin, Heidelberg.

[7] Pires, W. R., de Paula Figueiredo, T. H., Wong, H. C., & Loureiro, A. A.
F. (2004, April). Malicious node detection in wireless sensor networks. In 18th International Parallel and Distributed Processing Symposium, 2004. Proceedings. (p. 24). IEEE.

[8] Jaint, B., Indu, S., Pandey, N., & Pahwa, K. (2019, October). Malicious node detection in wireless sensor networks using support vector ma- chine. In 2019 3rd International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE) (pp. 247-252). IEEE.

[9] Atakli, I. M., Hu, H., Chen, Y., Ku, W. S., & Su, Z. (2008, April). Malicious node detection in wireless sensor networks using weighted trust evaluation. In Proceedings of the 2008 Spring simulation multi-conference (pp. 836-843).

[10] Gomathi, S., & Gopala Krishnan, C. (2020). Malicious node detection in wireless sensor networks using an efficient secure data aggregation protocol. Wireless Personal Communications, 113(4), 1775-1790.

[11] Prabhan, A. P., Anand, S., & Sinha, S. (2019). Identifying faulty nodes in wireless sensor network to enhance reliability. International Journal of Recent Technology and Engineering (IJRTE) ISSN, 8(2), 2277-3878.

[12] Lakshmi, H. N., Anand, S., & Sinha, S. (2019). Flooding attack in wireless sensor network-analysis and prevention. International Journal of Engineering and Advanced Technology, 8(5), 1792-1796.

[13] Anusha, P. C., Anand, S., & Sinha, S. (2019). RSSI-based localization system in wireless sensor network. International Journal of Engineering and Advanced Technology (IJEAT), 8(5).

[14] Krishnapriya, K. M., Anand, S., & Sinha, S. (2019). A customised approach for reducing energy consumption in wireless sensor network. International Journal of Innovative Technology and Exploring Engineer-ing (IJITEE), 8(8).

[15] Nair, Devika S and BJ, Santhosh Kumar (2021, January). Identifying Rank Attacks and Alert Application in WSN. 2021 6th International Conference on Communication and Electronics Systems (ICCES) (pp. 798-802). IEEE.

[16] Anand, S., & Rr, A. (2018). A protocol for the effective utilization of energy in wireless sensor network. International Journal of Engineering & Technology, 7(3.3), 93-98.

[17] Kumar, N., Lohani, D., & Acharya, D. (2022). Vehicle accident sub- classification modeling using stacked generalization: A multisensor fusion approach. Future Generation Computer Systems, 133, 39-52.

[18] Mohammadi, M., Sharifi, M., & Rahmani, A. M. (2020). A compre- hensive review of security threats and defense mechanisms in wireless sensor networks. Journal of Ambient Intelligence and Humanized Com- puting, 11(10), 4273-4306.

[19] Badiuzzaman, M., Alshomrani, S., & Islam, S. (2021). Survey on security issues and challenges in wireless sensor networks: Taxonomy and future directions. Journal of Ambient Intelligence and Humanized Computing, 12(3), 2645-2670.

[20] Jin, Y., Wang, C., & Liu, Y. (2021). A survey on security in wireless sen- sor networks: Threats, countermeasures and open issues. IEEE Access, 9, 64016-64030.

[21] Mukhopadhyay, A., Anoop, A., Manishankar, S., & Harshitha, S. (2020, February). Network performance testing: a multi scenario contemplate. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) (pp. 1-7). IEEE.

[22] Alharbi, R. A., Al-Jumah, M. A., Alqarni, A. M., & Alshehri, M. A. (2021). A comprehensive survey on security in wireless sensor networks: Attacks and countermeasures. IEEE Access, 9, 42945-42969.

[23] Yang, X., & Yang, G. (2019). A survey on security issues in wireless sensor networks. Security and Communication Networks, 2019, 1-20.

[24] Joshi, Pallavi and Raghuvanshi, Ajay Singh(2022). A dual synchroniza- tion prediction-based data aggregation model for an event monitoring IoT network. Journal of Intelligent & Fuzzy Systems, 2022, 1-20.

[25] Saleh, Alaa and Joshi, Pallavi and Rathore, Rajkumar Singh and Sengar, Sandeep Singh (2022). Trust-Aware Routing Mechanism through an Edge Node for IoT-Enabled Sensor Networks. Sensors, 2022, 1-20.

[26] Rani, Pooja and Sharma, Nitin and Singh, Pariniyojit Kumar (2011). Performance comparison of VANET routing protocols. 2011 7th In- ternational Conference on Wireless Communications, Networking and Mobile Computing, 2011, 1-4.

[27] Biju, Rahul N and Akhil, K M and Sinha, Somnath (2022). RSSI Based Device Monitoring with IEEE 802.15 in Wireless Sensor Network. 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 503-508). IEEE.