# Comprehensive Study on Malicious Node Detection Models in Mobile Networks

Gotte Ranjith kumar[1,] Dr.K.Suresh babu[2]

*[1] Research Scholar, Department of Computer Science & Engineering, Jawaharlal Nehru Technological University, Kukatpally, Hyderabad, Telangana, 500085, India.*

*[1]Asst. Professor, School of CS&AI, SR University, Warangal - 506371, Telangana, India.*

*[2] Professor, Computer Science and Engineering, Jawaharlal Nehru Technological University, Kukatpally, Hyderabad, Telangana, India-500085.*

***Abstract*—Mobile networks enable communication through radio waves among users, over large geographical regions. However, the increasing number of interconnected devices in these networks heightens the potential for malicious attacks. These networks are highly vulnerable to malicious nodes. Robust security protocols, anomaly detection mechanisms, frequent software updates, encryption, and user awareness are essential strategies to protect mobile networks. Furthermore, machine learning (ML) and deep learning (DL) techniques offer significant improvements in anomaly detection capabilities. Despite these advances, mobile networks face ongoing challenges, such as resource constraints, high false positive rates, and sophisticated malicious nodes that mimic legitimate users. This paper explores various malicious node detection mechanisms, highlighting their limitations, and proposes that deep learning-based methods offer improved efficiency in terms of resource and energy consumption. A comparative analysis is conducted using three detection mechanisms: the Anonymous Handover Authentication (AHA) process, a Secure Blockchain-Based Authentication and Key Agreement (5GSBA) scheme, and the Elliptic Curve Cryptography-Based Diffie-Hellman (ECDH) method.**

***Index Terms*—Mobile networks, Malicious node detection, Handover Authentication process, Secure Blockchain-Based Authentication and Key Agreement scheme, and the Elliptic Curve Cryptography-Based Diffie-Hellman method.**

## I. INTRODUCTION

Mobile networks establish communication in the form radio waves among users. It consists of base stations; each station covers a defined area or cell. When joined, these stations provide a wide range of radio waves over wide geographical area. Mobile networks are dynamic in nature. The proliferation of interconnected devices in the network increases the chance for more attacks. Therefore, it is essential to understand the vulnerabilities in the network and development of security models. Mobile networks are highly vulnerable to malicious nodes [1]. These nodes can interrupt the communication and compromise the data integrity in the network [2]. Developing effective countermeasures needs thorough study of their behaviour in the network. Monitoring, identification, and isolation of these nodes is needed to mitigate their impact on the network.

A robust security protocols and anomaly detection mechanisms are need to be implemented to prevent the malicious node's activities. Frequent software updating and encryption mechanism can also strengthen network defences. Collaborative strategies like awareness among users plays a crucial role in early detection of malicious activities. Engaging in persistent security assessment will also help to cope up with the evolving network threats. With the help of machine learning (ML) and deep learning (DL) techniques anomaly detection capabilities in the network can be enhanced [3]. In mobile networks poses significant challenges due to their evolving tactics. False positives can overwhelm systems, leading to resource wastage. Additionally, sophisticated malicious nodes can mimic legitimate users, complicating detection processes. Continuous updates and refinements of detection algorithms are essential. Mobile networks (wireless networks) have limitations in terms of resources and energy. Many existing malicious node detection techniques are with high accuracy and good performance in detecting malicious node. The efficiency of the model depends on the consumption of resources and energy during the process of malicious node detection. The following section presents various malicious node detection mechanisms in mobile networks and their limitations. Malicious node detection using DL techniques will be efficient in terms of resource and energy consumption. This result analysis is by comparing three mechanisms such as Anonymous Handover authentication (AHA) process, a secure blockchain based authentication and key agreement (5GSBA) scheme, Elliptic Curve Cryptography based Diffie-Hellman (ECDH) method.

## II. MALICIOUS NODE DETECTION MECHANISMS

Malicious node detection techniques cover various strategies in order to address the unique challenges posed by the dynamic and decentralized nature of the mobile networks. Kiruba et al.[4] Employed an irregular set technique to identify malicious sensor nodes in wireless sensor networks (WSN). This mechanism help to distinguish between malicious node and legitimate node based on their behaviour. Each sensor node broadcast the information about adjacent nodes. The route entry table plays a crucial role to identify malicious node by utilizing broadcasted Meta data. Limitations of irregular set technique includes:

- This technique involves complex algorithms. It will be challenging and difficult to implement in real time scenario, especially in mobile networks.
- The effectiveness of this technique depends on broadcasting Meta data. If the data is incomplete, that may lead to incorrect identification of malicious nodes.
- As number of nodes getting increased in the networks, that will add computational overhead to this technique, which affects the performance. Moreover, this technique will not consider the broader nodes interactions, which could lead to false positive rate in malicious node detection.

Yannam et al.[5] Focused on analysing various characteristics like monitoring packets sent, receive and dropped to identify the node behaviour. Authors proposed a method “detection of jamming nodes” by utilizing packet delivery ratio and packet drop ratio to differentiate between malicious and legitimate nodes. This model heavily relies on packet delivery and drop ratio. This reliance may not capture all types of attacks on the nodes. Moreover, as network size is getting increased it becomes complex to monitor packet deliver and drop ratio. It effects performance of the network.

Zhao et al.[6] used isolated forest algorithm to analyse node behaviour by collecting trust evidence through trust evidence chain. This chain is dynamically updated using decay and control mechanism. The Isolated Forest algorithm is utilized to analyze node behavior, which helps in adjusting behavioural credibility through Bayes rule. The paper employs various clustering techniques, including K-Means, Gaussian Mixture Model (GMM), Three-way Decision, and Grey Cluster, to categorize nodes into trusted, suspicious, and malicious sets. The algorithm assumes that anomalies are rare and different from normal instances. If the distribution of anomalies is similar to that of normal data, the algorithm may struggle to identify them effectively. While Isolated Forest is generally efficient, it may face challenges when dealing with extremely large datasets, as the computational cost can increase with the number of trees and data points. The model's decision-making process can be opaque, making it difficult to interpret why certain nodes are classified as malicious or not, which can be a drawback in applications requiring transparency.

Jianmin Gu et al.[7] proposed a cross layer intrusion detection system that utilizes information from multiple layers of the OSI model to enhance detection accuracy of black hole attacks in mobile ad hoc networks (MANETs) .At the first level of the proposed system, data extracted from various layers is input into a fuzzy logic system. This system helps classify nodes as malicious, normal, or suspicious based on the gathered data.If a node is identified as suspicious, the second level of the system applies Dempster-Shafer theory to further verify the nature of that node. This method helps in confirming whether the node is indeed malicious. Dempster-Shafer theory suffers complexity issues when number of hypotheses are increased, which results in slower processing time in real time applications. The theory struggles with conflicting evidence. When multiple sources provide contradictory information, it can be challenging to reconcile these differences effectively, potentially leading to inaccurate conclusions. The results derived from Dempster-Shafer theory can sometimes be difficult to interpret, especially for users who are not familiar with the underlying concepts, which may hinder its practical application.

Muhammad Nouman et al.[8] proposed Histogram Gradient Boost (HGB) classifier , which is implemented in base station (BS) to any analyse the data received from cluster head (CH) in wireless sensor networks. The HGB classifier uses a method called boosting, which combines multiple weak learners to create a strong model. This helps in accurately identifying patterns in the data that indicate malicious behaviour. If the HGB classifier identifies a node as malicious, it quickly revokes that node's registration from the network. This prevents the malicious node from affecting the network further. While HGB is designed to be efficient, it still requires significant computational resources, especially when dealing with large datasets. This can be a limitation in environments with constrained resources, such as mobile networks. HGB can be seen as a "black box." This means that understanding how it makes specific decisions can be challenging, which may hinder trust in its predictions. If the input data contains a lot of irrelevant or misleading information, it can affect the classifier's performance, leading to incorrect classifications of nodes as malicious or legitimate.

Kanthimathi et al[9] proposed a model called a cluster-based trust entropy model, this helps in avoiding malicious nodes during routing in the wireless network. Authors created a data set from the simulation of this model. It crucial for applying machine learning algorithms to achieve high detection accuracy. This model address common security attacks like selective forwarding and denial of service attacks. Implementing this model requires significant computational resources. It will struggle to adapt quickly to dynamic changes in the network that can affect performance of the model.

Wang et al.,[10] proposed a dynamic trust management algorithm that is essential for detecting malicious nodes in Wireless Weak-link Sensor Networks (WWSNs). This algorithm evaluates node trust comprehensively by integrating type-2 fuzzy logic, which allows for a nuanced assessment of trust levels based on various factors. A key feature of the proposed strategy is the dynamic updating mechanism for trust values. This mechanism is designed to adapt to the changing environmental conditions typical of WWSNs, ensuring that the trust evaluations remain relevant and effective over time . The effectiveness of the dynamic trust management algorithm relies heavily on the selection and accuracy of the trust factors considered. If these factors are not well-defined or relevant, the trust evaluation may be compromised, leading to incorrect identification of malicious nodes. While type-2 fuzzy logic enhances the algorithm's ability to handle uncertainty, it also adds complexity to the implementation. This complexity may require more computational resources, which could be a limitation in resource-constrained environments typical of Wireless Weak-link Sensor Networks (WWSNs) . Although the algorithm includes a dynamic trust value updating mechanism, rapid or extreme changes in the network environment may still pose challenges. The algorithm might struggle to keep up with these changes, potentially affecting its performance in real-time scenarios.

Mohit kumar et al., [11] proposed Improved Deep Convolutional Neural Network (IDCNN) , analyses various parameters from each Sensor Node (SN) in the Wireless Sensor Network (WSN). This analysis is crucial for identifying patterns that indicate malicious behaviour. The IDCNN employs a detection mechanism that processes the input data from the SNs. By learning from the characteristics of both normal and malicious nodes, it can effectively distinguish between them based on the learned features. Once the IDCNN identifies a node as malicious, it isolates these nodes into a malicious list box during the Malicious Nodes Detection (MND) phase. This step is essential for ensuring that the identified MNs do not interfere with the network's operations. IDCNN performance relies on the quality and quantity of the training data. If the dataset contains noise or insufficient examples of malicious nodes, the detection accuracy may be compromised. The IDCNN may require significant computational resources for training and inference, especially in large-scale Wireless Sensor Networks (WSN). This can be a limitation in resource-constrained environments where sensor nodes have limited processing power. It will struggle to adapt to rapidly changing network conditions and new type of attacks.

S. Syed Jamaesha et al., [12] proposed Dendritic Cell with Adaptive Trust Q-learning Protocol (dDC-ATQP) to find malicious node. This mechanism assesses the behaviour of nodes within the network to identify potential malicious actors. By evaluating trust levels, it helps mitigate the impact of these malicious nodes on the overall system performance. The protocol includes an adaptive routing strategy that optimizes data transmission paths based on real-time network conditions. This helps in reducing latency and packet loss during data transmission. The performance of the protocol is measured through simulation by considering various metrics such as throughput, end-to-end delay, energy consumption, packet delivery ratio, and packet loss ratio.

Chencheng Hu et al[13] proposes a new authentication scheme that ensures user anonymity while allowing secure handover between access points in wireless mobile networks. This is achieved through the use of pseudonyms and a blockchain certificate model. The authors incorporate blockchain to manage user identities and certificates securely. This technology provides a tamper-resistant and distributed method for storing authentication data, which enhances security and efficiency. Focused on blockchain technology to make authentication process in mobile networks more secure and private. Anonymous Handover authentication (AHA) process is used to authenticate the user in mobile networks. Anonymous handover authentication process can also be used to find malicious node in the mobile networks. This model takes high amount of energy, faces scalability issues and transaction confirmation on blockchain will introduce delay in the authentication process. In the process of malicious node detection AHA obtained communication time 54.5ms, memory acquired 736.86 bytes, time cost 81.02 sec

Man Chun Chow et al.[14] Proposed a secure blockchain based authentication and key agreement (5GSBA) scheme for decentralized authentication to prevent attacks like DoS in mobile networks. 5GSBA employs one-time secret hash function as the device secret key to prevent device impersonation even if the database is compromised. Eventually user equipment will be protected from the adversaries. By allowing all base stations to handle authentication requests, single point failure can be avoided. 5GSBA is also used to find malicious nodes in the mobile networks with communication time 50.98ms, consumes memory 666.34 bytes and time cost 74.24 sec. 5GSBA introduces additional communication, computational and energy overhead. The performance of 5GSBA depends on blockchain. If blockchain experience any delay that will affect overall authentication process. 5GSBA is efficient to resist known attacks.

There is always risk of new attacks.

Adnan Shahid Khan et al.[15] Employed Elliptic Curve Cryptography based Diffie-Hellman (ECDH) method for mutual authentication, which enhances security wireless networks. One way has function is introduced to ensure that the data cannot be easily tampered with. Blockchain technology is integrated to achieve integrity, non-repudiation and traceability in authentication process of the node. This protocol is designed to reduce communication and computational overhead on the node. Through this authentication process malicious node can be detected. In the process of malicious node detection its communication time is 47.09ms, memory need is 603.08 bytes and time cost is 66.71sec.

Authentication mechanisms proposed by the authors[13] [14] [15] are used to detect malicious nodes in mobile networks. Performance of these mechanisms are compared in terms of communication time, memory required and time taken to find malicious node. Performance comparison is shown in the figure 1.

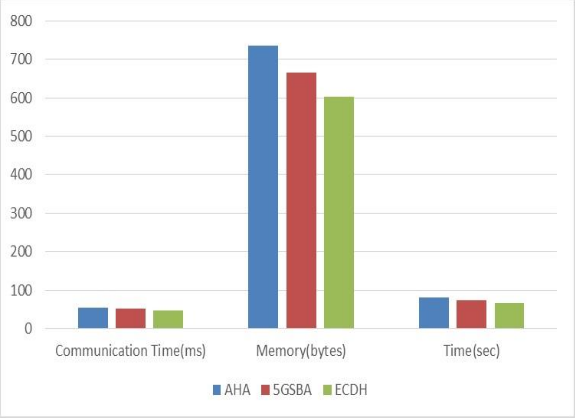

Figure 1: Performance comparison of AHA, 5GSBA and ECDH

The survey reveals a diverse range of malicious node detection mechanisms employed in wireless networks, each with its own set of strengths and weaknesses. A critical observation from this analysis is that the performance of many existing mechanisms is heavily reliant on the consumption of network resources during the detection process. In resource-constrained environments, such as those typical of wireless networks, this resource utilization can significantly impact network performance and even hinder critical applications. Therefore, a paramount objective for future research is to develop and refine malicious node detection mechanisms that minimize resource consumption while maintaining high levels of accuracy and efficiency. This will be crucial for ensuring the reliable and secure operation of wireless networks in various resource-constrained scenarios.

## III. SUMMARY OF MALICIOUS NODE DETECTION MECHANISMS

| Sl.no. | Title | Methodology | Limitation |
|---|---|---|---|
| 1 | A Proficient Obtrusion Recognition Clustered Mechanism for Malicious Sensor Nodes in a Mobile Wireless Sensor Network | Irregular set Technique | Increasing number of nodes will complicate the algorithm. |
| 2 | Analysis of Behavioral Characteristics of Jammers to Detect Malicious Nodes in Mobile ADHOC Networks | detection of jamming nodes | Network size limit the algorithm performance and will not work for new attacks. |
| 3 | A Cooperative Detection Scheme for Malicious Nodes Based on D-S Trust Evidence Reasoning in Mobile Crowdsensing Networks | Isolated Forest Algorithm | Computational complexity will be increased with the large data set. |
| 4 | Design of a Cross Layer Intrusion Detection System for Mobile Ad Hoc Networks to Mitigate Black Hole Attack | cross layer intrusion detection system | suffers from complexity issues when number of hypotheses are increased, |
| 5 | Malicious Node Detection Using Machine Learning and Distributed Data Storage Using Blockchain in WSNs | Histogram Gradient Boost (HGB) classifier | Not suitable for resource constrained environment. It is seen as a block box. |
| 6 | Exploring Machine Learning Algorithms for Malicious Node Detection Using Cluster-Based Trust Entropy. | cluster-based trust entropy model | Struggle to adapt to the dynamic change in the network. Requires more computational resources. |
| 7 | Malicious Node Detection in Wireless Weak-Link Sensor Networks Using Dynamic Trust Management | dynamic trust management algorithm | Not suitable for resource constraint environment. Struggle to adapt to dynamic change in the network. |
| 8 | Improved Deep Convolutional Neural Network Based Malicious Node Detection and Energy-Efficient Data Transmission in Wireless Sensor Networks | Improved Deep Convolutional Neural Network | This resource constrained mechanism. Struggle to adapt to new attacks. |
| 9 | Deep Artificial Immune System With Malicious Node Detection and Secure Routing Protocol in MANET | Dendritic Cell with Adaptive Trust Q-learning Protocol | Computational complexity, Energy consumption, scalability issues. |
| 10 | A Novel Blockchain-based Anonymous Handover Authentication Scheme in Mobile Networks | pseudonyms and a blockchain certificate model | Faces scalability issues and delay in authentication. |
| 11 | A Secure Blockchain-Based Authentication and Key Agreement Scheme for 3GPP 5G Networks | secure blockchain based authentication and key agreement (5GSBA) scheme | It introduces additional communication, computational and energy overhead |

## IV. CONCLUSION

Wireless networks, due to their open and broadcast nature, are inherently more susceptible to attacks compared to wired counterparts. The presence of malicious nodes within the network can significantly degrade performance, impacting factors such as data transmission rates, latency, and overall network stability. This research has conducted a comprehensive survey of various malicious node detection mechanisms, highlighting their strengths and weaknesses. The findings of this survey can serve as a valuable resource for researchers and practitioners in the field of wireless network security, guiding the development and implementation of more robust and efficient defence strategies against malicious activities in wireless environments.

## V. ACKNOWLEDGEMENT

I would like to express my sincere gratitude to SR University, Warangal, Telangana, India for providing the necessary infrastructure and support to carry out this research. I am particularly thankful to my supervisor, Dr.K.Suresh babu, Professor, Computer Science & Engineering, JNTU Hyderabad, Telangana, India for his valuable guidance, encouragement, and insightful feedback throughout the development of this work.

## VI. CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper. The research was conducted independently, without any commercial or financial relationships that could be construed as a potential conflict of interest. All funding sources, if any, have been acknowledged appropriately, and no external party influenced the study design, data collection, analysis, or decision to publish.

## REFERENCES

[1] G. Liu, N. Fan, C. Q. Wu, and X. Zou, “On a Blockchain-Based Security Scheme for Defense against Malicious Nodes in Vehicular Ad-Hoc Networks,” *Sensors*, vol. 22, no. 14, p. 5361, Jul. 2022, doi: 10.3390/s22145361.

[2] S. M. Udhaya Sankar, N. Jagadish Kumar, G. Elangovan, and R. Praveen, “An Integrated Z-Number and DEMATEL-Based Cooperation Enforcement Scheme for Thwarting Malicious Nodes in MANETs,” *Wirel. Pers. Commun.*, vol. 130, no. 4, pp. 2531–2563, Jun. 2023, doi: 10.1007/s11277-023-10391-7.

[3] K. K. S. Liyakat, “Detecting Malicious Nodes in IoT Networks Using Machine Learning and Artificial Neural Networks,” in *2023 International Conference on Emerging Smart Computing and Informatics (ESCI)*, Pune, India: IEEE, Mar. 2023, pp. 1–5. doi: 10.1109/ESCI56872.2023.10099544.

[4] D. Giji Kiruba, J. Benita, and D. Rajesh, “A Proficient Obtrusion Recognition Clustered Mechanism for Malicious Sensor Nodes in a Mobile Wireless Sensor Network,” *Indian J. Inf. Sources Serv.*, vol. 13, no. 2, pp. 53–63, Nov. 2023, doi: 10.51983/ijiss-2023.13.2.3793.

[5] A. Yannam, B. M. Suryadevara, T. Thabassum, V. M. Sai, and M. Vatturi, “Analysis of Behavioral Characteristics of Jammers to Detect Malicious Nodes in Mobile ADHOC Networks,” *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, no. 5s, pp. 494–510, Jun. 2023, doi: 10.17762/ijritcc.v11i5s.7111.

[6] G. Zhao, R. Chen, and J. Wang, “A Cooperative Detection Scheme for Malicious Nodes Based on D-S Trust Evidence Reasoning in Mobile Crowdsensing Networks,” 2023. doi: 10.2139/ssrn.4678010.

[7] L. Mekadem and M. Bourenane, “Design of a Cross Layer Intrusion Detection System for Mobile Ad Hoc Networks to Mitigate Black Hole Attack,” in *Proceedings of the 14th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2022)*, vol. 648, A. Abraham, T. Hanne, N. Gandhi, P. Manghirmalani Mishra, A. Bajaj, and P. Siarry, Eds., in Lecture Notes in Networks and Systems, vol. 648. , Cham: Springer Nature Switzerland, 2023, pp. 90–99. doi: 10.1007/978-3-031-27524-1_10.

[8] M. Nouman, U. Qasim, H. Nasir, A. Almasoud, M. Imran, and N. Javaid, “Malicious Node Detection Using Machine Learning and Distributed Data Storage Using Blockchain in

WSNs," *IEEE Access*, vol. 11, pp. 6106–6121, 2023, doi: 10.1109/ACCESS.2023.3236983.

[9] S. Kanthimathi, "Exploring Machine Learning Algorithms for Malicious Node Detection Using Cluster-Based Trust Entropy," *IEEE Access*, vol. 12, pp. 137913–137925, 2024, doi: 10.1109/ACCESS.2024.3465843.

[10] C. Wang, G. Liu, and T. Jiang, "Malicious Node Detection in Wireless Weak-Link Sensor Networks Using Dynamic Trust Management," *IEEE Trans. Mob. Comput.*, vol. 23, no. 12, pp. 12866–12877, Dec. 2024, doi: 10.1109/TMC.2024.3418826.

[11] M. Kumar, P. Mukherjee, K. Verma, S. Verma, and D. B. Rawat, "Improved Deep Convolutional Neural Network Based Malicious Node Detection and Energy-Efficient Data Transmission in Wireless Sensor Networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 5, pp. 3272–3281, Sep. 2022, doi: 10.1109/TNSE.2021.3098011.

[12] S. S. Jamaesha, M. S. Gowtham, and M. Ramkumar, "Deep Artificial Immune System With Malicious Node Detection and Secure Routing Protocol in MANET," *Trans. Emerg. Telecommun. Technol.*, vol. 35, no. 11, p. e70008, Nov. 2024, doi: 10.1002/ett.70008.

[13] ChenCheng Hu, Dong Zheng, Rui Guo, and AXin Wu, "A Novel Blockchain-based Anonymous Handover Authentication Scheme in Mobile Networks," *Int. J. Netw. Secur.*, vol. 22, no. 5, pp. 874–884, Sep. 2020, doi: 10.6633/IJNS.202009 22(5).19.

[14] M. C. Chow and M. Ma, "A Secure Blockchain-Based Authentication and Key Agreement Scheme for 3GPP 5G Networks," *Sensors*, vol. 22, no. 12, p. 4525, Jun. 2022, doi: 10.3390/s22124525.

[15] A. S. Khan *et al.*, "Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network," *IEEE Access*, vol. 11, pp. 20524–20541, 2023, doi: 10.1109/ACCESS.2023.3249969.