Journal of Cognitive Human-Computer Interaction

♦ ISSN: 2771-1463 Vol: 08, No. 01, 2024 ♦ PP. 10–13

Article DOI: https://doi.org/10.54216/JCHCI.080103

REVIEW ARTICLE

Sybil Attack Detection Techniques in Wireless Network: A Comprehensive Review

Lalzuitluanga[1,*] **Lalremruata**[1] **Vanlalhruaia**[2]

[1] Department of Computer Engineering, Mizoram University, Aizawl-796004, India

[2] Assistant Professor, Department of Computer Engineering, Mizoram University, Aizawl-796004, India

Emails: lalzuitluanga19@gmail.com · remruata1712@gmail.com · mzut160@mzu.edu.in

Received: October 05, 2023 Revised: January 12, 2024 Accepted: April 15, 2024 ⋆ Corresponding author

ABSTRACT

In today's rapidly evolving world, wireless technology has emerged as an essential solution for establishing connectivity in diverse environments. Wireless networks offer cost-effective deployment options and scalability, accommodating organizational growth without the need for extensive infrastructure changes. However, wireless networks are susceptible to various security attacks, including Sybil attacks. In this paper, we provide a comprehensive review of Sybil attack detection techniques in wireless networks, particularly Mobile Ad hoc Networks (MANETs) and Wireless Mesh Networks (WMNs). We analyse a range of methods proposed to detect and mitigate Sybil attacks, including approaches based on genetic algorithms, fuzzy logic, secure routing protocols, and hybrid techniques combining different detection mechanisms. Additionally, we explore bio-inspired algorithms, such as the Bacteria Foraging Optimization Algorithm (BFOA), and discuss strategies integrating node authentication and threshold-based mechanisms. By examining the strengths and limitations of each approach, this review offers valuable insights into the state of the art in Sybil attack detection in wireless networks, aiding researchers and practitioners in developing robust security solutions.

Keywords: Fake node ▪ Sybil Attack ▪ Wireless Mesh Networks (WMNs) ▪ MANET

1. INTRODUCTION

Wireless networks have revolutionized the way we connect and communicate with each other. They offer unparalleled flexibility and mobility compared to traditional wired setups. By transmitting data through radio waves instead of physical cables, wireless networks enable devices to share resources and communicate without being constrained by physical limitations. Among the various types of wireless networks, Mobile Ad hoc Networks (MANETs) and Wireless Mesh Networks (WMNs) stand out for their unique capabilities and applications.

Mobile Ad hoc Network: MANETs are dynamic networks composed of mobile nodes that communicate with each other without the need for a fixed infrastructure. Nodes are free to move independently, forming temporary connections with nearby nodes to establish network communication. These networks are characterized by their self-configuring nature, where nodes collaborate to maintain connectivity and facili-tate data transmission. MANETs are well suited for scenarios where infrastructure-based networks are impractical or un-available, such as military operations, emergency response, and vehicular communication systems.

Figure 1. Multi-hop communication in MANET.

Wireless Mesh Networks: WMNs are characterized by a mesh topology, where nodes are interconnected with one another. A WMN typically consists of devices such as routers, gateways, and other networking devices. By interconnecting multiple nodes in a non-hierarchical manner, mesh networks create a robust infrastructure capable of adapting to changing conditions and expanding coverage areas. This decentralized architecture ensures that even if one node fails or experiences interference, data can still find alternative paths to reach its destination, minimizing delays and failures. As a result, WMNs represent a promising technology for delivering next-generation wireless services with wider coverage, better connectivity, and increased flexibility.

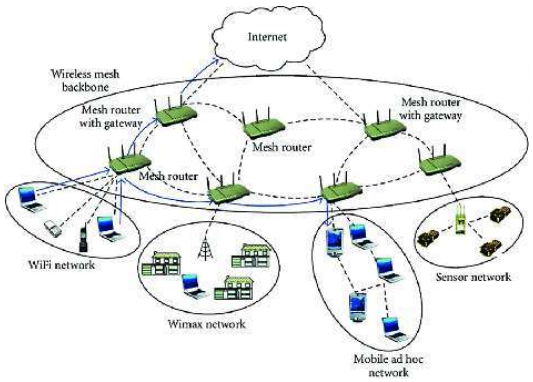

Figure 2. Wireless Mesh Network architecture.

1.1 Characteristics

MANETs and WMNs offer several unique characteristics that distinguish them from traditional wired and wireless networks [2, 3]:

- **Multi-hop communication:** both MANETs and WMNs support multi-hop communication, enhancing coverage and resilience.
- **Dynamic self-organization:** these networks autonomously discover and configure connections, enabling seamless deployment and operation in changing environments.
- **Scalability:** MANETs and WMNs can accommodate new nodes, expanding their reach and capacity to meet evolving connectivity demands.
- **Reliability and redundancy:** multiple transmission paths ensure high reliability, minimizing disruptions in case of node failure.
- **Flexibility:** MANETs and WMNs support diverse devices and applications, integrating with other network technologies.
- **Cost-effectiveness:** their decentralized architecture and reduced hardware requirements make them cost-effective, particularly in remote or underserved areas.
- **Power efficiency:** the distributed nature of MANETs and WMNs optimizes power usage, extending operational lifespan.

1.2 Security Issues

In MANETs, the absence of a centralized authority and the reliance on individual nodes to act as routers create vulnerabilities to both internal and external attacks [1]. WMNs also face security concerns due to their interconnected nodes and shared connections. The dynamic nature of these networks introduces challenges in maintaining the physical security of nodes, which can lead to network failures. Moreover, multi-hop wireless communication opens avenues for interception, eavesdropping, and data manipulation [4]. Routing protocols used in these networks often lack sufficient security features to detect and mitigate attacks. Protecting MANETs and WMNs therefore requires comprehensive security measures implemented at multiple levels of the network architecture.

Security attacks in these networks can be classified as follows [2].

1.2.1 Active and Passive Attacks

Attacks are classified as active or passive based on their intention to disrupt network operation. Active attacks intentionally disrupt network operation, while passive attacks aim to steal information and eavesdrop on communication within the network, compromising confidentiality.

1.2.2 Internal and External Attacks

This classification is based on the origin of the attacker in the network. External attacks are conducted by attackers not participating in the network and often involve jamming or injecting incorrect information. Internal attacks are conducted by members of the network, posing more severe threats and being harder to prevent than external attacks.

In wireless networks, security attacks at the network layer can have serious consequences. One common attack is the routing attack, where malicious nodes deliberately manipulate routing information to disrupt the network's normal operation [5]. For instance, they may forge routing updates to attract traffic through compromised routes or cause congestion by selectively dropping packets. Examples include denial-of-service attacks, blackhole attacks, wormhole attacks, grey-hole attacks, and Sybil attacks [1, 6].

2. SYBIL ATTACKS AND THEIR TYPES

A Sybil attack is a security attack in which a malicious node creates multiple fake identities, or Sybil identities, within the network. These Sybil nodes deceive neighbouring nodes and disrupt normal network-layer protocols, such as routing protocols, by providing false information about available routes, node locations, or network conditions. As a result, Sybil attacks can compromise the integrity and efficiency of network communication, making them a significant concern for wireless network security.

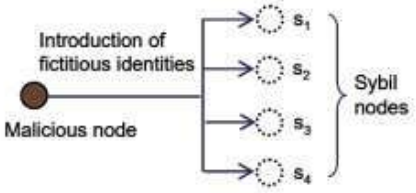

Figure 3. Malicious node presenting fake identities [8].

2.1 Types of Sybil Attack

The Sybil attack has two main types [6]: single Sybil attack, in which only one node acts as a fake node that collects all packets; and co-operative Sybil attack, in which more than one node combines and acts as fake nodes.

2.2 Dimensions of Attack

The Sybil attack is launched in three dimensions [7, 8].

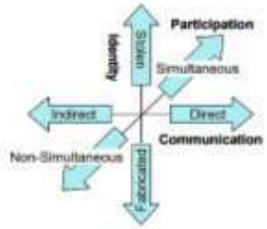

Figure 4. Dimensions of Sybil attack launch [8].

- **Direct and indirect attack:** in a direct attack, the legal node communicates directly with the malicious node. In an indirect attack, the malicious node acts between communications.
- **Fabricated and stolen identity attack:** fake nodes are created using identities of original nodes and are known as fabricated nodes. In stolen identity attacks, the attacker impersonates a legal node and then acts as a malicious node.
- **Simultaneous and non-simultaneous attack:** in a simultaneous attack, all malicious nodes participate at the same time. In a non-simultaneous attack, malicious nodes participate at different time intervals.

This review examines detection and mitigation techniques for Sybil attacks, focusing on their application in MANETs and WMNs to safeguard wireless network integrity and security.

3. LITERATURE SURVEY

Table 1. Existing Sybil attack detection techniques.

Ref.	Author(s) / Year	Technique Used	Advantage	Disadvantage
[10]	Rohit Lakhanpal and Sangeeta Sharma (2016)	Hybrid MAC and MAP technique	Reduces false positives and enhances accuracy; can be used in unicast and multicast communication.	Increased overhead and energy consumption.
[11]	Priyanka Yadav and Muzzammil Hussain (2017)	Cryptography	Ensures secure communication between nodes.	May introduce overhead and requires robust key management.
[13]	Deeksha Singh Chauhan and Shalley Bakshi (2018)	Genetic Algorithm with fuzzy logic	Improves efficiency and provides adaptive defence.	Computationally intensive; less robust in diverse environments.
[14]	S. Swathi and R. Vadivel (2020)	Bacterial Foraging Optimization (BFO)	Offers efficient detection and lower energy consumption.	Complex; depends on node density, communication range, and related factors.
[15]	S. Rethinavalli and R. Gopinath (2020)	Artificial Neural Networks (ANN)	Higher accuracy, higher TPR, and reduced FPR.	Requires a large amount of training data.
[16]	Dhanashri Saindane (2021)	Threshold sequence-number filtering	Simple and easy to implement.	Sybil nodes may adapt behaviour to bypass the threshold mechanism.
[17]	Meena Bharti, Shaveta Rani, and Paramjeet Singh (2022)	RSSI and trust-based method	Two-layer detection improves accuracy, reduces false positives, and minimizes detection time.	Increases complexity and resource needs.

Lakhanpal and Sharma [10] proposed a hybrid approach combining MAC address and MAP (Message Authentication and Passing Method) techniques to detect Sybil attacks in ad hoc networks. The MAC address acts as a unique identifier for nodes, detecting malicious activity by identifying discrepancies in packet routes. Meanwhile, the MAP method ensures secure packet transactions by verifying node identity and timestamp. Integrated with the AODV routing protocol, this hybrid approach combines identification with secure packet transmission.

Yadav and Hussain [11] presented a secure routing protocol that enhances a reactive routing protocol using node authentication. The protocol requires nodes to authenticate neighbours before forwarding data packets. Successful decryption of certificates ensures secure communication, while failure indicates potential malicious activity and prevents the node from being added to the neighbour list. This authentication-enhanced routing helps defend against wormhole, man-in-the-middle, and Sybil attacks.

Chauhan and Bakshi [13] introduced a method to mitigate Sybil attacks in MANETs by combining Genetic Algorithm (GA) optimization with fuzzy logic. Routes are initially discovered, the GA optimizes the route and extracts properties of normal and attacker nodes, and fuzzy logic is trained to distinguish between normal and malicious behaviour. This combination improves network security while increasing simulation efficiency.

Swathi and Vadivel [14] presented a bio-inspired networking approach using the Bacteria Foraging Optimization Algorithm (BFOA) to detect and mitigate Sybil attacks in MANETs. BFOA identifies and eliminates Sybil nodes from the network, thereby enhancing performance and extending network lifetime. The approach uses chemotaxis, reproduction, and elimination, mimicking bacterial behaviour to optimize network operations.

Rethinavalli and Gopinath [15] proposed a classification approach for detecting Sybil attacks in MANETs using Artificial Neural Networks (ANN). They employed feature-selection techniques such as chi-square, symmetrical uncertainty, and information gain, then combined them to improve accuracy. The technique improved the true positive rate and reduced the false positive rate compared with other classifiers.

Saindane [16] proposed a simple method for detecting and mitigating Sybil attacks using the AODV routing protocol. During route discovery, Sybil nodes may send fake replies with high sequence numbers. The proposed technique introduces a threshold value for sequence numbers so that, when multiple replies are received, only the reply with the highest sequence number below the threshold is considered valid.

Bharti, Rani, and Singh [17] highlighted the harmful impact of Sybil attacks, where nodes illegitimately join multiple times under fake identities and disrupt network operations. They classified Sybil attacks into whitewashing attacks and simultaneous multiple-identity creation. Because RSSI-based methods can suffer from high false positives and trust-based approaches can be time-consuming, they introduced a hybrid

approach combining RSSI-based and trust-based techniques.

4. CONCLUSION

After reviewing various methods proposed for detecting and mitigating Sybil attacks, it is evident that there is no perfect solution. Each method comes with its own set of advantages and limitations, and the choice of approach depends on factors such as network topology, resource constraints, and the specific requirements of the application. Further research and experimentation will be crucial in refining these methods and developing new approaches that can stay ahead of evolving threats in network security. The information provided in this review offers a relevant path and makes it easier for researchers to continue work in this field.

REFERENCES

[1] B. U. I. Khan et al., "A survey on MANETs: architecture, evolution, applications, security issues and solutions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 2, pp. 832–842, 2018.

[2] S. Kumar et al., "Routing protocols and security issues in MANET," in *2017 International Conference on Infocom Technologies and Unmanned Systems (ICTUS)*, IEEE, 2017.

[3] K. C. Karthika, "Wireless mesh network: A survey," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, IEEE, 2016.

[4] S. Y. Shahdad, A. Sabahath, and R. Parveez, "Architecture, issues and challenges of wireless mesh network," in *2016 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, 2016.

[5] K. Vijay, "Collaborating the textual reviews of the merchandise and foretelling the rating supported social sentiment," *Journal of Cognitive Human-Computer Interaction*, vol. 1, no. 2, pp. 63–72, 2021.

[6] R. Sachdeva and A. Singla, "Survey on privacy issues and security attacks in wireless mesh networks," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, 2013.

[7] H. S. Atwal and N. K. Rana, "A review of Sybil attack in MANET."

[8] P. S. Deswal, B. Rani, and M. A. Rai, "Review on the detection and prevention technique of Sybil attack," *Mukt Shabd Journal*, vol. 9, pp. 1–6, 2020.

[9] A. Vasudeva and M. Sood, "Survey on Sybil attack defense mechanisms in wireless ad hoc networks," *Journal of Network and Computer Applications*, 2018, doi: 10.1016/j.jnca.2018.07.006.

[10] R. Lakhanpal and S. Sharma, "Detection and prevention of Sybil attack in ad hoc network using hybrid MAP and MAC technique," in *2016 International Conference on Computation of Power, Energy Information and Communication (ICCPEIC)*, IEEE, 2016.

[11] P. Yadav and M. Hussain, "A secure AODV routing protocol with node authentication," in *2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA)*, vol. 1, IEEE, 2017.

[12] R. Venkatesan, A. Shaik, S. Kumar, V. Guria, and A. Raj, "Intelligent smart dustbin system using Internet of Things (IoT) for health care," *Journal of Cognitive Human-Computer Interaction*, vol. 1, no. 2, pp. 73–80, 2021.

[13] D. S. Chauhan and S. Bakshi, "Mitigation of Sybil attack in MANET using GA with fuzzy logic," *Management*, vol. 3, no. 4, pp. 12–19, 2018.

[14] S. Swathi and R. Vadivel, "Bio-inspired approach Sybil attack in AODV based MANET using BFOS algorithm," *International Journal of Engineering Research and Technology*, vol. 9, no. 7, 2020.

[15] S. Rethinavalli and R. Gopinath, "Classification approach based Sybil node detection in mobile ad hoc networks," *International Journal of Advanced Research in Engineering and Technology*, vol. 11, no. 12, pp. 3348–3356, 2020.

[16] D. Saindane, "Sybil attack detection in mobile ad hoc networks using AODV protocol," *Sybil*, vol. 8, no. 7, 2021.

[17] M. Bharti, S. Rani, and P. Singh, "RTBSAD: RSSI and trust-based Sybil attack detection in MANET," *Indian Journal of Computer Science and Engineering*, 2022.