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

Abstract

In today's rapidly evolving world, wireless technology has emerged as an essential solution for establishing connectivity in diverse environments. They 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 i.e. Mobile Ad hoc Network (MANET) and Wireless Mesh Networks (WMNs). In this paper, we analyze 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 the use of bio-inspired algorithms, such as the Bacteria Foraging Optimization Algorithm (BFOA), and discuss novel 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 seamlessly 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. These networks are discussed below:

Mobile Ad hoc Network: Mobile Ad-hoc Networks (MANETs) are dynamic networks composed of mobile nodes that communicate with each other without the need for a fixed infrastructure. In MANETs, 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 network connectivity and facilitate data transmission. MANETs are well-suited for scenarios where traditional infrastructure-based networks are impractical or unavailable, such as military operations, emergency response situations, and vehicular communication systems.

Doi : https://doi.org/10.54216/JCHCI.080103
Received: October 05, 2023 Revised: January 12, 2024 Accepted: April 15, 2024

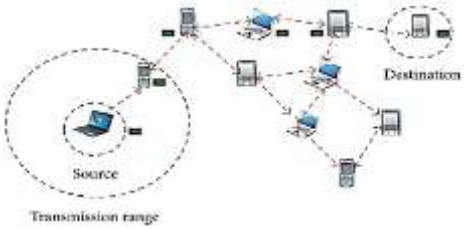

Figure 1: Multi-hop communication in MANET

Wireless Mesh Networks: Wireless mesh networks (WMNs) are characterized by a mesh topology, where nodes are interconnected with one another. It typically consists of various devices, including 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

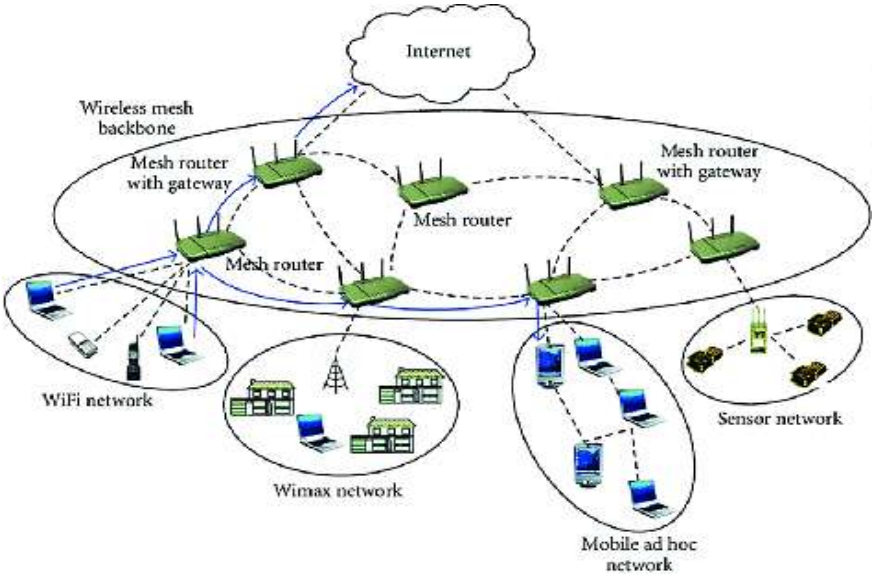

Figure 2: Wireless Mesh Network Architecture

1.2 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 easily 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.

Doi : https://doi.org/10.54216/JCHCI.080103
Received: October 05, 2023 Revised: January 12, 2024 Accepted: April 15, 2024

- **Flexibility:** MANETs and WMNs are versatile networks capable of supporting diverse devices and applications, integrating seamlessly with other network technologies.
- **Cost-effectiveness:** Their decentralized architecture and reduced hardware requirements make MANETs and WMNs cost-effective solutions, particularly in remote or underserved areas.
- **Power efficiency:** The distributed nature of MANETs and WMNs optimizes power usage, extending operational lifespan.

1.3 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]. And WMNs face security concerns due to their interconnected nodes and shared connections. The dynamic nature of these networks also introduces challenges in maintaining the physical security of nodes, which can lead to network failures. Moreover, the multi-hop wireless communication characteristic opens avenues for various attacks, including interception, eavesdropping, and data manipulation [4]. Also routing protocol used in these networks does not have security features to detect and mitigate security attacks. So, protecting both MANETs and WMNs requires comprehensive security measures implemented at multiple levels of the network architecture to mitigate the risks posed by these diverse and sophisticated security threats.

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

1.3.1 Active and Passive Attacks

Attacks are classified as either active or passive based on their intention to disrupt the network operation.

a. *Active Attacks:* Intentionally disrupt the network operation.

b. *Passive Attacks:* Aim to steal information and eavesdrop on communication within the network, compromising confidentiality.

1.3.2 Internal and External Attacks

Classifies attack based on the origin of the attacker in the network.

a. *External Attacks:* Conducted by attackers not participating in the network, often involving jamming or injecting incorrect information.

b. *Internal Attacks:* 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 attacks," 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 traffic congestion by dropping packets selectively. Examples includes Denial of Service attack, blackhole attack, wormhole attack, grey hole attack, sybil attack, etc. [1][6]

2. Sybil Attacks and its Types

Sybil attack is a type of 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 the normal operation of network layer protocols, such as routing protocols, by providing false information about available routes, node locations, or network conditions. As a result, the Sybil attack can compromise the integrity and efficiency of network communication at the network layer, making it a significant concern for the security of Wireless Networks.

Doi : https://doi.org/10.54216/JCHCI.080103
Received: October 05, 2023 Revised: January 12, 2024 Accepted: April 15, 2024

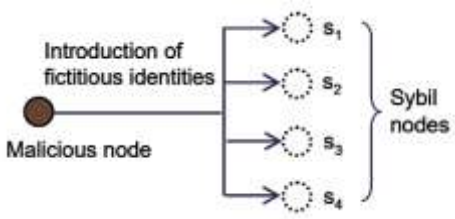

Figure 3: Malicious node presenting fake identities [8]

2.1 Types of sybil attack

The Sybil attack is off two types:[6]

a. **Single Sybil attack:** Only one node acts as a fake node that collects all the packets.

b. **Co-operative Sybil attacks*:*** More than one node combined and act as Fake nodes.

2.2 Dimension of attack

The sybil attack is done in three types or dimensions which are given below: [7][8]

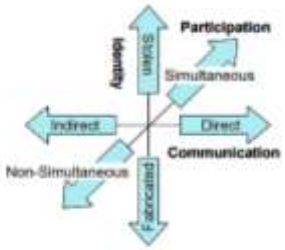

Figure 4: Dimension of Sybil attack launch [8]

a. **Direct and Indirect Attack:** In Direct attack, the legal node communicates directly to the malicious node. In an indirect attack, the malicious node acts between the communications.

b. **Fabricated and Stolen Identity Attack:** Fake nodes are created using the identities of the original node which are known as fabricated nodes. In stolen identity, the attacker impersonates the legal node and then acts as a malicious node.

c. **Simultaneous and Non-Simultaneous Attack:** In simultaneous, the participation of all malicious nodes occurs at same time in the network. While in non-simultaneous attack, the malicious nodes participate in different intervals of time.

In this comprehensive review, we delve into the detection and mitigation techniques for Sybil attacks, focusing on their application in MANETs and WMNs to safeguard the integrity and security of wireless networks.

3. Literature Survey

In **[9], Rohit Lakhanpal et al.** proposed a hybrid approach combining MAC (Media Access Control) address and MAP (Message Authentication & 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. They integrated this approach with the AODV routing protocol. By merging the MAC address's identifier aspect with the MAP method's security features, the hybrid approach enhances Sybil attack detection and prevention in Ad Hoc networks.

Doi : https://doi.org/10.54216/JCHCI.080103
Received: October 05, 2023 Revised: January 12, 2024 Accepted: April 15, 2024

In **[10], Priyanka Yadav et al.** presented a secure routing protocol that enhances a reactive routing protocol using node authentication. This protocol enhances security by requiring nodes to authenticate their neighbors before forwarding data packets. Successful decryption of the certificate ensures secure communication between nodes, while failure indicates potential malicious activity, preventing the addition of the node to the neighbor list. By reinforcing the routing protocol with authentication, malicious nodes are prevented from participating in the routing process, effectively safeguarding against security threats like wormhole attacks, man-in-the-middle attacks, and Sybil attacks.

In **[11] Deeksha Singh et al.** introduced a method to mitigate Sybil attack in MANET by combining Genetic Algorithm (GA) with fuzzy logic. The proposed approach involves the following steps:

a. **Route Discovery:** Initially, routes are discovered using the route discovery process.

b. **GA Route Optimization:** The routing protocol, along with the GA, optimizes the route and extracts properties of normal nodes and attacker nodes.

c. **Fuzzy Logic:** Based on the extracted properties, fuzzy logic is trained to distinguish between normal and attacker nodes, thus preventing attacks within the network.

The combination of GA optimization with Fuzzy logic not only enhances network security by effectively mitigating Sybil attacks but also improves the overall efficiency of the simulation process.

In **[12], S. Swathi et al**. presented a bio-inspired networking approach utilizing the Bacteria Foraging Optimization Algorithm (BFOA) to effectively detect and mitigate Sybil attacks in MANETs. BFOA offers a promising solution, efficiently identifying and eliminating Sybil nodes from the network, thereby enhancing network performance and extending its lifespan. The BFOA involves three key steps: chemotaxis, reproduction, and elimination, mimicking bacterial behavior to optimize network operations. In this paper, they present a three-phase approach for Sybil attack detection and mitigation in MANETs, involving the establishment of a network, identification of Sybil attacks through chemotactic movement and swarming behaviours, and subsequent recovery processes. This comprehensive method ensures network security and efficient data transmission.

In **[13], Dr. S. Rethinavalli et al.** proposed a classification approach for detecting Sybil attacks in MANETs, utilizing Artificial Neural Networks (ANN), which mimic biological neural networks. They employed feature selection techniques such as chi-square, symmetrical uncertainty, and information gain, and then combine them for enhanced accuracy. This technique manage to improved True Positive Rate (TPR) and reduced False Positive Rate (FPR) compared to other classifiers.

In **[14], Dhanashri Saindane** proposed a straightforward method for detecting and mitigating Sybil attacks using the AODV routing protocol. Route discovery is initiated by broadcasting route requests. Sybil nodes exploit this by sending fake replies during route discovery, often containing high sequence numbers. To address this, the proposed technique introduces a threshold value for sequence numbers. When multiple replies are received, only the reply with the highest sequence number below the threshold is considered valid. This filtering mechanism helps to identify and discard fake replies generated by Sybil nodes, thereby mitigating the potential impact of Sybil attacks in the network.

In **[15] Meena Bharti et al.** highlights the detrimental impact of Sybil attacks in networks, where nodes illegitimately join multiple times under fake identities, disrupting various network operations. They classify Sybil attacks into two types: whitewashing attacks, where Sybil identities are created and later erased, and simultaneous creation of multiple identities. Prior detection methods relying on RSSI values or trust-based models have limitations, with RSSI-based methods suffering from high false positive rates and trust-based approaches being time-consuming. To overcome these challenges, they introduced a hybrid approach combining RSSI-based and trust-based techniques.

Table 1: Existing Sybil attack detection techniques

Ref.	Author(s) / Year	Technique Used	Advantage	Disadvantage

Doi : https://doi.org/10.54216/JCHCI.080103
Received: October 05, 2023 Revised: January 12, 2024 Accepted: April 15, 2024

[9]	Rohit Lakhanpal & Sangeeta Sharma (2016)	Hybrid MAC & MAP technique	Reduces false positives and enhances accuracy Can be employed in both unicast and multicast communications.	Increased overheads Increased energy consumption.
[10]	Priyanka Yadav, & Muzzammil Hussain (2017)	Cryptography	Ensures secure communication between nodes.	May introduce additional overheads. Required robust key management
[11]	Deeksha Singh Swami Parmanand & Chauhan Shalley Bakshi (2018)	Genetic Algorithm with Fuzzy Logic	Improve efficiency Adaptive Defense Mechanism	Computationally intensive and complex. Less robust in diverse network environments
[12]	Ms. S. Swathi & Dr. R. Vadivel (2020)	Bacterial Foraging Optimization (BFO)	Offers an efficient and effective detection Lower energy consumption	Complex. Effectiveness depends on node density, communication range, etc.
[13]	Dr. S.Rethinavalli & Dr. R.Gopinath (2020)	Artificial Neural Networks (ANN)	Higher accuracy, higher TPR, and reduced FPR compared to other classifiers.	Required large amount of training data to effectively learn and classify patterns
[14]	Dhanashri Saindane (2021)	Filtering with threshold sequence no.	Simple and easy to implement	Sybil nodes could potentially adapt their behavior to bypass the threshold value mechanism
[15]	Meena Bharti, Shaveta Rani & Paramjeet Singh (2022)	Combination of RSSI & Trust-Based Method	Uses two-layer detection. Enhance detection accuracy, reduce false positives & minimize detection time.	The two-layer model increase complexity. Management of such a system require more resources.

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 pros and cons, 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 to stay ahead of evolving threats in network security. The information given through this paper will provide a relevant path and make it easier for the researchers to work in this field.

References

[1] Khan, Burhan Ul Islam, et al. "A survey on MANETs: architecture, evolution, applications, security issues and solutions." *Indonesian Journal of Electrical Engineering and Computer Science* 12.2 (2018): 832-842.

[2] Kumar, Sandeep, et al. "Routing protocols and security issues in MANET." *2017 international conference on infocom technologies and unmanned systems (trends and future directions)(ICTUS)*. IEEE, 2017.

Doi : https://doi.org/10.54216/JCHCI.080103
Received: October 05, 2023 Revised: January 12, 2024 Accepted: April 15, 2024

[3] Karthika, K. C. "Wireless mesh network: A survey." *2016 international conference on wireless communications, signal processing and networking (WiSPNET)*. IEEE, 2016.
[4] Shahdad, Syed Yasmeen, Asfia Sabahath, and Reshma Parveez. "Architecture, issues and challenges of wireless mesh network." 2016 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2016.
[5] Vijay K. "Collaborating The Textual Reviews Of The Merchandise and Foretelling The Rating Supported Social Sentiment." Journal of Cognitive Human-Computer Interaction, Vol. 1, No. 2, 2021 ,PP. 63 - 72.
[6] Sachdeva, Ratika, and Aashima Singla. "Survey on Privacy Issues and Security Attacks in Wireless Mesh Networks." *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSE)* 3 (2013).
[7] Atwal, Harsatnam Singh, and Narinder Kumar Rana. "A REVIEW OF SYBIL ATTACK IN MANET."
[8] Deswal, Paramveer Singh, Bindu Rani, and M. A. Rai. "Review on the Detection and Prevention Technique of Sybil Attack." *Mukt Shabd J* 9 (2020): 1-6.
[9] Vasudeva, A., Sood, M., 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] Lakhanpal, Rohit, and Sangeeta Sharma. "Detection & Prevention of Sybil attack in Ad hoc network using hybrid MAP & MAC technique." *2016 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC)*. IEEE, 2016.
[11] Yadav, Priyanka, and Muzzammil Hussain. "A secure AODV routing protocol with node authentication." *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*. Vol. 1. IEEE, 2017.
[12] R. Venkatesan ,Althaaf Shaik ,Suraj Kumar,Vipul Guria ,Abhishek Raj. "Intelligent Smart Dustbin System using Internet of Things (IoT) for Health Care." Journal of Cognitive Human-Computer Interaction, Vol. 1, No. 2, 2021 ,PP. 73 - 80.
[13] Chauhan, Deeksha Singh, and Shalley Bakshi. "Mitigation of Sybil attack in MANET using GA with Fuzzy Logic." *Management* 3.4 (2018): 12-19.
[14] S. Swathi , Dr. R. Vadivel, 2020, Bio-Inspired Approach Sybil Attack in AODV based MANET using BFOS Algorithm, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 07 (July 2020),
[15] Rethinavalli, S., and R. Gopinath. "Classification Approach based Sybil Node Detection in Mobile Ad Hoc Networks." *International Journal of Advanced Research in Engineering and Technology* 11.12 (2020): 3348-3356.
[16] Saindane, Dhanashri. "Sybil Attack Detection in Mobile Ad-hoc Networks using AODV protocol." *Sybil* 8.07 (2021).
[17] Bharti, Meena, Shaveta Rani, and Paramjeet Singh. "RTBSAD: RSSI AND TRUST-BASED SYBIL ATTACK DETECTION IN MANET." *Indian Journal of Computer Science and Engineering* (2022)

Doi : https://doi.org/10.54216/JCHCI.080103
Received: October 05, 2023 Revised: January 12, 2024 Accepted: April 15, 2024