International Journal of Advanced Engineering: Artificial Intelligence, Robotics and Automation
ISSN 3049-396X
Vol.:2 Issue: 1
Published online on: Dec 2025
PP. 46-50

A Comprehensive Survey of Sybil Attack Mitigation in Ad hoc Wireless Networks

Anil Kewat[1], Sandeep K Tiwari[2], Surjeet Singh Parihar[3], Gargi Singhal[4]
[1]Bundelkhand University, Jhansi, India
[2,3,4] Vikrant university, , Gwalior, India

***Abstract*— A wireless ad hoc network is an infrastructure-free, self-configuring network made up of mobile devices (such as laptops, smartphones, sensors, etc.) connected by wireless links. This kind of network operates independently. In order to ensure secure communication in a hostile environment, security is a major concern. There are still certain issues with wireless ad hoc networks that need to be resolved. Routing, limited capacity, short battery life, dynamically changing topology, and other issues are among these difficulties. The basic problems, security issues, and various forms of attacks related to wireless ad hoc networks are discussed in this study. We examine Sybil attack detection and prevention in this paper. This attack's characteristic is that it displays two distinct identities on the network. The suggested security plan will identify . Ad hoc wireless networks require less infrastructure for self-configuration. The suggested security plan will identify network attacks and stop all of their malicious activity. Performance metrics will be used to gauge the network's performance.**

Index Terms— MANET, Ad-hoc Network, Sybil attack,

INTRODUCTION

An ad hoc network is a wireless network that lacks a permanent infrastructure. In an ad hoc network, each movable node serves as both a host and a router and moves at random. A group of "peer" mobile nodes that can communicate with one another without assistance from a fixed infrastructure make up a wireless ad hoc network. It is possible for the connections between nodes to change continuously and arbitrarily. Wireless links allow nodes that are close to one another to interact directly, while distant nodes use other nodes as relays. Nodes often broadcast and receive signals at the same frequency band and share the same physical media. However, MANETs are susceptible to a variety of assaults because of their intrinsic dynamic architecture and lack of centralized management security. The flexibility of a wireless system is restricted by a fixed supporting framework. A user interacts directly with an access point or base station in infrastructure wireless networks, but a MANET is a self-configuring, infrastructure-less network of mobile devices connected by wireless that never depends on a fixed infrastructure to function.

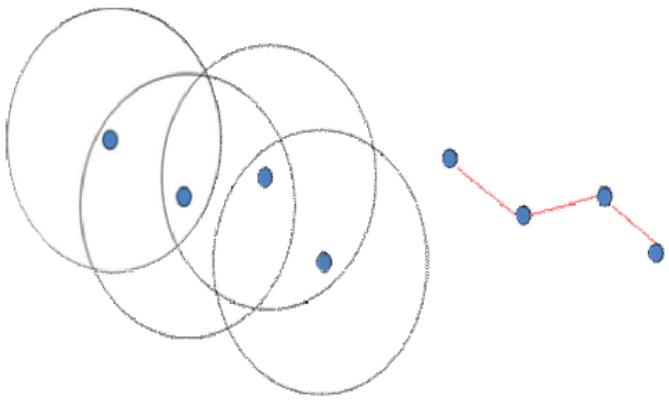

Figure 1 Wireless Ad hoc network

Due to a lack of infrastructure support, the mobile devices or WANTES nodes are free to travel, enter, and exit over time. They can also function as routers, forwarding packets. Ad hoc networks also make it simple to add and remove devices, as well as to keep devices connected to the network. The network is decentralized because of this node mobility characteristic, which causes the network's topology to vary dynamically. In many situations, MANETs are more vulnerable than wired networks because of node mobility.

SECURITY ATTACKS AGAINST ROUTING IN MANETS

- While there are many different forms of attacks in mobile ad hoc network routing, nearly all of them fall into one of two categories:

Corresponding Author's E-mail ID:-anil.kewat2007@gmail.com

1. External attacks: In this type of attack, the attacker seeks to disrupt nodes' ability to provide services, spread false routing information, or create congestion. These are attacks in which the adversary seeks to obtain regular network access and engages in network activities

2. Internal attacks either by directly compromising an existing node and using it as a base for its malicious actions, or by using some malicious impersonation to gain access as a new node

- **Denial of Service (DoS):** Its goal is to prevent a specific node or even the services of the entire ad hoc network from being available. In a classic wired network, denial-of-service (DoS) assaults are executed by flooding the target with network traffic in order to deplete its processing capacity and render its services unavailable.
- **Impersonation:** Impersonation attacks pose a severe danger to the security of mobile ad hoc networks. If an appropriate authentication mechanism isn't in place, the adversary can take control of some network nodes and make them appear innocuous. In this way; compromised nodes can join the network as normal nodes and begin doing destructive things like disseminating, erroneous routing information , and gaining unfair access to private information.
- **Eavesdropping:** Another type of attack that frequently occurs in mobile ad hoc networks is eavesdropping. It seeks to gather some private information that needs to be kept under wraps throughout the conversation. The nodes' locations, public and private keys, and even their passwords may be included in the data. Such information should be protected from unauthorized access since it is crucial to the nodes' security condition.
- **Sinkhole attack:** The attacker node attempts to present an alluring link, such as one to a gateway. As a result, a large amount of traffic avoids this node. The sinkhole attack can be used with other attacks, such as denial of service or selective forwarding, in addition to basic traffic analysis.
- **Sybil attack:** In particular, distributed system environments are the target of the Sybil assault. The assailant has several roles. Instead of acting as a single identity or node, it attempts to operate as multiple. This enables him to fabricate the outcome of a vote that is utilized for threshold security techniques in order to obtain additional information. From the outside, the cloud looks to be made up of several nodes.

Traffic Analysis: The purpose of this passive attack is to learn which nodes connect with one another and how much data is handled.

Related work

"Lightweight Sybil Attack Detection in MANETs" by **Sohail Abbas, Madjid Merabti, David Llewellyn-Jones**, and Kashif Kifayat [1] In this title, we describe a simple method to identify the new identities of Sybil attackers without the need for any additional gear, like directional antennae or a geographical positioning system, or a centralized trusted third party. We are able to show that our suggested approach discovers Sybil identities with good accuracy even in the presence of mobility with the use of comprehensive simulations and real-world test bed trials.

Balachandran Nitish [2] "A Review of Sybil Attack Mitigation Strategies" The various types of Sybil attacks, including those that take place in peer-to-peer reputation systems, self-organizing networks, and even social network systems, are covered in this title. Additionally, many strategies that have been proposed over time to reduce or eliminate their risk entirely are also e xamined, along with their methods of operation..

Chris Piro Shields of Clay Brian Levine, Neil [3] "Identifying the Sybil Attack in Ad hoc Mobile Networks" In this title, we demonstrate how mobility may improve security. In particular, we demonstrate that a Sybil attacker using multiple network identities at once can be identified by nodes that passively monitor network traffic. Through simulation, we demonstrate that a single node can perform this detection, or that several trusted nodes can collaborate to increase detection accuracy. Next, we demonstrate that even though the detection technique will mistakenly identify groups of nodes traveling together as a Sybil attacker, , we can extend the protocol to monitor collisions at the MAC level to differentiate between a single attacker spoofing many addresses and a group of nodes travelling in close proximity.

Rakesh Kumar and Himani Yadav [4] The goal of "Identification and Removal of Black Hole Attack for Secure Communication in MANETs" is to create a method for both identifying and eliminating Black Hole Attacks in Mobile Ad-hoc Networks (MANETs). Network Simulator (NS2) is used for simulation.

Idris Z. Bholebawa, Dr. Upena D. Dalal, and Rakesh Kumar Jha.[5] "Black Hole Attack Performance Analysis on WiMAX-WLAN Interface Network" The performance analysis of Black Hole Attack on WiMAX-

Corresponding Author's E-mail ID:-anil.kewat2007@gmail.com

WLAN Interface Network was examined in this title. An intruder in this kind of attack is a malicious node with a smaller buffer size that travels along a predetermined path and exits the WiMAX-WLAN converter. In a black hole attack, a rogue node advertises that it has the quickest path to the destination node or the packet it wishes to intercept using its routing protocol. Without consulting its routing database, this aggressive node promotes the availability of new routes.

Ms.Heena Bhalla [6] "ANALYSIS OF MANET PERFORMANCE PRIOR TO AND AFTER BLACK HOLE ATTACK" In order to investigate how Black Hole attacks affect network performance, we examine simulated MANETs with and without Black Holes in this title. The average packet drop rose from 0.25% to 90.69% as a result of the Black Hole Attack. The Black Hole effect caused the network's throughput to drop by 93.56%.

N. Marchang, R. Datta [7] R. Datta and N. Marchang [7] We address a light-weight trust-based routing protocol under the title "Light-weight trust-based routing protocol for mobile ad hoc networks." It is lightweight because the intrusion detection system (IDS) that determines how much confidence one node has in another uses a small amount of computing power. Additionally, it ensures scalability by utilizing just local data. The black hole attack and the grey hole assault are the two types of attacks that our lightweight intrusion detection system handles. Although our suggested method can be integrated into any routing protocol, the authors have evaluated it and provided a performance analysis using AODV as the foundation routing protocol.

Muhammad Nawaz Khan, Muhammad Ilyas Khatak, Muhammad Faisal [8] "Ad hoc Mobile Network Intrusion Detection System" In this title, we examine distributed-ID, where a smart agent in every mobile node examines routing packets and verifies MANETs' general network behavior. It uses a Markov process and functions similarly to a client-server approach. The false positive and false negative rates are balanced in the suggested local distributed IDS.

Liang Xiao, IEEE Student Member; Larry J. Greenstein, IEEE Life Fellow; and Narayan B. Mandayam, IEEE Fellow [9] "Channel-Based Sybil Attack Detection in Wireless Networks" By taking use of the spatial variability of radio channels in settings with abundant scattering, which are common in indoor and urban settings, we analyze an improved physical-layer authentication technique to identify Sybil assaults. For both wideband and narrowband wireless systems, such WiFi and WiMax systems, we develop a hypothesis test to identify Sybil clients. Our approach can be implemented separately or in conjunction with other physical-layer security techniques, such as spoofing attack detection, with little overhead based on the current channel estimate mechanisms.

Peng Ning, Krishnendu Chakrabarty, Romit Roy Choudhury, and Tong Zhou [10] "P2DAP: Identifying Sybil Attacks in Vehicle Ad Hoc Networks" In this article, we examine a scalable and lightweight approach for Sybil attack detection. Through passive overhearing by a group of stationary nodes known as road-side boxes (RSBs), a malicious user posing as several (other) vehicles can be identified in a distributed way using this protocol. Since no vehicle in the network needs to reveal its identity in order to identify Sybil attempts, privacy is always protected. To illustrate the overhead for a centralized authority like the DMV, the false alarm rate, and the detection latency, simulation results are shown for an actual test situation**.**

Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones [11] "Identity-based Attacks Against Reputation-based Systems in MANETs" In this title, we will discuss these attacks and their countermeasures in the context of the reputation-based schemes. We will also discuss how our non-monetary, entry fee based scheme that is incorporated in a reputation system can deter these attacks.

John Brooke, Sarosh Hashmi, [12] "Toward Mobile Ad hoc Networks with Sybil Resistant Authentication" In this title, we provide a MANET authentication method that uses each node's hardware ID for authentication. The hardware ID of the authenticating node is confirmed by an authentication agent. To defend the authentication agent against a variety of static and dynamic threats from a possibly hostile authenticate node, a thorough defensive model is used. By using a TTP to sign the authentication agent and ensure that it will only carry out its intended role and is safe to execute, the security of the authenticate node is guaranteed. The suggested authentication method provides stronger defense against the Sybil attack with this low TTP involvement

Saurabh Bagchi and Issa Khalil [13] "Detecting and Countering Stealthy Attacks in Wireless Ad Hoc Networks" In this title, we will talk about two SADEC strategies that may be used on top of simple local monitoring: giving each neighbor some checking responsibility and requiring the neighbors to keep extra information about the routing path. Additionally, by significantly expanding the number of nodes in a neighborhood that are capable of monitoring, SADEC offers a novel way to make greater use of local monitoring.

Corresponding Author's E-mail ID:-anil.kewat2007@gmail.com

G. Srinivasarao, S. Satish Kumar [14] "Mobile Ad-hoc Networks: An Effective Intrusion Detection System" In this topic, we'll talk about data mining methods and mobile agents for network node monitoring. Additionally, before sending the data, gather information from nearby house agents to ascertain the association between the detected aberrant patterns. It lessens attacks and false positive alarms.

E. Friedman and P. Resnick [15] provide new participants the lowest possible reputation value in order to deter them from doing maliciously. They contend that in situations where it is easy to shift identities, this encourages identity persistence. Unfortunately, using this approach will deter new, legitimate users, but it is still possible to manipulate this poor reputation by altering one's identity.

A**. Cheng and E. Friedman [16] classify reputation as symmetric or asymmetric.** An identity's reputation in symmetric reputation systems is entirely dependent on the trust graph's topology, and the author has formally demonstrated that these reputation systems are susceptible to Sybil assaults. under contrast, the author demonstrates the limited circumstances under which Sybil's can be avoided in asymmetric reputation systems, where a trusted node learns the reputation of every other node.

PROPOSED WORK

Due to its changeable architecture, mobile ad hoc networks are more vulnerable than wireless networks. Making routing decisions is essential when using a MANET system. The behavior of Sybil attacks and methods for detecting or preventing them are examined in this work. Identification spoofing, or Sybil attack, occurs when attacker nodes provide the sender nodes with numerous identities at the same moment or at various times. Because the attacker utilizes various addresses for different senders, the attack is a type of routing attack. The detection of Sybil attackers and their deterrence in mobile ad hoc networks are the main topics of this research. In order to prevent Sybil attacks, we also suggested a defensive mechanism. To do this, some nodes are treated as watcher nodes, which monitor traffic in specific paths and node IDs. Additionally, any node that gives multiple identities to two or more nodes that the watcher notifies each sender of prevents the sender from communicating with them, and the watcher node blocks the attacker node from communicating further. Both network security and dependability are enhanced by such effort.

CONCLUSION

This paper examines different methods for detecting and preventing Sybil attacks. In situations where a standard infrastructure network is practically unfeasible, mobile ad hoc networks can establish a network and facilitate communication. There are several technological problems, and research on MANET security is still in its infancy. It is necessary to increase capacity and bandwidth, which calls for improved frequency and spectral reuse. Compared to traditional wired networks, MANET is more susceptible to security threats because of its mobility and open media characteristics. Therefore, in order to guarantee safe communication, MANETs need higher security mechanisms than conventional networks. . Research in the field of security is still open, in future we can design a security mechanism by which we can minimize or can completely remove effect of sybil attacks.

REFERENCES

[1] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat “Lightweight Sybil Attack Detection in MANETs” IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013.

[2] Nitish Balachandran “A Review of Techniques to Mitigate Sybil Attacks” Int. J. Advanced Networking and Applications 11 July 2012.

[3] Chris Piro Clay Shields Brian Neil Levine “Detecting the Sybil Attack in Mobile Ad hoc Networks” NSF grants CNS-0133055, CNS-0534618, and CNS-0087639.

[4] Himani Yadav and Rakesh Kumar “Identification and Removal of Black Hole Attack for Secure Communication in MANETs” **I**nternational **J**ournal of **C**omputer **S**cience and **T**elecommunications [Volume 3, Issue 9, September 2012].

[5] Rakesh Kumar Jha, Dr Upena D Dalal, Idris Z. Bholebawa. “Performance Analysis of Black Hole Attack on WiMAX-WLAN Interface Network”

[6] Ms.Heena Bhalla “PERFORMANCE ANALYSIS OF MANET BEFORE AND AFTER BLACK HOLE ATTACK” Heena Bhalla ,Int.J.Computer Technology & Applications,Vol 3 (1),273-276.

Corresponding Author’s E-mail ID:-anil.kewat2007@gmail.com

[7] N. Marchang, R. Datta “Light-weight trust-based routing protocol for mobile ad hoc networks” Published in IET Information Security Received on 7th July 2010.
[8] Muhammad Nawaz Khan, Muhammad Ilyas Khatak, Muhammad Faisal “Intrusion Detection System for Ad hoc Mobile Networks” International Journal of Computer Applications (0975 – 8887) Volume 35– No.2, December 2011.
[9] Liang Xiao, Student Member, IEEE, Larry J. Greenstein, Life Fellow, IEEE, Narayan B. Mandayam, Fellow, IEEE, “Channel-Based Detection of Sybil Attacks in Wireless Networks” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 3, SEPTEMBER 2009.
[10] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty “P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks” IEEE journal on selected areas in communications, vol. 29, no. 3, March 2011.
[11] Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones “Identity-based Attacks Against Reputation-based Systems in MANETs” ISBN: 978-1-902560-25-0 © 2011 PGNet.
[12] Sarosh Hashmi, John Brooke, “Towards Sybil Resistant Authentication in Mobile Ad hoc Networks” 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies.
[13] Issa Khalil and Saurabh Bagchi “Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure” 1536-1233/10/$26.00 © 2010 IEEE.
[14] G. Srinivasarao, S. Satish Kumar “An Efficient Intrusion Detection System in Mobile Ad-hoc Networks” © 2012 IJAIR ISSN: 2278-7844
[15] E. Friedman and P. Resnick, "The Social Cost of Cheap Pseudonyms," Journal of Economics & Management Strategy, vol. 10, pp. 173-199, 2001.
[16] A. Cheng and E. Friedman, "Sybil proof reputation mechanisms," in Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems Philadelphia, Pennsylvania, USA: ACM, 2005.

Corresponding Author’s E-mail ID:-anil.kewat2007@gmail.com