Detection and Prevention of Sybil Attack in MANET using MAC Address

Anamika Pareek
M.tech (CSE)
Sanghvi Institute of Management and Science, Indore

Mayank Sharma
Asst. Professor
Sanghvi Institute of Management and Science, Indore

ABSTRACT

A Mobile Adhoc Network is a network that does not relay on fixed infrastructure .It is a collection of independent mobile nodes that can communicate to each other via radio waves. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. As in ad- hoc network communication medium is air so it would be easy for attacker to fetch information from air medium using sniffing software tool. There is an attack which causes so much destruction to a network called Sybil attack. In the Sybil attack a single node presents multiple fake identities to other nodes in the network. In this research, we implemented the Sybil Attack Detection technique which is used to detect the Sybil nodes in the network and also prevent it. Simulation tool used for the implementation is NS2.35.

Keywords

MANET, Sybil attack, fakes Identity, Multiple Identity, and Sybil Node

1. INTRODUCTION

Ad hoc network is emergence of technology of wireless communication for mobile nodes. In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology.

Figure 1: Ad hoc Network

Due to infrastructure less nature of MANET and as there is no central authority to maintain and control the network makes it vulnerable to various attacks. Ad hoc networks can be used for battlefield emergency, law enforcement, and rescue missions.

Nodes in MANET communicate with each other on the basis of unique identity that forms the one to one mapping between an identity and an entity and that is

Usually assumed either implicitly or explicitly by many protocol mechanisms; hence two identities implies two distinct nodes. But the malicious nodes can illegitimately claim multiple identities and violate this one-to-one mapping of identity and entity philosophy.

Sybil attack is an attack which uses several identities at a time and increases lot of misjudgments among the nodes of a network or it may use identity of other legitimate nodes present in the network and creates false expression of that node in the network. Like this, it disturbs the communication among the nodes of the network.

To have secure communication it is necessary to eliminate the Sybil nodes from the network [1]. The following goals must be fulfilled by security algorithm used to detect the attack [2]:

1. Authentication: It means that each and every node, participating in communication must be genuine and legitimate node.
2. Availability: All services should be available all the time to all the nodes for the proper functioning and security of the network.
3. Integrity: It gives the assurance that the data received by the receiver will be same as the data send by the sender.
4. Confidentiality: It means that some data is only accessible by the authorized users.
5. Non-repudiation: It means sender and receiver cannot deny that they didn't send or receive the data

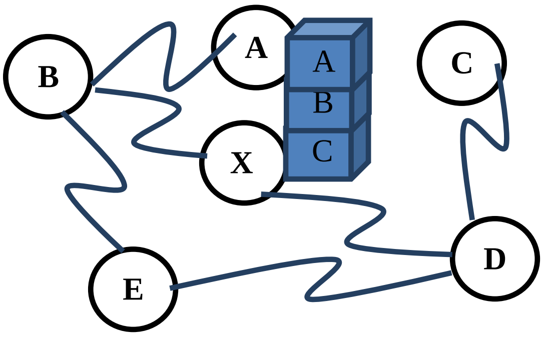

Figure 2: A Sybil attacker with multiple Identities

Figure 2 represents a malicious node X along with its three Sybil nodes (A, B and C). If this malicious node communicates with any legitimate node by presenting all its identities, the legitimate node will have illusion that it has communicated with four different nodes. But in actual, there exists only one physical node with multiple IDs.

This paper is organized as follows:

In Section 2 we present related work. Section 3 Proposed Detection Technique Section 4 Result and Section 5 Conclusion.

2. RELATED WORK

Sybil attack was first introduced by Douceur. According to Douceur [2] there is no practical solution for this attack. Deploying Trusted Certification is the only scheme that can completely eliminate the Sybil attack. However, it suffers from costly initial setup, lack of scalability and a single point of attack or failure. Also, it's based on the assumption that each entity has single identity which is very difficult to achieve on the large network.

Piro et al. [3] proposed a detection technique for detection of Sybil nodes by examining the behavior of nodes. According to the Piro, nodes which move freely, independently in different directions are considered as legitimate nodes and the nodes which moves together are considered as Sybil nodes and it keeps observing these suspected nodes

J. Newsome et al. [5] proposed a scheme in which radio resource testing and randomly pre key distribution is done to detect the Sybil nodes.

Roopali et al. [6] propose a technique in which when node enters a network, then it's all three parameters are checked i.e. speed, energy and frequency and if value of all these parameters are less than threshold value then node is considered as legitimate node otherwise as Sybil node.

Nidhi et al [7] proposed the RSS based detection approach along with the authentication of node which will correctly identify the Sybil identity with Higher True Positive. For the authentication of node, Message Authentication Code (MAC) is used. Authentication of node allows only legitimate node to come in to the network. As well as Lower-bound detection threshold is used, and compare with Received Signal Strength (RSS) value, if the comparison is greater than or equal to RSS value, then it's a Sybil identity (Whitewash identity). Otherwise it's a legitimate node in the network.

Danish Shehzad el at.[8] Proposed a detection technique based on Hash Function, only messages along with their hash function are accepted each individual node detects Sybil attackers by validating the Hash received along with message by neighbor, after receiving message node gets Hash of sender and compares it with the previous Hash received in Hello message for the validation of its identity. If Identity or Hash differs to that of Hash received along with hello message than node is nominated as Sybil and node is blocked from any communication.

Sohail Abbas el at. [9] Proposed an RSS-based detection mechanism to safeguard the network against Sybil attacks. The scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware. We demonstrated through various experiments that a detection threshold exists for the distinction of legitimate new nodes and new malicious identities.

Yamini D.Malkhed el at. [10] Proposed a detection technique which is based on RSS along with the authentication of node which will correctly identified the Sybil identity with Higher True Positive. By Authentication means only legitimate nods are allowed to come in to the network. As well as Lower-bound detection threshold is used, and compare with Received Signal Strength (RSS) value, if the comparison is greater than or equal to RSS value, then it's a Sybil identity (Whitewash identity). Otherwise it's a legitimate node in the network.

P.Kavitha el at [11], proposed a detection technique which is based on NDD algorithm for detecting Sybil attacks. This algorithm is used to transfer the data from source to destination without any damage or loss as well as each node to have the neighbor's node address. Depends on the address the data will be transmitted in to correct destination.

3. PROPOSED DETECTION TECHNIQUE

In the proposed technique for detection of Sybil attack, any node can start the detection for Sybil node. In our case sender node starts detection for Sybil node before it sends packets to the receiver node. Firstly sender node broadcast a request packet which in return wants a reply message which contain logical (IP) address and physical address (MAC).sender nodes maintain a table for that and checks if a node with same physical address reply with different logical address then the node with different logical identity is declared as a Sybil node and the sender node chooses another path for sending packets to destination. The flow for the detection and prevention is shown in fig 3

Steps taken to detect and prevent Sybil Attack

Step 1 : Broadcast the message

Step 2 : Receive Reply message with Logical and Physical Address.

Step 3 : Compare MAC Address of nodes from different routes.

Step 4 : If MAC Address of any node matches with different IP address
Add node as a Sybil Node and find another route to send message.

Step 5 : Else, Accept Node as legitimate node.

Step 6 : Stop

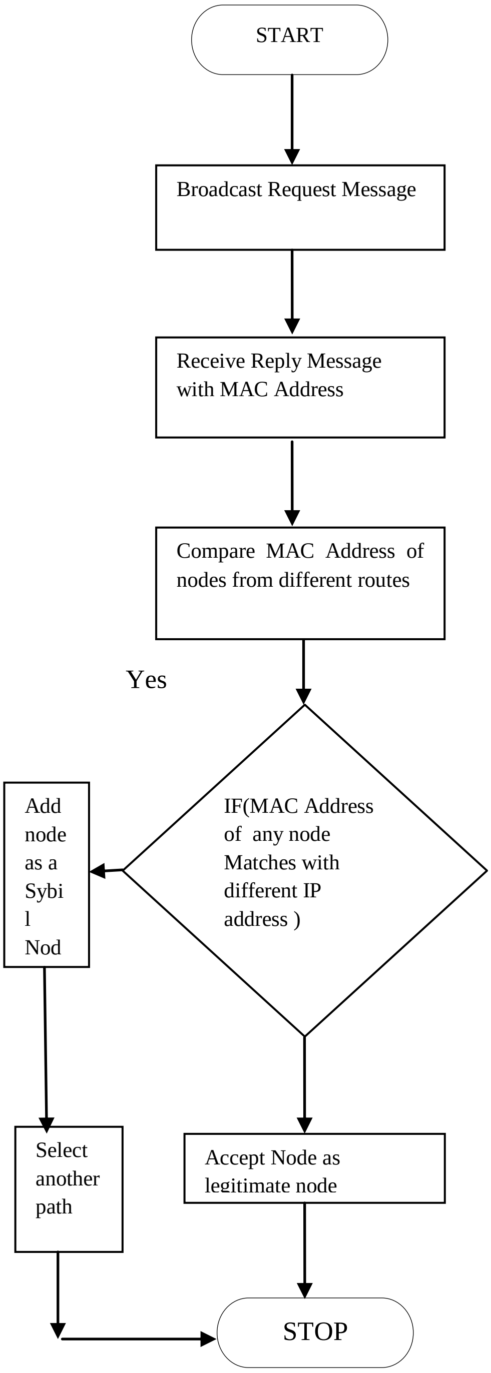
START
Broadcast Request Message
Receive Reply Message with MAC Address
Compare MAC Address of nodes from different routes
Yes
IF(MAC Address of any node Matches with different IP address)
Add node as a Sybi l Nod
Select another path
Accept Node as legitimate node
STOP

Fig 3: Architecture for detection and prevention of Sybil node

4. SIMULATION RESULTS

The simulation tool used for implementation is NS 2.35. In this we implemented the Sybil attack detection and prevention technique using MAC address.

Parameters used for performance measurement are following:

1. Throughput: Total number of packets delivered over the total simulation time.
2. Packet Delivery Ratio (PDR): Ratio of data packets received by the destination to those generated by source

Simulation Parameters

Table 1: shows the parameters

Parameters	**Level**
Area	1200*1200
Speed Pause Time 4s	2 to 16 m/s
Radio Propagation model	TwoRayGround
Number of nodes	50
Data Packets	100
Routing Protocol	AODV

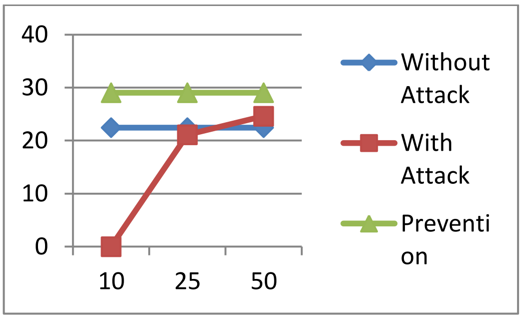

Fig 4: Throughput

In Fig 4 graph is showing the throughput for different number of nodes for different situation like when there is no attack in the network, when attacker attacked on the network and when attack is detected and prevented

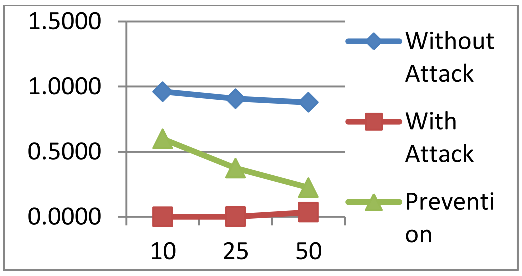

Fig 5: Packet Delivery Ratio (PDR)

In Fig 4 graph is showing PDR for different number of nodes for different situation like when there is no attack in the network, when attacker attacked on the network and when attack is detected and prevented.

5. CONCLUSION

MANET is vulnerable to various attacks due to its infrastructure less or wireless nature. To have safe Communication it is must be secure network. There are various attacks in MANET and there is one attack which is very dangerous called Sybil attack, it uses multiple identities or uses the identity of another node present in the network to disrupt the communication or reduce the trust of legitimate nodes in the network. In this paper we proposed detection and prevention technique which uses MAC Address to detect Sybil nodes to safeguard the network.

6. REFRENCES

[1] Adnan Nadeem and Michael P. Howarth,``A survey of MANET Intrusion Detection & Prevention

Approaches for Network layer Attacks," IEEE Communication Surveys & Tutorials, pp.1-19, 2012.

[2] J. R. Douceur,"The Sybil Attack," presented at the Revised Papers from the first Int. Workshop on Peer-to-Peer Systems, pp.251-260,2002

[3] C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks," in Proc. Securecomm Workshops, 2006, pp. 1–11

[4] Yu, H., M. Kaminsky, P. Gibbons, & A. Flaxman . Sybilguard: Defending against sybil attacks via social networks. Networking, IEEE/ACM Transactions on 16 (3), 576–589 2008.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis &defenses," in Proceedings of the third internationalsymposium on Information processing in sensor networks. Berkeley, California, USA: ACM, 2004.

[6] Roopali Garg, Himika harma "Proposed Lightweight Sybil Attack Detection Technique in MANET" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 3, Issue 5, May 2014

[7] Nidhi Joshi,Prof Manoj Challa,"Secure Authentication Protocol to Detect Sybil Attacks in MANETs" International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345 Vol. 5 No. 06 Jun 2014

[8] Danish Shehzad, Dr. Arif Iqbal Umar, Noor Ul Amin, and WaqarIshaq" A Novel Mechanism for Detection of Sybil Attack in MANETs" International conference on Computer Science and Information Systems (ICSIS'2014) Oct 17-18, 2014 Dubai (UA).

[9] 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.

[10] Yamini D Malkhede,Purnima Selokar "ANALYSIS OF SYBIL ATTACK DETECTION IN MOBILE ADHOC NETWORK" Proceedings of 19 th IRF International Conference , 1st February 2015, Pune, India, ISBN: 978-93-84209-85-8.

[11] P.Kavitha, C.Keerthana, V.Niroja, V.Vivekanandhan," Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network", International Journal of Communication and Computer Technologies Volume 02–No.02 Issue: 02 March 2014