A Survey Paper on Detection of Sybil Attack in MANET

Faizan Khan *(Author)*
B.E. Scholar
SVCE Indore, (R.G.P.V.)
Indore, India

Mayuri Sonar *(Author)*
B.E. Scholar
SVCE Indore, (R.G.P.V.)
Indore, India

Mosmi Tiwari Vyas(*Guide)*
Asst. Professor
SVCE Indore, (R.G.P.V.)
Indore, India

***Abstract*—Mobility cause a main problem when we talk about security in Mobile Ad-hoc networks. It doesn't depend on fixed architecture, the nodes are continuously moving in a random fashion. In this article we will focus on identifying the Sybil attack in MANET. It uses air medium for communication so it is more prone to the attack. Sybil attack is one in which single node present multiple fake identities to other nodes, which cause destruction. We show through simulation that this detection can be done by simply using the tool NS2.35 .**

Keywords : MANET, Sybil attack, Fake identity

I. Introduction

Mobile Ad-hoc Network: MANET is a combination of sensor node that can proceed on their own and connect with the physical environment. Mobile nodes have the ability of computing, sensing and communication like static nodes.

For mobile nodes, Ad-hoc network is the new technology of wireless communication. Unlike wireless sensor network where are base stations or mobile switching centers, here in MANET the mobile nodes communication directly which are near and those which are far rely message through other nodes.

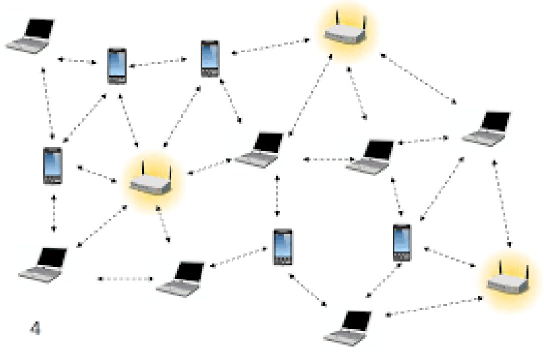

Fig. 1 – MANET Network

The medium in which the MANET operates on is air, so it is more vulnerable to various types of attack. In MANET the nodes communication with each other on the basis of their unique identity which is mapped in form of one to one mapping in between an identity and an entity. Various protocols are there to form an Ad-hoc network among the mobile and radio equipped devices [2,3]. There is an attack called Sybil attack [1], Which fails the security applied by various protocol. An example [4] , of Sybil attack, where their must be assurance that each identity is actually one entity. This assurance requires costly manual intervention by which we can restrict the number of identities.

To ensure secure communication it is necessary that we should eliminate the malicious node from our network [5]. In this paper, we show that the mobility can only be used for the detection or to identify the malicious nodes. We can also use various algorithm, but the algorithm must satisfy on these points first:

- Authenticity: It means the trueness and validness of the node participating in the communication.
- Availability: All nodes and their service must present all the time.
- Confidentiality: Authorize access must be their for the user.
- Non-repudiation: Sender and Receiver can't deny that they have send the message.

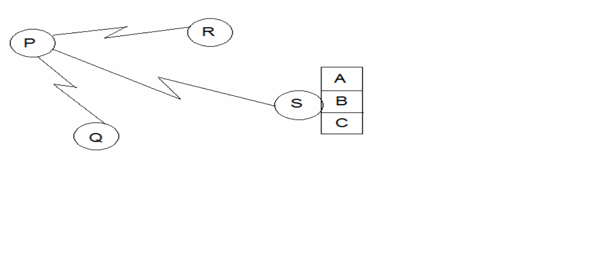

Fig. 2 – Sybil attacker with multiple identities

In this figure the node S is a malicious node with multiple identities A,B,C, When a node communicate with S then it will have an illusion like it has communicated with 4 other node while it is the single. In actual it is the one node which have multiple ID's.

The two method to identify are :

- Passive Ad-hoc Sybil attack detection which is based on MAC address.
- PASID with Group detection, in which we will see the false identity or the node with multiple ID's are more dense.

II. Related Work

J. Newsome et al. [6] proposed a solution for detect on through radio resource testing and randomly pre key distribution. They present an excellent discussion of threat that Sybil attack poses to sensor network, all of which apply to MANET. The work was on wireless sensor network where we require the active participation of the neighbor node to identify the identity, which is difficult to implement in MANET or there are changing nodes in its environment.

Generally Sybil attack occurs in distributed systems which does not have any central authorities because here each entity is only aware of other through message over the channel. An entity can determine the set of entities are distinct by testing resources limits, but this is problematic. If a single Sybil attacker pretends to be multiple entities, it may not have the same computational, storage and bandwidth capabilities as multiple independent identities.

Douceur [7] was the first to introduce the Sybil attack, Douceur has shown that a Sybil attacker can not be prevented by test of finite resources. Douceur also suggested that there is no practical solution for Sybil attack. For eliminating it completely, Trusted certification is the only scheme. But it too suffer from costly initial set up and a single point of failure.

Sohail Abbas el at. [8] proposed a n RSS-based detection mechanism. This work by using IEEE 802.11 standard on MAC layer, without any hardware.

P. Kavitha el at. [9] proposed a detection technique using NDD algorithm. In this the algorithm is used to transfer data from source to destination without any loss. Address are stored by the neighbor and which ensure the correct destination.

Roopali et al. [10] propose a technique in which all three parameters are checked when node enters a network, the parameters are 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.

Yamini D.Malkhed el at. [11] 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.

Sybil attacker wishes to keep their multiple identity same as the system. There is a difference between the legitimate node and a Sybil attacker , in General the independence node are mobile but that of Sybil node the identity move together and this provide a way to find Sybil attack in a network.

III. PRPOSED DETECTION TECHNIQUE

Sybil attacker establishes the identity by IP address, MAC address or public key, these differ from the real node in several ways. As the resources of single node is used to simulate multiple identities. Douceur has proposed that it is difficult to prevent from the test of finite resources. The Sybil attacker must share the same set of resources unlike the other entities.

In our proposed solution any node can start the detection for the Sybil node.

In our simulation the node which will cat as detecting node will be the sender, when the sender wants to sned a message "HELLO", before sending this message this message the sender wants will broadcast request message and will wait for the reply message. Sender will compare the logical address that is IP and physical address that is MAC. Here the sender will observe those node which are having the same MAC address but the reply is different in form of IP address. Everything the logical address is changed over the MAC address, and these types of nodes are declared to be the Sybil node

A. Following are the steps which involves in the detection:

- Sender Broadcast the request message.
- Message received by all nodes present in MANET.
- Sender receives the reply message containing MAC and IP address.
- Comparison of MAC address from all nodes.
- If two IP having same MAC address then Sybil node and find another route to send message.
- Else otherwise accept the packet and send.
- Exit.

The flow chart diagram for the detection of the Sybil attack in the MANET is shown below which will show the flow of the message in the nodes ,when the sender sends the message it will generate a request message before it and will broadcast the message, the sender will wait for the reply message and when it get the message will inquiry on its aspects of IP and MAC address and thus identify the malicious node in the network.

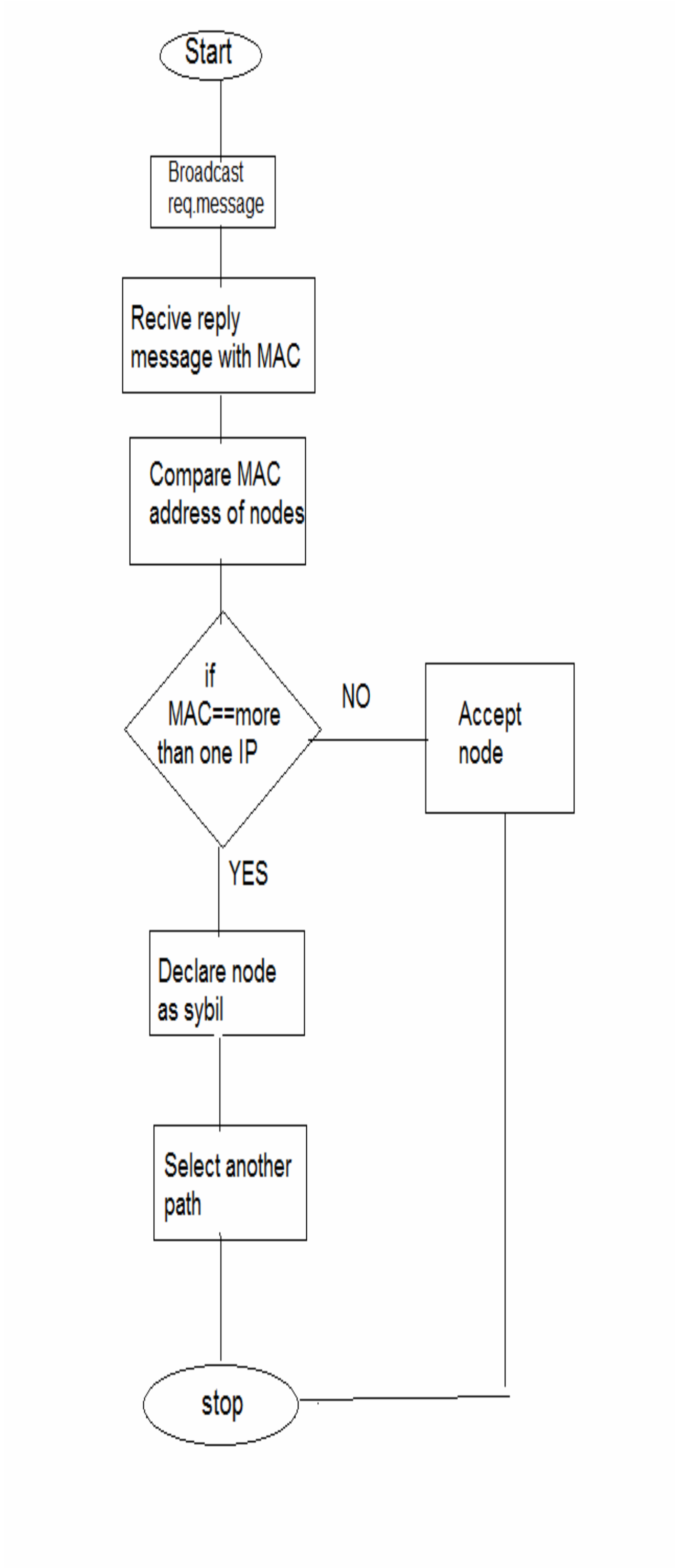

Fig 3: Architecture for detection and prevention of Sybil node

IV. REFRENCES

[1] J. R. Douceur. The Sybil Attack. In Intl Wkshp on Peer-to-Peer Systems, March 2002.

[2] D. Johnson and D. Maltz. Dynamic Source Routing in Ad hoc Wireless Networks. In Mobile Computing, volume 353. Kluwer Academic Publishers, 1996.

[3] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks. In Proc. Intl Conference on Mobile Computing and Networking, Sep. 2002.

[4] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil Attack in Sensor Networks: Analysis & Defenses. In Proc. Intl Symp on Information Processing in Sensor Networks, 2004.

[5] Adnan Nadeem and Michael P. Howarth,``A survey of MANET Intrusion Detection & Prevention .Approaches for Network layer Attacks," IEEE Communication Survey & Tutorials, pp.1-19, 2012.

[6] 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.

[7] 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 .

[8] 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.

[9] 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 .