A Review of Sybil Attack in Mobile Adhoc Network

Ms. Yamini D. Malkhede
Department of CSE
G. H. Raisoni Institute of Engineering & Technology for Women,Nagpur, India
yamini.m089@gmail.com

Prof.Purnima Selokar
Assistant Professor, Department of CSE,
G. H. Raisoni Institute of Engineering & Technology for Women,Nagpur, India
purnima_456@yahoo.co.in

***Abstract*—** Mobile ad hoc networks (MANET) is a very complicated distributed systems that comprise of mobile nodes in wireless network that can easily and freely arrange themselves into random and momentary ad hoc network topologies as per the situation in network. The changing topology and resource restriction are the main characteristics which pose a number of tasks for efficient and lightweight security protocols design. Centralized identity management is not present in case of MANETs. The requirements of a unique, distinct, and permanent identity each node are primary requirements for their security protocols, due to this Sybil attacks create a harmful threat to such networks. Many or single identity in ad hoc network, can be created by a Sybil attacker in order to release coordinated attack on the network or can change identities in order to make it weak for the detection process, thereby alter it in lack of accountability in the network. This is the research which will be implemented to detect the identities created by attackers illegitimate node with a lightweight scheme without using any extra hardware, like directional antennae or a geographical positioning system**.**

Keywords- *Security, MANET, Sybil Attack , Intrusion Detection In MANET*

*****

I. INTRODUCTION

Mobile Adhoc network (MANET) is nothing but the collection of nodes which collectively forming a provisional or permanent network without depending on any centralized architecture. Nodes can enter to join or leave the network at anytime, as well as can travel across the network freely. Each node within route acts as a host as well as a router, forwarding the data to extend the limited range by forming connectivity between the source and destination nodes which are not present within direct range of each other. Communication & data transfer in MANETs are usually based on Unique Identifier (Uid), which represents node entity. MANET is susceptible to many security attack. No centralized identity management in MANET and the requirement of exclusive and distinctive as well as persistent identity for each node for their security protocol to be viable, Sybil attack propose a dangerous impact to such a network. A Sybil attack is in which a malicious node in the network, illegally claims to have many identities on a single physical device. A Sybil attacker can harm to the ad hoc networks in one or various ways. For example, a Sybil attacker can interrupt location-based or multipath routing by participating in the routing, giving the fake impression of being legal nodes on different locations or node-disjoint paths.

In wireless sensor networks, a Sybil attacker can change the complete aggregated reading outcome by participating many times as a different node. Therefore, Sybil attacks will have a serious effect on the normal operation of wireless ad hoc networks. It is very important to detect Sybil attacks and remove them from the network. The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, in mobile ad hoc networks this approach is not suitable because it usually requires costly initial setup and overhead related to maintaining and distributing cryptographic keys. On the other hand, received signal strength (RSS) based localization is considered one of the resolving solutions for wireless ad hoc networks. However, this approach does not require any extra hardware, such as directional antennae or a geographical positioning system (GPS).

II. AD-HOC ON DEMAND DISTANCE VECTOR PROTOCOL (AODV)

Ad hoc on demand vector (AODV) [10] has two operating modes, i.e., route discovery and route maintenance. This section discusses both operating modes.

A. Route discovery mode

Fig. 1 illustrates a route discovery process at which the source node A needs to obtain a routing-path towards the destination node D. As shown in the figure, a source node broadcasts a route request (RREQ) message to all neighbors since the node does not have a route-path to the destination node D. After receiving the RREQ message, a relay node B will check its routing table to determine if the node has a route path to the destination node. Because the relay node does not have the route-path, the node then rebroadcasts the RREQ message.
However, before rebroadcasting the route request message, the node will record the route-path to the last node visited by the RREQ message. All the process will be repeated until the route request message arrives to the destination node. When the RREQ message reaches the destination node, the destination node will unicast a route reply (RREP) message as the response to the RREQ message.

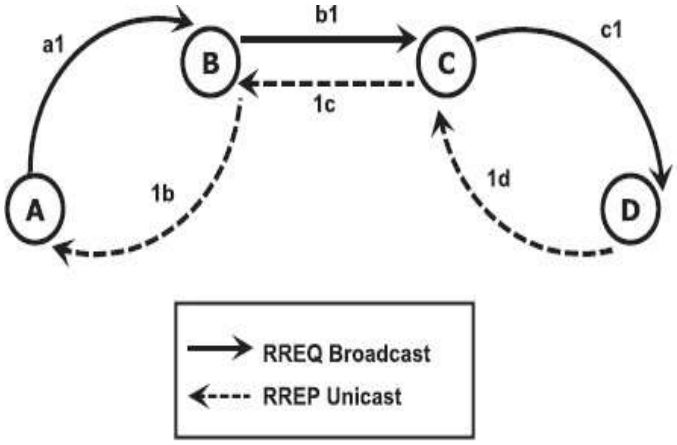

Fig.1. AODV Route Discovery

B. *Route Maintenance*

In routing, the network topology changes adapted by maintaining route maintenance. For the purpose of route maintenance, AODV must continuously listen to the communication channels of all nodes for detecting link failure. Incoming of RREQ and RREP messages every *n* seconds to a node indicates that the route paths exist and no link fails between the node and the sender of messages. However, the link problems indicate the unavailability of the messages for certain period s. Node send a hello message to check the failure, if the node detects a link failure,. Furthermore, the succeeding of link failure detection further proceed by all nodes answer each of the incoming messages.
Figure 2 shows the process taken by nodes when a broken link detected. As shown in the figure, node 6 has detected a link failure while transmitting the data to node 9. Node 6 could not receive any response from node 9 after a certain period of time. Node 6 then generated an RERR message, and propagated the message back towards node 2. When node 4 receives the RERR from node 6, it compares and removes any entry in its routing table that has the RERR destination. The RERR itself is then sent either through broadcast or unicast message transmission.

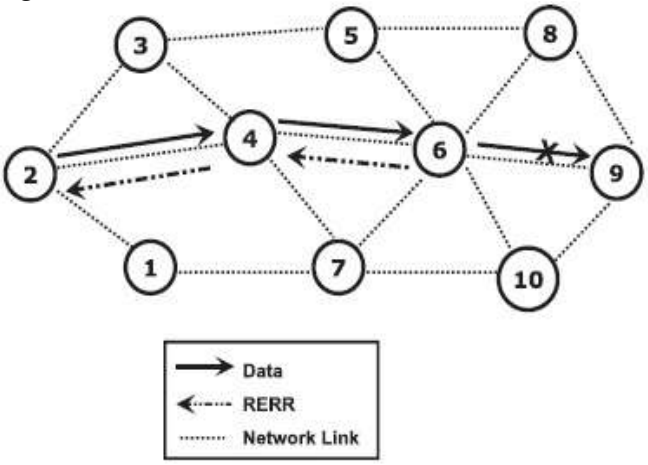

Fig.2. Router Error Detection

III. ATTACKS ON AODV-BASEDMANET AODV ATTACKS

Attacks at AODV routing in MANET can be classified into simple and sophisticated attacks as show below in Fig.3.

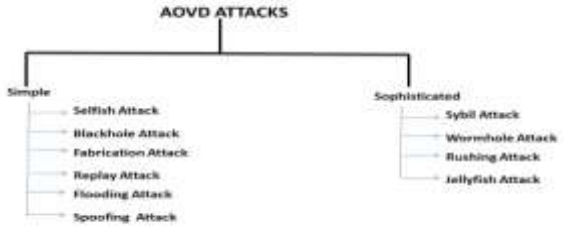

Fig.3. Attacks in MANET

The following is a list of the *Simple Attacks* that are much easier to detect and prevent.

A. Selfish Attack:
The attacker drops either route request (RREQ) or route reply (RREP), which it has received, without legitimate reason.

B. Blackhole Attack:
The attacker sends a forged RREP with the hop count metric decreased to the originator of a route request. It claims that it has an owned a shortest path towards the destination node. As a result, the sender will use the forged route for sending the messages in a future and has disregarded the legitimate route.

C. Fabrication Attack:
The attacker generates bogus route error RERR messages. It sends the messages to other nodes as a claim that the neighbor is unreachable.

D. Replay Attack:
The attacker records other node's valid control messages, and resends them later.
E. Flooding Attack (or Denial of Service - DoS - attack) :
The attacker disrupts the routing operation by flooding network channels with a large number of RREQs in a short period. The goal of this attack is to cause severe degradation of network performance.

F. Spoofing Attack:
The attacker impersonates a legitimate node by forging RREQ, RREP and RERR. This attack is possible due to the lack of authentication in the ad hoc routing protocols.

The following is a list of the *Sophisticated Attacks* that are much harder to be detected and prevented.

A. Sybil Attack :

The attackers generate a large number of fictitious entities in order to appear and function as distinct nodes. They use the entities for gain control to the network substantially.

B. Wormhole attack :

The attackers create tunnels to connect two distant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole nodes can start dropping the messages and cause network disruption.

C. *Rushing Attack:*

The attackers forward rushed route request (RREQ) messages faster than the victims.

D. JellyFish attack :

The attackers pretend to be benign nodes, but disturbing messages' traffic through themselves by reordering and dropping the messages periodically, or increasing the jitters values of the messages.

IV. PROPOSED WORK: DETECTION OF SYBIL ATTACKS

In our proposed system we are emphasizing on *Sybil Attack* i.e. sophisticated attack, which are much harder to detect and prevent. In our research work we will be proposing the methodology which will detect and prevent the *Sybil Attack* from the system.

Sybil Attack which was first introduced by Douceur in the context of peer-to-peer network. Douceur showed that there is no practical solution for this attack. Adapting Trusted Certification is the only scheme that can completely eliminate the Sybil attack. But it incurs from costly initial setup, lack of scalability and a failure.

If a malicious node impersonates some nonexistent nodes, it will appear as one or more illegitimate nodes conspiring together, which is called a Sybil attack. This attacks aims at network services when cooperation is necessary, and affects all co-ordinated schemes and secure allocation schemes based on trust model as well. However, there is no secure way to defeat Sybil attacks. Ad hoc networkis composed of mobile, wireless devices, in which nodes communicate only over a shared broadcast channel. One of the advantages is that there is no fixed infrastructure is required: a network for routing data can be formed from whatever nodes are available. Nodes forward messages for each other to provide connectivity to outside nodes. Each node needs a unique address and identity to participate in the routing. Hence Sybil Attack is very dangerous and harmful attack.

V. PREVENTION OF SYBIL ATTACK

Prevention of the Sybil Attacks can be achieved by two different methods as mentioned below:-

A. LIGHTWEIGHT SYBIL ATTACK DETECTION

It is used to detect Sybil nodes. By using this scheme it does not require any extra hardware or antennae. So its cost is very less.

a. Distinct Characters of Sybil Attack:

It has two characters, one is Join and Leave or Whitewashing Sybil attack and other is Simultaneous Sybil Attack. In Join and Leave or Whitewashing Attack, at a time, it uses its one identity only and discards all its earlier identities. In this, its main purpose is to remove all its previous malicious tasks performed by it. It also increases the lack of trust in the network. In Simultaneous Sybil Attack, at the same time, it uses all its identities. Its main motive is to create confusion and congestion in the network by utilizing more number of resources and make efforts to collect more information about the network.

b. Enquiry Based on Signal Strength:

In this step, each node collects the information about the RSS value of neighboring nodes. On the basis of RSS value, judgment can be made between legitimate and Sybil nodes. If the RSS value of the new node which joins the network is low, then that node is considered as legitimate node otherwise it is considered as Sybil node. Each node contain RSS information about neighbor nodes in the form of <Address, Rss-List <time, rss>>

c. Exposure of Sybil Nodes:

In this, there is always an assumption that no legitimate node can have speed greater than 10m/s which is called as threshold value or threshold speed . On the basis of speed, RSS value is calculated and if the RSS values of nodes are greater than or equal to threshold value than those nodes are detected as Sybil nodes otherwise it is considered as legitimate nodes.

B. ROBUST SYBIL ATTACK DETECTION

One more technique is used to detect the Sybil nodes. Some methods are required to implement this technique for the purpose of the correct observation of traffic. These methods are discussed below:

a. Robust Sybil Attack uses the authentication mechanism for the traffic observation. In this, each packet is signed by the sender's private key and also signed by the nodes which are traversed by it to reach the destination and in the end receiver authenticate it by its public key. So, it gives the proof that at what time and location sender sends the packet and in which direction the packet is send by the sender, so that it will reach to the destination.

b. To check the similarity of the path, it uses the novel location based Sybil attack detection mechanism. The nodes whose path is exactly similar to each other are detected as Sybil nodes.

VI. COMPARITIVE ANALYSIS OF EXISTING SYSTEM

TABLE 1. COMPARISON OF SYBIL ATTACK DETECTION TECHNIQUES

Algorithm	Parameters	Directional antennae	Cost
Cryptographic-based Authentication	distributing Cryptographic Keys	Required	costly
distributed key management framework	private keys distribution	required	costly
Robust Sybil Attack Detection Technique	Time, Location	Required	costly
Lightweight Sybil Attack Detection Technique	Speed, RSS	Not Required	Cheap

VII. CONCLUSION

In this proposed scheme the RSS based detection approach along with the authentication of node which will correctly identified the Sybil identity with Higher True Positive. 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. The scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware. This will be demonstrated through various experiments that a detection threshold exists for the distinction of legitimate new nodes and new malicious identities. This will confirmed this distinction rationale through simulations. The simulation results showed that our scheme works better even in mobile environments and can detect both join-and-leave and simultaneous Sybil attackers with a high degree of accuracy.

REFERENCES

[1] Haiying Shen and Lianyu Zhao "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs" , IEEE transactions on mobile computing, vol. 12, no. 6, June 2013.

[2] 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

[3] Nidhi Joshi, Prof. Manoj Challa," Secure Authentication Protocol to Detect Sybil Attacks in MANETs", International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 5 No. 06 June 2014.

[4] K. Kayalvizhi, N. Senthilkumar , G. Arulkumaran," Detecting Sybil Attack by Using Received Signal

[5] Strength in Manets", (IJIRSE) International Journal of Innovative Research in Science & Engineering,2014

[6] 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