

Effective Approach for Sybil Attack Detection in Mobile Adhoc Networks

Ms. Pragya G Katariya

Dept. of Computer Technology
Rajiv Gandhi College Of Engineering
Chandrapur, Maharashtra, India
e-mail: pragyak07@gmail.com

Asst.Prof. R.k.Krishna

Dept. Of Electronics & Tele-ommunication
Rajiv Gandhi College Of Engineering
Chandrapur, Maharashtra, India
e-mail: rkrishna16@gmail.com

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). Each node of the sensor network consists of three subsystem i.e. sensor subsystem which sense the environment, processing subsystem which performs local computation on the sensed data, and

communication subsystem is responsible for message exchange with neighboring sensor node.

II. ATTACKS ON AODV-BASED MANET ATTACKS

Attacks at AODV routing in MANET can be classified into simple and sophisticated attacks as show below in Fig.1.

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.

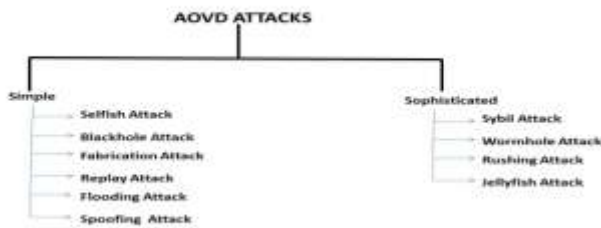


Fig.1. Attacks in MANET

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.

III. 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.

This proposed system include different modules as follows:

Designing of the Network:-

In this module we are going to design the complete Mobile Adhoc Network without centralize trusted third party, consisting of number of nodes. Where all the nodes will be having the unique id in the network.



Fig 2. Network Formation and communication amongst the nodes

Communication amongst the Node:-

In the second module we are going to provide the communication amongst the node. That any node in the network can send the data or communicate with any other node in the network. While the data between sender and destination will be flow through the intermediate nodes.

Providing the Security to the Network:-

In this module we will provide the security to the network by using the Pre random Key Distribution mechanism. In which we use the public key which is with all the nodes in the network and secret key with the nodes which are taking the part in communication.

Detection and Defending the network from Different Attacks:-

In this module we will the network, whether any attacker node is introduced in the network, our system will detect the attacker node based on certain parameters such as threshold, and keys. If the attacker node is detected then we will detect and remove the attacker node from the network.

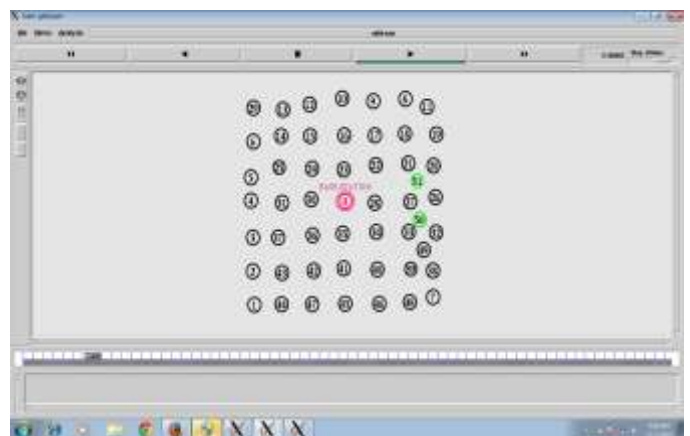


Fig.3. Detection of Malicious node

Evaluating the Results:-

In this module, once we design the entire network we will evaluate the results based on different parameters such as Packet Delivery Ratio, Throughput and Packet Dropping. In this module we will evaluate the results on the basis of graphs,

which will prove that our system is efficient as compared to the existing system

IV. DESIGNING OF SYSTEM

a. Workflow Diagram:

Node is first get Authenticated by using a secure Hash Function. After Authentication, received RSS value is first checked with lower bound detection threshold, if it's lower, it's a Legimate node; otherwise it's a Sybil identity. After this, the X & Y Coordinate value will help us to determine the exact location of Sybil identities in the network. For a Legitimate node, it's added to RSS-Table. Otherwise the address is added to malicious node list.

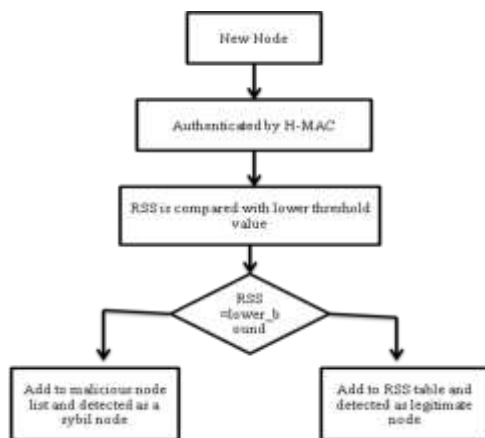


Fig 4. Flow of the Proposed System

The above fig.2. basically denotes the network formation, consisting of 50 sensor nodes and One base station.

In the network source node trying to communicate with destination node. Whenever source node wants to send any data to any node the source node broadcast the data in the network and searching for the destination.

The above fig.4. indicates the actual communication in the network. If any malicious node tries to enter in the network then that node identified as intruder node and wont allowed to attack the node. In the fig.4. Node 50 and 51 are detected as Intruder node as those are not the part of the network but inserted by attacker. So its identified as attacker node.

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 |

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.

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