IJCSN International Journal of Computer Science and Network, Volume 4, Issue 3, June 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Sybil Attack Detection in Mobile Adhoc Network

[1] Yamini D. Malkhede, [2] Purnima Selokar

[1] Department of CSE, G. H. Raisoni Institute
of Engineering &Technology for Women,
Nagpur, Maharashtra, India

[2] Department of CSE, G. H. Raisoni Institute
of Engineering &Technology for Women,
Nagpur, , Maharashtra, India

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***.**

1. 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).

2. Literature Survey

Haiying Shen and Lianyu Zhao[1] has discussed the Anonymous routing protocols in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers In order to provide high anonymity protection (for sources, destination, and route) with low cost, proposed an Anonymous Location-based and Efficient Routing protocol (ALERT). ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source.

Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat [2] has discussed unique characteristics of MANETs, such as dynamic topology and resource constraint devices, which pose a number of nontrivial challenges for efficient and lightweight security protocols design. Due to the lack of centralized identity management in MANET ,Sybil attacks pose a serious threat to such networks. This scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities. First, demonstrate the entry and exit behavior of legitimate nodes. Second, define a threshold. Third, tune the detected threshold by incorporating the RSS data fluctuation taken from our tested experimentation. Fourth, evaluate the scheme using extensive simulations.

Nidhi Joshi, Prof. M Nidhi Joshi, Prof. Manoj Challa [3] have discussed that when one node wishes to send data to another, the data is passed across, or routed, through several other nodes until its destination is reached. Nodes are able to be dropped and reconnected to the network as needed since their connections may be unstable.The traditional approach of preventing Sybil attack is to use Trusted Certification or Cryptographic-based-Authentication. However, this approach is not suitable because it requires costly initial setup and overhead involved in maintaining & distributing Cryptographic Keys. On the other hand, Received Signal Strength (RSS) is considered as a Lightweight solution for MANETs. However, this approach does not require any extra hardware such as antennas or Geographical Positioning System (GPS).

K. Kayalvizhi, N. Senthilkumar , G. Arulkumaran[4] has discussed that the wireless communication channel is a shared medium, exchanging messages without any security protection over the air can easily leak the information that users may want to keep private. Pseudonym based schemes have been proposed to preserve the location privacy of mobile. The centralized key management has some disadvantages. The tamper-proof device normally costs high. The framework to be developed in this paper does not require the expensive tamper-proof device. Here the technique used is a secure distributed key management framework. In this the road side units are responsible for secure group private keys distribution in a localized manner. When a vehicle approaches an, it gets the group private key from the RSU dynamically.

P. Kavitha, C. Keerthana, V.Niroja, V.Vivekanandhan[5] has one centralized server is maintainined to check authentication of source. It blacks unauthorized users or hackers.Passive ad hoc identity like as Neighbor discover distance (NDD) node to watch the transmission on the network. This system used the NDD Algorithm. Using these algorithms to transfer the data in 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. If there is any packet loss or some collision on network then immediately to inform the server to stop the data and maintaining source node information and header information of message. It checks the users using those details whether they are attackers or normal user. Hacker's information has not been transferred to destination.

3. Sybil Attack and Type of Sybil Attack

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. When a node illegitimately claims multiple identities or claims fake IDs, the MANET suffers from an attack called Sybil attack. There are several types of Sybil attack which are as follows :

3.1 Direct and Indirect Communication

In direct attack, the legitimate nodes communicate directly with Sybil nodes whereas in indirect attack, the communication is done through malicious node.

3.2 Fabricated and Stolen Identities

It creates a new identity for itself based on the identities of the legitimate nodes, that is, if legitimate nodes have an ID with length 32 bit integer, it randomly creates ID of 32 bit integer. These nodes have fabricated identities.

In stolen identities, attacker identifies legitimate identities and then uses it. The attack may go unidentified if the node whose identity has been stolen is destroyed. Identity replication is when the same identities are used many times in the same places.

3.3 Simultaneous and Non-Simultaneous Attack

In simultaneous, all the Sybil identities participate in the network at the same time. Since only one identity appears at a time, practically cycling through identities will make it appear simultaneous.

4. 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.

4.1 Radio Resource Testing

Consider that a node wants to verify that none of its neighbors are Sybil identities. It can assign each of its neighbors a different channel to broadcast some message on. It can then choose a channel randomly on which to listen. If the neighbor that was assigned that channel is legitimate, it should hear the message. The probability of detecting the Sybil node is s/n. A more difficult case is when there are not enough channels to assign each neighbor a different channel.

4.2 Registration

One obvious way to prevent the Sybil attack is to perform identity registration. To detect Sybil attacks, an entity could poll the network and compare the results to the known deployment. To prevent the Sybil attack, any node could check the list of "known-good'' identities to validate another node as legitimate.

4.3 Position Verification

Another promising approach to defending against the Sybil attack is position verification. In this approach, the network verifies the physical position of each node. Sybil nodes can be detected using this approach because they will appear to be at exactly the same position as the malicious node that generates them.

4.4 Based on RSSI

By having the position of the nodes based on signal strength, we can find whether there is Sybil attack or not in wireless sensor networks [4]. Initially all the nodes have the same power, computing capability and the positions of nodes are fixed.

This proposed system include different modules as follows:

4.5 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.

4.6 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.

4.7 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.

4.8 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.

4.9 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.

5. Designing of System

5.1Workflow 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 Legitimate 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

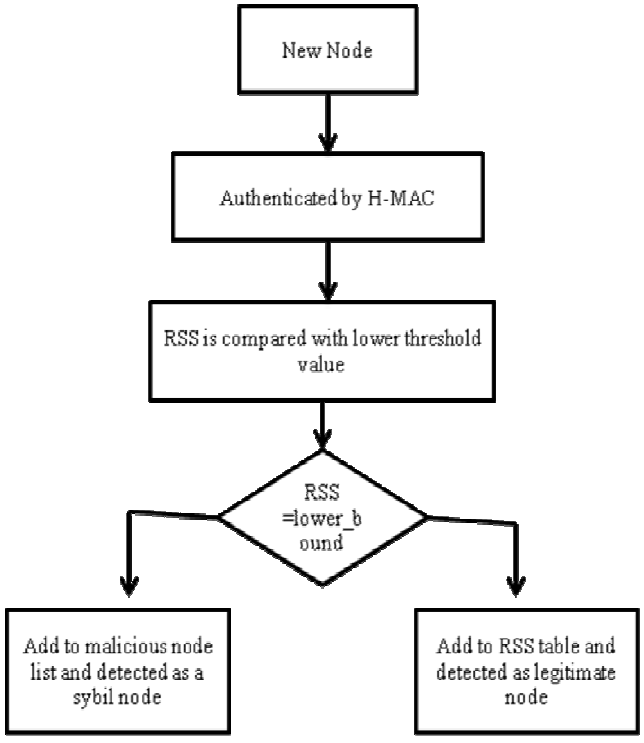

Fig1. Flow of the Proposed System

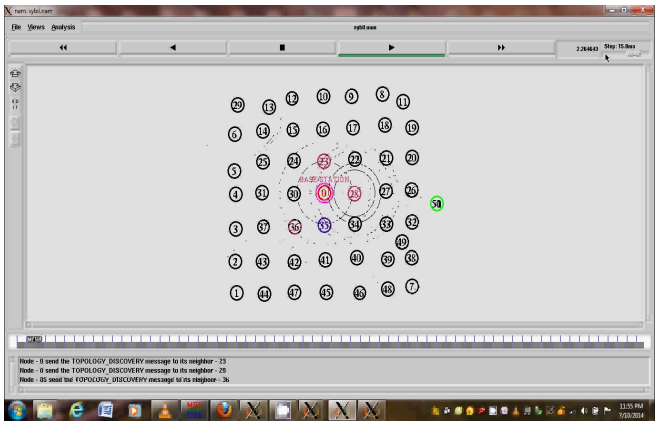

Fig 2. Network Formation and communication amongst the nodes

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.

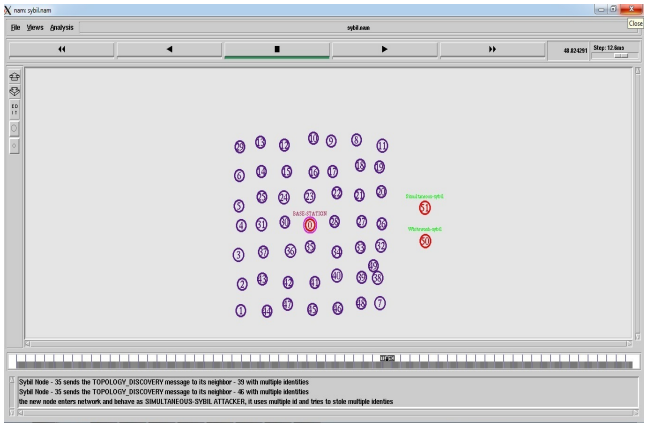

Fig.3.Detection of Sybil node

The above fig.3. 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.3. Node 50 and 51 are detected as Sybil node as those are not the part of the network but with the help of different identities they tries to access the network. So its identified as attacker node.

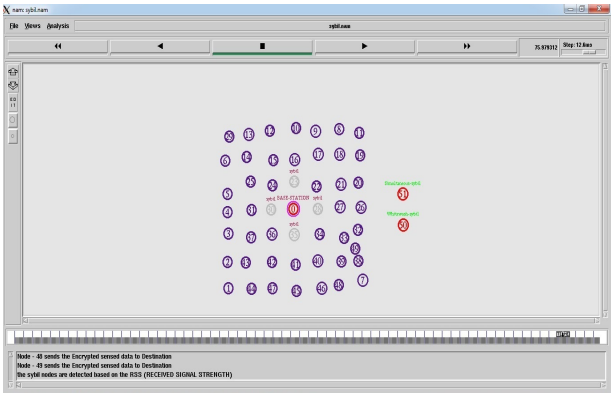

Fig 4. Detecting all the different types of Sybil attacks

The above fig 4. Shows attacker try to gain the access to the resources in the network. But all the Sybil nodes within the network detected.

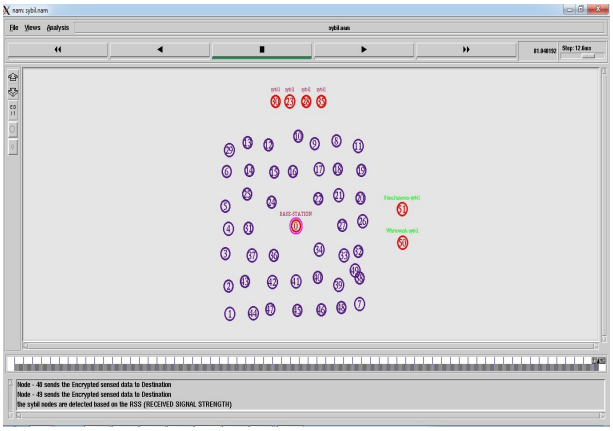

Fig 5. Sybil nodes removed from network

Fig 5. Shows after detecting all the Sybil nodes they are removed from the network to make the network more secure and then the communication between the nodes takes place

6. Prevention of Sybil Attack

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

6.1 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.

6.1.1 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.

6.1.2 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>>

6.1.3 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.

6.2 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.

7. 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 Strength in Manets", (IJIRSE) International

[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.

[6] S.Sharmila, G Umamaheswari," Detection Of Sybil Attack In Mobile Wireless Sensor Networks", International Journal Of Engineering Science & Advanced Technology Volume-2, Issue-2, Mar-Apr 2012