IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 5 (May. 2019), ||S (IX) || PP 43-50

Advanced Security Mechanism, to Detect and to Remove the Attacks from the MANET

Ms. Bhargavi Charde, Dr. Shrikant Sonekar
1Department of Computer Science Engg ,JDCOEM, Nagpur, DBATU University, Lonere
2Department of Computer Science Engg ,JDCOEM, Nagpur, DBATU University, Lonere

Abstract *- Mobile ad hoc networks (MANET) is a very complicated distributed systems that comprise of mobile nodes which are mobile in nature, in wireless network this nodes can be 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, as such network can get compromised and can get attacked by any third party. Centralized identity management is not present in case of MANETs. The requirements of a unique, distinct, and permanent identity of each node in the network are primary requirements for their security protocols, due to this Sybil attacks create a harmful threat to such networks, which creates 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 in which we will be implementing the system 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.*

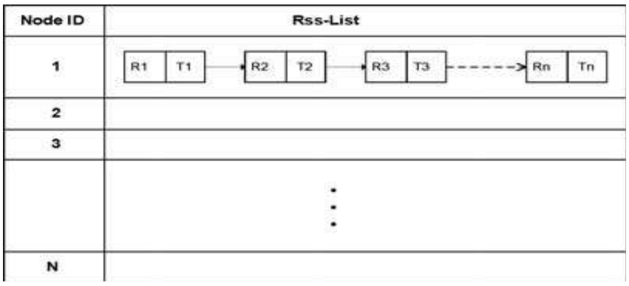
Keywords *- Security, MANET, Sybil Attack , Intrusion Detection In MANET*

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.

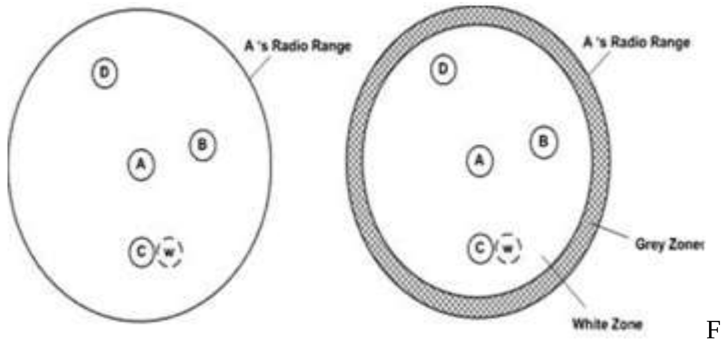
No centralized identity management in MANET and the requirement of exclusive and distinctive as well as persistent identity for each node for their security protocol to be viable,

Sybil attacks will have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect Sybil attacks and eliminate them from the network. The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. Onhe other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless adhoc networks. However, this approach requires extra hardware, such as directional antennae or a geographical positioning system (GPS).



Node ID	Rss-List
1	R1 T1 → R2 T2 → R3 T3 - - - - - → Rn Tn
2	
3	
	⋮
N	

Fig 1.1 Neighbor List Based on RSS



F

Fig.1.2 (a) Without **Fig 1.2 (b)** with categorization of radio range.

As shown in the fig 1.1 RSS in order to differentiate between the legitimate and Sybil identities. As shown in Fig 1.2(a) first, we demonstrate the entry and exit behavior of legitimate nodes and Sybil nodes using simulation and tested experimentation. Second, we define a threshold that distinguish between the legitimate and Sybil identities based on nodes' entry and exit behavior. Third, we tune our detection threshold by incorporating the RSS data fluctuation taken from our tested experimentation. As shown in Fig1.2(b) we evaluate our scheme using extensive simulations, and the results show that it produces about 90% true positives (detecting a Sybil node as Sybil) and about 10% false positives (detecting a normal node as a Sybil node) in mobile environments. The scheme can be applied to both scenarios of Sybil attacks, i.e., whether the new identities are created one after the other or simultaneously make no difference to the detection process. This proposed scheme does not use localization technique for Sybil attack detection and hence does not need any directional antennae or any GPS equipment and does not use centralized trusted third party.

II. Literature Servey

In paper" Lightweight Sybil Attack Detection in MANETs" , Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat [2] has discussed that Mobile ad hoc networks (MANETs) represent complex distributed systems. In MANET, wireless mobile nodes that can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies. Due to this people and devices to seamlessly internetwork in areas where no pre-existing communication infrastructure exists, for example disaster recovery environments. Dynamic topology and resource constraint devices, pose a number of nontrivial challenges for efficient and lightweight security protocols design which is unique characteristics of MANETs. The requirement of a unique, distinct, and persistent identity per node for their security protocols to be viable, Sybil attacks pose a serious threat to such networks due to the lack of centralized identity management in MANETs. For example, communications in wireless networks are usually based on a unique identifier that represents a network entity: a node. An address is used for Identifiers to communicate with a network entity. In wireless sensor networks a Sybil attacker, the whole aggregated reading outcome can change by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic. Therefore, Sybil attacks will have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect Sybil attacks and eliminate them from the network. The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys.

In paper " Secure Authentication Protocol to Detect Sybil Attacks in MANETs", Nidhi Joshi, Prof. M Nidhi Joshi, Prof. Manoj Challa [3] discussed the authors have discussed the Communication & data transfer in MANETs is usually based on Unique Identifier (Uid), which represents the node entity. 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. This works well for the devices as most devices in MANETs are typically low- power with a small transmission range but are still capable of routing information over large distances by bouncing off other device in a MANET. A Sybil attack creates a serious impact on the normal operation of the network. So, it's required that as soon as the Sybil identity identified in the network, it should be eliminated from the network. 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). In this, node share & manage identities of Sybil and Non-sybil identities in a distributed manner. Although, it is a Lightweight scheme, but cannot accurately identifying Sybil identity in the network. As people will be encouraged to use a secured network, it is important to provide MANET with reliable security mechanisms if we want to see this exciting technology become widely used in a next few years.

In paper" Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network" , P. Kavitha, C. Keerthana, V.Niroja, V.Vivekanandhan[5] has discussed that hackers cannot act as source, because one centralized server is maintaining to check authentication of source. It blacks unauthorized users or hackers. to provide a key based data transmission and id based network. Passive ad hoc identity like as Neighbor discover distance (NDD) node to watch the transmission on the network. This system used the NDD Algorithm. Use 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. Destination has not been receiving any attacker information.

III. Proposed System

3.1 Objective

1) To implement attack detection technique without any requirement of any extra hardware or directional antennae.

2) To detect and remove the masquerading attacks in the network.

3.2 Problem Definition

A Sybil attacker can cause damage to the ad hoc networks in several ways. For example, a Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or node-disjoint paths. In reputation and trust-based misbehavior detection schemes, a Sybil node can disrupt the accuracy by increasing its reputation or trust and decreasing others' reputation or trust by exploiting its virtual identities. In wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic. Therefore, Sybil attacks will have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect Sybil attacks and eliminate them from the network. The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys.

3.3 Proposed Lightweight Sybil Attack Detection :-

It is the improved version of Lightweight Sybil Attack detection technique. In above lightweight technique, sometimes there is Sybil nodes whose speed is less than10m/s and these nodes are detected as legitimate nodes. To remove this drawback of above technique, it is modified. In above lightweight technique only one parameter is used i.e. speed which is nothing but the times taken by then to cover the same distance.

$$\text{Speed} = \left(\frac{\text{Distance}}{\text{Time}}\right)$$

Here one more parameter i.e. frequency is added.

$$\text{Frequency} = \left(\frac{\text{Number of packet send}}{\text{In given time}}\right)$$

By using this parameter it is giving better results than previous. In this threshold value of speed is taken as same i.e.10m/s and threshold value of frequency are set as average frequency of network

This proposed system include different modules as follows:

Module 1: Topology Formation:-

The aim of the topology formation is to build the structure in which there are nodes connected to each other directly or via a path which can be made up of multiple nodes . The basic idea behind the construction of network is to build an arrangement of nodes that can subsequently be treated as a communicating partner or intermediate node which can form the path between two communicating parties. Irrespective of the methods used to generate node movement, the topography for mobile nodes needs to be defined. Normally flat topology is created by specifying the length and width of the topography using val(x) and val(y) as the boundaries used in simulation.

Module 2: Communication amongst the Node:-

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. Key confirmation is achieved at both communicating parties whereas in other systems key confirmation is achieved at one end. Overall, we conclude that the proposed system is efficient compared with the existing protocols.

A. After key confirmation, communication amongst the node takes place. 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. We use the AODV mobile ad hoc routing protocol. Ad hoc on demand vector (AODV) has two operating modes, i.e., route discovery and route maintenance. This section discusses both operating modes.

Route Discovery :-

Fig. 3.1 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.

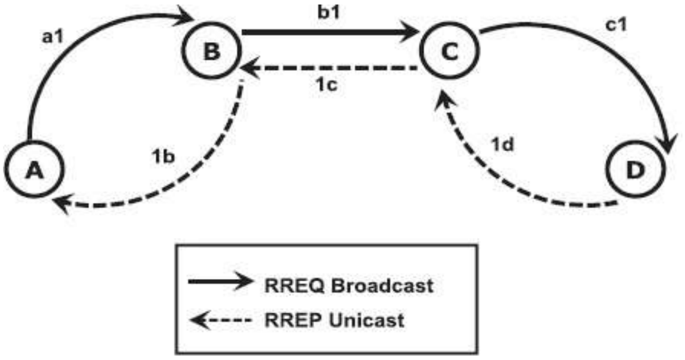


Figure 3.1 AODV Route Discovery

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.

Module 3: Detection of Attacks:-

Ad hoc network is composed of mobile, wireless devices, referred to as nodes those communicate only over a shared broadcast channel. An advantage of such a network is that 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 nodes outside direct broadcast range. Each node needs a unique address to participate in the routing.

In this proposed system we are detecting two different attacks such as Sybil attack and **Masquerading** attack. The identities established by a Sybil attacker — whether represented by IP addresses, MAC addresses, or public keys — differ from those of an honest node in several ways. Because the resources of a single node are used to simulate multiple identities, any particular assumed identity is resource constrained in computation, storage, or bandwidth. However, unlike separate entities, all identities of a Sybil attacker must share the same set of resources. **Similarly in Masquerading** attack , the attackers acts *as if* he was some other user or entity in the system which is also identity based attack. Masquerade attacks will occur in many alternative ways. In normal terms, a system might get access to a legitimate user's account either by stealing a victim's credentials, or through a possibility in and installation of keylogger. In either case, the user's identity is illegitimately non inheritable.

.

Module 4: Detection and Defending the network from Different Attacks:-

In this module we will provide security to the network. The system will aim to detect whether any attacker node is introduced in the network. The proposed system will detect the attacker node based on certain parameters such as RSS value, Threshold value, and entry-exit behavior. Sybil Attack is an attack in which a malicious node obtains multiple identities at a time and creates lot of misjudgment in the network. Similarly in **Masquerading** attack usually includes one of the other forms of active attack. If the attacker node is detected for both the attacks then there is need to remove the attacker node from the network. To have a safe communication network must be secured. There are number of encryption algorithm which generate private or public keys and encrypt the data, the data which is send from the source to destination. We evaluate that there are two kind of encryption algorithm that is symmetric and asymmetric. AES is a symmetric block cipher. This means that it uses the same key for both decryption and encryption. AES (which is a standardized version of Rijndael) became a FIPS standard. The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys – 128,192,256 bits. To encrypt the data AES algorithm is most significant standard for block ciphers because AES provide strong encryption. The AES has fast speed and very low resources consumption.

Module 5: Evaluating the Results:-

In order to implement and evaluate our scheme, we use Network Simulator NS-2. There are some parameters of the network that are mainly responsible for affecting the accuracy of Sybil attack detection scheme. There are some attributes of the network that are mainly responsible for affecting the accuracy of our Sybil attack detection scheme. These attributes are number of network connections, node density and transmission rate. The design of the entire network is structured such that evaluated 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

4.1 Simulation Parameter:

The table given below shows the parameter set for simulation.

Table 4.1. parameters for simulation

Parameters	Values
Routing protocol	AODV
Simulation time	80 seconds
Number of Nodes	50
Traffic Type	CBR
Performance Parameter	Throughput, delay, PDR , RSS value
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
MAC	802.11
Energy level	100 joules

4.2 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

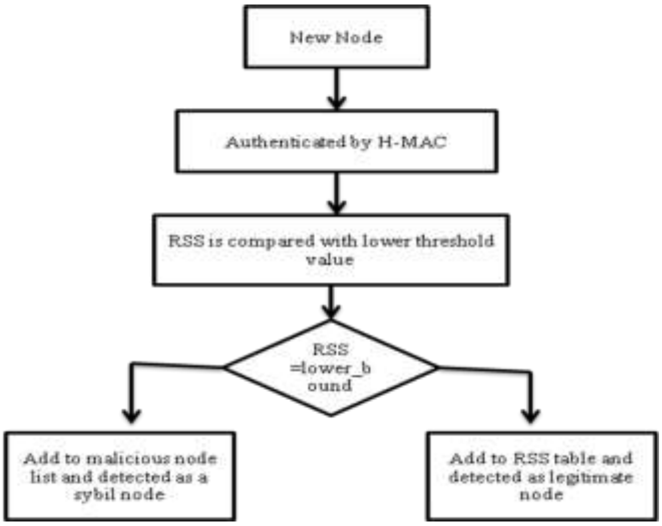
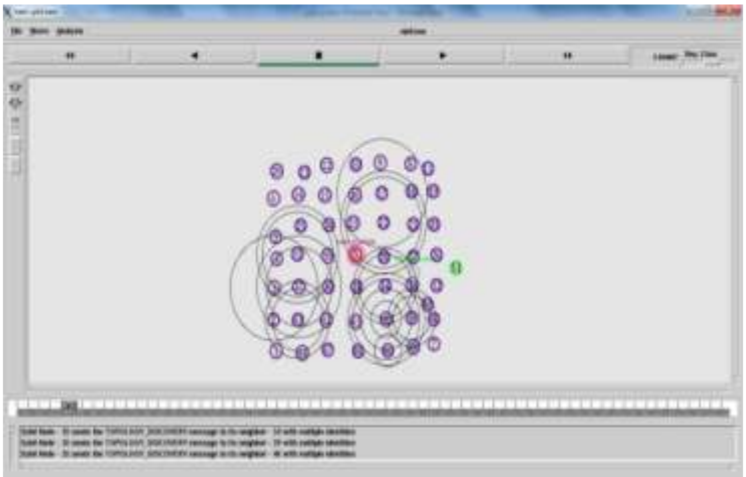

New Node
Authenticated by H-MAC
RSS is compared with lower threshold value
RSS =lower_b ound
Add to malicious node list and detected as a sybil node
Add to RSS table and detected as legitimate node

Fig 4.1. Flow of the Proposed System

Network Formation and Communication



Sybil Node - [illegible] sends the TOPOLOGY_DISCOVERY message to its neighbor - [illegible] with multiple identities
Sybil Node - [illegible] sends the TOPOLOGY_DISCOVERY message to its neighbor - [illegible] with multiple identities
Sybil Node - [illegible] sends the TOPOLOGY_DISCOVERY message to its neighbor - [illegible] with multiple identities

Fig 4.2. Network Formation and communication amongst the nodes

In fig 4.2 Source node trying to communicate with destination node within the network. For communication source node broadcast HELLO message to show neighboring nodes that source node is ready to send the data packets to destination. Broadcasting often provides a building block for route discovery from source to destination. Although a wireless signal broadcast causes more contention and collisions in the shared wireless channel, it also allows a single transmission to reach multiple neighboring nodes. The challenge lies in securing communication and maintaining connectivity in the presence of adversaries, across an unknown, frequently changing multi-hop wireless network topology.

Packet Loss During Communication

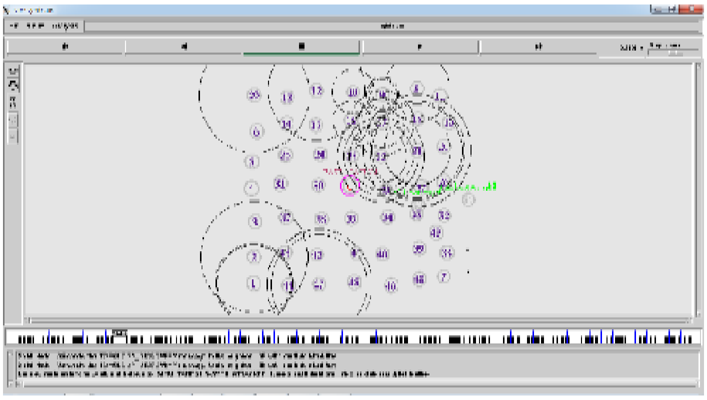


Fig 4.3 Packet loss during communication amongst the nodes

In fig 4.3 Packet loss problem is much more complicated in mobile ad hoc networks, because wireless links are subject to transmission errors and the network topology changes dynamically. A packet may lose due to transmission errors, no route to the destination, broken links, congestions, etc. The effects of these causes are tightly associated with the network context. In proposed system Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic. . In mobile ad hoc networks, wireless link transmission errors, mobility, and congestion are major causes for packet loss.

Detection of Sybil Nodes

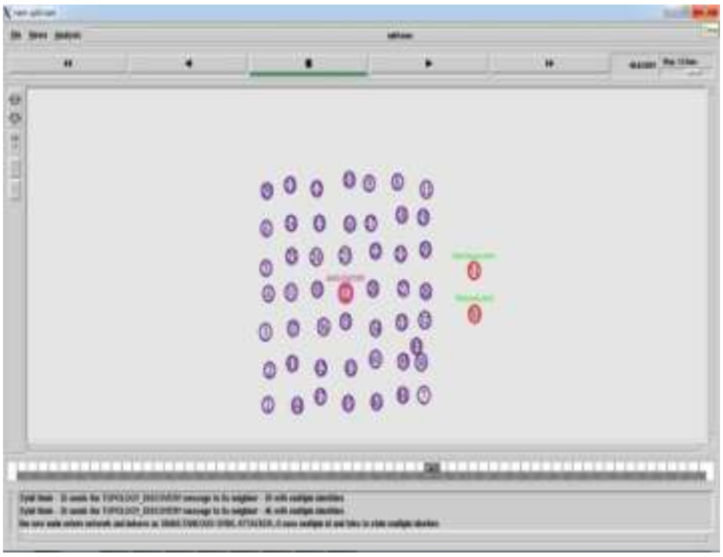


Fig 4.4 Detecting Sybil nodes

The above fig.4.4. 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..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. In our scheme, individual nodes that wish to detect Sybil attackers monitor all transmissions they receive over many time intervals. These intervals are chosen long enough to capture behavior from all the Sybil identities of an attacker, including data transmissions, HELLO and keep-alive messages, and routing requests and replies. The node keeps track of the different identities heard during the interval. Having made many observations, the node analyzes the data to find identities that appear together often and that appear apart rarely. These identities likely comprise a Sybil attack. Like all detection systems this system produces accurate and desirable true positive results when it determines that a particular identity is part of a Sybil attack and true negative results when it correctly labels a independent node as such. It produces false positives by identifying an independent node as being part of the Sybil attack and false negatives by concluding a Sybil identity is just an independent node.

Modules to be Implemented:-

- Detecting masquerading attack
- Removing Sybil attacker node from network
- Removing Masquerading attacker node from network
- Result Analysis on the parameters like PDR, Throughput, Packet Dropping, transmission vs. speed

V. Prevention Of Sybil Attack

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

B. 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.

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.

VI. Conclusion

In this proposed scheme the RSS based detection approach As well as Lower-bound detection threshold is used, and compare with Received Signal Strength (RSS) value, along with the authentication of node which will correctly identified the Sybil identity with Higher True Positive., if the comparison is greater than or equal to RSS value, then it's a Sybil identity (Whitewash identity). This will be demonstrated through various experiments that a detection threshold exists for the distinction of legitimate new nodes and new malicious identities. Our experimental set up not only detect the sybil and masquerading attacks but it will also removes those attack from the network to completely remove the probability of future attacks from the same attacker nodes.

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.

[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