International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 5, May 2014

Identifing The Sybil Node By Using Lightweight Scheme In Mobile Ad hoc Network

R. Kanni Selvam , Mr.C.Karthikeyan M.E

Abstract— **In this globalized network, Mobile Ad hoc networks are a group of wireless mobile nodes dynamically forming a network without any pre-existing infrastructure. Due to its self-motivated or mobility in nature the nodes are more vulnerable to security threats which stimulate the performance of the network. In view of the fact that a malicious node can use multiple network identities which can affect topology maintenance and fault tolerant schemes such as multi-path routing. It is known as Sybil Attacker. A Sybil Attacker can cause damage to ad hoc by participating in the multipath routing to give false impression and decrease the accuracy, by increasing its reputation. It is strongly desirable to detect Sybil attacks and eliminate them from the network. But, 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. The proposed work is to detect the Sybil attacker with different transmission power by using lightweight scheme, without using centralized trusted third party or any extra hardware such as directional antenna and global positioning system.**

IndexTerms—***Sybilidentity,ReceivedSignalStrenth,Legimate node,Mobile Ad hoc Neetwork***

I. INTRODUCTION

In recent years, the explosive growth of mobile computing devices ,which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices ,has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society[1]. In the ubiquitous computing environment ,individual users utilize, at the same time, several electronic platform through which they can access all the required information whenever and wherever they may be[2].The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method :it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous device .The Mobile network is one of the wireless networks that have attracted most concentrations from many researchers' Mobile Ad hoc network(MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [3].In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other .In these two situation, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features[4].Unreliability of wireless link between nodes .Because of the limited energy supply for the wireless nodes and the mobility of the nodes ,the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants. Constantly changing topology. Due to the continuous motion of nodes the topology of the mobile ad hoc network changes constanly:the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes . Lack of incorporation of security features in statically configured wireless routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks . Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks. The unique charactertics of MANETs, such as dynamic topology and resource constraint devices, pose a number of nontrivial challenges for efficient and lightweight security protocol design. Due to the lack of centralized identity per node for their security protocols to be viable, Sybil attacks pose a serious threat to such networks. For example, communications in wireless networks are usually based on a unique identifier that represents a network entity: a node.

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 [5] . 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 .On the other hand ,Received Signal Strength (RSS) based

Manuscript received May , 2014

*R.**Kanni Selvam**, Electronics and Communication Engineering , Anna University/Einstein College Engineering/Tirunelveli Tamil nadu,India.*

***Prof Mr.C.Karthikeyan**, Electronics and Communication Engineering, Anna University/ Einstein College of Engineering /Tirnelveli, Tamilnadu,India.*

ISSN: 2278 – 909X

localization is considered one of the most promising solutions for wireless ad hoc networks .However, this approach requires extra hardware, such as directional antenna or a Geographical Positioning System (GPS). In this paper, we will present our scheme that mobile nodes with different transmission power. In particular, our scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities.

II. EXISTING SYSTEM

The 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.

A. Disadvantage

- Existing approach uses extra hardware to provide security
- Cryptographic techniques consume more resources for computation.
- Deplete the energy level of the mobile node.

III. MOTIVATION

Sybil attack 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. So we go for a Sybil attack detection method without using any external hardware.

IV. PROPOSED SYSTEM

In Sybil attack, an attacker acquires multiple identities and uses them simultaneously or one by one to attack network operation. Such attacks pose a serious threat to the security of self-organized networks like Mobile Ad hoc Networks(MANETs) that require unique and unchangeable identity per node for detecting routing misbehavior and reliable computation of node's reputation.

A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, hereby promoting lack of accountability in the network. In this research , we propose a lightweight scheme to detect the new identies of Sybil attackers without using centralized trusted third party or any exte a hardware, such as directional antenna or a geographical positioning system. Through the help of extensive simulation, we are able to demonstrate that our proposed scheme detects Sybil identities with good accuracy even in the presence of mobility and also the nodes with variable transmission power.

A. Advantages

- The proposed scheme provides security against Sybil attack with less energy consumption.
- The proposed scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware.

B. Network Configuration

The mobile nodes in the MANET are assumed to move by using the random way point mobility model. Let be considered that each mobile node using Omni antenna for transmission and reception of signals. The Two way ground is used as the path loss model in our simulation scenario. The nodes are having the connection with the node switch are present inside its communication range . The AODV routing protocol is used as the routing protocol to route the data packets to the indented destination.

C. System Architecture and flow chart of sybil attacker

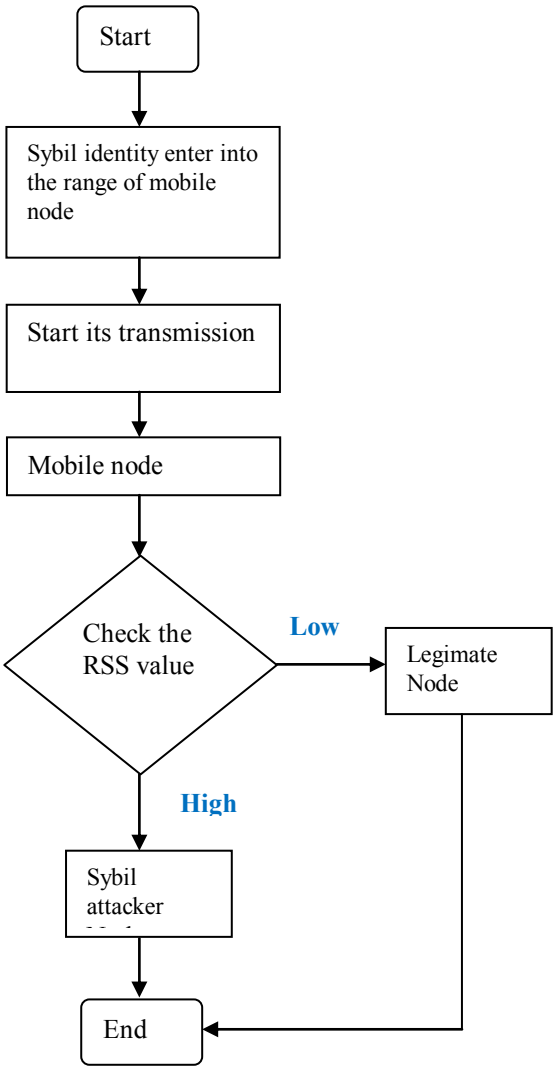

Fig 1. Flow diagram

ISSN: 2278 – 909X

A method was proposed using the Light weight scheme to verify the physical identity for preventing multiple-identity attacks. The multiple-identity attacks usually use a single malicious node to confuse neighbor nodes, causing chaos among them, and finally the entire network is interfered and thus cannot function properly.

In order to detect new identities spawned by a whitewasher or Sybil attacker, the following algorithm checks every received RSS by passing it to the addNewRss function, along with its time of reception and the address of the transmitter. If the address is not in the RSS table, meaning that this node has not been interacted with before, i.e., it is a new node and the RSS received is its first acknowledged presence. This first received RSS is compared against an *UB−THRESHOLD* (this threshold is used to check using the RSS whether the transmitter is in white zone, i.e., whitewasher). If it is greater than or equal to the threshold, indicating that the new node lies near in the neighborhood and did not enter normally into the neighborhood; the address is added to the malicious node list. Otherwise, the address is added to the RSS table and a link list is created for that address in order to store the recently received RSS along with its time of reception in it. Finally, the size of the link list is checked, if it is greater than the *LIST−SIZE*, the oldest RSS is removed from the list.

V. RECEIVED SIGNAL STRENGTH ANALYSIS

The distination between a new legitimate node and a new Sybil identity can be made based on their neighborhood joining behavior. For example, new legitimate nodes become neighbors as soon as they enter inside the radio range of other nodes; hence their first RSS at the receiver node will be low enough. In contrast a Sybil attacker, which is already a neighbor, will cause its new identity to appear abruptly in the neighborhood .When the Sybil attacker create new identity will be high enough to be distinguished from the newly joined neighbor.In order to analyze the difference between a legitimate newcomer and Sybil identity entrance behavior.Each node maintains a list of neighbors in the from <Address,Rss-List<time,rss>>,and records the RSS values of any directly received or overhead frames of 802.11 protocol,i.e., RTS,CTS,DATA,and ACK messages . In other words , each node will capture and store the signal strength of the transmissions received from its neighboring nodes. This can be performed when anode either takes part in the communication directly with nodes acting as a source or a destination or when a node does not take part in the direct communication .In the latter case it will capture the signal strength values of other communicating parties through overhead the control frames .Each Rss- List in front of the corresponding address contains Rn RSS values of recently received frames along with their time of reception,Tn.where n is the number of elements in the Rss-List that can be increased or decreased depending upon the memory requirements of a node.

A. Sybil Attack

There are two flavors of Sybil attacks.In the first one ,an attacker creates new identity while discarding its previously created one, hence only one identity of the attacker is up at a time in the network .This is also called a join-and –leave or whitewashing attack and the motivation is to clean out any bad history of malicious activies.This attack potentially promotes lack of accountability in the network. In the second type of Sybil attack ,an attacker concurrently uses all its identities for an attack, called simultaneous Sybil attack. The motivation of this attack is to cause distruption in the network or try to gain more resources, information, access etc . than that of a single node deserves in a network .The difference between the two is only the notion of simultaneity; however ,their applications and consequences are different. In this paper, we consider all the mobile nodes with different transmission power.

B. Block diagram

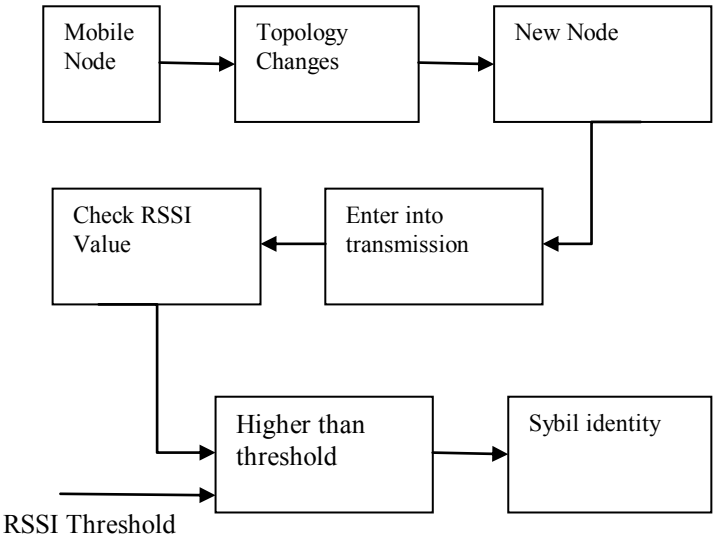

Fig 2. Identification Sybil identity

There may be so much of mobile nodes. To identify the new node the RSSI value is compared with that threshold value. If the RSS value is greater than the threshold value the new node is the Sybil node otherwise it is a normal node. Then eliminate the Sybil path and transfer the data in a new path.

The Network Inter phase layer serves as a hardware interface which is used by mobile node to access the channel. The wireless shared media interface is implemented as class Phy/WirelessPhy.

This interface subject to collisions and the radio propagation model receives packets transmitted by other node interfaces to the channel. The interface stamps each transmitted packet with the meta-data related to the transmitting interface like the transmission power, wavelength.

The performance of the proposed is evaluated by the Network Simulator(NS2).The NS2 is a discrete event time

ISSN: 2278 – 909X

driven simulator which is used to evaluvate the performance

Sl.o	Parameter	Value
1	Channel Type	Wireless Channel
2	Radio Propagation model	Two Ray Ground
3	Network interface type	WirelessPhy
4	Interface Queue Type	PriQueue
5	LL Type	Link Layer
6	Antenna Model	Omni Antenna
7	Routing Protocol	AODV

of the network.Two languages such as C++,OTCL(Object Oriented ToolCommon Language) is used in NS2.The parameters used in the simulation are tabulated as follows:

TABLE 1

SIMULATION PARAMETER USED FOR THE PROPOSED METHOD

VI. RESULT AND DISCUSSION

The data is transferred between sources to destination among multiple nodes. It have created the multiple nodes.

In our project, we are going to differentiate the Legimate node with the Sybil attacker node by its Received Signal Strength (RSS) value. The RSS value the transmission includes the transmission power of the node. In this project, we consider each and every node has the different transmission power in the wireless network.

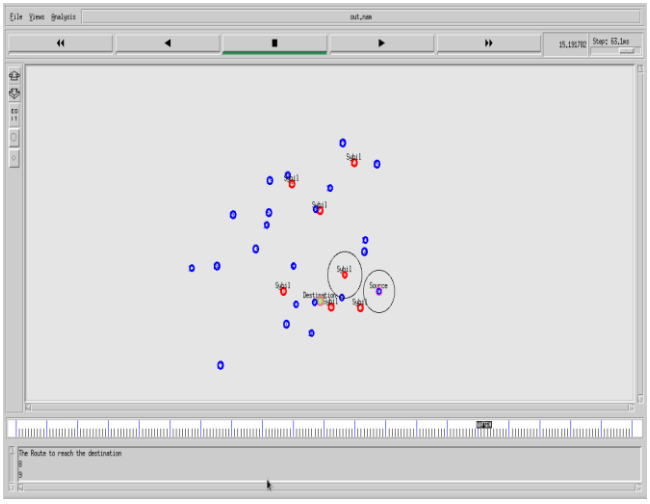

Fig 3.Identification of Sybil Attack

To create the number of nodes in the transmission range and during the data transfer between source to destination, a new node is entered into the coverage area.

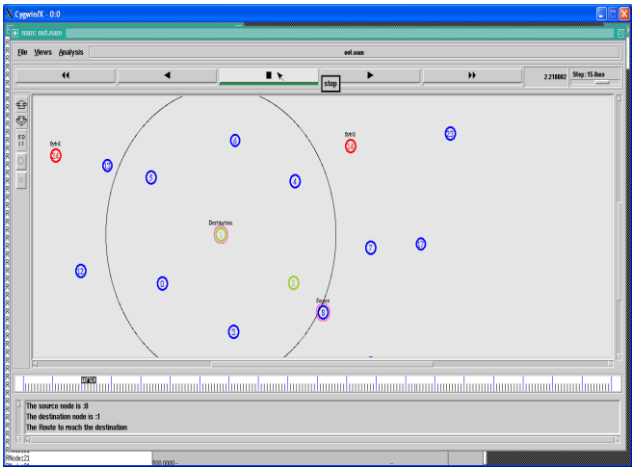

Fig 4. Compared RSS and Threshold Value

The RSS and Threshold value of new node is compared with our fixed RSS value. If the new node value is greater than our value, it is a Sybil node otherwise it is a normal node. After the identification of Sybil node eliminate the Sybil path.

The packet delivery ratio ,packet loss ratio, Bandwidth consumption and energy consumption are the parameters used in the simulation to evaluate the proposed method.

A. Packet Loss Ratio

Packet Loss Ratio is directly opposite to the Packet Delivery Ratio .The ratio of Number of packets dropped per unit time is called as Packet Loss Ratio.

ISSN: 2278 – 909X

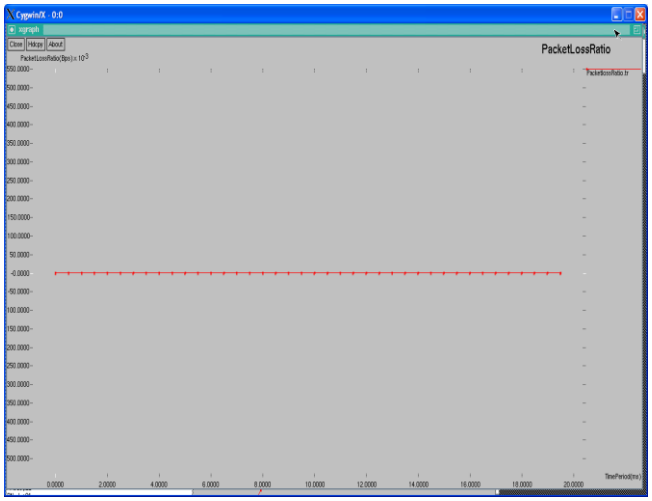

Fig 5. Packet Loss Ratio Vs Time

The Packet Loss Ratio is calculated by using the formula:

$$PLR = \frac{\text{Number of packets dropped}}{\text{Time}}$$

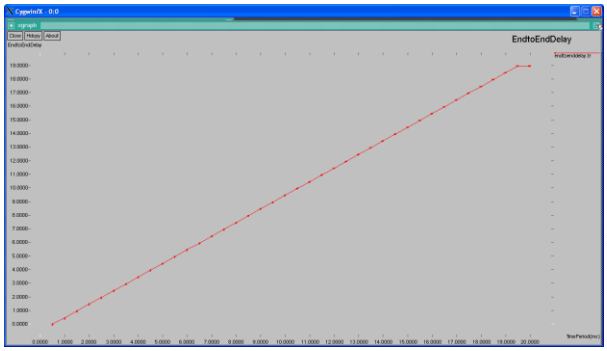

Fig 6. End to End Delay

End-to-end delay indicates how long it a packet takes to travel from the CBR source to the application layer of the destination.

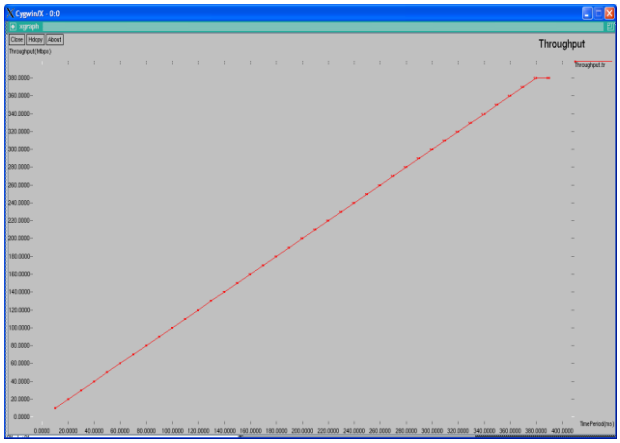

Fig 7.Throughput Vs Time

$$\text{Throughput} = \frac{\text{Recived Packet Size}}{\text{Time to Send}}$$

VII. CONCLUSION

In this paper ,we proposed an RSS-based detection mechanism to safeguard the network against Sybil attacks in the context of mobile nodes with different transmission power he scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware . We analyze the performance of the proposed scheme through simulation. We also showed the various factors affecting the detection accuracy, such as network connection, packet transmission rates, node density, and node speed .The simulation results showed that our scheme works better even in mobile environments.

VIII. CONCLUSION

In this paper ,we proposed an RSS-based detection mechanism to safeguard the network against Sybil attacks in the context of mobile nodes with different transmission power he scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware . We analyze the performance of the proposed scheme through simulation. We also showed the various factors affecting the detection accuracy, such as network connection, packet transmission rates, node density, and node speed .The simulation results showed that our scheme works better even in mobile environments.

REFERENCES

[1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.
[2] M. Weiser, The Computer for the Twenty-First Century, Scientific American, September 1991.
[3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.
[4] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in*Proc. 4th Workshop HotNets*, 2005, pp. 1–6.
[5] K. Hoeper and G. Gong, "Bootstrapping security in mobile ad hoc networks using identity-based schemes," in *Security in Distributedand Networking Systems* (Computer and Network Security). Singapore: World Scientific, 2007.
[6] S. Hashmi and J. Brooke, "Toward Sybil resistant authentication in mobile ad hoc networks," in *Proc. 4th Int. Conf. Emerging SecurityInform., Syst. Technol.*, 2010, pp. 17–24.
[7] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.
[8] M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within VANET," *Int. J. Netw. Security*, vol. 8, pp. 322–333, May 2009.

ISSN: 2278 – 909X

R.Kanni Selvam has received her B.E Degree in Electronics and Communication Engineering in 2012 from Einstein College of Engineering ,Tirunelveli(India).She is currently pursuing M.E in Electronics and Communication Engineering at Einstein College of Engineering ,Tirunelveli (India). Her area of interest are Network and digital Electronics.

C.Karthikeyan has received his B.E in Electronics and Communication Engineering in 2005 fromP.S.R. Engineering College ,Sivakasi and Master Degree in from MIT Anna university,Chennai India in 2008. Since 2010 he has been with Einstein College Of Engineering ,Tirunelveli,where he is currently work in as an Associate Professor in the Department of Electronics and communication Engineering.

ISSN: 2278 – 909X