Lightweight Scheme to Detect the New Identities of Sybil Attackers in MANETS

Winnarasi. A[1], Sasikala.V[2]
[1]ME-Applied Electronics, Magna college of Engineering,Chennai, Tamil Nadu,India.
[2]HOD - ECE Department, Magna College of Engineering, Chennai,Tamil Nadu, India

***Abstract*--** **Mobile adhoc networks are the temporary network without any infrastructure. Due to its complex nature various threats are caused in this network, where Sybil attack is one of the serious threats to such mobile adhoc networks. This Sybil node can be identified using the scheme which uses the RSS value to find the lightweight of the node in the mobile adhoc network. In particular, the scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities. The proposed 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. The detection scheme can work as a standalone scheme, but could equally be deployed as an add-on to existing schemes. The proposed scheme does not use localization technique, and does not need any directional antennae or any GPS equipment. This does not use centralized trusted third party also. In the scheme, nodes share and manage identities of Sybil and non-Sybil nodes in distributed manner. The evaluation of this scheme can be done using extensive simulations by using the simulator NS2.**

Keywords: Sybil node, MANET.

I. INTRODUCTION:

Mobile adhoc Networks are the network without any infrastructure and a temporarily formed network. This represents complex distributed systems with mobile nodes in an temporarily formed network with ad hoc network topologies. This allows people and devices to seamlessly internetwork in areas where no pre-existing communication infrastructure exists, for example disaster recovery environments. The unique characteristics of MANETs, such as dynamic topology and resource constraint devices, pose a number of nontrivial challenges for efficient and lightweight security protocols design. Due to the lack of centralized authority management in MANETs and 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.

A Sybil attacker is a node which imitates another node and can cause serious threats to the ad hoc network. It can disrupt any location based or multipath routing by participating in it in a different form. It decreases the accuracy and creates some false impression to divert the traffic. Therefore Sybil nodes create serious threats to the ad hoc networks It is strongly desirable to detect these nodes and to eliminate it. The commonly used approach is by using cryptographic based authentication or trusted certification or sometimes by using centralized party. Another promising method is by using the Received Signal Strength (RSS) based localization. This requires extra hardware such as directional antenna and GPS systems.

. Sybil attacks [1] refer to individual malicious users creating multiple fake identities (called sybil identities or sybil nodes) in open-access distributed systems. These open-access systems aim to provide service to any user who wants to use the service.

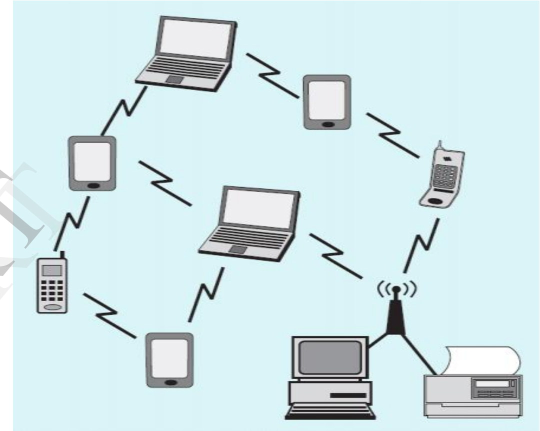

Fig 1 Mobile ad hoc network

Communications in wireless networks are usually based on a unique identifier that represents a network entity: a node. Identifiers are used as an address to communicate with a network entity. This forms a one to-one mapping between an identity and an entity and that is usually assumed either implicitly or explicitly by many protocol mechanisms; hence two identities implies two distinct nodes. Unfortunately malicious nodes can illegitimately claim multiple identities and violate this one tone mapping of identity and entity philosophy [2].

In this paper, the RSS value has been used to differentiate between legitimate node and Sybil node in order to detect and eliminate the Sybil node

The paper is organized as follows. Section 1 explains the introduction of the paper. Section 2 highlights the analysis of the existing systems. Section 3 shows the problem definition of the sybil nodes in the mobile ad hoc network. Section 4 deals with the experiments, models, system design and some outcomes. Section 5 highlights the performance evaluation. Section 6 gives the conclusion and future work of this paper.

II. ANALYSIS OF EXISTING SYSTEMS

In a sybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. By controlling a large fraction of the nodes in the system, the malicious user is able to "out vote" the honest users in collaborative tasks such as Byzantine failure defenses. SybilGuard is a novel protocol for limiting the corruptive influences of sybil attacks[]. This protocol is based on the "social network" among user identities, where an edge between two identities indicates a human-established trust relationship. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately small "cut" in the graph between the sybil nodes and the honest nodes. SybilGuard exploits this property to bound the number of identities a malicious user can create. This requires high set up cost.

Due to the broadcast nature of the wireless medium, wireless networks are especially vulnerable to Sybil attacks, where a malicious node illegitimately claims a large number of identities and thus depletes system resources. An enhanced physical-layer authentication scheme to detect Sybil attacks are proposed, exploiting the spatial variability of radio channels in environments with rich scattering, as is typical in indoor and urban environments. A hypothesis test to detect Sybil clients for both wideband and narrowband wireless systems, such as WiFi and WiMax systems can be built. Based on the existing channel estimation mechanisms, the method can be easily implemented with low overhead, either independently or combined with other physical-layer security methods, e.g., *spoofing* attack detection[]. The performance of the Sybil detector is verified, via both a propagation modeling software and field measurements using a vector network analyzer, for typical indoor environments. The evaluation examines numerous combinations of system parameters, including bandwidth, signal power, number of channel estimates, number of total clients, number of Sybil clients, and number of access points. For instance, both the false alarm rate and the miss rate of Sybil attacks are usually below 0.01, with three tones, pilot power of 10 mW, and a system bandwidth of 20 MHz. This is done within the indoor environment which is the disadvantage.

Sybil attacks have been shown to be unpreventable except under the protection of a vigilant central authority. They use an economic analysis to show quantitatively that some applications and protocols are more robust against the attack than others. In our approach, for each distributed application and an attacker objective, there is a critical value that determines the cost effectiveness of the attack. A Sybil attack is worthwhile only when the critical value is exceeded by the ratio of the value of the attacker's goal to the cost of identities. They show that for many applications, successful Sybil attacks may be expensive even when the Sybil attack cannot be prevented. Specifically, they proposed the use of a recurring fee as a deterrent against the Sybil attack. This requires more resources and cost.

The Sybil attack is one of the most harmful security threats for distributed hash tables (DHTs). This attack is not only a theoretical one, but it has been spotted "in the wild", and even performed by researchers themselves to demonstrate its feasibility. The Sybil attack whose objective is that the targeted resource cannot be accessed by any user of a Chord DHT, by replacing all the replica nodes that store it with sybils has been analysed. A simple, yet complete model that provides the number of random node-IDs that an attacker would need to generate in order to succeed with certain probability has been explained. Therefore, this model enables to quantify the cost of performing a Sybil resource attack on RELOAD/Chord DHTs more accurately than previous works, and thus establishes the basis to measure the effectiveness of different solutions proposed in the literature to prevent or mitigate Sybil attacks. The above method requires more resources.

III.PROBLEM DEFINITION

In Sybil attack, an attacker acquires multiple identities and uses them simultaneously or one by one to attack network operations. 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. Current authentication mechanisms for MANETs are vulnerable to Sybil attack unless they resort to some out of band method like physical contact between nodes for building trust or relying on a Trusted Third Party for issuing a unique and unchangeable identity to each node[1]. The traditional authentication mechanism for MANETs utilizes hardware id of the device of each node for authentication. An authentication agent is developed that verifies the hardware id of the authenticatee node. A comprehensive defense model is employed to protect the authentication agent from various static and dynamic attacks from a potentially malicious authenticatee node. Security of authenticatee node is assured by involving a TTP that signs the authentication agent, verifying that it will perform only intended function and is safe to execute. The main disadvantages are stated as follows,

- 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.
- This approach requires extra hardware, such as directional antennae or a geographical positioning system (GPS).

This can be avoided using the following proposed method,

Fully self-organized mobile ad hoc networks (MANETs) represent complex distributed systems that may also be part of a huge complex system, such as a complex system-of-systems used for crisis management operations. Due to the complex nature of MANETs and its resource constraint nodes, there has always been a need to develop lightweight security solutions. Since MANETs require a unique, distinct, and persistent identity per node in order for their security protocols to be viable, Sybil attacks pose a serious threat to such networks. 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, thereby promoting lack of accountability in the network. In this research, we propose a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system.

IV SYSTEM DESIGN

In the MANET, mobile nodes are in random motion to communicate with each other where in all the nodes inside its range are considered and their Received Signal Strength (RSS) is evaluated and processed. The mobile node with high RSS value is detected to be a Sybil Identity and the mobile node with low RSS value is considered for transmission. The Laptop at the end of the above architecture is detected to be the Sybil Identity and the other mobile node with lower RSS is found to be a legitimate node in the following figure.

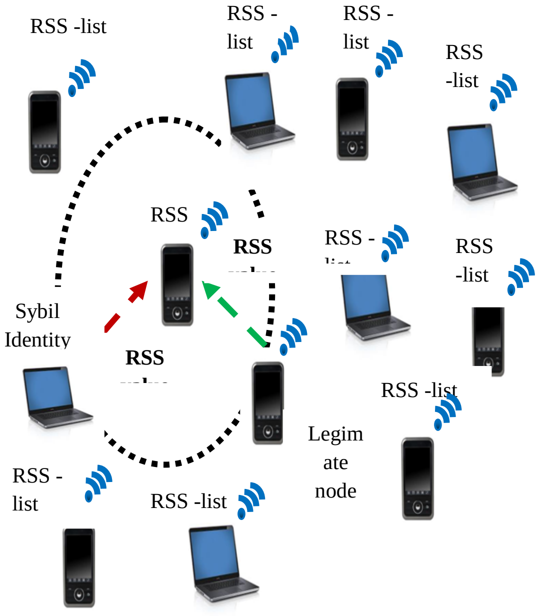

Fig 2 System architecture

In communication networks, a topology is a usually schematic description of the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology. The physical topology of a network is the actual geometric layout of workstations. Logical (or signal) topology refers to the nature of the paths the signals follow from node to node. As it is a MANET environment, the topology changes dynamically.

IV PERFORMANCE EVALUATION

The distinction 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 creates new identity, the signal strength of that identity will be high enough to be distinguished from the newly joined neighbor.

A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically.

The RSS value is used to denote the power level in the received signal. The RSS value is directly proportional to the distance between the transmitter and the receiver antenna. The standard formula is used to find the power level in the signal is as follows:

$$RSS = \frac{T_p G_t G_r Ht^2 Hr^2}{d^4}$$

Where,

T_p → Transmission Power

G_t →Transmitter Gain

G_r →Receiver Gain

Ht →Height of the transmitter antenna

Hr →Height of the Receiver antenna

d → Distance between source and destination

The performance of the proposed scheme is evaluated by means of the network simulator. The simulation results bring out some important characteristic functions of the proposed algorithm. The various parameters of the simulation by using record procedure are recorded. The recorded events are stored in the trace files. By executing the trace files by using xgraph or gnuplot the graph as the output is obtained. Here threshold value will be considered for some range. The value less than or equal to threshold value will be a legitimate node. The node with the value greater than the threshold value will be the Sybil node. Thus performance of the system can be evaluated.

The graph for the values of packets and the time can be given in Fig 3 linearly where the series 1 represents the gradual increase in the RSS value of the legitimate node. And series 2 represents the higher increase in the Sybil node which is to be eliminated.

The speed of the nodes is also considered since it is a mobile node. The threshold of the nodes is set so that the node above the threshold level will be considered as the Sybil node. Sybil node will not be holding any history since it appears suddenly. The result of the simulation will be better comparing to the previous methods. The transmit power of the nodes are also kept varying for the nodes and the detection of the nodes is thus performed improving the efficiency of the system.

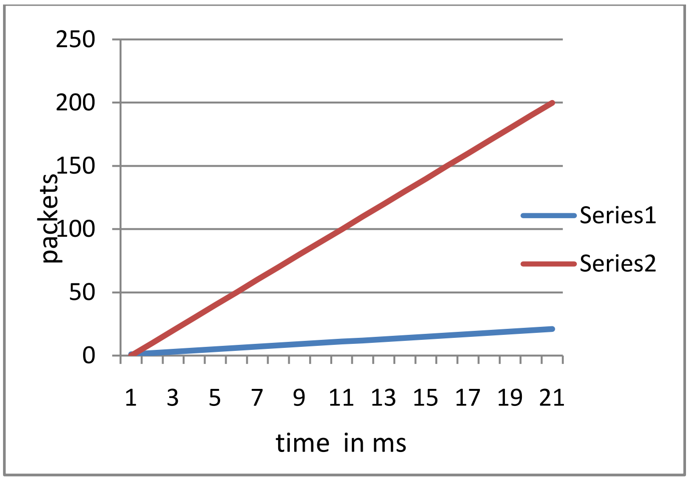

Fig 3 Packet ratio

On the simulation of the OTcl code that corresponds to the proposed algorithm, the Network Animator (NAM) produces the traces at various intervals of time. The main.tcl file is created and all the corresponding files are embedded inside the same to combine together as a single project. All trace files and gnu plots using xgraph and also the animator files are combined here and executed together as a single ".wish"file.

From the above analysis it is evident that our scheme work better in MANET environments where there are high network connections, node density, and packet transmission rate. The Sybil identity detection scheme is hence light weight and easy to achieve accuracy and also obtain good network performance.

V CONCLUSION

The mobile nodes in the network are formed without any infrastructure and also temporarily formed. The RSS value for the nodes is calculated to eliminate the Sybil node even with the varying transmit power which causes the improvement in the system. Thus the system performs in a better way in detecting the Sybil nodes and eliminating the Sybil node.

FUTURE WORK

Light weight sybil attack detection scheme can act as an efficient security scheme with any protocol. However, cannot stand on its own. In future, data security algorithms combined with this scheme can be used to develop a standalone routing protocol to route, detect sybil attacks and provide secure communication.

REFERENCES

1. J. R. Douceur, "The Sybil attack," presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.
2. J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defences," presented at the 3rd Int. Symp. Information Processing in Sensor Networks (IPSN), 2004, pp. 259–268
3. 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.
4. N. B. Margolin and B. N. Levine, "Quantifying resistance to the Sybil attack," in Financial Cryptography and Data Security. Berlin, Germany: Sprnger, 2008
5. V. A. Luis, B. Manuel, and L. John, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 2003, pp. 294–311.
6. Liang Xiao, et al, "Channel-Based Detection of Sybil Attacks in Wireless Networks", ieee transactions on information forensics and security, vol. 4, no. 3, september 2009.
7. Tong Zhou, "P2DAP –Sybil Attacks Detection in Vehicular Ad Hoc Networks", IEEE journal on selected areas in communications, vol. 29, no. 3, march 2011.
8. Shan Chang, et al, "Footprint: Detecting sybil attacks In urban vehicular networks", ieee transactions on parallel and distributed systems, vol. 23, no. 6, june 2012.
9. Khaleel mershad, et al, "a framework for secure and efficient data acquisition in vehicular ad hoc networks", IEEE transactions on vehicular technology, vol. 62, no. 2, february 2013.
10. Manuel Uruena, et al, "A Model to Quantify the Success of a Sybil Attack Targeting RELOAD/Chord Resources", IEEE communications letters, vol. 17, no. 2, february 2013.