NEW IDENTITIES OF SYBIL NODES DETECTION BASED ON RSS IN MANETs

P.S.Satheesh
PG Scholar (CSE)
Sri Sai Ram Engineering College,
Chennai-600 044

M.Suresh Anand, M.Tech.,(Ph.D)
Assistant Professor
Sri Sai Ram Engineering College,
Chennai-600 044

***Abstract*--The unique characteristics of mobile ad hoc networks (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 identity 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. Fully self-organized mobile ad hoc networks (MANETs) represent complex distributed systems. Due to the complex nature of MANETs and its resource constraint nodes, there has always been a need to develop lightweight security solutions. 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. We also showed the various factors affecting the detection accuracy, such as network connections, packet transmission rates, node density, and node speed. 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.**

***Index Terms*- Identity-based attacks, intrusion detection, mobile ad hoc networks, Sybil attacks.**

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are self-organized, complex distributed system that consists of wireless mobile nodes, infrastructure-less network and temporary ad hoc network topologies. The nodes in networks are take of security related tasks like authentications, trust managements etc. Nodes can enter or leave the network at any time and roam in the network freely. Each node is a host as well as a router, which is used for connectivity between the source and destination. Due to the lack of centralized identity management in MANETs and the requirement of a unique, Distinct and persistent identity nodes for their security protocol to be viable.

The Sybil attack is relevant threat to be secure and dependable operation of wireless ad hoc networks.

II. RELATED WORK

Nodes in an open MANETs run a Trust computation mechanism to identity malicious and selfish nodes. Sybil attackers can create an arbitrary number of nonexistent vehicles, which gives false information in the network to give wrong impression of traffic congestion to divert traffic. To prevent Sybil attack is to use cryptographic based authentication or trusted certificate. In Sybil attack, the attacker may use multiple identities simultaneously or one by one, to play with the trust computation system. Received signal strength (RSS) is one of the most promising solution for Wireless ad hoc networks. The RSS is used to differentiate between the legitimate and Sybil identities.

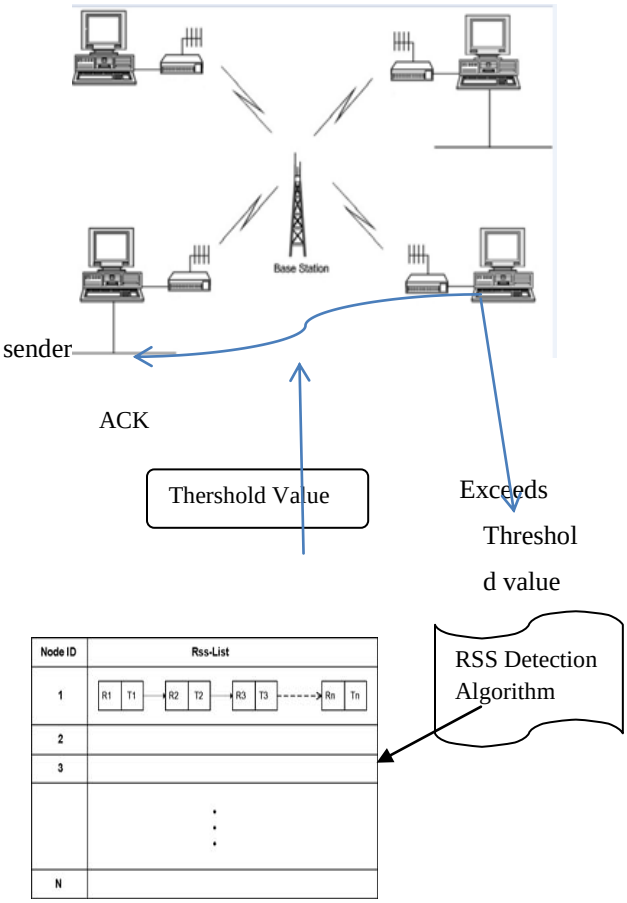

Fig. 2.1 Implementation diagram

III. DETECTION OF SYBIL IDENTITIES

1. ATTACK MODEL

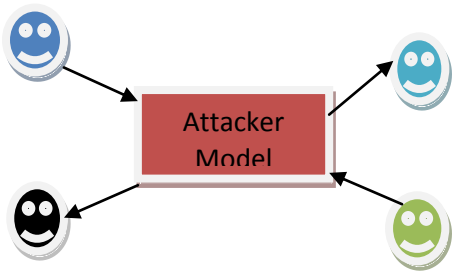

Fig. 1.1 Attack model

In this attack model there are two types of Sybil attacks. The first type is, an attacker used to create the new identity that used for discarding its previously created one; hence only one type of identity of the attacker are involve in a network at a time. This is also called as a Whitewashing attack or join and leave attack. The motivation of this attack is clean-out the bad malicious activities. The second types of Sybil attacker, all the identities are used for concurrently for attack. This type of attack is called as simultaneous Sybil attack. The aim of this type of attack is to cause disruption in the network or try to gain more information, resources etc. The strategy of our detection mechanism is used to detect every new identity created by a Sybil attacker, it does not matter it should be an identity for whitewashing or simultaneous Sybil attacks.

2. CREATING NEIGHBOUR LIST MODEL

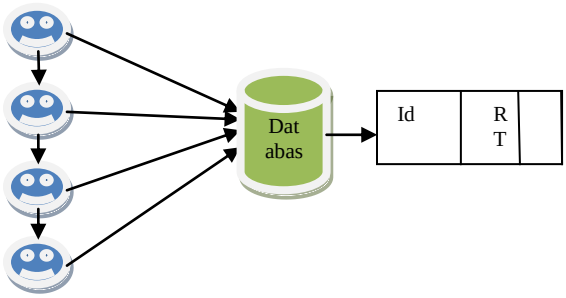

Fig. 2.1. Creating Neighbor List Model

Here, each node maintains a list of neighbors which is in the form of Address, Rss-List (time, rss). Records the Rss values of any directly received frames of 802.11 protocol, it should be a RTS, ACK message, DATA, CTS. Each Rss-List is contains the corresponding address contains Rn. RSS values that are recently received frames along with their time reception, Tn. When n is the number of elements in the Rss-List that should be increased or decreased depending upon the node. Each node should be capture and store the signal strength of the

transmissions received from the neighboring nodes. This node either take place a direct communication with other nodes acting as a source or destination or when a node does not take part a direct communication.

3. SIGNAL STRENGTH BASED ANALYSIS

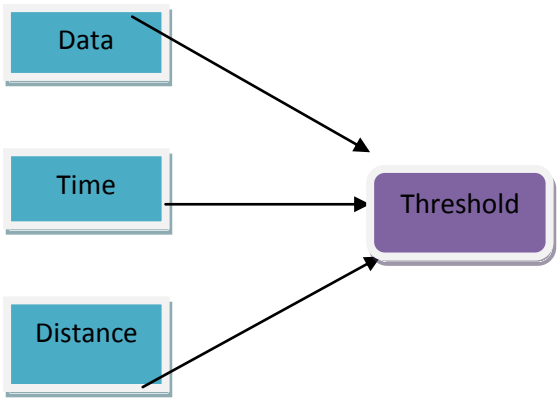

Fig. 3.1. Signal strength based value

The distinction between a new legitimate node and a new Sybil identity are the neighborhood joining behavior. The new legitimate nodes are neighbors nodes as soon as they become enter into radio range of other nodes. Each node can collects and maintains the RSS values of the neighboring node. The Sybil attacker, which is already a neighbor, will cause its new identity. When a Sybil attacker is a new identity, the signal strength of identity will be distinguished from the newly joined neighbor. We calculate the threshold values based on the data, time and distance covered. Have to analysis the difference between legitimate newcomer and Sybil identity entrance behavior.

4. TUNING THE THRESHOLD

Threshold is based on the maximum speed of the network. This threshold will be the first RSSs from newcomers, it enter into the neighborhood if the threshold is greater than the newcomer. The radio ranges are partition into two zones, i.e., gray zone and a white zone.

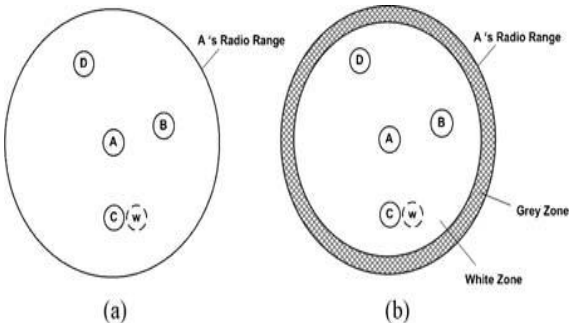

Fig. 4.1 (a) without and (b) with categorization of radio range

Fig 4.1 (b), is used for partitioning is based on the speed-based detection threshold. The higher speed thresholds produce wider gray zones. Whitewashing cannot be detected in this area, so the first appearance of a node in the gray zone represents as a normal entry into radio range of a node. We used 10 m/s as an upper bound speed because nodes cannot move faster than 10 m/s (36 km/h) i.e., why we choose it to be a good upper limit. Any new identities created in a white zone it will be detected as a Sybil identities or join-and-leave, because normal nodes cannot produce their first appearance. For example , if network maximum speed of a node is 2 m/s detection threshold produce narrow gray zone. If any node first captured is greater than the threshold, i.e., a node is in white zone.

5. ATTACKER DETECTION

To detect new identities by Sybil attacker or whitewashing. If the RSS is greater than the threshold, then the new node is lies near in the neighborhood and then it does not enter into the neighborhood. Then the address would be added into the malicious node list. When address is added to the RSS table and a link list is created for that address. This address is store in the received RSS along with time. At last the size of link is checked, if it is greater than the LIST-SIZE. The threshold is averaged RSS value when a transmitter is moving with 10 m/s speed. The LIST-SIZE is the maximum RSS records retained for identity of address. When a malicious node changes its identity, its previous identity record stays in the RSS table. Nodes join and leave the network at any time; hence nodes that depart from network.

IV. CONCLUSION

In this paper, we proposed an RSS-based detection mechanism to safeguard the network against Sybil attacks. The scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware. We demonstrated through various experiments that a detection threshold exists for the distinction of legitimate new nodes and new malicious identities.

REFERENCES

[1]. S.Abbas, M. Merabti, and D. Llewellyn-Jones and K.Kifayat, "Lightweight Sybil Attack Detection in MANETs," IEEE System Journal.,vol. 7, no. 2, june 2013.

[2]. S. Hashmi and J. Brooke, "Toward Sybil resistant authentication in mobile ad hoc networks" in Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol., 2010, pp. 17–24.

[3]. 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.

[4]. S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Deterring white washing attacks in reputation based schemes for mobile ad hoc networks," inProc. WD IFIP, 2010, pp. 1–6.

[5]. 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.

[6]. A. Tangpong, G. Kesidis, H. Hung-Yuan, and A. Hurson, "Robust Sybil detection for MANETs," in Proc. 18th ICCCN 2009, pp. 1–6.

[7]. D. Monica, J. Leitao, L. Rodrigues, and C. Ribeiro, "On the use of radio resource tests in wireless ad hoc networks," in Proc. 3rd WRAITS, 2009,pp. 21–26.