SYBIL ATTACK DETECT IN MANET'S

[1]Mrs.K.Deepalakshmi, [2]Ms.A.Sivasankari, [3]Mrs.B.Arulmozhi

[1,2,3] *Department of computer science, DKM College for women(Autonomous), Vellore, Tamil Nadu, India.*

Abstract: ***In this paper, we will present our scheme that detects Sybil identities. In particular, our scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities. First, we demonstrate the entry and exit behaviour 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 behaviour. Third, we tune our detection threshold by incorporating the RSS data fluctuation taken from our tested experimentation. Fourth, we evaluate our scheme using extensive simulations, and the results show that it produces about 90% true positives (detecting a Sybil nodes Sybil) and about 10% false positives (detecting a normal node as a Sybil node) in mobile environments.***

Keywords : *legitimate, Sybil ,nodes, RSS, evaluate*

1. INRODUCTION

1.1GENERAL

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. The Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. It represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ''ad-hoc'' network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure. Ad hoc networking concept is not a new one, having been around in various forms for over 20 years.

1.2. OBJECTIVE

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.

2. PROBLEM DEFINITION

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. On the other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc networks. However, this approach requires extra hardware, such as directional antennae or a geographical positioning system (GPS).

3. METHODOLOGY

3.1.RSS Detection Algorithm

In our scheme, nodes share and manage identities of Sybil and non-Sybil nodes in distributed manner. The rest of the paper is organized as follows. Detection of Cybil attack, we explain our scheme with the help of some experiments. Sun spot tested we describe how we conducted the scenarios as real-world tested experiments using Java Sun SPOT sensors in order to confirm our rationale. Tuning the threshold we discuss the issue of tuning the detection threshold for worst case scenarios. We will setup our detection threshold based on the maximum speed of the network; assuming that no node can move faster than this maximum speed. This threshold will make the distinction because the first RSSs from newcomers, if greater than the threshold imply abnormal entry into the neighbourhood.

3.2.User Interface

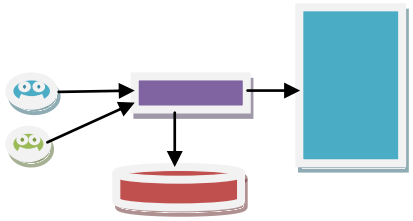

Fig 1:User Interface

4. MODULE DESCRIPTION

4.1.User Interface

In this case user interface is act like a server. We want to communicate with other users means user interface need to verify the username and password of the user and allow the user from the outside. User interface is the high integrity processes of a system are first measured and verified and these processes are then protected from accesses initiated by UN Authorized user integrity processes during runtime. In other words, the protection of high integrity process is verified by analyzing security policies and ensuring that the policies are correctly enforced .In this case no need to verify all software and hard ware component.

4.2.ATTACK MODEL

There are two flavours 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 ata 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 activities. 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 motivations of this attack is to cause disruption 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.

4.2.1.Attack Model

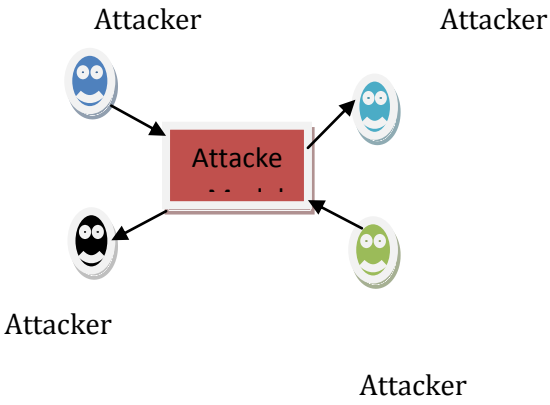

Fig:2 Atack Model

4.2.2.Creating the Neighbour List Mode

Each node maintains a list of neighbors in the for <Address, Rss-List <time, rss>>, and records the RSS values of any directly received or overheard 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 neighbouring nodes. This can be performed when a node either takes part in the communication directly with other 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 overhearing 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. In our simulation, we used *n* to be five elements; however, for real-world scenarios, it should be greater than that because of the time varying nature of RSS.

4.2.3.Creating the Neighbor List Model

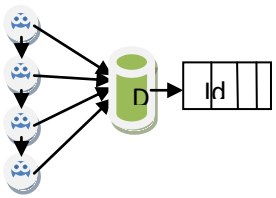

Fig :3 Creating he neighbour list model

5.SIGNAL STRENGTH BASED ANALYSIS

The distinction between a new legitimate node and a new Sybil identity can be made based on their neighbourhood joining behaviour. For example, new legitimate nodes become neighbours 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 neighbour, will cause its new identity to appear abruptly in the neighbourhood. When the Sybil attacker creates new identity, the signal strength of that identity will be high enough to be distinguished from the newly joined neighbour.

Signal Strength Based Analysis

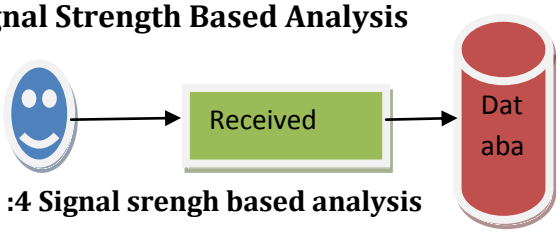

Fig :4 Signal srengh based analysis

5.1.Users

Sybil identity entrance behaviour, we setup some experiments in the following. Before we start, it is important to explain how each node collects and maintains the RSS values of the neighbouring nodes.

5.2. Tuning the Threshold

The main difference we found between the results obtained from our and from our Creating the Neighbour List Model is the variation in RSS values. As RSS varies, for a node *B* at a fixed distance *d* from a node *A*, the receiving node *A* can receive multiple different RSS values in the fluctuation range [−*v*, +*v*] (assuming +*v* is greater than −*v*) and hence these values do not represent an *exact* indication of distance. The detection threshold will be affected when it works based on a single RSS value. For example, node *A* can receive RSS from *B* at any particular time while *B* is a good node just outside the white zone of *A* with +*v* variance, the position of *B*. As a result, due to the +*v* variation in the RSS, *A* will consider *B* to be a new identity emerged in its white zone, and hence node *B* will incorrectly be detected as a Sybil identity.

Tuning the Threshold

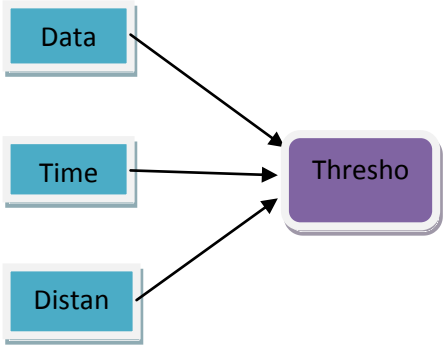

Fig:5 Tuning the treshold

6. ATTACKER DETECTION

We will setup our detection threshold based on the maximum speed of the network assuming that no node can move faster than this maximum speed. This threshold will make the distinction because the first RSSs from newcomers, if greater than the threshold imply abnormal entry into the neighbourhood. Now the question becomes, which speed should we adopt as the upper bound for our detection threshold Determining node presence with respect to different speeds. To answer this question and for clarity purposes, we logically partition the radio range of node *A* into two zones: a gray zone and a white zone, as shown in. Please note that this partitioning is based on the speed-based detection threshold. If we incorporate various speed-based thresholds from into it would become clear that higher speed thresholds produce wider gray zones. Whitewashing in this area cannot be detected, since the first appearance (or acknowledgment) of a node in the gray zone would usually represent a normal entry into the radio range of the node.

Attacker Detection

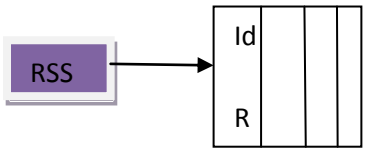

Fig :6 Attacker detection

7. CONCLUSION

Our future work includes tackling issues related to variable transmit powers and masquerading attacks 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.

8. REFERENCE

1.I. Chlamtac, M. Conti, and J. J.-N. Liu, “Mobile ad hoc networking:Imperatives and challenges,” Ad Hoc Netw., vol. 1, no. 1, pp. 13–64,2003.

2. 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.

3 .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.

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 Distributed and Networking Systems (Computer and Network Security). Singapore: World Scientific, 2007.