Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network

P.Kavitha, 2C.Keerthana, 3V.Niroja, 4V.Vivekanandhan,
Adhiyamaan College of Engineering,

Abstract—Mobility is often a problem for providing security services in ad hoc networks. Mobility can be used to enhance security. An advantage of such a network is that there is no fixed infrastructure is required. In the Sybil attack a single node presents multiple fake identities to other nodes in the network. Sybil attacks pose a great threat to decentralized systems like peer-to-peer networks and geographic routing protocols. In the method, use passive ad hoc identity method and key distribution. Detection can be done by a single node, or that multiple trusted nodes can join to improve the accuracy of detection. In Sybil attacks pose a great threat to decentralized systems like peer-to-peer networks and geographic routing protocols.

Keywords: Identity-based attacks, mobile ad hoc networks, Sybil attacks.

I. Introduction

Mobile ad hoc networks (manets) represent complex distributed systems that consist of wireless mobile nodes that can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies 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 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.

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. The attacker uses different identities at the same time. A single attacker could pretend nodes to report the existence of a false bottleneck in traffic. MANETs are mainly related to illegally gathering sensitive information about mobile nodes. To relate between a source and its destination, effect on data and transmission time on network.

II. Existing of sybil attack

In existing system, hackers easily can act as source node and sends message to destination. Destination receives wrong message from hackers. Destination believes that its correct message from source. Destination receives the wrong information from hackers. Messages are passed from sender to destination (receiver) without any security. 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. Message header holds source node information which sends the message to receiver. Hackers can easily change that header information and sends to destination. They have much loss of data and not a secure process on the network.

The disadvantages are destination gets the wrong information from hackers or malicious user, there is no server to detect hackers, overhead of packet loss and Low level network performance.
III. Proposed scheme

In this proposed system, 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. Our proposed 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 they have any packet loss are some collision on network 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. In our proposed method to use secure and avoid the attacking system on the network.

The benefits are to reduce the packet delay and detect the attacker, data delivery quickly from source to destination. Efficient data transmissions on network, Without any loss data will be send in destination and improve the network performance.

IV. Detection of sybil attack

Attack Model 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 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.
V. Algorithm

Step 1: Each node to know the neighbors node address.

Step 2: If neighbors node is centralized server node means, store data.

Else, search the centralized node.

Step 3: The server nodes have all source data as well as destination address.

Step 4: Each node has the individual keys. Depends on the keys the centralized server is to identify the destination address.

Step 5: In NDD algorithm and centralized server method is used to preventing the data into any attackers.

Step 6: The destination node easily to check the data is correct or not.

Step 7: If any attackers damage the data means destination node again send the data in to centralized server.

To detect Sybil attack use NDD (Neighbor Discover Distance) algorithm used to, Manet each and every nodes knows the neighbors address. Depends on the address easily transfer the data to destination without any attack or packet loss. Centralized server is used to collect the all data. Also knows the every node key address. Using these key data will be sending the destination without any damage. Use a random key distribute for an every node on the network. It has more security and efficient data transmission on their network. If they have key means to access the data from the source node on the network.

VI. Conclusion

The proposed NDD algorithm-based detection mechanism to Sybil attacks. 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. 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. In future our proposed method to use secure and avoid the attacking system on the network.

Acknowledgment

We would like to thank Prof. Mr. V. Vivekanandhan and Prof. Dr. D. Thilagavathy for helping to determine Sybil attack detection in MANET.

References


