Research Paper Engineering

Effect of Impersonation Attack on Mobile Ad Hoc Network

* Er. Aakansha Jain ** Er. Khushboo Sawant

* Assistant Processor, Department of Information Technology, Indore Institute of Science, & Technology, Indore, India

** Student of Master of Technology Department of Computer Science & Engineering, Lakshmi Narain college of Technology Indore, India

ABSTRACT

Mobile ad hoc network (MANET) is one of the most promising fields for research and development of wireless network. Security is essential requirement in MANET .In ad hoc network the communicating nodes do not necessarily relay on fixed infrastructure, which sets new challenges for the security architecture. Impersonation attack is special case of integrity attacks where by a compromise node impersonates a legitimate node one due to the lack of authentication in current ad hoc routing protocol. In this paper, we are describing the causes of impersonation attack and their vulnerable effects which give chance to a malicious node for doing other attacks too. Our approach is to detecting and eliminating impersonation attack using secure routing protocols.

Keywords: Impersonation Attack, Routing Protocols, Security.

I. INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration in such an environment. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self

Configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for Developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, Confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

II. SECURITY ISSUES

A major issue with wireless network is its security. As data is transmitted over the internet there is always the possibility of someone else hacking the data therefore in order to prevent a hacker from gaining access to the network and corrupting the data, it is vital that there is adequate security in place. For analyzing the security of wireless mobile ad hoc networks we need certain parameters. The basic parameters for a secure system are:

Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.

Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.

Authentication: Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.

Non repudiation: Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

Anonymity: Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software. Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

III. ROUTING PROTOCOLS

Routing protocols for MANETs are usually classified into table driven/proactive protocols, on-demand/reactive protocols, and hybrid protocols based on how routing information is acquired and maintained by mobile nodes. Table driven/proactive protocols use a proactive routing scheme, in which every network node maintains consistent up-to-date routing information from each node to all other nodes in the network. On-demand/reactive protocols are based on a reactive routing scheme, in which at least one route is established only when needed. A hybrid routing protocol is a combination of proactive and reactive schemes with the aim of exploiting the advantages of both types of protocols. Another classification into uniform and non-uniform routing protocols for MANETs is based on the network node roles in a routing scheme. In a uniform routing protocol all network nodes have the same role, importance and functionality. In a non-uniform routing protocol some network nodes carry out distinct management and/or routing functions. A uniform routing protocols is either reactive or proactive, while different classification schemes have been proposed for non-uniform routing protocol In this section some relevant reactive, proactive, and hybrid routing protocols for MANETs are presented.

Typical table driven protocols are highly dynamic Destination-Sequenced Distance Vector Routing (DSDV) and Optimized Link State Routing (OLSR).Table driven routing protocols have a low route acquisition delay because every node always has a fresh route to all other nodes in the network. However, the storage, bandwidth, and power requirements are high since each node must keep its routing table up to date (with route information to all other nodes) which mandates periodic routing message exchanges.

On-demand protocols incur a much lower load on the network, compared to table driven, since each node does not need to constantly keep their

routing tables up-to-date. However, route acquisition delay is high since routing messages must be exchanged every time before communication is possible over a new route. Two prominent MANET routing protocols, based on reactive routing schemes, are Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR), which will now be respectively considered.

In AODV, when a node wants to communicate with another, the source node floods the network with route request (RREQ) messages. If a node that receives a RREQ packet is not the destination or doesn't have a fresh route to the destination it creates a reverse route to the source (a route back to source with the node from where the RREQ came from as next hop). If the receiver of a RREQ is the destination node, it sends a route reply (RREP) message back to the source as a unicast packet over the route it received the RREQ. The destination node only sends a RREP to the first RREQ message it receives. Every node receiving a RREP also creates a route to the destination in the routing table. As a result, when the RREP reaches the source, all nodes in the shortest route path will have a route both to the source and destination.

As with AODV, DSR floods the network with route request messages as a result of route discovery initiation. However, compared with AODV, the destination node returns a route reply for each copy of route request message it receives. As a result, the source node will know more than one route to the destination node upon reception of all route replies. The addresses of all nodes through which both route request and route reply messages have traversed are added to the routing message headers, so a node knows not only the hop count values of all routes to a destination, but also all the intermediate nodes. Based on hop count and other route information, the source node finally selects the route with the lowest latency. Each data packet carries, in its header, the complete ordered list of intermediate nodes through which a packet is to be transmitted.

DSR has lower network overheads compared with AODV, mainly due to the multiple storage and source routing features. If a link fails, the source node does not need to reinitiate route discovery, as in AODV. Instead it selects another route from its routing table. Since the route information is included in all data packets, other nodes

forwarding or overhearing any data packet can cache the routing information for future use, which also eliminates the need for route discovery if the route is still fresh.

A proactive scheme is used to discover routes to nearby nodes and reactive schemes are used to discover long distance nodes. An example of a hybrid routing protocol is Zone Routing Protocol (ZRP). ZRP is also called a hierarchical routing protocol where the network can be grouped in clusters, trees, or zones where one node is chosen to be a leader that manages that particular routing area.

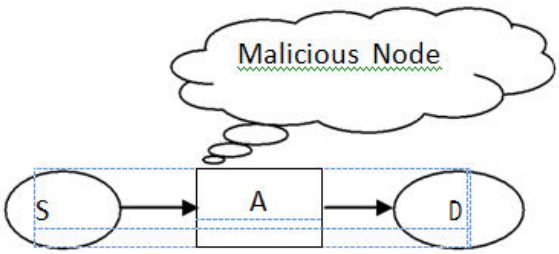
Hybrid protocols provide a lower route acquisition delay than reactive protocols and a lower overhead than proactive protocols. These protocols, however, are not suitable for highly dynamic MANET environments since in such network conditions it is simply infeasible to delegate roles to nodes and divide the network into zones.

IV. IMPERSONATION ATTACK

This type of attack is also called spoofing attacks in which a malicious node uses IP address of another node in outgoing routing packets. The aims of impersonation attacks to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key private key or even password of the nodes. A faulty node or an adversary may preset multiple identities to a peer to peer network in order to appear and function as distinct node. By becoming part of the peer to peer network the adversary may then overhear communication.

The introduction of impersonation attack in any network there is a reduction of throughput in the network. Packet delivery ratio also drops and there is an increases checksum error and packet loss ratio. in cryptography and computer security is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle). A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other — it is an attack on mutual authentication. So it is very important for any network to detect the impersonation nodes and isolate them from the network for the proper and smooth functioning of MANET.



In above figure S is the source and D is destination and A is intermediate node. Another node that is malicious node replaced its identity with intermediate node and hides its actual identity with other nodes. So when source send any message to other nodes within the network then that malicious node also get that massage and misused all the information Impersonation attack is main cause of colluding attack in which compromised node injected malicious node in to the network and make number of replicated copy of malicious node for doing future attacks in overall network. Colluding attack consist of mainly two phases:-

1) Node injection attack
2) Node Replication attack

V. PROTOCOLS TO BE FOLLOW

TAODV (Trusted AODV): In TOADV route selection is based on quantitative route trust and node trust values. Route trust from a source node to a destination node is define as the difference between the number of packets sent from source node and the number of related packet received by the destination node. Route trust is thus 0 for a perfect route. For calculation of node trust each

node monitors the behavior of all neighbor nodes by counting both successes and failures of event such as control packet received and drops.

ARAN (Authenticated Routing ad hoc network):

The purpose of the ARAN protocol is to detect and protect malicious action by third parties; it provided authentication message integrity and non repudiation.

ZRP (Zone Routing Protocol): ZRP is also called a hierarchical routing protocol where the network can be grouped in clusters, tree or zones where on node is chosen to be a leader that manages that particular routing area.

VI. CONCLUSION

Security is one of the biggest issues in mobile ad hoc network. In these paper we have discuss three of the MANET routing protocols, TAODV, ARAN and SRP. We briefly discuss one security problem in MANET i.e. impersonation attack. Finally we made a study of these three protocols as a countermeasure for impersonation attack in MANET. These secure architecture promise better and secure routing in mobile ad hoc network.

REFERENCES

[1] Farah Kandah, Yashaswi Singh, Chonggang Wang, Colluding Injected Attack in Mobile Ad-hoc Networks, published in IEEE INFOCOM 2011 Workshop on M2MCN-2011, , pp. 235−240, Apr. 2005 / | [2] Latha Tamilselvan and sankaranarayann,Tamilnadu ,Preventing Impersonation Attacks in MANET, , pp. | 118−123 march. 2007. | [3] S.Gopinath Assistant Professor Department of ECE, Muthayammal Engineering College,Rasipuram, The Modified Routing Protocol for Defending against Attacks in MANET Ad Hoc and Wireless Networks, pp. 1-5, jan. 2012