ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

An Insight into Network Layer Attacks in Mobile Adhoc Networks

S.kanmani[1], k.karthick[2], s.preetha[3]
Department of Computer Science and Engineering, Kongunadu College of Engineering and Technology, Trichy

Abstract: In this paper, we discuss about different security issues in the mobile networks. A MANET consists of mobile platforms, known as nodes, which are free to move at any speed in any direction and establish themselves randomly. The nodes in the network function as routers, clients, and servers. In MANET, all the nodes are actively discovered the topology and the message is transmitted to the destination over multiple-hops. The pervasive and practical aspects of wireless mobile ad hoc networks (MANET) made them very general as well. This created the need for securing MANET to provide users with authentic communications, secure and robust information exchanges and efficient security mechanisms. Finally we survey the current security solution for the mobile ad hoc networks.

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET), is a self-organizing, substructure less, multi-hop network. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth constrained wireless links. Each device in a MANET is free to move freely in any direction, and will therefore change its links to other devices regularly. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

A mobile ad-hoc network (MANET) consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their message, which efficiently builds connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts.
The mobility and autonomy introduces a dynamic topology of the networks not only because end-hosts are transient but also because intermediate hosts on a communication path are transient.

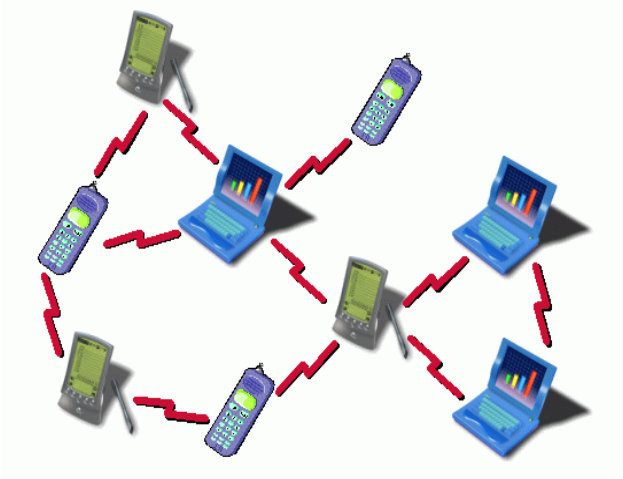

Fig 1: Mobile Adhoc Network

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

A. Characteristics of MANETs

A MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)—here in simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network.

MANET nodes are equipped with wireless transmitters and receivers using antennas which may be Omni directional (broadcast), highly- directional (point-to-point), possibly steer able, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the .nodes move or adjust their transmission and reception parameters.
MANETs have several salient characteristics:
1) Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology--which is typically multihop--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.
2) Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communication after accounting for the effects of multiple access, fading, noise, and interference conditions etc.--is often much less than a radio's maximum transmission rate. One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking applications rise.
3) Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.
4) Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

II. SECURE BOUNDARIES

Secure boundaries make the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can expose the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service.

2.1.1. Availability

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service.

2.1.2. Integrity

Integrity guarantees the identity of the messages when they are transmitted.

2.1.3. Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

2.1.4. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators [4]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

2.1.5. Nonrepudiation

Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

2.1.6. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

2.1.7. Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

III. TYPES OF ATTACKS IN MOBILE AD HOC NETWORKS

There are kinds of attacks in the mobile ad hoc networks. MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. Black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET).

A. Black Hole Attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created.. The method how malicious node fits in the data routes varies. Fig. 2 shows how black hole problem arises, here node “A” want to send data packets to node “D” and initiate the route discovery process. So if node “C” is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node “A” before any other node.

In this way node “A” will think that this is the active route and thus active route discovery is complete. Node “A” will ignore all other replies and will start seeding data packets to node “C”. In this way all the data packet will be lost consumed or lost.

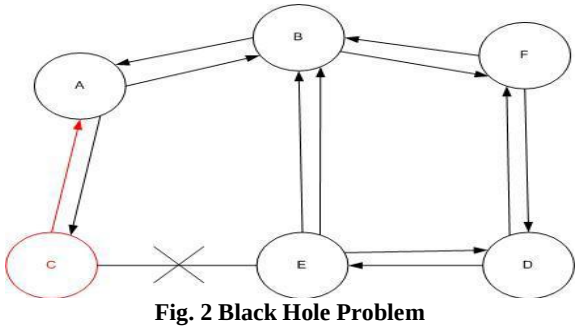

Fig. 2 Black Hole Problem

B. Black hole attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

1. Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself 20 an active data route element.At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

2. External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.

External black hole attack can be summarized in following points:

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.

C. Black hole attack in OLSR

In OLSR black hole attack, a malicious node forcefully selects itself as MPR which is discussed in chapter 3.Malicious node keep its willingness field to Will always constantly in its HELLO message. So in this case, neighbors of malicious node will always select it as MPR. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack. The effect of this attack is much vulnerable when more than one malicious node is present near the sender and destination nodes.

REPLICATION ATTACK

Replication attack where one or more nodes illegally claim an identity of legitimate node and replicated in whole MANET network as shown Figure 1. Reason for choosing this attack is that it can form the basic variety attacks such as Sybil attack, routing attacks and link layer attacks etc. also called as denial of service attacks which affects availability of network.

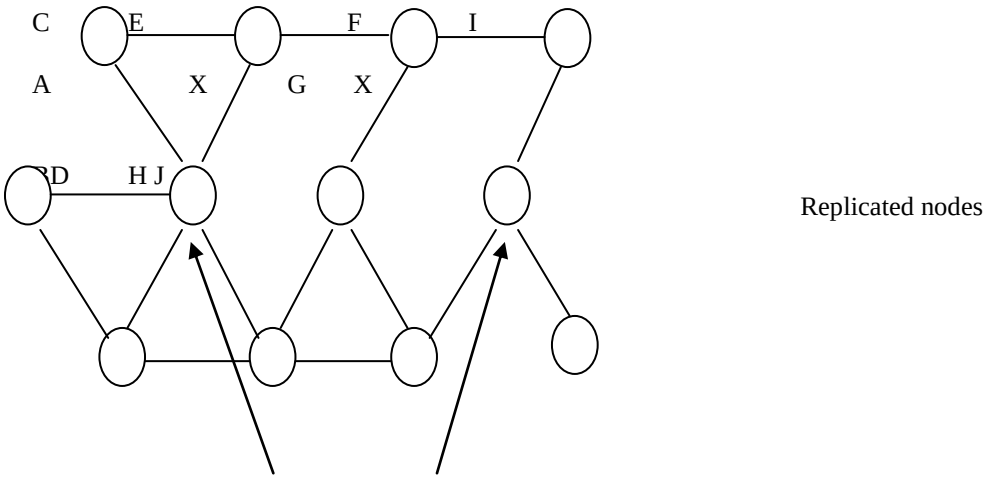

Fig. 3 Replication Attack

The detection of node replication attacks in a Mobile network is therefore a fundamental Problem. A few centralized and distributed solutions have recently been proposed. However, these solutions are not satisfactory. First, they are energy and me drawback for any protocol that is to be used in resource constrained environment such as a mobile network.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

V. DENIAL OF SERVICE ATTACK

In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots. (See botnet) DoS (Denial of Service) attacks are sent by one person or system.

VI. PACKET DROP ATTACK

In computer networking, a packet drop attack or black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent. The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every *n* packets or every *t* seconds, or a randomly selected portion of the packets. This is rather called a **gray hole attack**. If the malicious router attempts to drop all packets that come in, the attack can actually be discovered fairly quickly through common networking tools such as trace route. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a specific time period or over every *n* packet, it is often harder to detect because some traffic still flows across the network.

VII. CONCLUSION

This shows the different security attacks that occur in the network layer and its issues. The future work will improve the security measures of these attacks and provide secure data transfer.

REFERENCES

[1] Wenjia Li and Anupam Joshi, 'Security Issues in Mobile Ad Hoc Networks-A Survey'.

[2] Arbor Networks (2012), 'Top Security Concerns and Threats Facing Today's Mobile Network Operators'.

[3] Sonia Boora, Yogesh Kumar, Bhawna Kochar(2011),' A Survey on Security Issues in Mobile Ad-hoc Networks' Vol. 11, Issue 02.

[4] V. Manjulaand Dr.C.Chellappan (2011), 'Replication Attack Mitigations for Static and Mobile WSN' Vol.3.

[5] Bo Sun Yong Guan Jian Chen Udo W. Pooch, 'Detecting Black-hole Attack in Mobile Ad Hoc Networks'.

[6] Debdutta Barman Roy, Rituparna Chaki, 'Detection of Denial of Service Attack Due to Selfish Node in MANET by Mobile Agent'.

[7] Preeti Kamra, TanuPreet Singh, Dr. R.K Singh, 'Preventing Black hole Attacks in Mobile adhoc Networks: A Review '.

[8] Irshad Ullah, Shoaib Ur Rehman, 'Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols'.

[9] Mieso K. Denko, 'Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme'.

[10] Husain. Shahnawa, Gupta S.C, Chand Mukesh, 'Denial of Service Attack in AODV & Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network'.

[11] Michael Cooney,' 10 common mobile security problems to attack'.

[12] Sweta Gupta, Deepshikha Patel, Vijay K. Chaudhari , 'a Case Study: Security Issues In Mobile Ad Hoc Network'.

[13] Kuldeep Sharma, Neha Khandelwal, Prabhakar. M, 'An Overview Of security Problems in MANET'.

[14] Venkatesan Balakrishnan, Vijay Varadharajan, UdayaKiran Tupakula, 'Fellowship: Defense against Flooding and Packet Drop Attacks in MANET'.