A Study on Network Security attacks on ad hoc wireless networks

Dr. R. Madhanmohan
Associate Professor, Department of Computer Science and Engineering, Annamalai University, Annamalai nagar, India

***Abstract*- Attacks on ad hoc wireless networks can be classified into two broad categories, namely, passive and active attacks. A passive attack does not disrupt the operation of the network; the adversary snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an adversary is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of overcoming such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard**

INTRODUCTION

Designing a foolproof security protocol for ad hoc wireless is a very challenging task. This is mainly because of certain unique characteristics of ad hoc wireless networks, namely, shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among nodes, limited availability of resources, and physical vulnerability. An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. Active attacks can be classified further into two categories, namely, external and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are from compromised nodes that are actually part of the network. Since the adversaries are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks. A firewall is used to separate a local network from the outside world. It is a software which works closely with a router program and filters all packets entering the network to determine whether or not to forward those packets toward their intended destinations. A firewall protects the resources of a private network from malicious intruders on foreign networks such as the Internet. In an ad hoc wireless network, the firewall software could be installed on each node on the network.

CLASSIFICATION OF NETWORK ATTACKS

The classification of the different types of attacks possible in ad hoc wireless networks. The following diagram describe the various attacks.

Figure.1. Classification of Network Attacks

WORMHOLE ATTACK

In this attack, an attacker receives packets at one location in the network and tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network [1]. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through a single long-range wireless link or even through a wired link between the two colluding attackers. Due

to the broadcast nature of the radio channel, the attacker can create a wormhole even for packets not addressed to itself. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network. If proper mechanisms are not employed to defend the network against wormhole attacks, most of the existing routing protocols for ad hoc wireless networks may fail to find valid routes.

BLACKHOLE ATTACK

In this attack, a malicious node falsely advertises good paths (e.g., shortest path or most stable path) to the destination node during the path-finding process (in on-demand routing protocols) or in the route update messages (in table-driven routing protocols). The intention of the malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node concerned.

BYZANTINE ATTACK

Here, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, routing packets on non-optimal paths, and selectively dropping packets [2]. Byzantine failures are hard to detect. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be exhibiting Byzantine behavior.

INFORMATION DISCLOSURE

A compromised node may leak confidential or important information to unauthorized nodes in the network. Such information may include information regarding the network topology, geographic location of nodes, or optimal routes to authorized nodes in the network.

RESOURCE CONSUMPTION ATTACK

In this attack, a malicious node tries to consume/waste away resources of other nodes present in the network. The resources that are targeted are battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks. The attacks could be in the form of unnecessary requests for routes, very frequent generation of beacon packets, or forwarding f stale packets to nodes. Using up the battery power of another node by keeping that node always busy by continuously pumping packets to that node is known as a sleep deprivation attack.

Routing attacks: There are several types attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. In what follows, the various attacks on the routing protocol are described briefly.

Routing table overflow: In this type of attack, an adversary node advertises routes to non-existent nodes, to the authorized nodes present in the network. The main objective of such an attack is to cause an overflow of the routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes. Proactive routing protocols are more vulnerable to this attack compared to reactive routing protocols.

Routing table poisoning: Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes. Routing table poisoning may result in sub-optimal routing, congestion in portions of the network, or even make some parts of the network inaccessible.

Packet replication: In this attack, an adversary node replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

Route cache poisoning: In the case of on-demand routing protocols (such as the AODV protocol [3]), each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past. Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar objectives.

Rushing attack: On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack [4]. An adversary node which receives a RouteRequestpacket from the source node floods the packet quickly throughout the network before other nodes which also receive the same RouteRequest packet can react. Nodes that receive the legitimateRouteRequest packets assume those packets to be duplicates of the packet already received through the adversary node and hence discard those packets. Any route discovered by the source node would contain the adversary node as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the adversary node. It is extremely difficult to detect such attacks in ad hoc wireless networks.

TRANSPORT LAYER ATTACKS

This section discusses an attack which is specific to the transport layer in the network protocol stack.

Session hijacking: Here, an adversary takes control over a session between two nodes. Since most authentication processes are carried out only at the start of a session, once the session between two nodes gets established, the adversary node masquerades as one of the end nodes of the session and hijacks the session.

APPLICATION LAYER ATTACKS

This section briefly describes a security flaw associated with the application layer in the network protocol stack.

A. Repudiation

In simple terms, repudiation refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication. As mentioned in Section 9.8, non-repudiation is one of the important requirements for a security protocol in any communication network.

Multi-layer Attacks

Multi-layer attacks are those that could occur in any layer of the network protocol stack. Denial of service and impersonation are some of the common multi-layer attacks. This section discusses some of the multi-layer attacks in ad hoc wireless networks.

A. Denial of Service

In this type of attack, an adversary attempts to prevent legitimate and authorized users of services offered by the network from accessing those services. A denial of service (DoS) attack can be carried out in many ways. The classic way is to flood packets to any centralized resource (e.g., an access point) used in the network so that the resource is no longer available to nodes in the network, resulting in the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. Due to the unique characteristics of ad hoc wireless networks, there exist many more ways to launch a DoS attack in such a network, which would not be possible in wired networks. DoS attacks can be launched against any layer in the network protocol stack [20]. On the physical and MAC layers, an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could participate in a session but simply drop a certain number of packets, which may lead to degradation in the QoS being offered by the network. On the higher layers, an adversary could bring down critical services such as the key management service (key management will be described in detail in the next section). Some of the DoS attacks are described below.

Jamming

In this form of attack, the adversary initially keeps monitoring the wireless medium in order to determine the frequency at which the receiver node is receiving signals from the sender. It then transmits signals on that frequency so that error-free reception at the receiver is hindered. Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are two commonly used techniques that overcome jamming attacks.

SYN flooding: Here, an adversary sends a large number of SYN packets8 to a victim node, spoofing the return addresses of the SYN packets. On

receiving the SYN packets, the victim node sends back acknowledgment (SYN-ACK) packets to nodes whose addresses have been specified in the received SYN packets. However, the victim node would not receive any ACK packet in return. In effect, a half-open connection gets created. The victim node builds up a table/data structure for holding information regarding all pending connections. Since the maximum possible size of the table is limited, the increasing number of half-open connections results in an overflow in the table. Hence, even if a connection request comes from a legitimate node at a later point of time, because of the table overflow, the victim node would be forced to reject the call request. SYN packets are used to establish an end-to-end session between two nodes at the transport layer.

Distributed DoS attack: A more severe form of the DoS attack is the distributed DoS (DDoS) attack. In this attack, several adversaries that are distributed throughout the network collude and prevent legitimate users from accessing the services offered by the network.

Impersonation: In impersonation attacks, an adversary assumes the identity and privileges of an authorized node, either to make use of network resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the network by injecting false routing information into the network. An adversary node could masquerade as an authorized node using several methods. It could by chance guess the identity and authentication details of the authorized node (target node), or it could snoop for information regarding the identity and authentication of the target node from a previous communication, or it could circumvent or disable the authentication mechanism at the target node. A man-in-the-middle attack is another type of impersonation attack. Here, the adversary reads and possibly modifies, messages between two end nodes without letting either of them know that they have been attacked. Suppose two nodes X and Y are communicating with each other; the adversary impersonates node Y with respect to node X and impersonates node X with respect to node Y, exploiting the lack of third-party authentication of the communication between nodes X and Y.

CONCLUSION

This paper summarizes the various attacks on ad hoc wireless networks. This review dealt with the security aspect of communication in ad hoc wireless networks. The issues and challenges involved in provisioning security in ad hoc wireless networks were identified. This was followed by a layer-wise classification of the various types of attacks.

REFERENCES

[1] B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proceedings of IEEE WMCSA 2002, pp. 3-13, June 2002.

[2] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proceedings of ACM SIG-COMM 1994, pp. 234-244, August 1994. Y. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks," Proceedings of IEEE INFOCOM 2003, vol. 3, pp. 1976-1986, April 2003.

[3] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," Proceedings of the ACM Workshop on Wireless Security 2002, pp. 21-30, September 2002.

[4] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing," Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, February 1999.

[5] Y. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the ACM Workshop on Wireless Security 2003, pp. 30-40, September 2003.

[6] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, December 1999.

[7] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press,96.

[8] A. Khalili, W. A. Arbaugh, "Security of Wireless Ad hoc Networks, "http://www.cs.umd.edu /~aram/wireless/survey.pdf.

[9] N. Asokan and P. Ginzboorg, "Key-Agreement in Ad Hoc Networks," Computer Communications, vol. 23, no. 17, pp. 1627-1637, 2000.

[10] S. Capkun, L. Buttyan, and J. P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," IEEE Transactions on Mobile Computing, vol. 2, no. 1, pp. 52-64, January-March 2003.

[11] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad Hoc Routing for Wireless Networks,"Proceedings of ACM MOBIHOC 2001, pp. 299-302, October 2001.