Network security attacks Ad-hoc wireless Networks

Hiteshwer; Sanny; Ekta Sharma & Monika Chauhan
Guided By -Ms Pratibha Bharti , Dr. K.K Saini
Dronacharya Engineering College Gurgaon
kk.saini@ggnindia.dronacharya.info

Abstract-

Wireless communication is enhancing day by day. As the technology uplifts its security challenges also become more challengeable secure and safe. In this paper we have discussed the different types of attacks in Ad-hoc wireless network in its different layers. The attacks are on different layers are briefly described. These attacks are very severe as it may damage the complete data or information.

Keywords-

Ad-hoc; Wi-MAX ; WSN

Security challenges in Ad Hoc Wireless Networks

Due to the unique characteristic of the Ad-hoc wireless network, such networks are highly vulnerable to security attacks compared to wired networks or infrastructure-based wireless networks. The following sections discuss the various security requirement in ad hoc wireless network, the different types of attacks possible in such networks, and some of the solutions proposed for ensuring network security.

Network Security Requirements

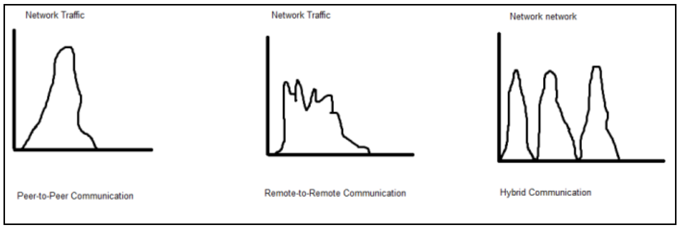
A security protocols for ad hoc wireless networks should satisfy the following requirements

1 Confidentiality: The data sent by the sender (source node) must be comprehensible only to the intended receiver (destination node).Though the intruder might get hold of the data being sent ,he/she must not be able to drive any useful information out of the data.

2 Integrity: The data sent by the source node should reach the destination node as it was sent: unaltered.

3 Availability: The network should remain operational all the time .It must be robust enough to tolerate link failures and also be capable of surving various attacks mounted on it. It should be able to provide the guaranteed services whenever an authorized user requires them.

4 Non-repudiation: Non-repudiation is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the receipt cannot deny having received the message.



Issues and Challenges in Security Provisioning

Designing a foolproof security protocol for ad hoc wireless is a very challenging task. This is mainly certain unique characteristics of ad hoc wireless-network, namely, shared broadcast, radio channel ,insecure operating environment, lack of central authority ,lack of association among nodes, Limited availability of resources, and physical vulnerability .

1 Shared broadcast radio channel: Unlike in wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc wireless network is broadcast in nature and is shared by all nodes in the network. Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network. This problem can be minimized to a certain extent by using directional antennas.

2 Insecure Operational Environment: The operating environment where Ad hoc wireless networks are used may not always be secure. One important application of such network is in battlefields. In such applications, node may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

3 Lack of central authority: In wired networks and infrastructure-based wireless networks, it would be possible to monitor the traffic on the network through certain important central points (such as routers, base stations and access points) and the implement security mechanism in such points, these mechanism cannot be applied in Ad-hoc wireless networks.

3 Lack of Association: Since these networks are dynamic in nature, a node can join or leave the network at any point of the time. If no proper authentication mechanism is used for associating nodes with a network, an intruder would be able to join into the network quite easily and carry out his/her attacks.

4 Limited resources availability: Resources such as band width , battery power, computational power (to a certain extent) are scare in Ad- hoc wireless networks. Hence it is difficult to implement complex cryptography-based security mechanisms in such networks.

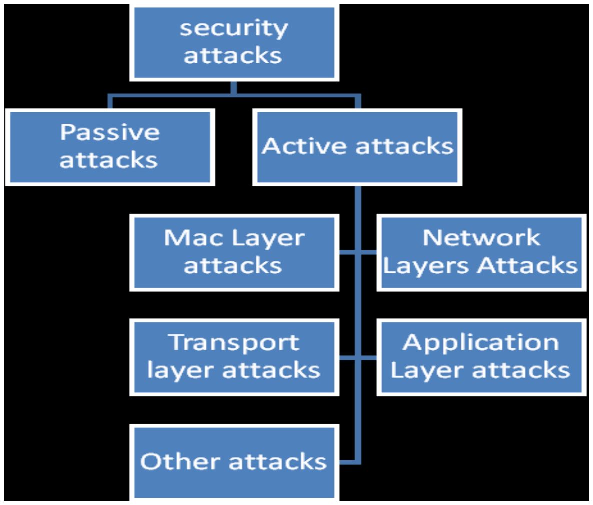
5 Physical Vulnerability: Nodes in these networks are usually compact and hand-held in nature. They could get damaged easily and are also vulnerable to theft.

Network security Attacks:

Attacks on Ad-hoc networks are classified two broad categories, namely passive attack 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 this problem is to use powerful encryption mechanism to encrypt the data being transmitted.

An active attack attempts to alter or destroy the data being exchanged in the network , thereby disrupting the normal functioning of the network. They are also further classified into internal and external attacks. External attacks are carried out by nodes that do not belong to the network . These attacks can be prevented by using standard security mechanism 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.



Network layer attacks

1 Wormhole attack: In is 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. This tunnel between two colluding attackers is referred to as wormhole.

2 Blackhole attacks ; 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 or in the route update message. 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.

3 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-optiomal paths, and selectively dropping packets. Byzantine failures are hard to detect.

4 Information attacks: 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.

5 Resource consumption attack; In this attack nodes 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.

CONCLUSION

After completing this paper we concluded that the ad-hoc wireless is a latest upcoming trend in wireless world. As we know now for transferring data must be secure and safe. We have discussed different types of attacks in Ad-hoc wireless network such as Wormhole attack, Blackhole attacks, Byzantine attack, Information attacks, Resource consumption attack. Out of these Byzantine attack is the most severe attack which is hard to detect. These attacks are so harmful that it can sometime destroys the whole data. In this attack nodes tries to consume /waste away resources of other nodes present in the network. For future work we will discuss these attacks Wi-Max, Wireless sensor Networ ,Wireless mesh network etc.

REFERERENCE

[1]. I.F. Akyildiz, X. Wang, W. Wang. Wireless Mesh Networks: a Survey . Computer Networks, Elsevier, Vol.47, No.4, 2005, pp445-487

[2]. Ping Yi, Yichuan Jiang , Yiping Zhong, Shiyong Zhang, security for mobile ad hoc networks, Acta Electronica Sinica, Vol.33, No. 5, 2005, pp893-899

[3]. Ping Yi, Yiping Zhong, Shiyong Zhang, Zhoulin Dai, Flooding Attack and Defence in Ad Hoc Networks, Journal of Systems Engineering and Electronics, Vol.17, No.2, 2006, pp410-416

[4]. Y-C Hu, A.Perrig, D.B.Johnso, Wormhole Detection in Wireless Ad Hoc Networks, Technical Report TR01- 384,Department of Computer Science, Rice University, December2001

[5]. Hongmei Deng,Wei Li and Dharma P.Agrawal, Routing Security in wireless Ad hoc Networks, IEEE Communications Magazine, pp.70-75, October 2002

[6]. Yih-Chun Hu, Adrian Perrig, and David Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, In Proceedings of the ACM Workshop on Wireless Security (WiSe 2003), September 19 2003, Westin Horton Plaza Hotel, San Diego, California, U.S.A.