Mobile Ad-Hoc Networks - Various Attacks

Krishan Kumar, Rajiv Munjal (Lecturer, CSE Deptt., B.P.R College of Engg., Gohana)
Yogesh Kumar (Sr. Lecturer, CSE Deptt., B.P.R College of Engg., Gohana)

ABSTRACT
An ad-hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Recent wireless research indicates that the wireless MANET (Mobile Ad hoc Network) presents a larger security problem than conventional wired and wireless networks.

In this paper we discuss various features of MANET due to which network is more susceptible to threats. We also analyze various attacks in MANET.

Keywords
MANET, Black hole, Gray hole, Sybil, Selfish, DoS.

1. INTRODUCTION TO AD-HOC
Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology.

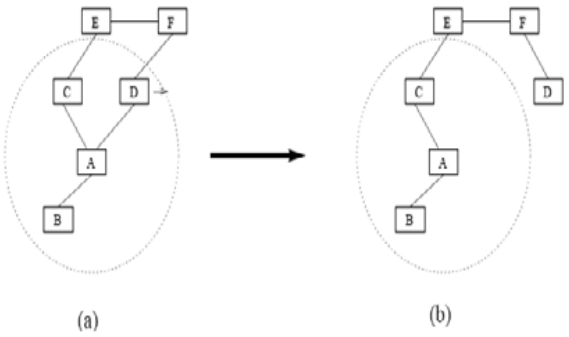

Figure 1: Topology change in ad hoc networks: nodes A, B, C, D, E, and F constitute an ad hoc network. The circle represents the radio range of node A. The network initially has the topology in (a). When node D moves out of the radio range of A, the network topology changes to the one in (b).

Figure 1 shows such an example: initially, nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken. However, the network is still connected, because A can reach D through C, E, and F. Military tactical operations are still the main application of ad hoc networks today. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

Mobile Ad hoc Network [1] is an autonomous, self-configuring system of mobile devices (laptops, smart phones, sensors, etc.) connected by wireless links. Each node operates not only as an end-system, but also as a router to forward packets. MANET does not require any fixed infrastructure, such as base stations. Therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously.

Although mobile ad hoc networks have several advantages over the traditional wired networks, on the other sides they have a unique set of challenges. Firstly, MANETs face Challenges in secure communication. For example the resource constraints on nodes in adhoc networks limit the cryptographic measures that are used for secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Secondly, mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network. Thirdly, static configuration may not be adequate for the National Conference on Advanced Computing and Communication Technology dynamically changing topology in terms of security solution. Various attacks like DoS (Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information. Finally, lack of cooperation and constrained capability is common in wireless MANET which makes anomalies hard to distinguish from normalcy. In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, and absence of central authorities, distribution cooperation and constrained capability.

This paper is organized as follows:

In Section 2 we present security issues in MANETs. Next section presents various features of MANET due to which network is more susceptible to threats. In section 4, we

describe security attacks in MANETs. We conclude in section 5.

2. SECURITY ISSUES

Security is an important issue for ad hoc networks especially for the more security sensitive applications used in military and critical networks [3, 10]. An ad hoc network can be considered secure if it holds the following attributes:

• **Availability:** Ensures that the network manages to provide all services despite denial of service attacks. A denial of service attack can be launched at any layer of an ad hoc network. On the physical and media access control layer a malicious user can employ jamming in order to interfere with signals in the physical layer. On the network layer, a malicious user can disrupt the normal operation of the routing table in various ways that are presented in a following section. Lastly, on the higher layer, a malicious user can bring down high-level services such as the key management service.

• **Confidentiality:** Ensures that certain information is never disclosed to unauthorized users. This attribute is mostly desired when transmitting sensitive information such as military and tactical data. Routing information must also be confidential in some cases when the user's location must be kept secret.

• **Integrity:** Guarantees that the message that is transmitted reaches its destination without being changed or corrupted in any way. .Message corruption can be caused by either a malicious attack on the network or because of radio propagation failure.

• **Authentication:** Enables a node to be sure of the identity of the peer with which it communicates. When there is no authentication scheme a node can masquerade as some other node and gain unauthorized access to resources or sensitive information.

• **Non-repudiation:** Ensures that the originator of a message cannot refuse sending this message. This attribute is useful when trying to detect isolated compromised nodes.

• **Access and usage control:** Access control ensures that access to information is controlled by the ad hoc network. Usage control ensures that the information resource is used correctly by the authorized node having the corresponding rights.

3. SECURITY THREATS

MANETs are a unique class of wireless multi-hop network comprising of autonomous mobile nodes. This causes the network topology to be dynamically changing, which gives rise to a wide range of characteristics such as transient links, unpredictable resource availability and complex route maintenance. In addition, nodes in MANETs have limited battery life, which is expended by packet transmission and reception.

Although security threats exist in both wired and wireless networks, the inherent nature of wireless networks such as MANETs results in them being more vulnerable to attacks. In the following, we describe how some of these MANET features [2] cause the network to be more susceptible to threats.

• Nodes in MANETs do not have any central base station to coordinate the transmission and authentication of packets. Thus, the delivery of data packets from source to destination nodes in the network is dependent on the cooperation of the (intermediate) nodes in the network.

• The wireless channel in MANETs is a shared broadcast medium, where as in wired scenarios channel can be configured to provide dedicated access to any particular user group. Therefore, nodes in wireless networks are often subject to interference (whether deliberate or not) from neighboring nodes within the transmission and interference ranges.

• The wireless links that are being used offers little protection towards authentication and Confidentiality of data packets. Each transmitted packet can easily be overheard and/or intercepted by all neighboring nodes, and each node will also inevitably hear all packets that are sent from its neighbors.

• The mobility of the nodes in the network also increases the challenge of node authentication, because nodes can easily venture into and out of the network.

4. SECURITY ATTACKS

The security attacks in MANETs can be categorized as active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. Various types of attacks in MANETs are: Modification, Impersonation, Fabrication, Eavesdropping, Replay, Denial of Service, Malicious Software and Lack of Cooperation. Table 1 Shows The Security Attacks On Each Layer In MANET.

LAYER	**ATTACKS**
Application layer	Repudiation, Data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, Blackhole, Selfish Node, Gray Hole, DoS, flooding, Resource consumption
Data link layer	Traffic analysis, Monitoring, Disruption MAC (802.11), WEP

	weakness
Physical layer	Jamming, Interceptions, Eavesdropping

Table 1: Security Attacks on each layer

Due to the lack of centralized monitoring and management point, and lack of clear line of defense various attacks exists in the MANET. Some of the important attacks are as follow:

• **Gray Hole Attack (Routing Misbehavior):** Gray hole attacks [8, 11] is an active attack type, which lead to dropping of messages. The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainty.

• **Black hole Attack:** This attack is also known as sequence number attack. The black hole attack [5] involves malicious node(s) fabricating the sequence number, hence pretending to have the shortest and freshest route to the destination. The attacker forges its destination sequence number, thus pretending to have the fresh enough route information to the destination. More precisely, upon receiving the broadcasted Route Request message, the attacker creates a reply message (Route Reply) with a spoofed destination sequence number; a relatively high destination sequence number in order to be favoured against others. Once the source node receives the reply from the attacker, it routes the data traffic through the attacker. Upon receiving the data packets, the attacker normally drops them and creates a 'black hole', as the attack name implies.

• **The Sybil Attack:** The Sybil attack [6, 7] is launched by a malicious node that illegally acquires multiple identities. The malicious node is able to deceive the other nodes into thinking there are several normal nodes including itself. Figure 2 shows an example of the Sybil attack. After the malicious node Ml joins the network, it continuously registers three virtual identities V1, V2, and V3 as normal ones. As the result of it, the network believes four new nodes are joined. The network will provide any possible services to them and consume information from them. In the example, the malicious node and virtual identities send normal messages to a central node that decides whether a intrusion is launched or not, while other nodes send alert messages. Since number of alert messages is smaller than that of normal ones, the central node will decide there is no attack.

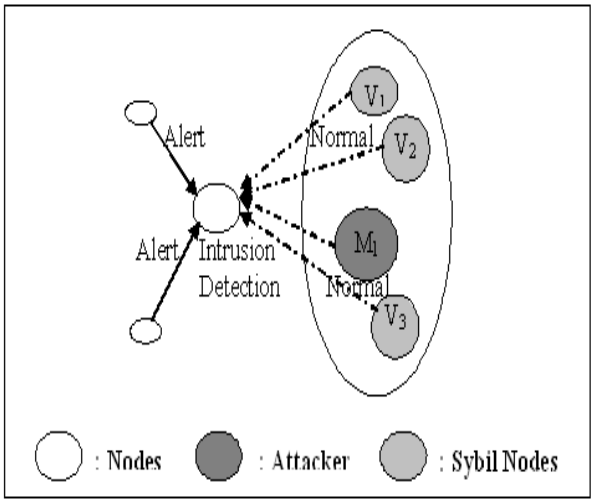

Figure 2: An example of Sybil Attack.

• **Selfish Nodes:** In this a node is not serving as a relay to other nodes which are participating in the network. This malicious node which is not participating in the network operations, use the network for its advantage to save its own resources such as power. For instance, selfish nodes do not even send any HELLO messages and drop all packets even if they are sent to it [12].

• **Denial of Service Attack (DoS):** A denial of service (DoS) attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources. A distributed denial-of-service (DDoS) attack [4, 9] is a DoS attack which relies on multiple compromised hosts in the network to attack the victim. A distributed denial of service attack is composed of four elements, as shown in Figure 3.

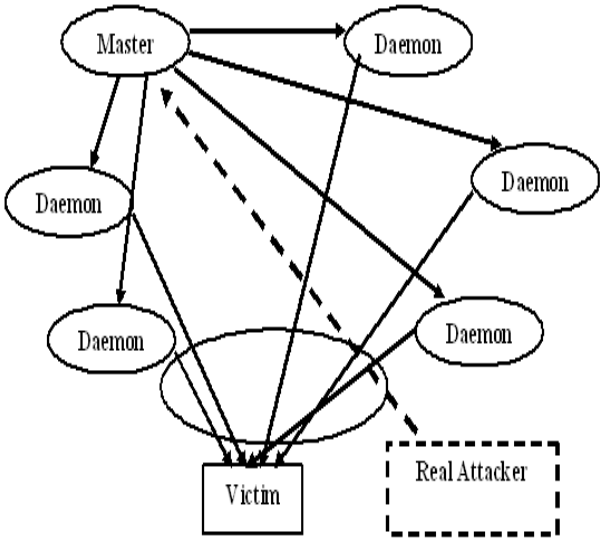

Figure 3: The four Components of DDoS Attacks.

First, it involves a victim, i.e., the target host that has been chosen to receive the brunt of the attack. Second, it involves the presence of the attack daemon agents. These are agent programs that actually conduct the attack on the target victim. Attack daemons are usually deployed in host computers. These daemons affect both the target and the host computers. The third component of a distributed denial of service attack is the control master program. Its task is to coordinate the attack. Finally, there is the real attacker, the mastermind behind the attack. By using a control master program, the real attacker can stay behind the scenes of the attack. The following steps take place during a distributed attack:

• The real attacker sends an "execute" message to the control master program.

• The control master program receives the "execute" message and propagates the command to the attack daemons under its control.

• Upon receiving the attack command, the attack daemons begin the attack on the victim.

5. CONCLUSION

In this paper, we have analyzed the security threats an ad hoc network faces and presented the security objectives that need to be achieved. On one hand, the security-sensitive applications of ad hoc networks require high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks.

6. REFERENCES

1] Han L, "Wireless Ad hoc Network", October 8, 2004.

[2] Kamanshis Biswas and Md. Liakat Ali, "Security Threats in Mobile Ad Hoc Network", Master Thesis, Thesis no: MCS-2007:07, March 22, 2007.

[3] Vesa Kärpijoki; Security in Ad Hoc Networks; Helsinki University of Technology; HUT TML 2000

.[4] Felix Lau, Stuart H. Rubin, Michael H. Smith and Ljiljana TrajkoviC; Distributed Denial of Service Attacks; 2275-2280/2004 IEEE.

[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[6] J. Douceur, "The Sybil attack", Peer-to-Peer Systems: First International Workshop (ITPTS 2002), Lecture Notes in Computer Science 2429, Springer-Verlag, March 2002, pp. 251-260

.[7] Sarosh Hashmi, John Brooke, "Authentication Mechanisms for Mobile Ad-hoc Networks and Resistance to Sybil Attack", Proceedings of The Second International Conference on Emerging Security Information, Systems and Technologies, 2008.

[8] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", Proceedings of 10th

[9] Stephen M. Specht and Ruby B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures", Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543- 550, September 2004.

[10] P. Michiardi and R. Molva, "Ad hoc Networks Security", IEEE Press Wiley, New York, 2003.

[11] Gao Xiaopeng Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks",Proceedings of International Conference on Network and Parallel Computing – Workshops, July 2007.[12] M. Just, E. Kranakis, and T. Wan,. "Resisting Malicious Packet Dropping. In Wireless Ad Hoc Networks", In Proceedings of ADHOC-NOW, Oct. 2003.