Security Attacks: Vulnerability in Ad Hoc Networks

Ishu Gupta[1], Harsh Sadawarti[2], S.N. Panda[3]
[1]*Department of Computer Science & Engineering, RIMT-MAEC, Mandi Gobindgarh (Punjab), India*
[2]*Department of Computer Science & Engineering, RIMT-IET, Mandi Gobindgarh (Punjab), India*
[3]*Department of Computer Science, RIMT, Mandi Gobindgarh (Punjab), India*

***Abstract*- Ad hoc networks are a new paradigm of wireless communication for mobile hosts, Ad hoc. They are usually set up in situations of emergency, for temporary operations or simply if there are no resources to set up elaborate networks. There are various challenges that are faced in the Ad hoc environment. The wireless nature of communication and lack of any security infrastructure raise several security problems. This paper outlines vulnerabilities to security attacks which are an important challenge in design of theses networks and a detailed classification of threats against ad hoc networks. Threats exist to ad hoc networks both from external nodes unauthorized to participate in the mobile ad hoc networks, and from internal nodes, which have the authorization credentials to participate in the mobile ad hoc network. Any protocols and simulations to test the properties should include the capability to handle each type of node and attack.**

***Keywords*—Security Attacks, Ad Hoc Networks, Vulnerabilities to networks, Security, Attack types.**

1. INTRODUCTION

1.1 Introduction to Ad hoc networks

An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other. Ad hoc networks, which cover a variety of network paradigms for specific purposes, such as mobile ad hoc networks, sensor networks, vehicular networks, underwater networks, underground networks, personal area networks, and home networks, promise a broad range of applications in civilian, commercial, and military areas [7]. These networks are ideal in situations where installing an infrastructure is not possible because it is too expensive or too vulnerable, the network is too transient, or the infrastructure was destroyed. A military base station on a battlefield is an example of vulnerable infrastructure. 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.

1.2 Security Requirements

Security is an important issue for ad hoc networks particularly for security-sensitive applications. To secure a network, we consider the following aspects [4]:

Availability ensures the survivability of network services despite denial of service attack which could be launched at any layer of ad hoc networks. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services.

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information such as strategic or tactical military information, requires confidentiality. Leakage to such information to enemies could have devastating consequences. Routing information must also remain confidential.

Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures such as radio propagation impairment.

Authentication enables a node to ensure the peer node with which it is communicating. Without authentication, an adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and inferring with the operation of other nodes.

Nonrepudiation ensures that the origin of a message cannot deny having sent the message. It is useful for isolation and detection of compromised nodes. When node A receives an erroneous message from need B, Nonrepudiation allows A to accuse B using this message and to convince other nodes that B is compromised [1].

Accountability-This will be required so that any actions affecting security can be selectively logged and protected, allowing for appropriate reaction against attacks.

Dependability and reliability-One of the most common applications for ad hoc networks is in emergency situations when the use of wired infrastructure is infeasible. Hence, routing must be reliable, and emergency procedures may be required [4]. For example, if a routing table becomes full due to memory constraints, a reactive protocol should still be able to find an emergency route to a given destination.

2. ATTACK CLASSIFICATION

Attacks on networks come in many varieties and they can be classified into groups in a different way [5]:

(1) Passive attacks which involve only eavesdropping on the data that is being communicated in the network. Examples of passive attacks include covert channels, traffic analysis, sniffing to compromised keys.
(2) Active attacks which involve specific actions performed by adversaries, for instance, the replication, modification, and deletion of exchanged data among the nodes.

One way to diversify attacks is to classify them by their source.

External attacks are committed by parties that are not legally part of the network. External attackers are not necessarily disconnected from the network, though. The targeted network might be a self-contained entity that is linked to other networks using that are using the same infrastructure or communication technology. This would make it possible to initiate attacks without even being authenticated in the targeted network. On the other hand, it would also be possible to jam the communication of the entire ad hoc network of a company from the parking lot in front of the company building [5].

Internal attacks are sourced from inside a particular network. A compromised node whose actions compromise the security of the whole ad hoc network with access to all other nodes within its range poses a high threat to the functional efficiency of the whole collective. Attacks can be executed more efficiently, since internal attacks are not as easy to prevent as external ones.

3. ATTACK TYPES

We will discuss some important attacks that could be launched against the ad hoc network as well as individual nodes.

3.1 Denial of service (DoS)

The most common threats lead to a denial of service attack, which in turn induces the ‘sleep deprivation torture’ attack. Malicious nodes cause other nodes to exhaust their resources by getting other mobile nodes to do unnecessary processing using correct or incorrect information. Those nodes which use up their power resources will eventually become unable to operate under normal circumstances. A sleep deprivation torture attack is particularly viable for ad hoc networks, due to the power constraints likely for mobile nodes [6]. There are a variety of ways to achieve the objective of this denial of service attack. For example, in proactive protocols a malicious node could advertise topology updates with lots of false routes and addresses so that the route table calculation will take more time and resource. This is also an attack on network integrity. Some of the examples of Denial of Service attacks are:

* SYN flooding- In this type of DoS attack, the adversary sends a large number of SYN packets to a victim node, spoofing the return address of the SYN packets. On receiving the SYN packets, the victim node sends back acknowledgement (SYNACK) packets to nodes whose addresses have been specified in received SYN packets and waits for ACKs from the senders, which never arrive. If sufficient connections are established among multiple senders and the victim, it is likely that its memory resources may be exhausted (table overflow), owing to the currently open connections and the victim cannot now accept a new legitimate request for a connection.

* Distributed denial of service attack-This type of attack is launched by a group of compromised nodes who are part of the same network and who collude together to bring the network down or seriously affect its operation.

* Jamming-This type of DoS attack is initiated by a malicious node after determining the frequency of communication used by the receiver and using the same frequency to send data to the receiver thereby interfering with its operation. Frequency hopping is an established technique to get around jamming attacks [10].

3.2 Impersonation

Impersonation attacks are also called spoofing attacks. The attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes. Usually this would be one of the first steps to intrude a network with the aim of carrying out further attacks to disrupt operation. Depending on the access level of the impersonated node, the intruder may even be able to reconfigure the network so that other attackers can (more) easily join or he could remove security measures to allow subsequent attempts of invasion. A compromised node may also have access to encryption keys and authentification information. Two well known impersonation attacks are Sybil and Trust [1].

∗ Sybil attack

In the Sybil attack a malicious node behaves as if it were a larger number of nodes by impersonating other nodes or simply by claiming false identities. In the worst case, a Sybil attacker may generate an arbitrary number of additional node identities, using only one physical device. The additional identities that the node acquires are called Sybil nodes. There are three possible dimensions in which a Sybil attack can be launched.

∗ Trust attack

A trust attack is another type of impersonation attack [3]. In simple security applications, in which the goal is to protect a given message or an item from passive or active attacks, user trust can be established as an authentication procedure between a system and a user. But there are applications which require multiple security levels. For example military applications have information that is categorized as unclassified (U), confidential (C), secret (S), or top secret (TS), and each type of information can require a set of authentication rules that have some sort of hierarchical structure, called a trust hierarchy.

A trust hierarchy is basically an explicit representation of trust levels that reflects organizational privileges. It associates a number with each privilege level, to reflect the security, importance, or capabilities of the mobile node and also of the paths.

3.3 Passive eavesdropping

This can allow unauthorised principals to listen to and receive messages including routing updates [2]. An unauthorised node will be able to gather data that can be used to infer the network topology and other information such as the identities of the more heavily used nodes which forward or receive data. Hence, techniques may be needed to hide such information. Eavesdropping is also a threat to location privacy. Passive eavesdropping also allows unauthorised nodes to discover that a network actually exists within a geographical location, by just detecting that there is a signal present.

3.4 Sinkhole attacks

By carrying out a sinkhole attack, a compromised node tries to attract the data to it from all neighboring nodes. Since this would give access to all data to this node, the sinkhole attack is the basis for many other attacks likes eavesdropping or data alteration. Sinkhole attacks make use of the loopholes in routing algorithms of ad hoc networks and present themselves to adjacent nodes as the most attractive partner in a multihop route. Even though by definition nodes on the network layer of an ad hoc network are equal, sinkhole attacks might be very effective on application level, where nodes may have different roles.

3.5 Wormholes

Closely related to the sinkhole attack is the wormhole attack [9]. In a wormhole attack, a malicious node uses a path outside the network to route messages to another compromised node at some other location in the net (just like a “conventional” wormhole presents a shortcut between two normally distant locations in space). Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Interestingly, a wormhole itself does not have to be harmful; for it usually lowers the time it takes for a package to reach its destination. But even this behavior could already damage the operation, since wormholes fake a route that is shorter than the according one within the network; this can confuse routing mechanisms which rely on the knowledge about distance between nodes. Wormholes are especially dangerous because they can do damage without even knowing the protocols used or the services offered in the network. In a wireless network it is relatively easy to eavesdrop on the communication and forward the packets to other known nodes before the packet sent within the network arrives [9].

3.6 Sleep deprivation

Usually, this attack is practical only in ad hoc networks where battery life is a critical parameter. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes, or by forwarding unnecessary packets to the node using, for example, a black hole attack. This attack is especially suitable against devices that do not offer any services to the network or offer services only to those who have some special credentials. Regardless of the properties of the services, a node must participate in the routing process unless it is willing to risk becoming unreachable to the network.

3.7 Black hole

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In a flooding-based protocol, the attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply consisting of an extremely short route [8]. If the malicious reply reaches the requesting node before the reply from the actual node, a forged route gets created once the malicious device has been able to insert itself between the communicating nodes; it is able to do anything with the packets passing between them. It can choose to drop the packets to perform a denial of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

4. CONCLUSION AND FUTURE WORK

Ad hoc networks present various threats due to their very different properties. These properties open up very different security risks from conventional wired networks, and each of them affects how security is provided and maintained. In Ad hoc networks attacks may vary depend on (1) which environment the attacks are launched, (2) what communication layer the attacks are targeting, and (3) what level of ad hoc network mechanisms are targeted. One can also see that there are several attack characteristics that must be considered in designing any security measure for the ad hoc network. Many attacks are only possible or only effective, if the malicious party is a participant of the network, so it is highly important to implement secure mechanisms to authenticate entities entering the network.

In a future work, various security solutions to secure routing protocols will be investigated and classified. The investigation will include various techniques that might be employed in protecting, detecting, and responding to the attacks against the routing messages. Some attacks are possible in the ad hoc networks because most of the current ad hoc routing protocols do not authenticate the routing packets. As a result, malicious nodes might exploit this loophole to masquerade as another node by modifying the contents of the packets.

REFERENCES

[1] Adam Burg, “Ad hoc network specific attacks” in Seminar on Ad hoc Networking: concepts, applications and security at *Technische Universitat Munchen,* 2003.

[2] Hammons Jr. A. Roger, Zhang, Qinqing and Haberman, Brian, “An Eavesdrop Vulnerability Analysis of Random Network Coding over Wireless Ad-Hoc Networks” in *IEEE Wireless Communications and Networking Conference (WCNC),* pp. 1-6, April 2010.

[3] Lei Guang, Assi, C., “Vulnerabilities of ad hoc network routing protocols to MAC misbehavior” in IEEE International Conference on *Wireless And Mobile Computing, Networking And Communications,(WiMob'2005),* pp. 146 - 153 Vol. 3, Aug. 22-24, 2005.

[4] L. Zhou and Z.J. Haas, "Securing Ad hoc Networks", *IEEE Networks*, volume 13, issue 6, pp. 24-30, Nov/Dec 1999.

[5] Mishra R., Sharma S. and Agrawal R., “Vulnerabilities and security for ad-hoc networks” in International Conference on *Networking and Information Technology (ICNIT),* pp. 192 - 196, June 2010.

[6] Subhadrabandhu, S. Sarkar, and F. Anjum. "A framework for misuse detection in ad hoc networks-Part I", *IEEE Journal on Selected Areas in Communications,* vo1.24, no. 2, pp. 274-89, Feb. 2006.

[7] Xiaoyan Hong, Nam Nguyen, Shaorong Liu and Ying Teng, “Dynamic Group Support in LANMAR Routing Ad Hoc Networks” in 4th *International Workshop on Mobile and Wireless Communications Network 2002* , pp. 304 – 308, 2002.

[8] Yunnan Wu , Chou, P.A. and Sun-Yuan Kung, “Minimum-energy multicast in mobile ad hoc networks using network coding “in *IEEE Information Theory Workshop,* pp. 304 – 309, 24-29 Oct. 2004.

[9] Y. Hu, A. Perrig, and D. Johnson. Packet leashes, “A defense against wormhole attacks in wireless ad hoc networks” In Proceedings of the *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies,* April 1-3, 2003, San Fransisco, CA, USA. Institute of Electrical and Electronics Engineers, IEEE Press, 2003.

[10] Z. Haas and M. Pearlman. ZRP, “A hybrid framework for routing in ad hoc networks” In C. Perkins, editor, *Ad Hoc Networking,* chapter 7, pages 221–253. Addison-Wesley, 2001.