I. J. Computer Network and Information Security, 2012, 6, 26-32
Published Online June 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.06.04

Security Aspects and Challenges in Mobile Adhoc Networks

G. Jose Moses, Prof.P.Suresh Varma, N.Supriya, G.NagaSatish
Department of Computer Science, Adikavi Nannaya University, Rajahmundry,A.P.INDIA
josemoses@gmail.com, vermaps@yahoo.com, nsupriyacse@gmail.com, gantinagasatish@gmail.com.

Abstract— The traditional notion of a Adhoc wireless network is one in which there are a few Base Stations or Access Points and a number of Mobile Stations or Nodes. Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. The Adhoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium and network topology. These challenges clearly make a case for building multifence security solutions that achieve both road protection and desirable network performance. The general security objectives like authentication, confidentiality, integrity, availability and non-repudiation, the ad hoc routing protocols should also address location confidentiality, cooperation fairness and absence of traffic diversion. In this paper we attempt to analyze Challenges, Overview of Security, attacks, threats faced by the Adhoc network environment and provide a classification of the various security mechanisms.

Index Terms— Adhoc Wireless Networks, Routing, Security, Topology

I. INTRODUCTION

An Adhoc network is a collection of mobile nodes forming a temporary network without any additional infrastructure and no centralized control. Adhoc network can be created on the fly, each node in the Adhoc network acts both as a router and host. The Adhoc networks can adjust its topology dynamically. Attacks from both external and internal nodes can easily affect the stability of the ad hoc networks.

A. Advantages in Adhoc Networks

Adhoc networks are wireless connections between two or more computers and/or wireless devices. A typical wireless network is based on a wireless router or access point that connects to the wired network and/or Internet. An Adhoc network bypasses the need for a router by connecting the computers directly to each other using their wireless network adapters.

1. *Router Free:* Connecting to files on other computers and/or the Internet without the need for a wireless router is the main advantage of using an ad hoc network. Because of this, running an Adhoc network can be more affordable than a traditional network.

2. *Mobility:* Adhoc networks can be created on the fly in nearly any situation where there are multiple wireless devices.

3. *Speed:* Creating an Adhoc network from scratch requires a few settings changes and no additional hardware or software. If you need to connect multiple computers quickly and easily, then an Adhoc network is an ideal solution.

B. Applications

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance with the increasing number of widespread applications. Adhoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Adhoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructured environment into the ad hoc context, a great deal of new services will be generated for the new environment. It includes:

- Military Battlefield
- Sensor Networks
- Commercial Sector
- Medical Service
- Personal Area Network

C. Characteristics of Adhoc networks

Adhoc networks have some characteristics which make them different from wired and wireless networks. They are as follows.

1. Mobility Induced Link Breakages: As the nodes in an Adhoc network are usually mobile, the nodes may go out of range of neighboring nodes resulting in break in the links between the nodes. These may leads to break in the route between source and destination nodes.

2. Sleep Period of Operation: To conserve energy, nodes in an Adhoc network may enter inactive state whereby they do not transmit at some instants of time.

3. Highly unfavorable environmental conditions: Adhoc networks are generally used in environments which are highly unfavorable for transmission and reception.

4. Looping Problem: Due to mobility temporary loops may result.

5.Misbehavior: Some nodes may misbehave transmitting their own data and refusing to transmit data from other nodes. Since Adhoc network uses multi hop routing this has to be controlled.

6. Addressing Problem: In an Adhoc network it is not possible to have fixed nodes acting as DHCP server, but nevertheless. All the nodes should follow a uniform addressing mechanism.

D. Working of a General Adhoc Network

The figure 1 shows how Adhoc networks generally works, how the nodes are communicating and make a secure network.

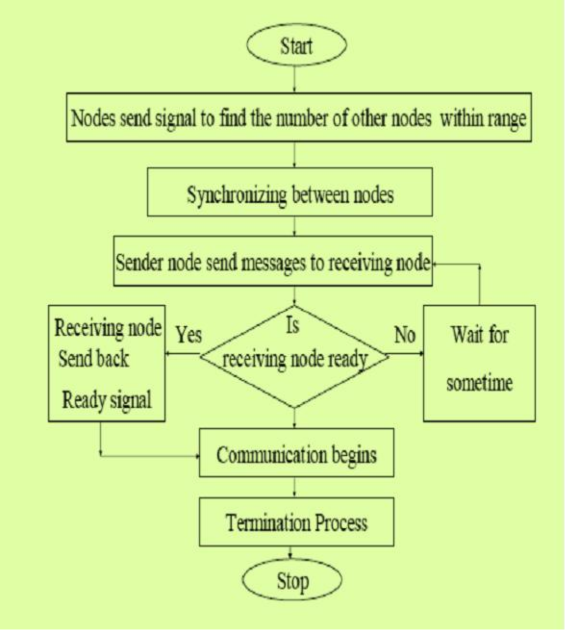
Start
Nodes send signal to find the number of other nodes within range
Synchronizing between nodes
Sender node send messages to receiving node
Receiving node Send back Ready signal
Yes
Is receiving node ready
No
Wait for sometime
Communication begins
Termination Process
Stop

Figure 1: Working of an Adhoc Network

II. SECURITY MODEL: CHALLENGES AND GOALS

A. Security Challenges

Providing adequate security measures for Adhoc networks is a challenging task.

1. Wireless communications are easy to intercept and difficult to contain. Next to this it is easy to actively insert or modify wireless messages. This means that unprotected Adhoc wireless networks are open to a wide range of attacks, including node impersonation, message injection, loss of confidentiality, etc.

2. In many situations the nodes may be left unattended in a hostile environment. This enables adversaries to capture them and physically attack them. Proper precautions are required to prevent attackers from extracting secret information from them. Even with these precautions, we cannot exclude that a fraction of the nodes may become compromised. This enables attacks launched from within the network.

3. The dynamic topology and the absence of a supporting infrastructure render most of the existing cryptographic protocols useless as they were not developed for this dynamic environment. Any security solution with a static configuration would not suffice. Security mechanisms should be able to adapt on-the-fly to these changes in topology.

4. Many wireless nodes will have a limited energy resource Security solutions should be designed with this limited energy budget in mind.

Finally, an Adhoc network may consist of thousands of nodes. Security mechanisms should be scalable to handle such a large network.

B. Goals/Requirements of a Security System

Security is an important issue for Adhoc networks, especially for those security-sensitive applications. To secure an ad hoc network, we consider the following attributes

1) Availability: Ensures survivability despite Denial Of Service (DOS) attacks. On physical and medium access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

2) Confidentiality: Ensures certain information is never disclosed to unauthorized entities.

3) Integrity: Message being transmitted is never corrupted.

4) Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

5) Non-repudiation: Ensures that the origin of a message cannot deny having sent the message.

III.OVERVIEW OF SECURITY

To address the security needs of an organization effectively and to evaluate and choose various security products and policies, the manager is responsible for security needs. Some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. One approach is to consider three aspects of information security:

Security Attack: Any action that compromises the security of information owned by an organisation.

Security Mechanisms: A mechanism that is designed to protect, detect or recover from a security attack.

Security Service: A service that improves the security of the data of an organisation. These services are meant to work against security attacks, using some security mechanisms to provide the service.

A useful categorization of these attacks is in terms of Passive attacks and Active attacks are shown in figure 2. These two broad classes are subdivided into other types of attacks.

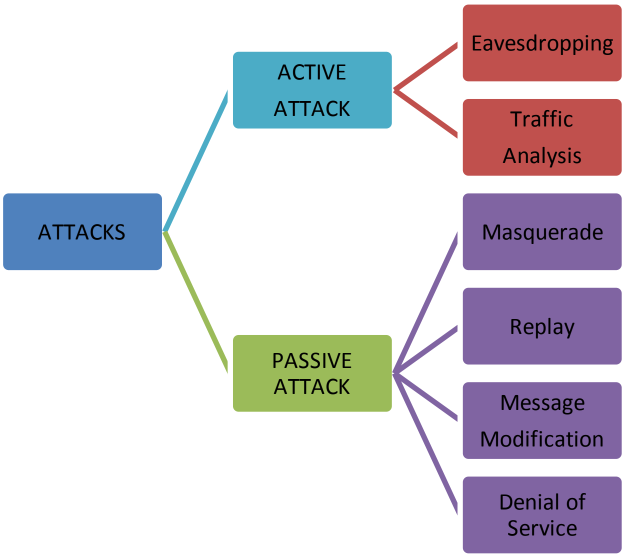

Figure2: Information on Attacks

A. Attacks

1. Passive Attacks: This is an attack in which an unauthorized party gains access to an asset and does not modify its content. Passive attacks can be either eavesdropping or traffic analysis.

Eavesdropping: the attacker monitors transmissions for message content.

Traffic Analysis: the attacker gains intelligence by monitoring the transmission and gaining information about the amount and sources of traffic.

2. Active Attacks: These attacks involve some modification of the data stream or file and can be divided into four categories:

Masquerade: This takes place when one entity pretends to be a different entity.

Replay: The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.

Modification of Messages: This simply means that some parts of message are altered or the messages are changed or reordered.

Denial of Service: Is an attack that causes a loss of service to users, like loss of network connectivity and services, or overloading the computational resources.

B. Generic Threats in Adhoc Wireless Networks

A complete information assurance risk assessment requires a focus on the threats against the three key: Confidentiality, Integrity, and Availability (CIA).

1. Traffic Analysis: This is a simple technique whereby the attacker can determine the load on the communication medium by the number and the size of packets being transmitted. The attacker only needs a wireless card operating in promiscuous (i.e. listening) mode and software to count the number and the size of packets being transmitted. Traffic analysis allows the attacker to obtain the following information:

- Identification that there is activity on the network.
- Identification and physical location of wireless Access Points (APs) in the surrounding area.
- The type of protocol being used in the transmissions.

2. Passive Eavesdropping: In this attack the attacker passively monitors the wireless session figure 3. Assuming that the session is not encrypted, the attacker can gain two types of information from passive eavesdropping. The attacker can read the data transmitted in the session and can also gather information indirectly by examining the packets in the session, specially their source, destination, size, number, and time of transmission.

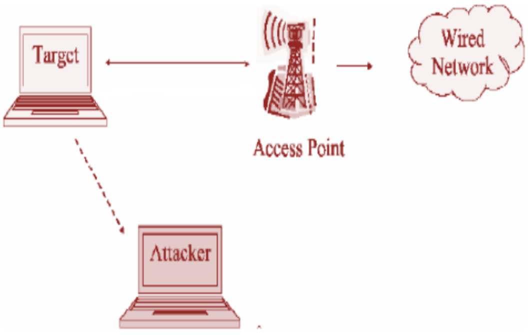

Figure 3: Passive Eaves dropping

3. IP Spoofing: This attack is active eavesdropping, where the attacker not only monitors the wireless session as in passive eavesdropping but actively injects messages and determines the contents of messages. In IP spoofing, the attacker changes the destination of the packet to the IP address of a host he or she controls. As in figure 4, attacker 1 intercepts and modifies the packets in the message. He changes the destination IP address and nothing else. The packet then continues through the access point and to the gateway where they are decrypted. The plain text packets then continue to attacker machine where they are collected and read.

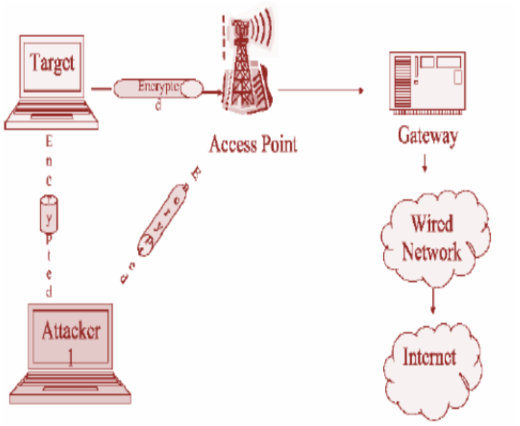

Figure 4: IP Spoofing

4. Unauthorized Access: Unauthorized access is different from any of the previous types of attacks that we have discussed in that it is not directed at any individual user or set of users. It is directed against the network as a whole. Once an attacker has access to the network, he can then launch additional attacks or just enjoy free network use.

5. Man in the Middle Attack: Here the attacker can read private data from a session or modify packets, thus violating the integrity of a session. Figure 5 illustrates how this attack works. The attacker first breaks the connection between the target and the access point. Then, he presents himself as an access point and allows the target to associate and authenticate with his machine. The target believes that he is dealing with the legitimate access point, because the attacker has established a valid session with the access point using his own credentials, at the same time the attacker associates and authenticates with the access point on behalf of the target.

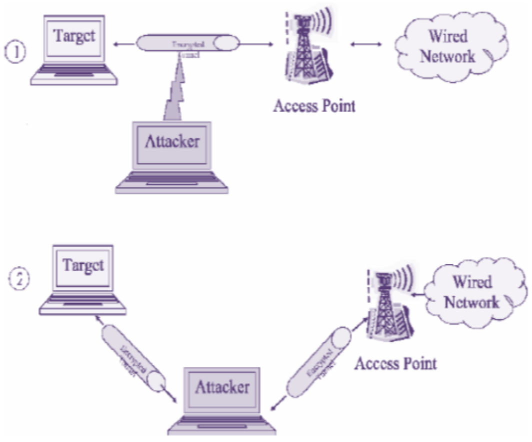

Figure 5: Man in the Middle Attack

6. Session Hijacking: This attack is against the integrity of a session. The attacker monitors the session then takes over or hijacks the ongoing connection. The attacker masquerades as the target to the wireless network, and collects enough information from the session to conduct the attack. Then he blocks access from the target to the access point and continue masquerading as the target to the access point.

7. Replay Attack: Replay attacks are also aimed at the integrity of the information on the network—the integrity of specific session. The attacker captures the authentication of a session, then either replays the session at a later time or uses multiple sessions to analyze the authentication part of a session for replay. The attacker may interact with the network using the target's credentials.

8. Denial of Service Attacks: This attack is aimed at degrading services. It occurs when a malicious attacker tries to reduce the quality of the target or even damage the target so that it is unusable to others. The DoS attack is illustrated in the figure 6.

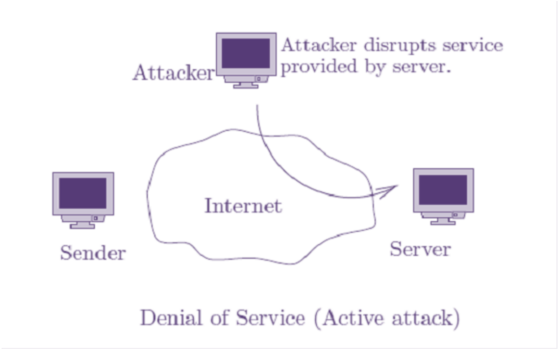
Attacker
Attacker disrupts service provided by server.
Internet
Sender
Server
Denial of Service (Active attack)

Figure 6: Denial of Service Attacks

IV. SECURITY MECHANISMS

The nodes in Adhoc wireless networks act both as regular terminals and as routers for other nodes in the network. The absence of dedicated routers makes the provision of security a challenging task in Adhoc networks, where the task of ensuring secure communication is also made difficult by factors including the mobility of nodes, limited processing power and limited availability of resources such as battery power and bandwidth. The requirements of a secure routing protocol for Adhoc wireless networks are as follows:

A. Detection of malicious nodes

If there are malicious nodes in a network, then a secure routing protocol should be able to detect them and avoid selecting them in the routing process.

B. Guarantee of correct route discovery

The protocol should be able to find a route when one exists between the source and the destination; it should also ensure that it is correct.

C. Confidentiality of network topology

Malicious nodes will be able to view disclosure and information regarding network topology that may lead to an attack on these networks. The confidentiality of the network topology is an important requirement in order to prevent a potential attacker from studying the traffic pattern of the network. Thus, the attacker will not be able to discover the active nodes in Adhoc wireless networks and all attempts to mount e.g. Denied of Service (DoS) attacks against such bottleneck nodes will fail.

D. Stability against attacks

The routing process in Adhoc wireless networks should not be disrupted permanently by passive or active attackers. The routing protocol must be self-sustainable; thus it must be able to revert to its normal operating state within a finite amount of time after a passive or active attack. The protocol must ensure Byzantine robustness; that is, the protocol should work correctly even if some of the nodes which have previously participated in the routing process turn out later to be malicious or are intentionally damaged.

The table I shows some of the security-aware routing protocols proposed for ad hoc networks along with their requirements.

V. CONCLUSION

Security in Adhoc network is important, because every organization needs to secure its data or information. However, everyone has a different idea of what “security” is, and what levels of risk are acceptable. The idea behind building a secure network is to define what security means to one’s own organization. Once that policy has been defined, everything that goes on with the network can be evaluated with respect to that policy. In this paper we mentioned some of the threats to Adhoc Wireless networks. Understanding these threats is a critical task in security. We have analyzed some of the Security mechanisms commonly available for Adhoc wireless networks. Finally, there is no such thing as perfect security. Following these technologies, will not ensure that a network will not be attacked or broken into, but it will drastically reduce the risk of such a break-in. Adhoc wireless networks can be extremely useful and can dramatically increase productivity. If used correctly, they can be made as a secure as other corporate networks.

TABLE I
Requirements of the secure ad hoc routing solutions

ARAN	Online trusted certification authority. Each node knows a priori the public key of the CA.
SAR	Key distribution or secret sharing mechanism.
SRP	Existence of a security association between each source and destination node. Malicious nodes do not collude within one step of the protocol process.
SEAD	Clock synchronization, or a shared secret between each pair of nodes.
Ariadne	Clock synchronization and the existence of a shared secret between each pair of nodes.
SAODV	Online key management scheme for the acquisition and verification of public keys.
TIARA	Online public key infrastructure.

On-demand Secure Routing Protocol	Online public key infrastructure and shared symmetric keys between source and probe nodes.
SLSP	Nodes must have their public keys certified by a TTP. No collusion between malicious nodes.
BISS	The target node of a route discovery must share secret keys with all the intermediate nodes. An offline trusted authority has certified the public keys of all the participating nodes.
Watchdog and Pathrater	No collusion between malicious nodes.
CONFIDANT	Nodes cannot change their identifier to get rid of their reputation rating. Pre-defined lists of friendly nodes.
Packet leashes: temporal	Extremely precise clock synchronization.
Packet leashes: geographical	Geographical location information and loosely synchronized clocks.
IPsec	Prearranged common secrets between each pair of nodes, or an online trusted third party.

REFERENCES

[1] L. Zhou and Z.J. Haas, "Securing Ad hoc Networks", IEEE Networks, 13(6): 24- 30, Nov/Dec 1999.

[2] "Security Technologies in Wireless Networks" Tayseer Fath Elrahman.

[3] H. Anthony Chan. Wireless data networks and systems, Lecture notes, University of Cape Town, http://www.local.eleceng.uct.ac.za/staff/achan/eee458/security/. May, 2004.

[4] Karan Singh, R. S. Yadav, Ranvijay "A Review Paper On Ad Hoc Network Security"

[5] Yih-chun hu, adrian perrig, "A Survey of Secure Wireless ad hoc routing" IEEE security & privacy May-June 2004

[6] F. Anjum, Anup K. Ghosh, nada golmie, paul kolodzy, radha poovendran, rajeev shorey, d. Lee, j-sac, "Security in Wireless Ad hoc Networks", ieee journal on selected areas in communications, vol. 24, no. 2, February 2006.

[7] H.-A. Wen, C.-L. Lin, and T. Hwang, "Provably Secure Authenticated Key Exchange Protocols for Low Power Computing Clients," Computers and Security, vol. 25, pp. 106-113,2006.

[8]Yuh-Ren Tsai, Shiuh-Jeng Wang, "Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks" Chung-Shan Institute of Science and Technology, Taiwan, R.O.C., under Grant BC-93-B14P and the National Science Council, Taiwan, R.O.C., IEEE 2004.

[9] K.Seshadri Ramana, Dr. A.A. Chari, Prof. N.Kasiviswanth, "A Survey On Trust Management For Mobile Ad Hoc Networks" April 2010.

[10] Nishu Garg and R.P. Mahapatra, "MANET Security Issues". *In IJCSNS International Journal of Computer Science and Network Security*, 9**,** No.8, August 2009.

[11] Er. Tushar Gohil "Overview of Security Threats in Mobile Ad-hoc Network", Journal of High Performance Communication Systems and Networking Volume. 2 (1-2), January-December 2010, pp. 1–10.

Author's profile:

Mr. G. Jose Moses is a Research Scholar in the Department of Computer Science, Adikavi Nannaya University, Rajahmundry, A.P., India. He obtained his B.Tech from JNTU, Kakinada, M.Tech from Acharya Nagarjuna University. His research interests lies in Computer Networks, Cloud Computing.

Dr. P. Suresh Varma received the Master's degree M.Tech in Computer Science & Technology from Andhra University. He received Ph.D. degree in Computer Science & Engineering from Acharya Nagarjuna University. He is currently working as Professor in Department of Computer Science in Adikavi Nannaya University, Rajahmundry, A.P., India. He published several papers in National and International Journals. He is active member of various professional bodies. His current research is focused on Computer Networks, Cloud Computing and Data Mining.

Mrs. N.Supriya Working as Academic Consultant, in the department of Computer Science, Adikavi Nannaya university, Rajahmundry. She is at present pursuing Ph.D at Acharya Nagarjuna University. Her research interests lies in Software Engineering, Data Mining and Computer Networks.

Mr.G.NagaSatish currently working as Associate Professor in P.G.Department of CS, Ideal College of Arts & Sciences, Kakinada, Andhra Pradesh, India. His qualifications are M.Sc, M.Phil, M.Tech. He is pursing Ph.D at Adikavi Nannaya University. He has presented and published papers in national and International conferences. His areas of interest include Computer Networks.