Security Threats in Mobile Ad Hoc Network

Anuj Joshi[1*], Pallavi Srivastava[2] and Poonam Singh[3]

ABSTRACT

Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration. Due to this unique property, the main challenge is the vulnerability to security attacks. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is quickly spreading for, security challenges has become a primary concern to provide secure communication. In this paper, we identify the existent security threats an ad hoc network faces, the security services required to be achieved and the countermeasures for attacks in each layer. To accomplish our goal, we have done literature survey in gathering information related to various types of attacks and solutions, as well as we have identified the challenges and proposed solutions to overcome them. In conclusion, we focus on the findings and future works which may be interesting for the researchers like robust key management, trust based systems, data security in different layer etc. However, in short, we can say that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET.

Keywords: *MANET, blackhole, wormhole,Denial of Service(DoS), routing, masquerade*

1. INTRODUCTION

AN ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other

mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multihop paths through the network to any other node. This idea of Mobile ad hoc network is also called infrastructureless networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly [1]. 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 ad hoc 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 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

[1*] Anuj Joshi is with the Dept. of Computer Science, Amity University Lucknow, , E-mail: know.anuj@gmail.com

[2] Pallavi Srivastava is with the Dept. of Computer Science, Lal Bahadur Shastri Institute of Management and development studies

[3] Poonam Singh is with the Dept. of Computer Science, Amity University Lucknow.

cooperation and constrained capability [1].

2. SECURITY SERVICES

The ultimate goals of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, authentication, nonrepudiation, anonymity and availability to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. There is no single mechanism that will provide all the security services in MANETs. The common security services are described below.

2.1 Availability

Availability is concerned with the (unauthorized) upholding of resources. A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures such as authentication and encryption whereas others require some sort of action to prevent or recover from loss of availability of elements or

services of a distributed system. Availability ensures the survivability of network services despite of various attacks. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network. Again, in higher levels, an adversary could bring down high-level services such as key management service, authentication service [2].

2.2 Confidentiality

Confidentiality ensures that certain information is only readable or accessible by the authorized party. Basically, it protects data from passive attacks. Transmission of sensitive information such as military information requires confidentiality. Release of such information to enemies could have devastating consequences. Routing and packet forwarding information must also remain confidential so that the enemies could never take the advantages of identifying and locating their targets in a battlefield. With respect to the release of message contents, several levels of protection can be identified.

2.3 Integrity

Integrity guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that a message being transmitted is never corrupted. As with confidentiality, integrity can apply to a stream of messages, a single message or selected fields within a message. But, the most useful and straightforward approach is total stream protection. A connection-oriented integrity service, one that deals with a stream of messages assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under integrity service. Thus it addresses both message stream modification and denial of service (DoS).

2.4 Authentication

Authentication ensures that the access and supply of data is done only by the authorized parties. It is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function is to assure the recipient that the message is from the source that it claims to be from. Without authentication, an adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operations of the other nodes [2].

2.5 Nonrepudiation

Nonrepudiation prevents either sender or receiver from denying a transmitted message.Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. On the other hand, after sending a message, the sender can prove that the message was received by the alleged receiver. Nonrepudiation is useful for detection and isolation of compromised nodes.

2.6 Scalability

Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network [9]. Otherwise, the newly added node in the network can be compromised by the attacker and used for gaining unauthorized access of the whole system.

3. TYPES OF ATTACKS IN MANET

The current Mobile ad hoc networks allow for many different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure in such a network. Current MANETs are basically vulnerable to two different types of attacks: 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. The attacks are classified as modification, impersonation, fabrication, wormhole and lack of cooperation.

3.1 Attacks Using Modification

Modification is a type of attack when an unauthorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct DoS attacks by modifying message fields or by forwarding routing message with false values. In this way, malicious nodes can easily cause traffic subversion and denial of service (DoS) by simply altering protocol fields: such attacks compromise the integrity of routing computations. Through modification, an attacker can cause network traffic to be dropped, redirected to a different destination or to a longer route to reach to destination that causes unnecessary communication delay.

3.2 Attacks Using Impersonation

As there is no authentication of data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a benign node can gather.

3.3 Attacks through Fabrication

Fabrication is an attack in which an unauthorized party not only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication is used to refer the attacks performed by generating false routing messages. Such kind of attacks can be difficult to verify as they come as valid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted [3].

3.4 Wormhole Attacks

Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

3.5 Lack of Cooperation

Mobile Ad Hoc Networks (MANETs) rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But one of the different kinds of misbehavior a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources. This can endanger the correct network operation by simply not participating to the operation or by not executing the packet forwarding. This attack is also known as the black hole attack.

Table- 1

Security Attacks on each layer in MANET[4]

Layer	Attacks
Application layer	Repudiation[4], data corruption[5]
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming[4], interceptions, eavesdropping[4]

Table - 2

Security Issues for MANET[6]

Layer	Security Issues
Application layer	Detecting and preventing viruses, worms, malicious codes and application abuses
Transport layer	Authentication and securing end-to-end or point-to-point communication through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Data link layer	Protecting the wireless MAC protocol and providing link layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

4. COUNTERMEASURES

Security is a primary concern in MANET in order to provide protected communication between the communicating parties. It is essential for basic network functions like routing and packet forwarding. Network operation can easily be jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design[3].

Table - 3

Countermeasures on each layer in MANET

Layers	Solutions
Application layer	Cooperation enforcement (Nuglets, Confidant, CORE) mechanisms, Firewalls, IDS etc.
Transport layer	Authentication and securing end-to-end or point-to-point communication, use of public cryptography[7]
Network layer for	Source authentication and message integrity mechanisms to prevent routing message modification, Securing routing protocols to overcome blackhole, impersonation attacks, packet leashes[2], SECTOR mechanism wormhole attack etc.
Data link layer	No effective mechanism to prevent trafficanalysis and monitoring, secure link layer protocol like LLSP, using WPA[9] etc.
Physical layer	Using Spread spectrum mechanisms

A variety of security mechanisms have been developed to counter malicious attacks. There are two mechanisms which are widely used to protect the MANET from the attackers

4.1 Preventive mechanism

In preventive mechanism, the conventional approaches such as authentication, access control, encryption and digital signature are used to provide first line of defense. Some security modules, such as tokens or smart card that is accessible through PIN, pass phrases or biometrics verification are also used in addition.

4.2 Reactive mechanism

Reactive mechanism uses the schemes like intrusion detection system (IDS), cooperation enforcement mechanisms etc. in MANET. Intrusion detection systems are used to detect misuse and anomalies. Cooperation enforcement such as Nuglets, Confidant, CORE and Token-based reduce selfish node behavior.

5. CONCLUSION AND FUTURE DIRECTION

Mobile Ad Hoc Networks have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Whether ad hoc networks have vast potential, still there are many challenges left to overcome. Security is an important feature for deployment of MANET. In this paper, the challenges and solutions of the security threats in mobile ad hoc networks have been overviewed. Though significant research in MANET has been ongoing for many years, but still in an early stage. The first research question is 'What are the vulnerabilities and security threats in MANET? Which level is most vulnerable to attack?' The second research question is 'How the security services like confidentiality, integrity and authentication can be achieved from mobile ad hoc networks? What steps should be taken?' The answer is that security services can be achieved through following the preventive and reactive countermeasures on the basis of particular attack. The third question is 'What are the countermeasures? How the security of the entire system is ensured?' In addition, we can say that security must be ensured for the entire system since a single weak point may give the attacker the opportunity to gain the access of the system and perform malicious tasks. Another interesting question for research is 'What are the potential dangers that may be crucial in future?' Everyday, the attackers are trying to find out the new vulnerability in MANET. Existing solutions are well-suited only for specific attack. They can cope well with known attacks but there are many unanticipated or combined attacks remaining undiscovered. Resource consumption DoS attack is still unclear. More research is needed on secure routing protocol, robust key management, trust based systems, integrated approaches to routing security, data security in different level and cooperation enforcement. Cryptography is one of the most common security mechanisms and its strength relies on the secure key management. The public cryptography scheme depends upon centralized CA (Certificate Authority) which is known as a security weak point in MANET. Symmetric cryptography is efficient but suffers from potential attack on key distribution. Hence, efficient key agreement and distribution in MANET is an ongoing research area. Finally, Building a sound trust-based system and integrating it to the current preventive approaches, solution of the node selfishness problem can be considered in future research. Identifying new security threats as well as new countermeasures demands more research in MANET.

ACKNOWLEDGMENT

First and foremost, I would like to express my heartiest gratitude to honorable Asst. Prof. Dr. Deepak Arora for his suggestions, guidance, constant encouragement and enduring patience throughout the progress of the paper. I would also like to express my sincere thanks to K K Agrawal for his advices and all-out cooperation.

REFERENCES

[1] H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless ad hoc networks," Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804.

[2] L. Zhou, Z.J. Haas, Cornell Univ., "Securing ad hoc networks," IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044.

[3] P. Michiardi, R. Molva, "Ad hoc networks security," IEEE Press Wiley, New York, 2003.

[4] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Department of Computer Science and Engineering, Florida Atlantic University, http://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf

[5] R. Ramanathan, J. Redi and BBN Technologies, "A brief overview of ad hoc networks: challenges and directions," IEEE Communication Magazine, May 2002, Volume: 40, page(s): 20-22, ISSN: 0163-6804

[6] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s): 38- 47, ISSN: 1536-1284

[7] C. Kaufman, R. Perlman, and M. Speciner, "Network Security Private Communication in a Public World," Prentice Hall PTR, A division of Pearson Education, Inc., 2002

[8] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense AgainstWormhole Attacks inWireless Ad Hoc Networks," Proc. of IEEE INFORCOM, 2002.

[9] IEEE Std. 802.11i/D30, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security," 2002.