Volume 1,Issue-1,December-2011 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research paper

Available online at www.ijarcsse.com

A Study of Various Security Attacks and their Countermeasures in MANET

Rajni Sharma[1], Alisha saini[2],

U.I.E.T, Kurukshetra University, Kurukshetra[1, 2]

[1]rajni.sharma2307@gmail.com, [2]alisha191@rediffmail.com

***Abstract*— Mobile Adhoc Networks are the new paradigm of wireless networks that are capable of operating without the support of any fixed infrastructure. The most indispensable service of wireless network is security. The various security goals should be achieved such as confidentiality, integrity, authentication, availability, non repudiation etc for the secure routing in MANETS. In this paper, we have attempted to present an overview of various security attacks and their counter measures in MANET. We had given an overview of the various attacks at different layers followed by the measures taken to counter these attacks.**

***Keywords*— Manet, Security attacks, Countermeasures.**

I. INTRODUCTION

An Adhoc network is a collection of nodes which are often mobile. To maintain the connectivity, these nodes are applied with wireless communication forming the network known as Mobile Adhoc Network (MANET). MANET is totally different from the conventional wired network, comprising of centralized monitoring system. It is a highly dynamic network. The mobile nodes in this network establish routing among themselves to build their own network on the fly. Due to this reason MANETS are more prone to attacks than the wired networks. Some of the salient characteristics of MANETS are communication via wireless means, dynamic network topology, infrastructure less, no centralized controller. Few of the possible applications of MANETS include battlefield communication for military, disaster relief operations, accessing information and services regardless of geographic position.

Security challenges have become a primary concern to provide a secure communication. In this paper, we identify the existent security threats an ad hoc network faces and the countermeasures for attacks in each layer.

II. VARIOUS CLASSIFICATION OF ATTACK

Roughly there are two main categories always considered as shown in figure 1.

- Passive attacks
- Active attacks

Passive attacks: Those attacks that do not disrupt the normal functionality of MANET while obtaining data exchanged from network.[2]

Active attacks: Those attacks that disrupt the normal functionality of MANET such as doing data interruption, modification or fabrication.

Other type of classification of attacks is

- External attack
- Internal attack

External attack: carried out by nodes that do not belong to the particular domain of the network.

Internal attack: carried out by the compromised nodes, which belong to the domain of the network and more secure than external attacks.

Several other attacks are classified according to the network protocol stack. Some attacks are cryptography related and some are non cryptography related.

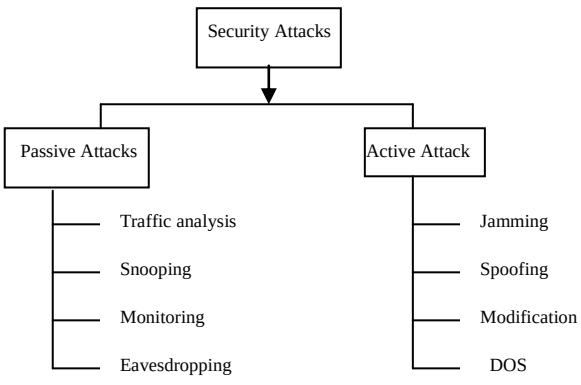

Fig. 1 Classification of security attacks

III. VARIOUS SECURITY ATTACKS AND THEIR COUNTERMEASURES AT EACH LAYER OF PROTOCOL STACK

A. Physical Layer Attacks

This section tests and gives brief description of the attacks pertaining to the physical layer

1. *Interception and jamming:* an adversary could employ signal with some frequency strong enough to interfere with communication on physical channel[15].
2. *Eavesdropping:* The unintended receiver could read the original message and could inject fake message to the network.[4]

Countermeasures for physical layer

- Frequency hopping spread spectrum and direct sequence spread spectrum technology is used to transmit data. This method is secure until the eavesdropper could not identify the spreading code.

B. Data Link Layer Attacks

1) *WEP weakness:* Wired equivalent privacy is security provided by IEEE 802.11. some of its weaknesses are Lack of key management. The combined use of non cryptographic integrity algorithm CRC32 with the stream cipher is a big security risk.[15]

2) *Traffic monitoring and analysis*: It identify the communication parties and functionalities

3) *Denial of service by binary exponential backoff scheme and disruption on MAC DCF*: The malicious nodes do not follow the normal operation of MAC protocol and do not cooperate among with the neighboring nodes. Link layer is attacked by the malicious nodes by corrupting the frequency. It could also exploit binary expo backoff scheme in which heavily loaded nodes tend to capture the physical channel making lightly loaded nodes to backoff endlessly. Malicious nodes could take advantage of this capture effect vulnerability.[4]

Countermeasures for Data link layer

- *Traffic analysis* could be prevented by encryption. But still we do not have effective mechanism. Nodes should continuously on time to time lookup for the malicious or selfish neighboring node to prevent from their selfishness and misbehavior.
- *WEP weakness* could be removed by using link encryption to hide the end to end traffic flow information. LLSP protocol could be used.

C. Network Layer Attacks

1) *Routing Attack:*

- *Routing Table Overflow:* Routes are created to non existed nodes by the attackers. The goal of this attack is to overflow the target systems routing table and to prevent of new routing table entries to authorized nodes[4].
- *Routing table poising attack*: In this case, the compromising nodes sends fictitious routing updates or modify genuine route update packets sent to other authorized nodes. It results in congestion in a portion of network or makes that part inaccessible[4].
- *Routing cache poising*: In reactive routing protocols each node maintains a route cache. This attack occurs when information to be stored is deleted or altered with false information in cache. It has same objectives as same as routing table poising attack.
- *Rushing Attack*: This attack is extremely difficult to detect. An attacker on receiving RREQ packet quickly floods the packet throughout the network before other node can react who receive the same RREQ.[17]
- *Packet Replication:* Attacker replicate stale packets to consume additional bandwidth and battery power resource.

2) *Blackhole attack*: In this attack, a malicious node falsely advertises good path shortest to the destination node. During route discovery process, the purpose is to hinder path finding process on to intercept data packets being sent between source and destination.[2]

3) *Wormhole Attack:* In this case, an attacker node receives packet at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two malicious nodes is called wormhole. No harm is done if the wormhole is used properly for efficient relaying of packets, it put the attacker in a powerful position in the network and it could compromise with the security of network.[2]

4) *Byzantine attack:* Here in this attack, a compromise intermediate node or a set of compromised intermediate node works in collusion and carry out attacks such as creating routing loop, routing packets on non-optimal paths and selectively dropping packets. This attack is hard to detect because network seem to be operating normally while this attack works.[2]

5) *Information Disclosure:* tthe malicious node leaks confidential information to unauthorized nodes in the network. The confidential information could be regarding geographic location of nodes, network topology.[2]

6) Resource consumption attack: The attacker node tries to consume/waste away resources of other nodes in the network. Resources ,could be battery power, bandwidth and computational power. The attacker send excessive RREQ or unnecessary packets to the victim node in order to consume the battery or bandwidth.[2]

TABLE I
ATTACKS ON PARTICULAR ROUTING PROTOCOLS

Name	Advantages	Attacks
AODV	Simple, require less memory, no extra traffic	Blackhole Attack
DSR	Hop by hop forwarding, source route modification is possible	Warmhole Attack
ARAN	Detects & protects against malicious action, authentication, message integrity	Rushing Attack
ARIADNE	Point to point authentication of routing of messages	Warmhole Attack, Rushing Attack
SEAD	Message authentication	Warmhole Attack

Countermeasures for Network layer attacks:

- *Routing attack:* These attacks could be prevented by mechanism source authentication and message integrity either hop by hop or the end to end approach. SEAD (Secure efficient Adhoc Distance Vector routing)[19] protocol can prevent from DoS attacks all types of routing attacks and resource consumption attacks.
- *Wormhole attack:* It can be detected by an unaltered and independent physical metric such as delay or geographical location. Packet leashes are used to combat wormhole attacks [6].
- *Blackhole attack*: The solution is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out by the destination node. SAR[18] is used to defend against blackhole attack.
- *Byzantine attack:* We can use secure routing protocol that provide a method to overcome this attacks using public key cryptography. Byzantine failures could be reduced by adaptive probing techniques .
- *Information Disclosure attack:* SMT (Secure Data Transmission in MANETs), provides a method for overcoming this attack.
- *Resource consumption attack:* SEAD (Secure Efficient Aware Adhoc)[19] routing protocol is mainly designed for DSDV and can overcome resource consumption attack. This protocol uses authentication to differentiate between malicious and non-malicious nodes, which reduces resource consumption attacks launched by attacker nodes.

D. Transport layer Attacks:

1) Session hijacking: Since, all the authentication process are carried out in the beginning of session. The adversary take advantage of this and spoof IP address of destination node and masquerades as one of the end nodes of the session and hijacks the session as a legitimate system.

2) SYN flooding: This is a DoS attack in which attacker creates a large number of half open end TCP connection with a victim node. An 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 out SYN-ACK packets to the sender and waits for ACK packets. The victim node stores all the SYN packets in a fixed-size table as it waits for the ACK packet. These pending connection request could overflow the buffer and may make the system unavailable for long time.

3) TCP ACK Storm: First TCP session hijacking attack is performed, then the adversary send injected session data and one of the end node sent ACK packet to other end node. The other end node receive the ACK packet with uneven sequence number and try to resynchronize the TCP session by sending an ACK packet with an intended sequence number. This result in TCP ACK storm.[4]

Countermeasures:

- *Session hijacking :* In this case, only authentication and secure end-to-end or point-to-point data encryption gives message confidentiality at this layer in two end system. Various TCP protocols were developed but none of them fit well in MANET and failed to provide security. Secure Socket layer[20], transport layer security(TLS)[20] and Private Communication Transport(PLT)[20] protocols were designed to provide secure communication using public key cryptography .
- *SYN flooding :* Various firewalls at higher level can be used to prevent SYN flooding attacks.

E. Application layer Attack

1) Repudiation attack: This attack refers to the denial or attempted denial by a node involved in a communication of having participates in all or part of the communication.

Countermeasures:

- *Repudiation attacks:* ARAN[14] can be used to prevent repudiation attack. Authentication and

non- repudiation services are provided by ARAN using predetermined cryptographic certificate for end-to-end authentication.

- *Virus and worm attacks:* Firewall are effective way to prevent various attacks as well as we can use Intrusion Detection System(IDS) to prevent gaining unauthorized access to a service

F. Other multilayer attack

1) DoS: In this case, an adversary attempt to prevent legitimate and authorized users of services offered bt the network from accessing those services

TABLE II

VARIOUS DOS ATTACKS AT DIFFERENT LAYERS

Layer name	Type of DoS Attack
Physical layer	Jamming
Data link layer	Capture effect
Network layer	Packet dropping, table overflow or poisoning
Transport layer	SYN flooding, session hijacking
Application layer	Malicious programs can cause DoS attacks

2) *Impersonation attack:* This attack is just the first step for most attacks and are used to launch further sophisticated attacks.

3) *Man-in-middle attack*: An adversary sits between sender and the receiver and sniffs information interchanges between them.

Countermeasure:

- *DoS***:** End-to-End authentication can prevent many DoS attacks, SEAD and ARIADNE protocols can also be use to protect against DoS attacks.
- *Man-in Middle attack:* Secure Socket layer can help in secure data transmission and can also help to prevent man-in-middle attacks. SSL is based on public key cryptography.
- *Impersonation* **:** ARAN can be used to prevent impersonation. Authentication and non-repudiation services are provided by ARAN using predetermined cryptography certificates for en-to-end authentication

TABLE III

VARIOUS SECURITY ATTACKS AND PROPOSED SOLUTION

layer	Security Threats	Defense Metrics/ Proposed solution
Physical layer	Eavesdropping, Noise	Spread Spectrum mechanism i.e. FHSS, DSSS
	Interference and jamming	
Data link layer	WEP weakness	Secure link layer protocol i.e. LLSP, use link encryption to hide end-to-end traffic using WPA
	DoS by binary exponential backoff scheme and Disruption on MAC DCF	Neighbors should keep looking for selfish/ malicious node misbehavior
	Traffic analysis and monitoring	No effective mechanism to prevent. But encryption could be used.
Network layer	Routing Attacks: Routing table overflow attack	Authentication and integrity mechanism either the hop by hop or the end-to-end approach
	Routing Attacks: Routing cache poisoning attack	
	Routing Attacks: Rushing attack	SEAD[19]
	Routing Attacks: Illegal modification of routing message	Prevented by mechanism source authentication and message integrity
	Routing Attacks: Packet Replication	
	Wormhole attack	Packet leashes[6], SECTOR mechanism
	Blackhole attack	Security Aware adhoc routing protocol (SAR) [18]
	Byzantine attack	SRP[2]
	Resource consumption attack	SEAD[19]
	Information(location) disclosure attack	SRP[2], NDM[2], SMT[2]
Transport layer	SYN Flooding	Authentication and secure end-to-end or point-to-point approach through data encryption public key cryptography
	Session hijacking	
	TCP ACK Storm	Use of public key cryptography
Application layer	Repudiation attacks	ARAN[14]
	Virus and worm attacks	Application layer firewall or IDS can be used. Co-operation enforcement
Multi-layer Attacks	DoS	SEAD[19], ARIADNE[16]
	Impersonation attack	ARAN[14]
	Man-in-middle attack	Secure Socket Layer SSL[20]

IV. CONCLUSION

Security is the most important feature for deployment in mobile Adhoc network. In this paper we identify the existent layer attacks an Adhoc network faces and the defenses for attacks at each layer**.** Firstly we have presented the various

classification of attacks. Then we reviewed security attacks at each layer along with there proposed solutions. Finally we had summarized the security attacks along with there threats and defense metrices. The field of mobile ad hoc networks is changing and growing rapidly. There are still many challenges that need to be met and most often, such networks will see widespread use in nearby future.

V. REFERENCES

[1] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security (IJCSS) Volume: 4 Issue: 3.

[2] C.S.R.Murthy and B.S.Manoj, *Ad Hoc Wireless Networks*, Pearson Education, 2008.

[3] A. Tanenbaum, *Computer Networks*, PH PTR, 2003.

[4] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ," Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

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

[6] Y.C. Hu, A. Perrig, and D.B.Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Network," Proc. 22nd Annual Joint Conf. IEEE Computer and Communication Societies San Francisco, CA, April 2003.

[7] Sukla Banerjee , "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[8] N.Shanthi, Dr.Lganesan and Dr.K.Ramar , "Study of Different Attacks on Multicast Mobile Ad hoc Network," Journal of Theoretical and Applied Information Technology.

[9] Hoang Lan and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad hoc Networks", Proceedings of ICNICONSMCL'06, 0-7695-2552-0/06@ 2006 IEEE.

[10] Amitabh Misgra and Ketan M. Nadkarni, "Security in Wireless Ad hoc Networks", in Book The Handbook of Ad hoc Wireless Networks(Chpter 30),CRC Press LLC, 2003.

[11] Ping Yi, Yue Wu and Futai Zou and Ning Liu, "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[12] P. Yi, Y.P. Zhong, S.Y. Zhang, and Z.L.Dai, "Flodding Attack and Defence in Ad hoc NEtwork", J Syst Engineer Electro, Vol. 17 , no. 2, pp. 410-6, 2006..

[13] Lidong Zhou, Zygmunt J. Haas:," Securing Ad hoc Networks",IEEE Network Magzine, 13, 6, Pages 24-30, 1999.

[14] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, "*Secure routing protocol for ad hoc networks,"* In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. 12-15 Nov. 2002, Page(s): 78- 87, ISSN: 1092-1648

[15] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions. *IEEE Wireless Communications*, pp. 38- 47, 2004.

[16] Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. *Proc. of MobiCom 2002*, Atlanta, 2002.

[17] Y. Hu, A. Perrig, and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. *Proc. of the ACM Workshop on Wireless Security* (WiSe), pp. 30-40, 2003.

[18] S. Yi, P. Naldurg, and R. Kravets, Security-Aware Ad-hoc Routing for Wireless Networks. Report No.UIUCDCS-R-2002-2290, UIUC, 2002.

[19] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance VectorRouting in Mobile Wireless Ad-Hoc Networks. *Proc. of the 4th IEEE Workshopon Mobile Computing Systems and Applications* (WMCSA'02), pp. 3-13, 2002.

[20] 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

