ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Comprehensive Study of Security Attacks in Wireless Ad-hoc Network

Meenu Vijarania

Assistant Professor, Department of Computer Science Engineering, Amity University, Haryana, India

ABSTRACT: Mobile ad hoc network (MANET) is a self-configured network which formed automatically through wireless links by a collection of mobile nodes without any centralized administration. These mobile nodes organize themselves dynamically in random and unpredictable topologies. Due to dynamic nature, the ad hoc networks are more susceptible to attacks. Attacks on ad hoc network routing protocols disrupt network performance and reliability. Hence, there are lots of requirement for an understanding of the various problems associated with the wireless mobile networks. In this paper a comprehensive survey on security criteria and various attack types of the mobile ad hoc networks is presented . Different types of attacker attempts different approaches to decrease the network performance and throughput. In this paper the principal focus is on routing and security issues associated with mobile ad hoc networks which are required in order to provide secure communication. Assessment for the various secured multicast routing protocols against the identified attacks is also presented.

KEYWORDS: Security, Mobile ad hoc network(MANET) , attacks, multicast, layer

I. INTRODUCTION

Wireless networks have emerged as a popular technology to provide wireless Internet access anywhere any time [1]. Multicasting in wired and wireless networks has been advantageous and used as a vital technology in many applications such as multiplayer social gaming, audio/ video conferencing, corporate communications, multicast TV , collaborative and groupware applications, distance earning, stock quotes, distribution of software, news and etc [1]. The efficient way of transmitting same data stream to several clients simultaneously is done through multicast transmissions .At the same time security in multicast routing is the main concern ,failing to address security issues of a routing protocol in wireless network can severely disrupt network services and extensively affect performance [5]. MANETs present a new set of nontrivial challenges to security design. These challenges include shared wireless medium ,open network architecture, limited resource constraints, and extremely random network topology. Thus the need for more effective security measures arises as many passive and active security attacks can be launched from the outside by malicious hosts or from the inside by compromised nodes [2]. Key management is a fundamental part of secure routing protocols; existence of an effective key management framework is also vital for secure routing protocols. Several security protocols have been proposed for MANETs, there is no approach fitting all networks, because the nodes can vary between any devices. There are various security threats that exist in MANETs, such as denial of service, black hole, resource consumption, location disclosure, wormhole, host impersonation, information disclosure, and interference [1], [2].Two approaches for security , prevention-based (such as user authentication) and detection-based (such as intrusion detection), can be used to protect high security MANETs. User authentication needs to be performed continuously and frequently, since the chance of a device in a hostile environment being captured is extremely high. Intrusion detection systems (IDSs) are also important in high security MANETs to effectively identify malicious activities. In the MANETs, host-based IDSs are suitable since no centralized gateway or router exists in the networks

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

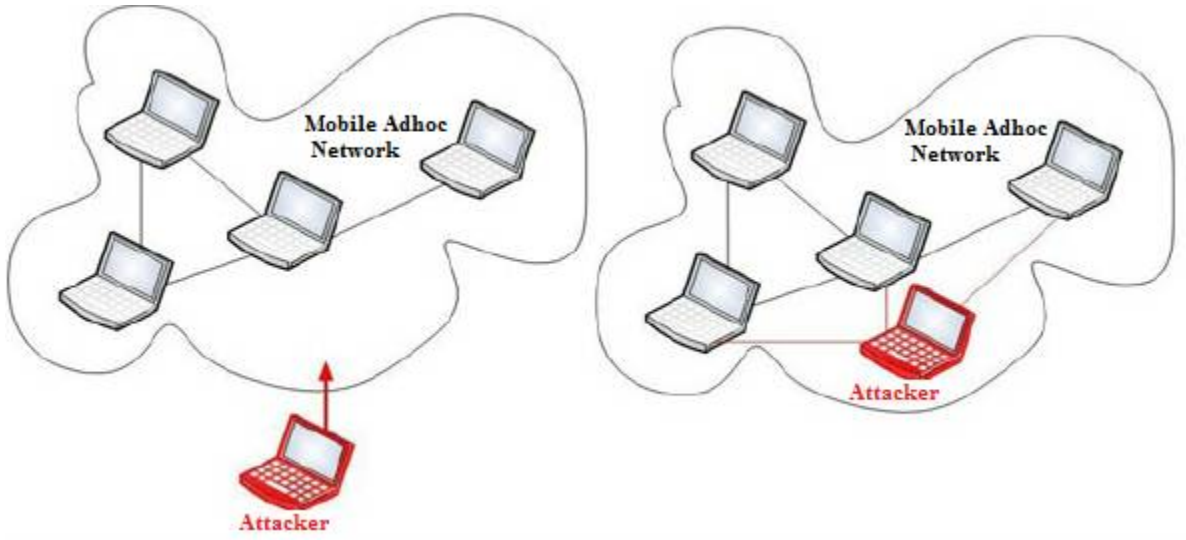

Figure 1: Mobile ad-hoc networks with attacking node

II. CATEGORIZATION OF ATTACKS IN MANETS

In multicasting environment the security issues of MANETs[3] are more challenging with various senders and receivers. There are different kinds of attacks by malevolent nodes that can harm a network and that make the communication unreliable .These attacks can be classified as active and passive attacks. An active attack disrupts the normal operation of a network by modifying the packets in the network. Active attack can be further classified as internal and external attacks. External attacks are carried out by nodes that do not have part of the network. Internal attacks are formed by nodes that are in communication. A passive attack is one in which the information is intercepted by an attacker without disrupting the network activity. Many characteristics might be used to classify attacks in the ad hoc networks. Examples would include looking at the behaviour of the attacks (passive vs. active), the source of the attacks (external vs. internal).Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from inside i.e. network itself. Ad hoc network are mainly subjected to two different levels of [4] attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level tries to damage the security mechanisms employed in the network

Internal Attacks

Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. These attacks may broadcast wrong routing information to other nodes. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more reliable nodes. The inaccurate routing information generated by malicious nodes is difficult to identify.

External attacks

These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc [2]. External attacks prevent the network from normal communication and producing additional overhead. External attacks can divided into two categories:

Passive vs. active attacks

Passive attacks are launched to steal valuable information in the targeted networks. Examples of passive attacks in ad hoc network are eavesdropping attacks and traffic analysis attacks. Detecting this kind of attack is difficult because neither the system resources nor the critical network functions are physically affected to prove the intrusions [3]. While passive attacks do not intend to disrupt the network operations, active attacks on the other hand actively alter the data with the intention to obstruct the operation of the targeted networks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

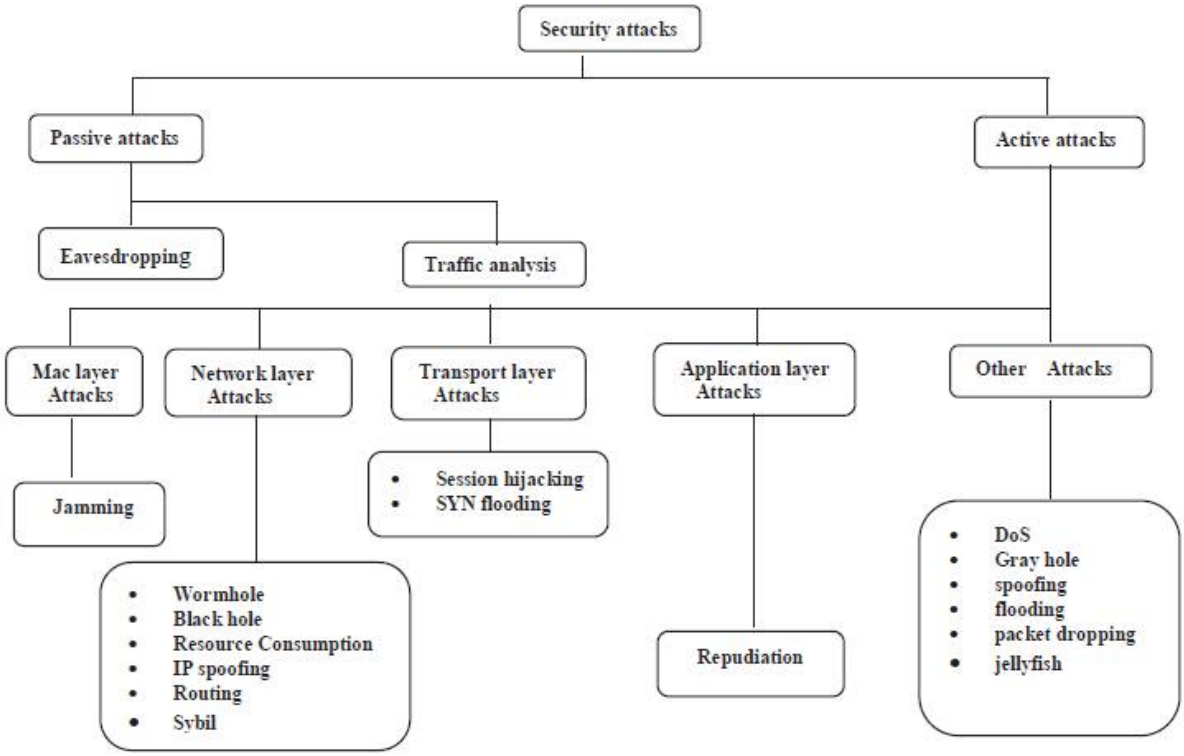

Figure 2. Type of Attacks

III. TYPES OF ACTIVE ATTACKS

1. *Wormhole attack*

The wormhole attack is a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication.

2. *Black hole Attack*

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node (e.g., by implementing rushing attack) in order to intercept data packets of the multicast session. It then drops some or all data packets it receives instead of forwarding them to the next node on the routing path. This type of attack often results in very low packet delivery ratio.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

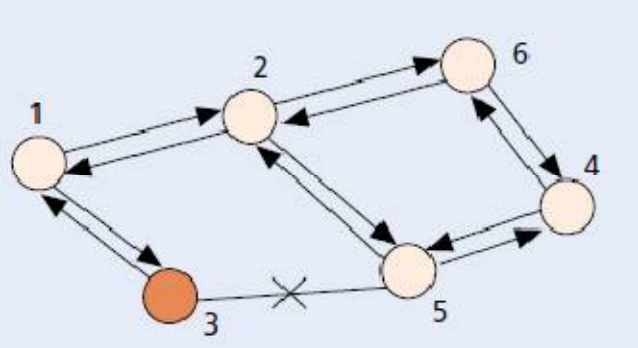

Figure 3 The black hole problem

3. Byzantine Attack

problem" is the term that refers to the circumstances where a few defective/corrupted members of the group acts in an arbitrary way and cause a system malfunction. A compromised intermediate node or a set of compromised intermediate nodes[1] works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths,or selectively dropping packets, which results in disruption or degradation of the routing services.Byzantine wormhole attacks, Byzantine Overlay network wormhole attacks, gray hole attacks, flood rushing attacks and selfish node attacks are the various kinds of byzantine attacks in adhoc networks.

4. Sybil Attack

Sybil attack is defined as an attack by a malicious device adopting multiple identities illegitimately and the additional identities are known as Sybil nodes .The Sybil attack can occur in a MANET since it operates without a central authority which can verify the identities of each communicating entity [1]. Because each entity is only aware of others through messages over a communication channel, a Sybil attacker may take different identities during transmission of message to the legitimate node.

5. Jamming Attack

Jamming attack can deliberately lead to the stoppage or disruption of wireless communication. Interferences at the transmissions are due to jamming attack. A jammer can easily fulfilled by listening to the shared medium and transmitting in the same bandwidth as network, with noneed of particular hardware. Any station equipped with a transceiver can spy on going transmissions, inject fake messages, or block the transmission of legitimate ones. One of the essential keys for damaging the network performance is by jamming wireless transmissions. the scamper distorts transmitted messages due to interferences in the network's operational frequencies, and in closeness to the targeted receivers.

6. Session hijacking

Session hijacking takes advantage of the fact that most communications are protected at session startup, but not thereafter. The attacker adopts the victim's IP address, determines the right sequence number that is expected by the target node, and then performs a Denail of service attack on the victim. Thus the attacker take place of the the victim node and continues the session with the target.

7. *Repudiation Attack*

Repudiation attack is the main application layer level attack. Repudiation refers to the rejection or attempted denial by a node involved in a communication of having contributed in a part or the entire communication [3]. Non-repudiation is one of the key requirements for a security protocol in any communication network and assures that a node cannot later deny the data was sent by it.

8. *Denial of service*

In denial of service attack the attackers makes an attempt to make the network resources or a node or machine temporarily unavailable to its actual users. They sends fake requests to the target so that it becomes unavailable to service its intended users A malicious node launches the DoS attack by transmitting false control packets and using all the network resources. DoS can be launched by transmitting false routing messages or data packets. It can be identified if a node is generating control packets that are more than the threshold count in a particular time interval.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

9. *Jellyfish Attack*

Jellyfish attack is a type of passive attack which is difficult to detect because the attacker don't disobey any of the protocol rules. Cutting down the good put of the traffic to minimum or zero either by dropping the data packets or by changing the order of the data packets is the main objective of this attack. It is similar to blackhole attack, the only means by which it is different from blackhole attack is that in blackhole attack the attacker node drops the data packets but in jellyfish attack packets are delayed before transmission of packets and after reception of packets in the network. Jellyfish attack targets closed loop flows because such flows react to the network conditions like loss of packet and packet delay [6]. The first step to be taken by jellyfish attacker is to gain access to the routing mesh and intrude into the forwarding group [1]. Jellyfish attack is of 3 types [6]:

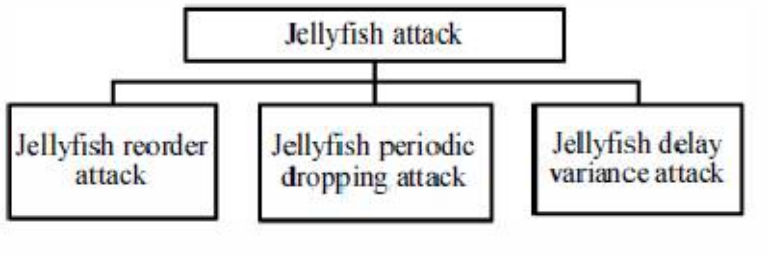

Figure 4 Types of Jellyfish attack

10. *Link Spoofing Attacks*

In a link spoofing attack, a malicious node advertises fake links with non-neighbours to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target‟s two-hop neighbours. This causes the target node to select the malicious node to be its multipoint relay (MPR). As an MPR node, malicious node can then manipulate date or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks .

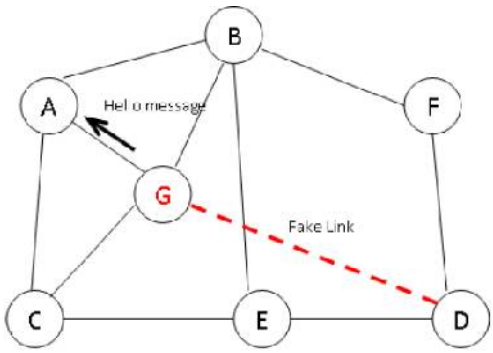

Figure 5 Link spoofing attack

Figure 5 shows an example of the link spoofing attack in an OLSR MANET. In the figure, we assume that node G is the attacking node, and node A is the target to be attacked. Before the attack, nodes B, C and G are MPRs for node A. During the link spoofing attack, node G advertises a fake link with node A‟s two-hop neighbour, that is, node D. According to the OLSR protocol, node A will select the malicious node G as its only MPR since node G is the minimum set that reaches node A‟s twohop neighbours. By being node A‟s only MPR, node G can then drop or withhold the routing traffic generated by node A .

Table 1 Comparison of Security Attacks in MANET

Attack	Attack Type	Layer	Security Attribute	Attack Category	Prevention Technique
DoS	Malicious, Active , Insider,	Multiyaer Attack	Availability	Active	Evasion,LMAC
Black Hole	Passive,	Network Layer	Availability	Active	SAODV

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

	Outsider	Attack			
Sybil Attack	Insider	Network Layer Attack	Authentication	Active	Light weight and robust detection technique
Worm Hole	Outside Malicious, Monitoring Attack	Network Layer	Confidentiality, Authentication	Active	DELPHI,SAW,HMTI
Byzantine	Active	Network Layer Attack	Authentication	Active	1. Response and recovery engine 2. Attack Defence System In MANET Using Game Theory.
Jamming	Active	MAC Layer Attack	Availability	Active	ARIDANE
Session Hacking	Active	Transport Layer Attack	Authentication , confidentiality	Active	ARAN, DSR
Repudiation	Active	Application Layer Attack	Availability	Active	SAODV
Jelly Fish	Active	Multilayer Attack	Availability	Active	Packet reordering using hashing concept
Link Spoofing	Active	Network Layer Attack	Availability, Authentication	Active	SEAD

IV. CONCLUSION

As MANETs continue to grow in capability and are becoming increasingly useful in many emerging applications, security is becoming inevitably a pressing property in the design of such networks. Known protocols and techniques for multicast routing, cryptography, and protection and attack detection that are used in conventional wired and wireless networks can be difficult to apply in MANETs. Substantial research efforts over the last decade have been focused on developing and implementing routing protocols and security techniques that better suite the nature of MANETs. In this paper various security attacks have been studied in detail and comparison of security attacks is done. Moreover, the table highlights which attacks are covered by each security technique and which attacks not fully covered yet.

REFERENCES

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Trans. Wireless Commun., vol. 11, pp. 38–47, Feb. 2004.
[2] Hoang Lan Nguyen *, Uyen Trang Nguyen,"A study of different types of attacks on multicast in mobile ad hoc networks", Elsevier, Ad Hoc Networks 6 (2008) 32–46
[3] Riteshkumar Vasava , Pradeep Gamit," A Survey of Attacks in Mobile Ad Hoc Network ",International Journal for Innovative Research in Science & Technology| Volume 1 | Issue 9 | February 2015
[4] Ahmed. M. Abdel Mo'men, Haitham. S. Hamza, IEEE Member, and Iman. A. Saroit," A Survey on Security Enhanced Multicast Routing Protocols in Mobile Ad Hoc Networks",2010 IEEE.
[5] Mohammed-Alamine El Houssainia, Abdessadek Aarouda, Ali El Horea, Jalel Ben Othmanb "Detection of Jamming Attacks in Mobile Ad Hoc Networks using Statistical Process Control", The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)
[6] Er.Kiran Narang, Sonal,"A Study Of Different Attacks In Manet And Discussion About Solutions Of Black Hole Attack On Aodv Protocol ",International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013
[7] Simranpreet Kaur, Rupinderdeep kaur, R.K Verma,"Jellyfish attack in MANETs: A Review", 2015 IEEE
[8] Amandeep Kaur1, Dr. Amardeep Singh2 ,"A Review on Security Attacks in Mobile Ad-hoc Networks",IJSR, Volume 3 Issue 5, May 2014
[9] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang," Security Mobile Ad Hoc Networks:Challenges And Solutions", Ieee Wireless Communications ,February 2004