IJCSN - International Journal of Computer Science and Network, Volume 3, Issue 6, December 2014
ISSN (Online): 2277-5420 **www.IJCSN.org**
Impact Factor: 0.274

The Comparative Study of Security Mechanism in Mobile Ad-hoc Networks

[1] Balamurugan G, [2] Somasundaram R, [3] Sumithra K

[1,2,3] M.TECH, Department of Computer Science & Engineering,
Manakula Vinayagar Institute of Technology,
Pondicherry University, Pondicherry, India

Abstract - Security mechanism in wireless ad-hoc networks is a highly a challenging concern. Security in the MANET communication network is significant for secure transmission of information. Many security mechanisms for mobile ad-hoc network (MANET) have been proposed in the day to day events. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more susceptible to cyber attacks than wired network there are a number of attacks that affect MANET. In MANET, all networking functions such as routing and packet distribution are performed by nodes in a self organizing manner. Due to these reasons, securing a Mobile Ad-hoc Network is very challenging.

We consider the most common types of attacks, namely rushing attack, black hole attack, neighbor attack and jellyfish attack. Exclusively, we study how the number of attackers affects the performance metrics of a multicast session such as throughput, end-to-end delay, packet delivery ratio and delay jitter.

Keywords - *MANET, Security mechanism, rushing attack, black hole attack, neighbor attack and jellyfish attack***.**

1. Introduction

A Mobile Ad-hoc Network is a set of independent mobile nodes which will communicate with one another node via Radio waves. The mobile nodes that are in radio vary of every different will directly communicate, whereas others nodes are got to aid of intermediate nodes to route their packets. Every of the node contains a wireless interface to speak with one another. These networks are distributed totally, and may work anyplace while not the assistance of any mounted infrastructure as access points or base stations. In MANET, all networking functions like routing and packet forwarding, are performed by nodes themselves during a self-organizing manner. For these reasons, securing a mobile ad -hoc network is incredibly difficult. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

1.1 Availability

Availability relates both data and to services. It ensures the stability of network service despite denial of service attack.

1.2 Confidentiality

Confidentiality provides that computer-related resources are accessed solely by approved parties. It wants to be protected against any revealing attack like eavesdropping-unauthorized reading of message.

1.3 Integrity

Integrity means resources will be changed solely by approved parties solely in approved manner. Integrity assures that a message being transferred isn't corrupted.

1.4 Authentication

Authentication is actually guarantees that the nodes in communication are genuine and not impersonators. The recourses of network ought to be accessed by the genuine nodes.

1.5 Authorization

Authorization property assigns completely different access rights to differing kinds of users. as an example a network management will be performed by network administrator solely.

1.6 Resilience to Attacks

In this property assigns completely different access rights to differing kinds of users. As an example a network

management will be performed by network administrator solely.

1.7 Freshness

It ensures that malicious node does not resend previously captured packets.

2. Classification of Security Attacks

The attacks can be categorized on the basis of behavior of the attack i.e. Passive or Active attack.

2.1 Passive Attacks

A passive attack does not alter the data broadcasted within the network. But it includes the unauthorized "view" to the network traffic or accumulates data from it. Passive attacker does not disturb the operation of a routing protocol but attempts to discover the important information from routed traffic.

2.2 Active Attacks

Active attacks are very severe attacks on the network that avoid message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside basis that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks.

These attacks produce unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS (Denial of service), congestion etc.

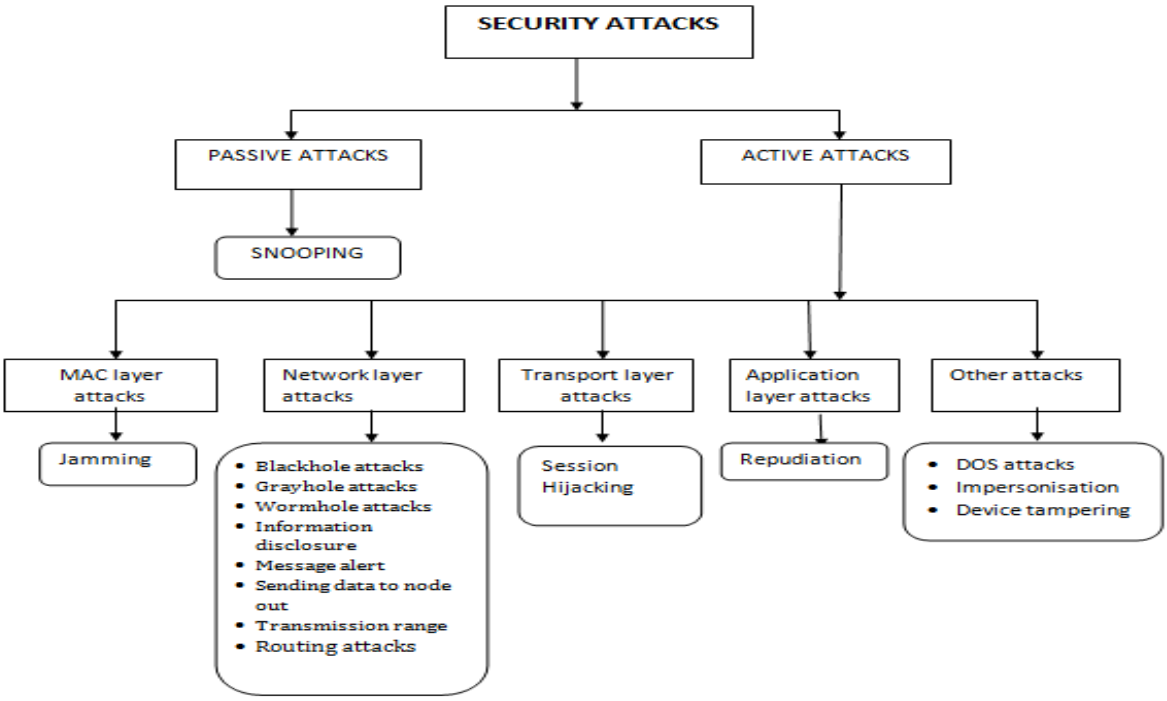

Fig. 1 Classification of Security Attacks for different layers.

Active attacks are classified into three groups:

Dropping Attacks: Compromised nodes or malicious nodes can drop all packets that are not meant for them. Dropping attacks can prevent end-to-end communications between nodes.

Modification Attacks: These attacks modify packets and disturb the overall communication between network nodes. Sinkhole attacks are the example of modification attacks.

Fabrication Attacks: In fabrication attack, the attacker send false message to the neighboring nodes without receiving any connected message.

The characteristics of MANETs make them vulnerable to many new attacks. These attacks can occur in different layers of the network protocol stack.

Table 1: Attacks in different layers of the network

LAYER	TYPES OF ATTACKS
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attacks, SYN Flooding attack
Network	Blackhole,wormhole,Sinkhole,Link spoofing, Rushing attacks, Replay attack, Link withholding, Resource consumption attack, Sybil attack
Data Link	Selfish misbehavior, malicious behavior, traffic analysis
Physical	Eavesdropping, jamming, active interference

2.3 Attacks at Physical Layer

Some of the attacks identified at physical layer include eavesdropping, interference, and jamming etc.

2.3.1 Eavesdropping

It can also be defined as interception and reading of messages and conversations by unintended receivers. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication.

2.3.2 Jamming

Jamming is a special class of DoS (Denial of service) attacks which are initiated by malicious node after determining the frequency of communication. Jamming attacks also prevents the reception of legitimate packets.

2.3.3 Active Interference

An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications.

2.4 Attacks at Data Link Layer

The data link layer can classify attacks as to what effect it has on the state of the network as a whole.

2.4.1 Selfish Misbehavior of Nodes

The selfish nodes may refuse to take part in the forwarding process or drops the packets purposely in order to preserve the resources and to preserve of battery power.

2.4.2 Malicious Behavior of Nodes

The main task of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighboring nodes. Attacks of such type are fall into following categories.

2.4.3 Denial of Service (DoS)

The avoidance of unauthorized access to resources or delaying of time-critical operations. A denial of service (DoS) attack is characterized by an attempt by an attacker to prevent genuine users of a service from using the desired resources and attempts to “flood” a network, thereby preventing genuine network traffic.

2.4.4 Misdirecting Traffic

A malicious node advertises wrong routing information in order to get protected data before the actual route.

2.4.5 Attacking Neighbor Sensing Protocols

Malicious nodes advertise false error messages so that important links interface are marked as broken.

2.5 Attacks at Network Layer

The basic idea behind network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic.

2.5.1 Black hole Attack

In this type of attacks, malicious node claims having a finest route to the node whenever it receives RREQ packets, and sends the RREP with highest destination sequence number and minimum hop count value to originator node, whose RREQ packets it wants to stop.

For example, in figure 2, when node "S" source wants to send data to destination node "D", it initiates the discovery of route process. The malicious node "M" when receives the route request, it directly sends response to source. If reply from node "M" reaches first to the source than the source node "S" ignores all other reply messages and begin to send packet via route node "M". As a result, all data packets are consumed or lost at malicious node.

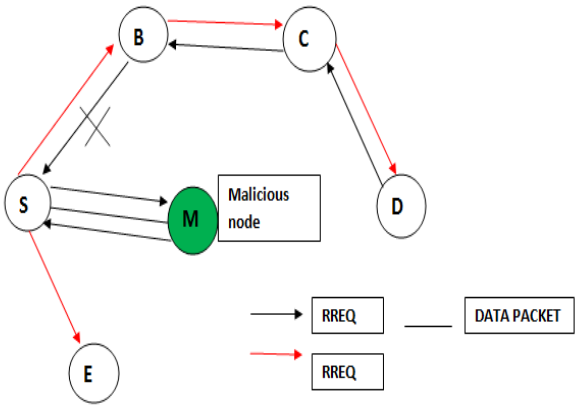

Fig 2 Black hole attack.

2.5.2 Rushing Attack

In rushing attacks when negotiation node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet For example; in figure 3 the node "4" represents the rushing attack node, where "S" and "D" represents to source and destination nodes. The rushing attack of compromised node "4" quickly broadcasts the route request messages to ensure that the RREQ message from itself arrive earlier than those from other nodes.

This result in when neighboring node of "D" i.e. "7" and "8" when receive the actual (late) route request from source, they simply discard requests. So in the presence of such attacks "S" fails to discover any useable route or safe route without the involvement of attacker.

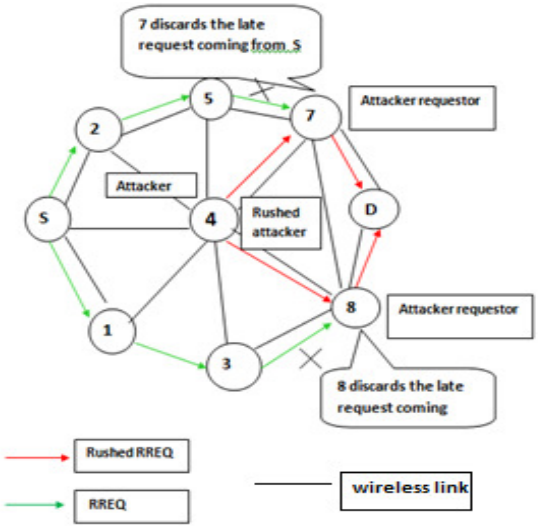

Fig. 3 Rushing attack.

2.5.3 Wormhole Attack

In wormhole attack, malicious or vulnerable node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious nodes is said to as a wormhole. For example in figure 4, the nodes "X" and "Y" are malicious node that forms the tunnel in network. The Originating node "S" when initiate the RREQ message to find the route to node "D" destination node.The immediate neighbor node of originating node "S", namely "A" and "C" forwards the RREQ message to their respective neighbors "H" and "X". The node "X" when receive the RREQ it immediately share with it "Y" and later it initiate RREQ to its neighbor node "B", through which the RREQ is delivered to the destination node "D". Due to high speed link, it forces the source node to select route <S-A-B-D> for destination. It results in "D" ignores RREQ that arrives at a later time and thus, cancel the genuine route <S-C-H-E-F-D>.

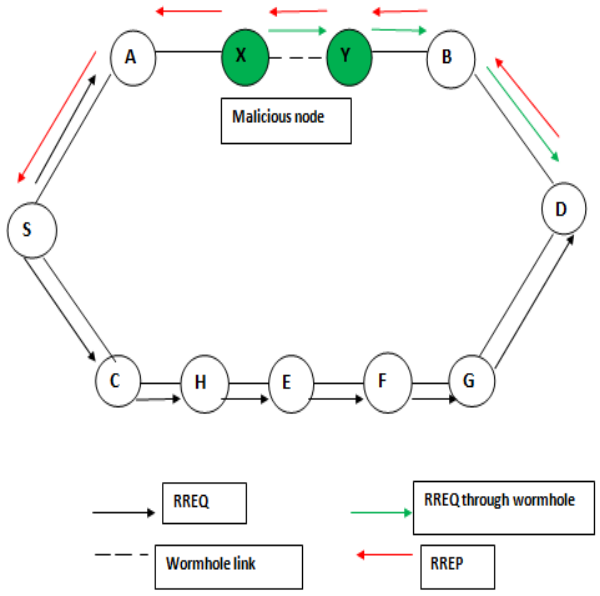

Fig. 4 Wormhole attack.

2.5.4 Grey Hole Attack

In this type of attacks, malicious node maintains having an optimum route to the node whose packets it wants to stop. It is similar to black hole attack but it drops data packet of a particular node.

2.5.5 Sinkhole Attack

In sinkhole Attack, a compromised node or malicious node publicize wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving whole network traffic it modifies the secret information, such as changes made to data packet or drops them to make the network complex. A malicious node tries to attract the secure data from all neighboring nodes.

2.5.6 Sybil Attack

Sybil attack refers to the many copies of malicious nodes. It can be happen, if the malicious node distributes its secret key with other malicious nodes. This way the number of malicious node is increased in the network and the possibility of the attack is also increased. If we use the multipath routing, then the possibility of choosing a path in the network, those contain the malicious node will be increased. The Sybil attack particularly aims at distributed system environments. The attacker tries to act as several different identities/nodes rather than one. Since Ad-hoc networks depend on the communication between nodes, many systems relate redundant algorithms to make sure that the data gets from source to destination. A consequence of this is that attackers have a harder time to destroy the integrity of information

2.6 Attacks at Transport Layer

2.6.1 Session Hijacking

Attacker in session hijacking takes the advantage to develop the unprotected session after its initial setup. In this attack, the attacker spoofs the injured node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks.

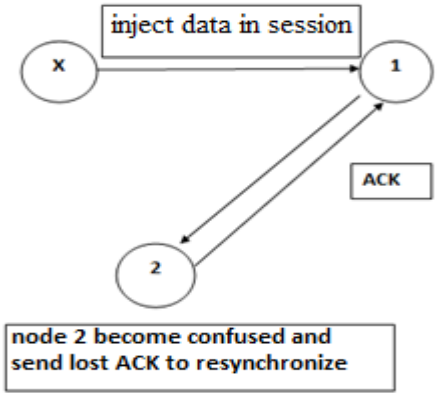

Fig. 5 Session Hijacking.

2.7 Attacks at Application Layer

2.7.1 Malicious Code Attacks

Malicious code attacks includes Viruses, Worms can affect both operating system and user application.

2.7.2 Multi-layer Attacks

2.7.2.1 Denial of Service In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network.

2.7.2.2 Distributed DoS Attack Distributed denial of service attack is more severe form of denial of service attack because in this attack several opposition that are distributed throughout the

network scheme and prevent legitimate users from accessing the services offered by the network.

2.7.2.3 Jamming attack involves in, the attacker initially keeps examining the wireless medium in order to determine the frequency at which the destination node is receiving signals from the sender. It then transmits signals on that frequency so that error free reception at the receiver is hindered.

2.7.2.4 Impersonation attacks are launched by using other node's identity, such as IP or MAC address. Impersonations attacks are sometimes are the first step for most attacks, and are used to launch further, more sophisticated attacks.

2.7.2.5 Mobile virus and worm attacks include in the application layer contains user data, and it normally supports many protocols such as HTTP, SMTP and FTP. Malicious code, which includes viruses and worms, is applicable across operating systems and applications.

As we know, malicious programs are widely increased in networks. There are a number of techniques by which a worm can discover new machines to exploit. One example is IP address scanning used by Internet worms. That technique consists of generating probe packets to a vulnerable UDP/TCP port at many different IP addresses. Hosts that are hit by the scan respond, receive a copy of the worm, and hence get infected. The Code Red worm is one of the scanning worms.

3. Conclusions

Maintaining of dynamic topology and the distributed operation on MANET is more vulnerable to many attacks. In this paper, we discuss various types of security attacks and its function. Different security mechanisms are introduced in order to prevent MANET and also identify the type of attack which has been occurred in the MANET.

References

[1] Priyanka Goyal, Vinti Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[2] Gaga deep, Aashima and Pawan Kumar "Analysis of Different Security Attacks in MANETs on Protocol Stack". International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012

[3] Mohammad Wazid, Rajesh Kumar Singh and R. H. Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques "International Journal of Computer Applications® (IJCA) International Conference on Computer Communication and Networks CSI- COMNET2011.

[4] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao " A survey of black hole attacks in wireless mobile ad hoc networks" Human-centric Computing and Information Sciences 2011

[5] Sunil Taneja and Ashwani Kush, " A Survey of Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, 279-285, August 2010.

[6] Gary Breed Editorial Director, "Wireless Ad-Hoc Networks: Basic Concepts", High Frequency Electronics, March 2007.

[7] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks" IEEE Communications Magazine • October 2002

[8] Mohseni, S.; Hassan, R.; Patel, A.; Razali, R, "Comparative review study of reactive and proactive routing protocols in MANETs", 4th IEEE International Conference on Digital Ecosystems and Technologies, 304-309, 2010.

[9] Humayun Bakht, "Survey of Routing Protocols for Mobile Ad-hoc Network", International Journal of Information and Communication Technology Research, 258-270, October 2011.

[10] Mohit Kumar and Rashmi Mishra "An Overview of MANET: History, Challenges and Applications", Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.

[11] C. Perkins, E. Belding-Royer and S. Das, "Ad-Hoc On-Demand Distance Vector (AODV) Routing", RFC3561, July 003.

[12] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Low Price Edition, Pearson Education, 2007, pp. 521.

[13] Dokurer, Semih."Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, Atılım University, September 2006.

[14] Payal N. Raj, Prashant B. Swadas. "DPRAODV: A Dynamic Learning System against Black hole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, 2:54-59, 2009.

[15] Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering, 2:1, 2008.

[16] Emmanouil A. Panaousis, Levon Nazaryan, Christos Politis,"Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications", Mobimedia'09, September 7-9, 2009, London, UK.

[17] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

Authors

BALAMURUGAN G , M.Tech., student in a stream of Computer Science & Engineering at Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.

SOMASUNDARAM R , M.Tech., student in a stream of Computer Science & Engineering at Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.

SUMITHRA K, M.Tech., student in a stream of Computer Science & Engineering at Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.