zDiverse Attack Vulnerabilites in MANET

Er. Reema Gupta Sukhvir Singh Pardeep Maan Pooja
NCCE, Israna (Panipat)

Summary
A MANET is an infrastructure-less type network, which consists of number of mobile nodes with wireless network interfaces In order to make communication among nodes, the nodes dynamically establish paths among one another. Security is an essential service for wired and wireless network communications. The success of mobile ad hoc networks (MANET) strongly depends on people's confidence in its security. In this paper we discuss various types of attacks on various layers under protocol stack. All these vulnerabilities attempt to affect the overall performance and throughput of the network. On the basis of the nature of attack interaction, the attacks against MANET may be classified into active and passive attacks. Attackers against a network can be classified into two groups: insider and outsider. Whereas an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs.

Keywords
MANET; MANET Attack; passive attack;Active attack; Vulnerabilities in MANET.

I. Introduction

Mobile ad hoc networks are collection of wireless networks, which consists of large number of mobile nodes. Nodes in MANETs can join and leave the network dynamically. There is no fixed set of infrastructure and centralized administration in this type of networks. Nodes are interconnected through wireless interface. The basic requirements for a secured networking are secure protocols which ensure all the principles of security (confidentiality, availability, authenticity, integrity) of network. Many existing security solutions for wired networks are ineffective and inefficient for MANET environment. There are a wide variety of attacks that target the weakness of MANET[1,9]. Attacks can be passive as well as active attack. Active attacks are those attacks which attempt to alter, inject, delete or destroy the data being exchanged in the network. But the passive attacks are those attacks which attempt to learn or make use of information but do not affect the system resources. Such an attack has no intention to damage the network & network operations because it does not modify the contents of the packets. In MANET both types of attacks occurred. On the basis of Location, security vulnerabilities can be of 2 types: Internal and External Attacks. External attacks which are carried out by nodes or group of nodes that do not belong to the network. Internal attacks which are carried out by nodes or group of nodes that are actually part of the network.

This paper is organized as follows. Section II includes Classification of security attacks in MANET on the basis of behaviour, location of attack. Section III presents the MANET protocol stack. Section IV security vulnerabilities on various layers of MANET stack. Section V describes the conclusion and future scope.

I. CLASSIFICATION OF SECURITY ATTACKS IN MANET

Due to lack of security in MANET, this network is vulnerable to various attacks not only from outside but also from within the network itself. MANET attacks can be categorized into various types based on behavior of attack, source of attack.

A. BASED ON BEHAVIOUR OF ATTACK

1. *PASSIVE ATTACK*:

These attacks do not affect system resources but steal vulnerable information of the network, system. Such an attack has no intention to damage the network & network operations because it does not modify the contents of the packets. Example: Eavesdropping, Release of message contents and Traffic analysis. This type of attack is difficult to find out in the network as it does not interrupt any ongoing operation in the network.

2. *ACTIVE ATTACK*:

This attack affects our system resources and has an intention to damage network, system. Example: Fabrication or masquerading attacks message modifications, message replays and DOS attacks. Attackers may or may not part of network. Attacker if already in the network, the attack also called internal attack. If attacker is not part of the network, the attack called external attack.

B. BASED ON LOCATION[2] OF ATTACK

1. *INTERNAL ATTACK*:

This type of attack is carried out by an authorized node or a group of node that are part of network. Internal attack is difficult to detect as compared to other attacks. Node that act for this type of attack may be compromised node or a misbehave node. Node called to be compromised if it works on instructions given by external attacker but carried out by internal node. In case a node called misbehave if it under utilizes resources and do not follow rules of the network wholly.

Manuscript received March 5, 2015
Manuscript revised March 20, 2015

2. *EXTERNAL [2,3] ATTACK*:
Those attacks which are carried out by nodes or group of nodes that do not belong to the network. Such attacks send fake packets in order to interrupt the performance of the network. External attacks try to cause congestion in the network, denial of services and advertising wrong routing information so that delay in the routing or congestion increases and performance degrades.

2. Overview of manet protocol stack

MANET Protocol stack is same as that of TCP/IP[10] consists of 5 layers (Physical layer, Data link layer, Network layer, Transport layer, Application layer).But the difference is that MANET protocol stack is susceptible to more attacks as compared to other networks due to dynamic topology and movement of one node from one network to another. Active attacks make compromise of integrity, authentication (principles of secure network) that should be followed for secure transmission are compromised in the MANET. There is need of defense mechanism against these type of attacks in MANET to make secure data transmission in the network.

APPLICATION LAYER
TRANSPORT LAYER
NETWORK LAYER
DATA LINK LAYER
PHYSICAL LAYER

Fig. 1 MANET PROTOCOL STACK

3. Security Vulnerability [1,3,4]on various layers of manet stack

A. **Security Vulnerabilities at Physical Layer :**
The attacks that fall at the physical layer of stack is done with help of hardware. These attacks do not need to understand complete technology or process. Under this layer eavesdropping, Jamming and active interference types of attack comes into the role.
1. *Eavesdropping* -
Secretly[9] listen to a network to gather some secret private information in the network. It is passive attack that is unknown to both sender and receiver. After receiving secret messages or secret information fake messages can be transmitted to receiver imposed like real sender. Gaining secret information like login information, id, password, key used for encryption purpose.
2. *Jamming and Active Interference* -
Radio signal corrupt the message that is send by the attacker which is more powerful as compared to other signals. For this attack to come into existence attacker passively listen the network to know the frequency at which sender sends the data.

B. **Security Vulnerabilities at Data Link Layer:**
1. *Selfish Misbehaviour of Nodes* -
In the MANET data transmission is done from node to node from one network to another. So the behavior of node matter, if the node act as selfish, do not forward packets to other node performance degrades. Packet dropping is one of the main attacks in selfish misbehavior of nodes which leads to congestion and help to prevent communication between determined nodes.
2. *Malicious Behaviour of nodes*-
In this node want to degrade the performance by disrupting the operations. Node introduces wrong routing information, fake advertisement of messages and fake error messages so that link between determined node set as infinity or broken.
3. *Traffic Analysis* –
By monitoring the traffic between nodes, the type of communication, location of nodes among which communication take place, topology of nodes in network, routing algorithm used known to the attacker.

C. Security Vulnerabilities[8] at Network Layer:
Routing decisions are done in network layer. The network layer protocols enable the MANET nodes to be connected with another through hop-by-hop.
1. *ROUTING ATTACK*:
In this attack attacker inject between the node that are communicating and control the flow of traffic and divert the packets that introduce delay[8] and degrade the performance.
Routing table overflow attack is one type of attack comes under this category. The attacker tries to create enough routes to prevent new routes from being created. The proactive routing algorithms are more vulnerable to table overflow attacks because proactive routing algorithms attempt to discover routing information before it is actually needed.
2. *BLACKHOLE ATTACK*:
In this attack attacker node consumes all the data packets as it reply fast to the RREQ of a source node with highest no. the requesting nodes assume that route discovery process is completed and ignore other RREP messages and keep sending packets over malicious node. Malicious node may forward one or two packets with delay or may not forward the packets to destination. Malicious node may send fake RREP to source node regarding messages.
3. *WORMHOLE ATTACK*[2,5] :
In wormhole attack, malicious 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 referred to as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack

is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

4. *Byzantine* [2] *ATTACK*:

A compromised intermediate node works alone, or a set of compromised intermediate nodes 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.

5. *Sinkhole*[3] *Attack*:

Sinkhole attacks affects the performance of Ad hoc networks protocols such as AODV by using flaws as maximizing the sequence number or minimizing the hop so that the path presented through the malicious node appears to be the best available route for the nodes to communicate.

6. *SYBIL ATTACK*:

In Sybil attack, Sybil attacker may generate fake identities of number of additional nodes. In this, a malicious node produces itself as a large number of instead of single node. The additional identities that the node acquires are called Sybil nodes. Real node realize that it has N neighbours but in reality it has M neighbours (N>M) ; N-M shows the fake identities of additional nodes.

7. *REPLAY ATTACK* :

In MANETs, the topology is not fixed; it changes frequently due to mobility of nodes. In replay attack, a malicious node record control messages of other nodes and resends them later. This results in other nodes to record their routing table with stale routes. These replay attacks are later misused to disturb the routing operation in a MANETs.

D. **Security Vulnerabilities at Transport Layer :**

The objectives of Transport layer protocols in MANET include setting up of end-to-end connection, end-to-end reliable delivery of packets, flow control, congestion control, clearing of end-to-end connection. In the Internet, the mobile node is vulnerable to the classic SYN flooding attack
or session hijacking attacks.

1. *SYN flooding attack* :

The SYN flooding [10]attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection.

During the attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The SYNACK packets are sent out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the response of ACK packet. Without any response of ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed-size table while it awaits the acknowledgement of the three-way handshake, all of these pending connections could overflow the buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection.

2. *Session hijacking* :

Session hijacking takes advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter. In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. Thus the attacker impersonates the victim node and continues the session with the target.

E. **Security Vulnerabilities at Application Layer:**

End user applications are accessed by the users with the help of this layer. This end user application needs to be connected with storage devices and applications. Since storage devices are prone to many viruses so security vulnerabilities at this layer. Protocols such as HTTP, SMTP, TALNET and FTP, which provides many vulnerabilities and access points for attackers.

1. *Malicious code attacks* : Malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application. These malicious programs usually can spread themselves through the network and cause the computer system and networks to slow down.

2. *Repudiation attack* : Repudiation refers to a denial of participation in all or part of the communications.

4. Conclusion And Future Work

This paper concludes the various categories of attacks in MANET. Due to dynamic infrastructure of MANETs and having no centralized administration makes such network more vulnerable to many attacks. MANET is growing field but requires special countermeasures against attacks. In this paper, different attacks on MANET stack has been discussed. Therefore, our aim is to develop secure routing protocols, algorithms and trust based systems to avoid these security vulnerabilities to disrupt the mobile ad-hoc network operations.

References

[1] "Protocol Stack based Security Vulnerabilities in MANETs", Jatiner Pal Singh,Anuj Kr. Gupta

[2] "Attacks against Mobile Ad Hoc Networks Routing Protocols" S. A. Razak, S. M. Furnell, P. J. Brooke

[3] " A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei

[4] "Analysis of Different Security Attacks in MANETs on Protocol Stack Review" Gagandeep, Aashima, Pawan Kumar International Journal of Engineering and Advanced

Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012
[5] "Security Issues in Mobile Ad Hoc Networks - A Survey". Wenjia Li and Anupam Joshi
[6] "Analysis and Diminution of Security Attacks on Mobile Ad hoc Network". K.P. Manikandan, Dr. R .Satyaprasad, Dr. Rajasekhararao IJCA Special Issue on "Mobile Ad-hoc Networks "MANETs, 2010
[7] "Security Threats in Mobile Ad Hoc Networks". Sevil ¸ Sen, John A. Clark, and Juan E. Tapiador
[8] "Security Threats in Mobile Ad Hoc Network" Kamanshis Biswas and Md. Liakat Ali
[9] "Security Aspects in Mobile Ad Hoc Network(MANETs): Technical Review" Monika, Mukesh Kumar & Rahul Rishi International Journal of Computer Applications (0975 – 8887) Volume 12– No.2, November 2010.
[10] "A Protocol Layer Survey of Network Security"John V. Harrison,Hal Berghel Center for Cybersecurity ResearchUniversity of Nevada , Las Vegas
[11] C. Murthy and B. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols.

Reema Gupta received B.Tech. In Computer Science & Engineering from Guru Jambheshwar University, hissar in 2012. Presently She is pursuing her M.Tech in Computer Science & Engineering from N.C College of Engineering , ISRANA(Panipat) and qualified GATE with 97%.

Sukhvir Singh received M.tech in software engineering and system analysis from state engineering university of Armenia in 1996 and doctor of Philosophy (PHD) from MDU University, Rohtak in 2013.
Presently working as Associate Professor & Head of the department in Computer Science & Engineering department of NCCE, ISRANA.

Pardeep Maan received B.SC. in Computer Science in 2006 and MCA from N.C. College of Engineering in 2009 . Presently working as Lecturer in MCA Department of NCCE(NCICS), Israna, Panipat. He has qualified UGC-Net in 2012.

Pooja Dahiya received P.G.D.C.A. from I. B. COLLEGE, PANIPAT in
2011 and M.sc (CS) from KUK in 2012. Now she is pursuing M.tech
Computer Science & Engineering from N.C College of Engineering ,
ISRANA(Panipat).