International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 2 Issue 9, Nov.-Dec., 2013, pp: (26-29), Available online at: **www.erpublications.com**

A survey on different attacks in MANET

Patel Chirag R.[1], Patel Tushar S.[2]
ME (CSE Student), S. P. B. Patel Engineering College, Mehsana, Gujarat, India
IT Department, S. P. B. Patel Engineering College, Mehsana, Gujarat, India

Abstract: With the progression of computer networks extending boundaries, Mobile ad hoc network (MANET) has emerged as a new frontier of technology to provide anywhere, anytime communication. Due to its deployment nature, MANETs are more vulnerable to malicious attack. The absolute security in the mobile ad hoc network is very hard to achieve because of its fundamental characteristics, such as dynamic topology, open medium, limited power and limited bandwidth. The Prevention methods like authentication and cryptography techniques alone are not able to provide the security to these types of networks. Therefore, efficient intrusion detection must be deployed to facilitate the identification and isolation of attacks. In this paper define all layer attacks with its description, Challenges & characteristics.

I. Introduction

A mobile ad hoc network (MANET) is comprised of mobile hosts that can communicate with each other using wireless links. It is also possible to have access to some hosts in a fixed infrastructure, depending on the kind of mobile ad hoc network available. Some scenarios where an ad hoc network can be used are business associates sharing information during a meeting, emergency disaster relief personnel coordinating efforts after a natural disaster such as a hurricane, earthquake, or flooding, and military personnel relaying tactical and other types of information in a battlefield. In this environment a route between two hosts may consist of hops through one or more nodes in the MANET. An important problem in a mobile ad hoc network is finding and maintaining routes since host mobility can cause topology changes.

Defending MANET networks is much more challenging than defending traditional enterprise networks for a variety of reasons. Characteristics such as volatility, mobility, as well as the ease of listening to wireless transmissions make the network inherently less secure. Existing tools usually assume a well-structured and static network and therefore can not be used as they are. MANET networks are also much more dynamic and unpredictable because connectivity depends on the movements of nodes, terrain, changes in the mission (e.g. for a military application or a first responder application), node failures, weather, and other factors. As a result, it is difficult to accurately characterize normal behavior. Hence, it is often difficult to distinguish malicious behavior from normal but unexpected events.

The rest of the paper is organized as follow: Section 2 describes various possible attacks on mobile as hoc networks. Section 3 describes overview of AODV protocol and flooding attack description. Section 4 describes various existing techniques for detecting flooding attack in MANET. Finally conclusion is presented in the last section.

II. Various Attacks on MANET

(1) Wormhole Attack:

In wormhole attack, a malicious node, receives packets 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 colluding attackers is referred to as wormhole.

(2) Black hole Attack:

An attacker listen the requests for the routers in a flooding based protocol .When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route and enters into the pathway to do anything with the packets passing between them.

(3) In this attack, a compromised intermediate node or a asset of compromised intermediate nodes works in collision and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which result in disruption or degradation of the routing services.

(4) Resource Consumption Attack: In this attack, an attacker tries to consume or waste away resources of the other nodes present in the network. The resources that are targeted are battery power, band width and computational power.

(5) Session Hijacking: At first the attacker spoofs the IP address of target machine and determines the correct sequence number. After that he performs s DOS attack on the victim. As a result the target system becomes unavailable for sometimes. The attacker now continues the session with the other system as a legitimate system.

(6) Denial of service (DoS): In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network.

(7) Jamming: In this form of attack, the attacker initially keeps monitoring 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.

III. Classification

Table of Different Layer Attacks

Attacks	Sub-Attacks	Description
Active Attacks	Modification Message	It means that some portion of legitimate message is altered, or that message is delay or reordered to produce an unauthorized effect.
	Denial of service	Prevent normal use or management of communication facilities.
	Replay	Involves the passive capture of a data unit and subsequent retransmission to produce an unauthorized effect.
	Masquerade	Takes place when one entity pretends to be a different entity
Passive Attacks	Release of message contents	It can easily understood like telephone conversation ,electronic mail, etc. But not modification in it.
	Traffic analysis	It captured the message and know about which pattern is use in this message but could not abstract the information
Modification	Packet misrouting attacks	malicious nodes reroute traffic from their original path to make them reach the wrong destinations
	Impersonation attacks Or spoofing attacks	are attacks where malicious node assumes the identity of another node in the networks
Interception	Wormhole attacks	a compromised node in the ad hoc networks colludes with external attacker to create a shortcut in the networks.
	Black hole attacks	malicious nodes trick all their neighboring nodes to attract all the routing packets to them
Fabrication	Sleep deprivation attacks	The aim is to drain off limited resources in the mobile ad hoc nodes (e.g. the battery powers), by constantly makes them busy processing unnecessary packets.
	Route salvaging attacks	Route salvaging attacks are launched by the greedy internal nodes in the networks.
Interruption	Packet dropping attacks	Direct interruption to the routing messages could be done by using the packet dropping attacks.
	Flooding attacks	Adversaries also might interrupt the normal operations in the packet forwarding process by flooding the targeted destination nodes with huge unnecessary packets.
	Lack of cooperation attacks	Lack of cooperation from the internal nodes to participate in the network operations can also be seen as an attempt to launch a refusal of service attack

IV. Characteristics

1. Dynamic topology
2. Distributed operation
3. Resource constraints
4. Some other kind of characteristics
   - 4.1 Behaviors of the attacks (passive vs. active)
   - 4.2 The source of the attacks (external vs. internal)
   - 4.3 The processing capability of the attackers (mobile vs. Wired)

V. Challenges:

Regardless of the attractive applications, the features of MANET introduce several challenges that must be studied carefully before a wide commercial deployment can be expected. These include [15, 16]:

9.1 Routing: Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multi cast routing is another challenge because the multi cast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

9.2 Security and Reliability: In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility-induced packet losses, and data transmission errors.

9.3 Quality of Service (QoS): Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services.

9.4 Inter-networking: In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management
.

9.5 Power Consumption: For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.
9.6 **Multicast**: Multicast is desirable to support multiparty wireless communications. Since the multicast tree is no longer static, the multicast routing protocol must be able to cope with mobility including multicast membership dynamics (leave and join).

VI. Related Work

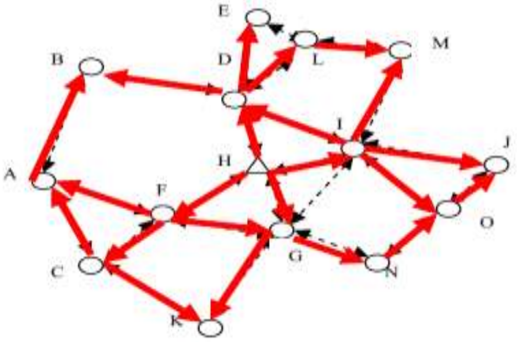

Fig.: Demonstration of flooding attack [4]

A simple mechanism proposed to prevent the flooding attack in the AODV protocol [2]. In this approach, each node monitors and calculates the rate of its neighbors' RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. The limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake.

In [3], the authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. Similar to [2], in this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the preset time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed in [2], where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

Resisting flooding attacks in ad hoc networks presented in [4] describes two flooding attacks: Route Request (RREQ) and Data flooding attack. In RREQ flooding attack the attacker selects many IP addresses which are not in the network or select random IP addresses depending on knowledge about scope of the IP address in the network. Using neighborhood suppression, a single threshold is set up for all neighboring nodes. In Data flooding attack the attack node first sets up the path to all the nodes and send useless packets. The given solution is that the data packets are identified in application layer and later path cutoff is initiated.

A new trust approach based on the extent of friendship between the nodes is proposed which makes the nodes to co-operate and prevent flooding attacks in an ad hoc environment in [5]**.** All the nodes in an ad hoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighboring nodes. A trust estimator is used in each node to evaluate the trust level of its neighboring nodes. The trust level is a function of various parameters like length of the association, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, average time taken to respond to a route request etc. Accordingly, the neighbors are categorized into friends (most trusted), acquaintances (trusted) and strangers (not trusted).

To prevent RREQ flooding, the threshold level is set for the maximum number of RREQ packets a node can receive from its neighbors [5]. To prevent DATA flooding, the intermediate node assigns a threshold value for the maximum number of data packets it can receive from its neighbors. If Xrs, Xra, Xrf be the RREQ flooding threshold for a stranger, acquaintance and friend node respectively, Xrf > Xra > Xrs. If Yrs, Yra, Yrf be the DATA flooding threshold for a stranger, acquaintance and friend node respectively then Yrf > Yra > Yrs. If the specified threshold level is reached, further RREQ packets from the initiating node are ignored and dropped. Thus, flooding is prevented in the routing table.

VII. Conclusion

Most of the MANET IDSes tend to have the distributed architectures and their variants. The IDS architecture may depend on the network infrastructure. We have presented several existing methods to detect flooding attack in mobile ad hoc networks. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the security system itself. Accordingly, the study of the defense to such attacks should be explored as well.

References

[1]. H.–Y. Chang, S.F. Wu and Y.F. Jou, "Real-Time Protocol Analysis for Detecting Link-State Routing Protocol Attacks", ACM Tran. Inf. Sys.Sec., 1, Pp. 1-36, 2001.

[2]. Yi Ping, Hou Yafei, Bong Yiping, Zhang Shiyong & Dui Zhoulin, "Resisting Flooding Attacks in Ad Hoc Networks", International Conference on Information Technology: Coding and Computing (ITCC'05).

[3]. S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[4]. Abdul Hadi Abd Rahman and Zuriati Ahmad Zukarnain, ― Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks., European Journ al of Scientific Research, ISSN 1450-216X Vol.31 No.4, pp. 566-576, 2009.

[5]. Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao, "Performance Analysis of Flooding Attack Prevention Algorithm in MANETs", World Academy of Science, Engineering and Technology 56 2009.