International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 14, Issue 01) and (Publishing Month: June 2014)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

A Survey Paper on Attacks in Mobile Ad-Hoc Network

Poonam[1] and Sheetal Chaudary[2]

[1]MKJK Mahavidyalya, Rohtak, Haryana (India)
[2]M.D.U. Rohtak, Haryana (India)

Abstract

Mobile ad hoc networks are a new paradigm of wireless communication. A Mobile Ad hoc Network (MANET) is a dynamic wireless network that can be formed infrastructure less connections in which each node can act as a router. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. There are various challenges that are faced in mobile ad hoc environment. In Present years, the security is an essential requirement in mobile ad hoc network. In comparison to wired network the mobile ad hoc network (MANET) is more exposed to being attacked. Because of its fundamental Properties, such as dynamic topology, limited power and limited bandwidth, it is very hard to achieve absolute security in the mobile ad hoc network. . MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In this paperwork we pay attention to the different attacks within Mobile ad hoc networks such as active (flooding, black hole, spoofing, and wormhole) and passive (eavesdropping, traffic monitoring, and traffic analysis) attacks with description.

Keywords: *MANET, Survey, Security attacks, DoS.*

1. Introduction

A **mobile ad hoc network** (**MANET**) is self-configuring, infrastructure-less network of mobile devices connected by wireless link. Ad-hoc is Latin word and means "for this purpose".[5]Each device in a MANETs is free to move independently in any direction, and will therefore change its links to other devices frequently. MANETs have been developing rapidly and are increasingly being used in many applications, ranging from military to civilian and, many commercial purposes, since setting up such network can be done without the help of any infrastructure. For example data collection, virtual classrooms and conferences where mobile devices and laptop share wireless medium and make communication to each other.MANETs is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANETs are more prone to malicious attacks. As the MANETs becoming widely used, the security issues has becoming one of the major concerns and security solutions are another important issues for MANETs, especially for those selecting sensitive applications [3, 4] .If we have the ability to detect the attacks once it come into the network, we can stop it from doing any damage to the system or any data. Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols[1,2]The primary focus of this paperwork is to provide a survey on various types of attacks that affect the MANETs..

2. Security aspect of ad-hoc networks

Ad-hoc networks are an emerging area of mobile computing. No fixed infrastructure such as base station as mobile switching is setup. Nodes within each other radio range communicate directly via wireless links while those which are far apart rely on other nodes to relay messages. Node mobility causes frequently change in topology.

Security Goals

- **Confidentiality** is to keep the information sent unreadable to unauthorized users or nodes. MANETs uses an open medium, so usually all nodes within the direct transmission range can obtain the data .Ensure certain information is never disclosed to unauthorized entity. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.[10]

- **Availability** means that a node should maintain its ability to provide all the designed services regardless of the security state of it [11]. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service [12].
- **Authentication** is to be able to identify a node or a user, and to be able to prevent impersonation. In wired networks and infrastructure-based wireless networks, it is possible to implement a central authority at a point such as a router, base station, or access point. But there is no central authority in MANET, and it is much more difficult to authenticate an entity in MANET.
- **Integrity** guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [13]:
    - Malicious altering
    - Accidental altering

  A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.
- **Non-repudiation** is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it. By producing a signature for the message, the entity cannot later deny the message.

3. Types of Security Attacks

Security is a highly challenging issue in wireless adhoc networks. Understanding possible form of attacks is the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information.[4]Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber-attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

3.1. Internal vs. External attacks

Internal attacks are from compromised nodes that are part of the network and External attacks are carried out by nodes that do not belong to the network. External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. The security attacks in MANET can be roughly classified into two major categories, namely active attacks and passive attacks [14][19]. The active attacks further divided according to the layers.

4. Passive attacks

Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected. One of the solutions to the problem is to use powerful encryption mechanism.

4.1. Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

4.2 Traffic Monitoring

It can be developed to identify the communication parties and functionality which could provide information to launch further attacks .It is not specific to MANET, other wireless network such as cellular, satellite and WLAN also suffer from these potential vulnerabilities.

4.3 Traffic Analysis

Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

5. Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. Active attacks can be internal or external. Since in case of Internal attacks, the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication.

(i) Black hole Attack

In black hole attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it.[6] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

(ii) Wormhole Attack

The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network.An attacker records packet at one location in the network and tunnels them to another location. This tunnel between two colluding attackers is referred as a wormhole [15] [18]. 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 AODV,the attack could prevent the discovery of any routes other than through the wormhole.

(iii) Gray hole attack

We now describe the gray hole attack on MANETS. The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainly. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.

(iv) Repudiation attack

In the network layer, firewalls can be installed to keep packets in or keep packets out. In the transport layer, entire connections can be encrypted, end-to-end. But these solutions do not solve the authentication or non-repudiation problems in general. Repudiation refers to a denial of participation in all or part of the communications. Forexample, a selfish person could deny conducting an operation on a credit card purchase, or deny any on-line bank transaction, which is the prototypical repudiation attack on a commercial system.

(v) Fabrication

The notation “fabrication” is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted [7]

(vi) Jamming attack

Jamming is the particular class of DoS attacks. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets.

(vii) Replay attack

A replay attack is one of the attacks that degrade severely the performance of MANET. A replay attacker does this attack by interception and retransmission of the valid signed messages. The validation of signed messages is verified by a timestamp discrepancy fixed by sender and receiver nodes. This attack usually attack on the freshness of routes[6]

(viii) Neighbor attack

Upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node. However, if an attacker simply forwards the packet without recording its ID in the packet, it makes two nodes that are not within the communication range of each other believe that they are neighbors (i. e. one-hop away from each other), resulting in a disrupted rout.

(ix) Packet dropping attacks

Direct interruption to the routing messages could be done by using the packet dropping attacks. In a standard packet dropping attack, an adversary collaborates as usual in the route discovery process and launches the constant packet dropping attacks if it is included as one of the intermediate nodes. In addition, instead of constantly dropping all the packets, adversaries might vary their techniques using random, selective, or periodic packet dropping attacks to help their interrupting behavior remain concealed.

(x) Man-in-the-middle attack

An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate.

(xi) Sleep deprivation attack

These kinds of attacks are most specific to wireless ad hoc networks, but may be encountered in conventional or wired networks as well. The idea behind this attack is to request the services a certain node offers, over and over again, so it cannot go into an idle or power preserving state, thus depriving it of its sleep (hence the name). This can be very devastating to networks with nodes that have limited resources, for example battery power. It can also lead to constant business of the component, hindering other nodes to (legitimately) request services, data or information from the targeted entity. This is also known asResource consumption attack . An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

(xii) Sinkhole attack

The attacking node tries to offer a very attractive link e.g. to a gateway. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack.

(xiii) Rushing Attack

On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack [16]. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne [17].

(xiv) IP Spoofing attack

In conflict-detection allocation, the new node chooses a random address (say y) and broadcast a conflict detection packet throughout the MANET. Any veto from a node will prevent it from using this address. If the malicious node always impersonates a member that has occupied the same IP address and keeps replying with vetoes, it is called an IP Spoofing attack

(xv) Jellyfish attack

Similar to the black hole attack, a jellyfish attacker first needs to intrude into the forwarding group and then it delay data packets unnecessarily for some amount of time before forwarding them. This result in significantly high end-to end delay and delay jitter, and thus degrades the performance of real time applications.

(xvi) State Pollution attack

If a malicious node gives incorrect parameters in reply, it is called the state pollution attack. For example, in best effort allocation, a malicious allocator can always give the new node an occupied address, which leads to repeated broadcast of Duplication Address Detection messages throughout the MANET and the rejection of new node.

(xvii) Sybil attack

If a malicious node impersonates some nonexistent nodes, it will appear as several malicious nodes conspiring together, which is called a Sybil attack. This attacks aims at network services when cooperation is necessary, and affects all the auto configuration schemes and secure allocation schemes based on trust model as well. However, there is no effective way to defeat Sybil attacks.

(xviii) Byzantine 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[20].

(xix) Session hijacking attack

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.

(xx) Location disclosure attack

An attacker discover the Location of a node or structure of entire networks and disclose the privacy requirement of network through the use of traffic analysis techniques [10], or with simpler probing and monitoring approaches [14]. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating.

(xxi) Flooding

Malicious nodes may also inject false packets into the network, or create ghost packets which loop around due to false routing information, effectively using up the bandwidth and processing resources along the way. This has especially serious effects on ad hoc networks, since the nodes of these usually possess only limited resources in terms of battery and computational power. Traffic may also be a monetary factor, depending on the services provided, so any flooding which blows up the traffic statistics of the network or a certain node can lead to considerable damage.

(xxii) Modification

In a message modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks. Since nodes in the ad hoc networks are free to move and self-organize, relationships among nodes at some times might include the malicious nodes. These malicious nodes might exploit the sporadic relationships in the network to participate in the packet forwarding process, and later launch the message modification attacks. Examples of attacks that can be classified under the message modification attacks are packet misrouting and impersonation attacks.

(xxiii) Impersonation attack

This is a special case of integrity attacks whereby a compromised node impersonates a legitimate one due to the lack of authentication in the current ad hoc routing protocols. The main result of the spoofing attack is the misrepresentation of the network topology that may cause network loops or partitioning. This is also known as spoofing attack.

(xxiv) Device tampering attack

Unlike nodes in a wired network, nodes in ad hoc wireless networks are usually compact, soft, and hand-held in nature. They could get damaged or stolen easily. In the process of route discovery, control messages created by a node must be signed and validated by a receiving node. Thus the route discovery prevents anti-authenticating attacks, such as creating routing loop, fabrication because no node can create and sign a packet in the name of a spoofed or invented node. In the absence of centralized administration it is easy for MN's to change their identities. Authentication in routing protocols creates fabrication attacks that result in erroneous and bogus routing messages.

(xxv) Link spoofing attack

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

(xxvi) Denial of Service attack

Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network. Denial of service: Denial of service (DoS) attacks could be launched from several layers. An attacker can employ signal jamming at the physical layer, which disrupts normal communications. At the link layer, malicious nodes can occupy channels through the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table over-flow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks.

(xxvii) SYN flooding

This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes.

(xxviii) Desynchronization attack

In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence these messages are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information. This will cause a considerable drainage of energy of legitimate nodes in network in an end-less synchronization-recovery protocol.

6. Conclusion

In this survey paper, we have analyzed the security threats in the mobile ad-hoc networks, which may be a main disturbance to the operation of it. Due to nature of mobility and open media MANET are much more prone to all kind of security risks, such as denial of service, information disclosure etc. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider applications. This leaves Ad-hoc networks wide open for research to meet these demanding application. The research on MANET security is still in its early stage. During the survey, we also find some points that can be further explored in the future, such as to find some effective security solutions and protect the MANET from all kinds of security risks. We will try to explore deeper in this research area, and we can design a security mechanism by which we can minimize or completely remove many of those attacks.

References

[1] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. /E€€ SlCON '97, Apr. 1997, pp. 197-21

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91

[3] Z. Karakehayov, “Using REWARD to Detect Team Black Hole Attacks in Wireless Sensor Networks,” Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[4] S. Lee, B. Han, and M. Shin, “Robust Routing in Wireless Ad Hoc Networks,” 2002 Int’l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

[5] Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". O'Reilly Wireless Dev Center. Retrieved 2009-01-20.

[6] Jyoti Raju and J.J. Garcia-Luna-Aceves, “ A comparison of On-Demand and Table-Driven Routing for Ad Hoc Wireless etworks’,” in Proceeding of IEEE ICC, June 2000.

[7] 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,

[8] Karan Singh, R. S. Yadav, Ranvijay “A REVIEW PAPER ON AD HOC NETWORK SECURITY” under International Journal of Computer Science and Security, Volume (1): Issue (1)

[9] S. Murphy, “Routing Protocol Threat Analysis,” Internet Draft, draft-murphy-threat-00.txt, Octomber 2002.

[10] 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.

[11] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[12] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.

[13] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity

[14] S. Yi and R. Kravets, Composite Key Management for Ad Hoc Networks.Proc. of the 1st Annual International Conference on Mobile and UbiquitousSystems: Networking and Services (MobiQuitous'04), pp. 52-61, 2004.

[15] M. Ilyas, The Handbook of Ad Hoc Wireless Networks, CRC Press, 2003.

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

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

[18] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, A SecureRouting Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols(ICNP),pp78-87,2002.

[19] R. Oppliger, Internet and Intranet Security, Artech House, 1998.

[20] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demandSecure Routing Protocol Resilient to Byzantine Failures. Proceedings of theACM Workshop on Wireless Security, pp. 21-30, 2002.

[21] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[22] C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999.