International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 11, Issue 01) and (Publishing Month: February 2014)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

A Survey on Attacks in MANET

Parvinder[1] and Dr. V.K. Suman[2]

[1]Research Scholar, Shri Venkateshwara University, U.P.
parvinder.bangar@gmail.com

[2]Professor & Dean, IIMT-IET, Meerut, U.P.
suman.glbitm@yahoo.co.in

Abstract

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. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an ―infrastructure less‖ network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Security is an essential requirement in mobile ad hoc network (MANETs). Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. This paper provides an overview on how different attacks affect the performance of the network and find out the security issues which have not solved until now. The results enable us to minimize the attacks on integrated MANET-Internet communication efficiently.

Keywords: *MANET, Security, Attacks.*

I. Introduction

A Mobile Ad-Hoc Network (MANET) is a collection of wireless nodes that can be connected to each other dynamically anytime and anywhere without the requirement of the existence of architecture to support the network. It is a self organizing system made of mobile nodes that communicate with each other using wireless link with no central administration such as base stations or access points. [1,2] Nodes in a MANET act as both hosts and routers to forward packets to each other. [3] The nodes that are within the radio range of each other communicate directly while others use intermediate nodes as relay points. These networks have gained ample interest in recent times due to its various advantages as compared to the networks that require a basic infrastructure to work. The promise held by the application of wireless ad hoc networks is immense. It ranges across the horizon and the number of real world problems that could be solved with the application of Mobile Ad hoc Networks is growing by the day. A network of this kind is well suited for highly critical applications like disaster management, emergency relief, military operations, mining activities and terrorism response where no pre deployed infrastructure for communication exists.
[3] For example, in the case of an earthquake, ad hoc networks could be used for communication when conventional communication networks could be damaged. [4].

Securing in wireless ad hoc networks has recently gain a momentum and became a primary concern in attempt to provide secure communication in a hostile wireless ad hoc environment. Numerous proposals were suggested without deriving a general solution. Securing a wireless ad hoc network is particularly difficult for many reasons including the [5]:

- *Vulnerability of Channels:* Message can be eavesdropped and fake messages can be injected into the network, with no necessity of physical access:
- *Vulnerability of Nodes:* Nodes can be easily captured or stolen and can fall under the control of the attacker;
- *Absence of Infrastructure*: Ad hoc networks operate independently of any infrastructure, which makes inapplicable any classical solutions based on certification authorities and on-line servers;
- *Dynamically Changing Topology*: Sophisticated routing protocols designed to

follow the permanent changes in topology can be attacked by incorrect routing information generated by compromised nodes, which is difficult to distinguish.

Now how Mobile Ad hoc networks generally works; how the nodes in MANETs are communicating and make a secure network [5].

II. Attacks in MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information.[6]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. The malicious node(s) can attacks in Mobile Ad-Hoc Network using different ways, such as transfer fake messages many times, fake routing information, and advertising fake links to disrupt routing operations. In this, current routing attacks in Mobile Ad-Hoc Network are discussed in detail below Figure: 1.

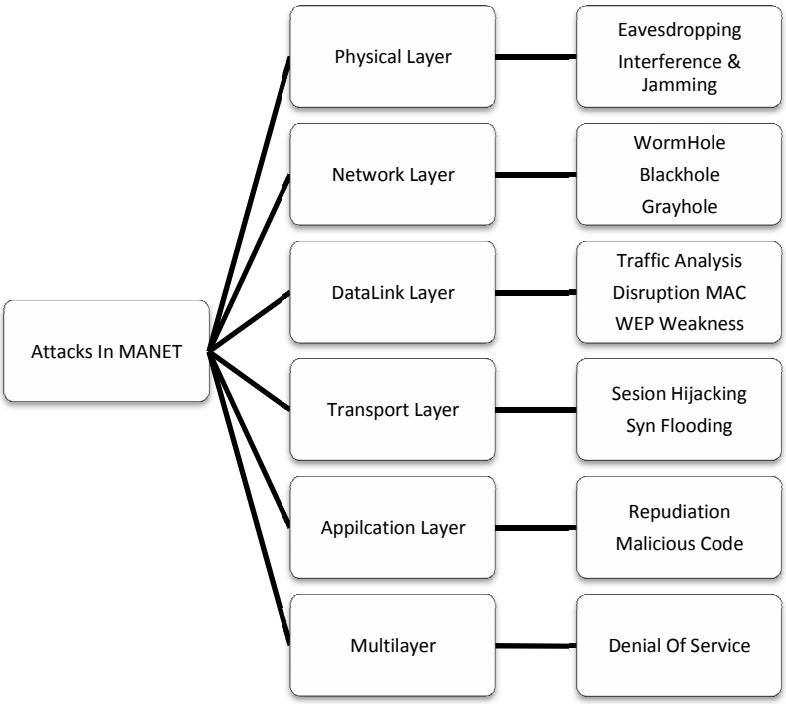

Figure 1: Classification of Attacks on MANET

In this paper we are discussing the attacks on network layer. Network layer attacks could be impersonation (masquerading or spoofing), modification, fabrication and replay of packets. Specifically, fabrication attacks where an intruder generates false routing information in order to disturb network operation or to consume other node resources. [1]

A. Network Layer Attacks

In Adhoc networks routing mechanism has three layers namely Network, Physical and MAC layers play a vital role [7]. As we all know MANETs are more vulnerable to various attacks, all these three layers suffer from different attacks and it cause

routing disorders. The different kind of attacks in the network layer varied such as selective forwarding attack and modifying some parameters of routing messages [8]. The list of different types of attacks on network layer and their brief descriptions are given below:

a. 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 a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel. For example in Figure 3.14, **X** and **Y** are two malicious nodes that encapsulate data packets and falsified the route lengths [9].

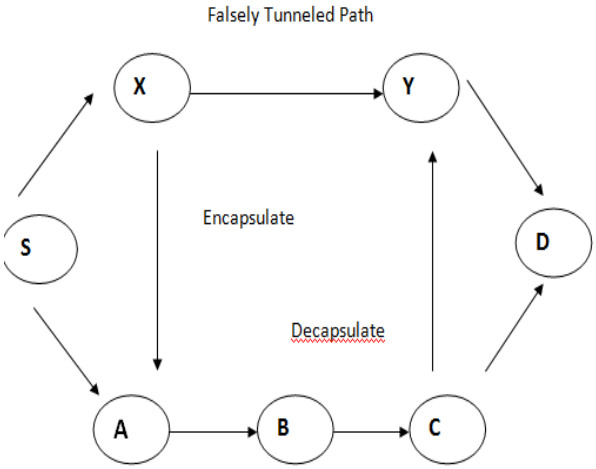

Figure 2:Wormhole Attack [85]

Suppose node **S** wishes to form a route to **D** and initiates route discovery. When **X** receives a route request from **S, X** encapsulates the route request and tunnels it to **Y** through an existing data route, in this case {**X** --> **A** --> **B** --> **C** -->**Y**}.

When **Y** receives the encapsulated route request for **D** then it will show that it had only traveled {**S** --> **X** --> **Y** --> **D**}. Neither **X** nor **Y** update the packet header. After route discovery, the destination finds two routes from **S** of unequal length: one is of 4 and another is of 3. If **Y** tunnels the route reply back to **X**, **S** would falsely consider the path to **D** via **X** is better than the path to **D** via **A**. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network.

The wormhole attack is particularly dangerous for many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. For example, when used against an on-demand routing protocols such as DSR [10], a powerful application of the wormhole attack can be mounted by tunneling each route-request packet directly to the destination target node of the request. When the destination node's neighbors hear this request packet, they will follow normal routing protocol processing to rebroadcast that copy of the request and then discard without processing all other received route request packets originating from this same route discovery.

This attack thus prevents any routes other than through the wormhole from being discovered, and if the attacker is near the initiator of the route discovery. This attack can even prevent routes more than two hops long from being discovered. Possible ways for the attacker to then exploit the wormhole include discarding rather than forwarding all data packets, thereby creating a permanent Denial-of-Service attack or selectively discarding or modifying certain data packets. So, if proper mechanisms are not employed to protect the network from wormhole attacks, most of the existing routing protocols for ad hoc wireless networks may fail to find valid routes.

b. Black hole Attack

MANETs face various securities threats i.e. attack that are passed out against them to interrupt the normal performance of the networks. Black hole attack is one of the security threat in which the traffic is redirect to such a node that actually does not exist in the network. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc

networks (MANET). In black hole attack, a malicious node uses its routing protocol in order to endorse itself for having the shortest path to the destination node or to the packet it wants to interrupt [11].

This destructive node advertises its availability of new routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the response of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it is up to the node whether to drop all the packets or promote it to the unknown address.

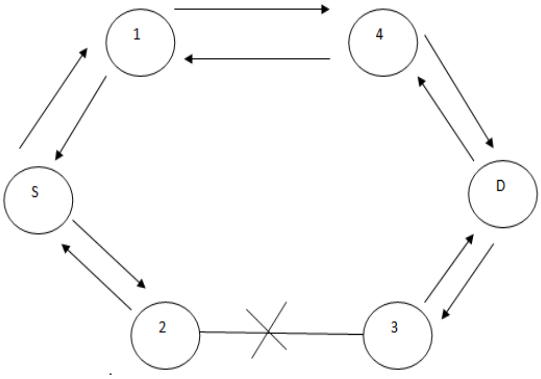

Figure 3: Black hole Attack [11]

The black hole attack has two properties. First, the node exploits the mobile ad-hoc routing protocol, such as AODV, to promote itself as having a valid route to a target node, even though the route is false, with the aim of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighbouring nodes will check and represent the ongoing attacks. There is a more delicate form of these attacks when an attacker selectively forward packets. An attacker suppress or modifies packets originating from some nodes, while leaving the data from the other nodes unchanged, which limits the suspicion of its wrongdoing [87].

c. Gray Hole Attack

A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are[8]

- Dropping all UDP packets while forwarding TCP packets.
- Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures.

Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node. If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbor, by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source. A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination.

The gray hole attack has two phases:

Phase 1:

A malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intention of interrupting packets of spurious route.

Phase 2:

In this phase, the nodes has been dropped the interrupted packets with a certain probability and the detection of gray hole attack is a difficult process. Normally in the gray hole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Both normal node and attacker are same. Due to this behavior it is very hard to find out in the network to figure out such kind of attack. The other name for Gray hole attack is node misbehaving attack [8].

d. Malign

Watchdog and pathrather are used in ad hoc routing protocols to keep track of perceived malicious nodes

in a blacklist. An attacker may blackmail a good node, causing other good nodes to add that node to their blacklists, thus avoiding that node in routes [5] .

e. Routing Attacks

There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Various attacks on the routing protocol are described briefly below [12]:

1) Routing Table Overflow:

In this attack, the attacker attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. Proactive routing algorithms attempt to discover routing information even before it is needed, while a reactive algorithm creates a route only once it is needed. An attacker can simply send excessive route advertisements to the routers in a network. Reactive protocols, on the other hand, do not collect routing data in advance.

2) Routing Table Poisoning:

Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes. Routing table poisoning may result in suboptimal routing, congestion in portions of the network, or even make some parts of the network inaccessible.

3) Packet Replication:

In this attack, an adversary node replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

4) Route Cache Poisoning:

In the case of on-demand routing protocols (such as the AODV protocol), each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past. Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar objectives.

f. Rushing Attack

On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. An adversary node which receives a Route Request packet from the source node floods the packet quickly throughout the network before other nodes which also receive the same Route Request packet can react. Nodes that receive the legitimate Route Request packets assume those packets to be duplicates of the packet already received through the adversary node and hence discard those packets. Any route discovered by the source node would contain the adversary node as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the adversary node. It is extremely difficult to detect such attacks in ad hoc wireless networks [12].

g. Partition (Network Layer Attach)

An attacker may try to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another [5].

h. Detour (Network Layer Attack)

An attacker may attempt to cause a node to use detours through suboptimal routes. Also compromised nodes may try to work together to create a routing loop [5].

III. Conclusion

In these days, the Mobile ad hoc network (MANET) technology spreads widely. A MANET is a promising network technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. However, many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security. Security is an essential service for wired and wireless network communications. The success of MANET strongly depends on whether its security can be trusted. In this study, we try to inspect the security threats in the MANETs that may vary depend on what communication layer the attacks are targeting.

References

[1] Ramana, V. V., Reddy, A., & Sekaran, K. C. (2012). Bio Inspired Approach to Secure Routing in MANETs. arXiv preprint arXiv:1208.3486.

[2] Jameela Al-Jaroodi, (2007), "Routing Security in Open / Dynamic Mobile Ad Hoc Networks".The International Arab Journal of Information Technology,Vol.4.
[3] Sanjay Ramaswamy, HuirongFu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, (2003), "Prevention of Cooperative Black Hole Attack in Wireless AdHoc Networks". Proc.International Conference on Wireless Networks.
[4] Shailender Gupta and Chander Kumar, (2010), "Shared information based security solution for Mobile AdHoc Networks". International Journal of Wireless & Mobile Networks, Volume:2.
[5] Ajay Jangra, Nitin Goel, Priyanka & Komal Bhatia (2010) Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture, International Journal of Electronics Engineering, 2(1), 2010, pp. 189-196.
[6] Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: Vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management, 11(2011), 32-37.
[7] Abel, V. S. (2011). Survey of Attacks on Mobile Adhoc Wireless Networks.International Journal on Computer Science and Engineering, 3(2), 826-829
[8] Shanmuganathan, V., & Anand, T. A Survey on Gray Hole Attack in MANET.International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN, 2250-3501.
[9] Rai, A. K., Tewari, R. R., & Upadhyay, S. K. (2010). Different types of attacks on integrated MANET-Internet communication. International Journal of Computer Science and Security, 4(3), 265-274.
[10] Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In Mobile computing (pp. 153-181). Springer US.
[11] Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), 1-16
[12] Jawandhiya, P. M., Ghonge, M. M., Ali, M. S., & Deshpande, J. S. (2010). A survey of mobile ad hoc network attacks. International Journal of Engineering Science and Technology, 2(9), 4063-4071.