SIMULATION BASED STUDY OF ATTACKS ON DIFFERENT LAYERIN MOBILE AD HOC NETWORK (MANET)

[1] MR. NIKHILESH B. KAPDI, [2] MR. BRIJESH B. DETROJA,
[3] MR.BRIJESH H. HANSALIYA

Master of Engineering [Computer Engineering Branch] Student,
V.V.P Engineering College, Rajkot.
Enrollment number:- 120470702010, 120470702006, 120470702017
Gujarat Technological University (GTU)

kapdinikhilesh@gmail.com, brijesh.detroja22@gmail.com, hansaliya.brijesh@gmail.com

ABSTRACT:*Security on different layer is most important and essential requirement in MANETs (mobile ad hoc networks). Here we present a simulation-based study of different attacks on different layer in MANATEs. Here we consider four different layer attacks: MAC layer attacks, NETWORK layer attacks, TRANSPORT layer attacks, APPLICATION layer attack. .In MANET at a same time multiple receivers and senders can communicate with each other and the resources are limited,lack of centralized authorityand also the network topology is dynamic due to these characteristics MANET is more vulnerable to the different security attacks. Basically the attacks in MANET are active or passive. The attacks on different layer are belong to active attacks.Active attack can be INTERNAL or EXTERNAL. These type of attacks are attempt to destroy or alter the data being transferredin a network. The attack carried out by the internal node of the network is known as the internal active attack. And the attack carried out by the node which is not belong to the network is known as external active attacks.*

Keywords: MANET (Mobile ad hoc network), Different layer's attacks.

(I) INTRODUCTION:

In MANET (mobile ad hoc network), mobile hosts act as nodes that are communicate with each other in temporary wireless network which has no any centralized administration and any fixed infrastructure. And also MANET is referred as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets of data. Hence, MANETs are suitable for applications in which no infrastructure exists such as military, emergency services, communications with mobility and mining operations. Also the design of network protocols for these networks is a complex issue. There are some major security aspects that need to be addressed for maintain a secure and reliable mobile ad-hoc network environment.
Those are as following:

Confidentiality of information:
Protection from all unintended entities that expose any type of information. This aspect is very difficult to achieve because in MANET it is very easy for the intermediate node to expose the information as it is use packet routing algorithm.

Verification of user:
Authentication of each node is essential otherwise unwanted entity can access the unauthorized node or sensitive information or also can interfering with the operation of other nodes.

Integrity of message: Message is never altered when it is transmit.

Non-repudiation: Ensures that sending and receiving node can never deny ever while sending or receiving the message.

Availability of service:
Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming

techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol.On higher layers, the attacker could bring down high level services.

(II) DIFFERENT LAYER ATTACKS:

- **MAC layer attacks:**

1. DENIALS OF SERVICE (DOS) ATTACKS:

Denials of service attacks are commonly detect in the internet. And also it is very hard to prevent any security system of the network. These attacks might attempt to disrupt/degrade the functionality of the whole network or may harm a specific mobile node.Harming of the whole network or may harm a specific node. Traditional DOS attacks involve overwhelming a particular host. However, in MANET, mobility, limited resources and bandwidth, routing functionalities associated with each node, etc. present many new opportunities for launching a DOS. While we defer the discussion of the various types of DOS attacks in ad hoc networks to a later sub-section we point out that these attacks might be at the at the MAC layer.

Following are the type of DOS attacks:

a) The intermediate node simply drops a certain number of the data packets even if itparticipates in a route. This causes the quality of the connections to deteriorate and further ramifications on the performance.

b) The intermediate node transmits falsified route updates. The effects could lead to frequent route failures thereby deteriorating performance.

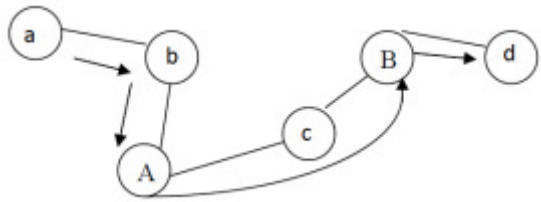
c) The intermediate node could potentially replay stale updates. This might again lead to false routes and degradation in performance.

d) Reduce the time-to-live field in the IP header so that the packet never reaches the destination.

- **Network layer attacks:**

1. WORMHOLE ATTACK:

In a wormhole attack, an attacker receives packets at one point in the network, 'tunnels' them to another point in the network, and then replays them into the network from that point. Which is shown in figure Attacker attempt the wormhole attack on node [A][B].

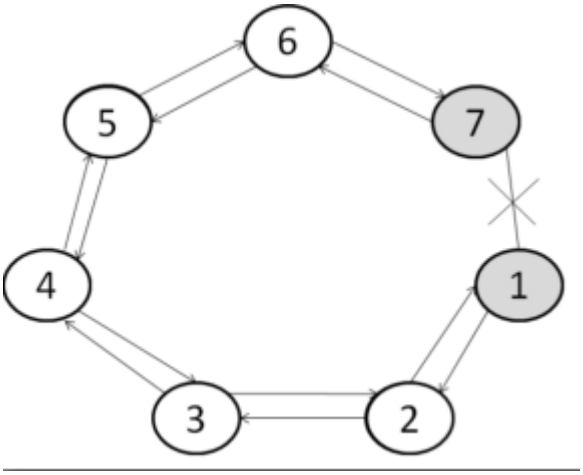


Worm hole attack node [A][B].

In the presence of "wormholes", the attacking nodes can selectively let routing messages get through Figure. "Wormhole" link has higher probability to be chosen as part of multi-hop routes due to its excellent packet delivery capability.
The wormhole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways.
The wormhole attack is particularly dangerous against 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 that node. For example, when used against an on-demand routing protocol such as DSR or AODV,This attack prevents any routes other than through the wormhole from being discovered.

2. BLACKHOLE ATTACK:

A black hole attack [3] is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and absorb them without forwarding them to the destination.
As shown in the figure node 1. Want to send data to node 7. But In the process of route discovery if node 7 is malicious node it replies to Node 1 as soon as it receives RREQ, the existence of a path through it to node 7. Node 1 an receiving the reply from node 7, will ignore another route replies from rest of nodes in MANET without checking the validity of path received from node 7. Node 7 will consume all the packets or drops.



Black hole attacks on node 7.

The black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks.

3. ROUTING ATTACK:

There are many type of attacks in MANET mounted on the routing protocol that causes disrupting the operation of the network and also responsible for loss of the information. Various attacks on routing protocol are explain below.

a) Rushing attacks:

On-demand routing protocols that use duplicate suppression during the route discovery processare 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.

b) 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.

c) Routing table overflow:

In this attack, the attacker attempts to create routes to nonexistent nodes. The goal is to create enough outes 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 reactivealgorithm 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.

d) 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.

e) 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 routingprocess.

- **Transport layer attacks:**

1. SESSION HIJACKING ATTACK:

Session hijacking takes advantage of the fact that most communications are protected (by providing credentials) atsession 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.

In session hijacking the malicious node spoofs the IP address of the victim and concludes the right sequence number and implements a DOS attack. Session hijacking giving an opportunity to a malicious node to act as an authorized node. Once the DOS attack is performed the target nodes become occupied for time

being. The malicious node masquerades as one of end nodes of the session and hijack the session.

- **Application layer attacks:**

1. 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. For example, 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

(III) CONCLUSION:

In this survey paper, we try to find the impact of different layer's attacks on the security system in the mobile adhoc networks, which may be a maindisturbance to the operation of it. Due to nature of mobility dynamic structure and open media MANET are much more unsecure to allkind of security risks as covered. As a result, the security needs in the MANET are much higher than those in thetraditional wired networks.

During the survey, we also find some points that can be explored in the future, such as to find some effectivesecurity solutions and protect the MANET from all kinds of security risks. We will try to explore deeper in thisresearch area.

REFERENCES:

[1] Abhay Kumar Rai, Rajiv RanjanTewari&Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security (IJCSS) Volume: 4 Issue: 3.

[2] D. DjeNouri and L. Khelladi, " A Survey of Security Issues In Mobile Ad Hoc And Sensor Networks", IEEE Communications surveys and Tutorials, Fourth Quarter 2005, vol. 7, no. 4., pp. 2-28.

[3] D.B. Johnson, D.A. Maltz, Y.C. Hu, and J.G. Jetcheva,Dynamic Source Routing in Ad Hoc Wireless Networks,Mobile Computing, Kluwer Academic Publishers, Vol. 5,pp. 153-181, 1996.

[4] Pissinou, N., Ghosh, T. and Makki, K.Collaborative trust-based secure routing in multi hopad hoc networks. Networking (Athens, Greece2004). Lecture Notes in Computer Science, vol.3042, 2004, 1446-145l.

[5]. H.Deng, H.Li, and D.P.Ararwal, "Routing security in wireless Ad hoc networks", *IEEECommunication magazine*. Vol. 40, No.10. Oct.2002.

[6]. J-P. Hubaux, L. Buttyan, and S. Capkun. TheQuest for Security in Mobile Ad Hoc Networks. *In Proceedings ACM Symposium on Mobile Ad hoc Networking and Computing (MOBIHOC)*, 2001.

[7] J. G. Jetcheva and D.B. Johnson, "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks", *Proceedings of ACM MobiHoc '01*, Long Beach, CA, Oct. 2001, pp. 33-44.

[8] Xin Li , ZhipingJia, Peng Zhang, Haiyang Wang,"A Trust-based MuItipath Routing Framework forMobile Ad Hoc Networks" , 7th FSKD, 20 I O.

[9] A. Perrig, Y-C Hu, and D. B. Johnson, "Wormhole Protection in Wireless Ad Hoc Networks," Technical Report TR01-384, Dept. of Computer Science, Rice University, 2001.