Injection of Attacks in MANETs

Konagala Pavani[1], Dr. Damodaram Avula[2]

[1]*(Department of Computer Science and Engineering, Vaagdevi College of Engineering, Jawarharlal Nehru Technological University, Hyderabad, Andhra Pradesh)*
[2]*(Director, Academic Audit Cell SE, JNTU, Hyderabad, Andhra Pradesh)*

Abstract: *Mobile ad-hoc networks are widely used in the tactical battlefield, emergency search and rescue missions. They are also well used in civilian ad-hoc situations like conferences and classrooms due to the ease and speed in setting up such networks. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The wireless ad-hoc networks are mostly vulnerable to security attacks because of its features of open medium, dynamic topology, lack of centralized management and node mobility. In this paper we proposed a means to inject black hole attack and wormhole with a protocol Ad-hoc On Demand Distance Vector (AODV) and conducted experiments using NS2 simulator. The results show that performance of network decreased in presence of attacks.*

Keywords: *MANET, AODV, Black hole attack, Wormhole attack, security*

I. Introduction

A mobile ad hoc network (MANET) sometimes called as mobile mesh network consists of a collection of peer mobile nodes that are capable of communicating with each other without help of a fixed infrastructure. As MANETs provide mobile nodes with reliable routing services in the absence of a network infrastructure, they are emerging as a promising platform for a variety of applications in military and civilian domains, sensor networks, rescue operations, students on campus, free internet connection sharing.

Further, MANETs are decentralized networks and the network topology is unpredictably dynamic because of node mobility. As a result, mobile nodes in MANETs act as both hosts and routers and need to discover the dynamic topology and deliver messages by themselves. These mobile nodes establish the routing tables by exchanging routing messages with each other and then deliver the data packets for others. Therefore, developing a system to maintain routing tables reliably is the most fundamental and critical issue related to MANETs.

1.1 Features of wireless open network

- Temporary meshed network formed by a collection of mobile nodes
- Fully self-organized network
- MANETs do not rely on any established infrastructure for the network initialization and operation
- Multi-Hop: due to limited transmission range
- Distribuited approch: lack of infrastructure to support network operation
- Dynamic topography: MANET entities are mobile nodes
- Nodes cooperation: basic operations are performed by whole community
- Peer-to-Peer (P2P) analogies

1.2 Security Issues in MANET

MANETs are much more vulnerable to attacks [1][2] than wired networks. This is because of the following reasons.

1.2.1. Open Medium

Eavesdropping is much easier than in wired network because of wireless links. In wired networks an attacker must gain physical access to the network by passing through firewalls and gateways. But in wireless ad hoc networks an attacker may attack from all the directions and damage any node.

1.2.2. Dynamically changing network topology

Mobile node appears and disappears from the network; thereby any malicious node joins in the network without being detected. The dynamic and cooperative nature of ad-hoc networking without a centralized authority for authentication and monitoring is susceptible to attacks that breaks down or exploit the cooperative behavior of the ad-hoc routing. The mobile nodes that are roaming independently may have inadequate physical protection and can be captured and compromised. Attackers using these captured nodes can perform far more damaging attacks from within the network and such attacks are much harder to detect since the captured nodes will contain the private keys and passwords used within the network.

II. Related Work

Despite the fact of popularity of MANET [3], these networks are very much exposed to attacks. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [4]. Different kinds of attacks have been analyzed in MANET and their affect on the network.

III. Routing Protocols

The primary goal of routing protocols [5] in ad-hoc network is to establish optimal path (min hops) between source and destination with minimum overhead and bandwidth consumption so that packets are delivered in a timely manner. A MANET protocol should function effectively over a wide range of networking context from small ad-hoc group to larger mobile Multihop networks.MANET routing protocols can be classified according to the protocols mechanism of route discovery and route update, into three categories: proactive (table-driven), reactive (on-demand) and hybrid.

3.1 Proactive routing protocols

These are used to maintain up-to-date route information from one node to other node in the network.
eg.DSDV (Destination Sequence Distance Vector)

3.2 Reactive routing protocols

Contrary to proactive routing protocols, reactive routing, as the name may imply, establish and discover the route node only when there is a demand for that node.
eg: Ad-hoc On-Demand Distance Vectoring [1] [2] (AODV), Dynamic Source Routing (DSR).

3.3 Hybrid routing protocols

These protocols show the characteristics of both reactive and proactive routing protocols. Reactive routing protocols are used to adjust the network connectivity changes using minimal routing overhead by avoiding unnecessary periodic route information update at each node.
Eg: Zone Routing Protocol (ZRP), ZHLS etc.

IV. AODV Routing Protocol

In this paper we have taken AODV [2] [6] routing protocol. It is a pure on-demand routing protocol. For sending messages to destination, AODV discovers and establishes routes only when needed and maintains only those that remain active. The protocol consist two essential procedures: route discovery and route maintenance. It broadcasts RREQ messages to its immediate neighbors. These neighbors in turn rebroadcast them to their neighbors. This process continues unless the RREQ message reaches the destination. Upon receiving the first RREQ message from the source node, it sends a RREP to the source node following the same reverse path. All the intermediate nodes also set up forward route entries in their table. Upon detecting error in any link to a node, the neighboring nodes forward route error message to all its neighbors using the link. These again initiate a route discovery process to replace the broken link.

V. Types of Attacks

Attacks can be classified as internal and external attacks based on the source of attacks. External attacks are done by unauthorized users and these attackers are not necessarily disconnected from the network, though. The targeted network might be a self-contained entity that is linked to other networks using the same infrastructure or communication technology .Whereas internal attacks are sourced from inside a particular network. A compromised node with access to all other nodes within its range poses a high threat to the functional efficiency of the whole network.

Another type of classification is active attack and passive attack. Some attacks are classified depending on the layer of occurrence.

5.1 Network Layer Attack
The list of different types of attacks on network layer is:

5.1.1 Black hole attack: An attacker may create a routing black hole [7], in which all packets are dropped. By sending forged routing packets, the attacker could route all packets for some destination to itself and then discard them.

5.1.2 Wormhole attack: In the wormhole [8] attack, a malicious node tunnels messages received in one part of the network over a low latency link and replays them in a different part. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.

5.1.3 Byzantine Attack: In this attack, a compromised intermediate node or a set 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.

5.1.4 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
- Computational power

5.1.5 Routing Attack:

There are several attacks[9] [10] which can be mounted on the routing protocols and may disrupt the proper operation of the network such as routing table overflow, packet replication, rout cache poisoning and rushing attack.

5.2 Transport layer attack

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

5.3 Application Layer Attack

5.3.1 Repudiation: In simple terms, repudiation refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication.

5.4 Multi Layer Attack

5.4.1 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.

5.4.2 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.

5.4.3 SYN Flooding: In this form of attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return address of the SYN packets.

5.4.4 Distributed DOS Attack: Distributed Denial of Services is more severe form of DoS

In this paper we have implemented black hole and worm hole attacks.

VI. Black Hole Attack

Black hole attack is an active attack type, which leads to dropping of messages.In this type of attack, malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. In the same manner the malicious node attacks all RREQ messages and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called as black hole attack which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network.

If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack. The black hole attack affects the whole network.

VII. Worm Hole Attack

The AODV routing protocol is vulnerable to wormhole attack since the colluding nodes involved in this attack uses a high speed channel to send messages. In wormhole attack, the attacker receives packets at one point in the network, forwards them to another point in the network through a link with much less latency than the default links used by the network. This link or tunnel between two attackers is called as wormhole. It can be established through a single long-range wireless link or a wired link between the two attackers. Hence it is simple for an attacker to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route.

VIII. Simulation Environment

Simulations are often used to model natural, machine or human systems in order to gain insight into their functioning. Simulators for communication networks can provide near accurate reproductions of most features in the environment, like noise, probability of loss or alteration of data. Network Simulator ns-2 [11] [12] [13] is used to run MANET simulations.NS-2 is a simulation project developed by the University of California Berkley. NS is part of software of VINT [14] project which is supported by DARPA since 1995. It is one of the most widely used network simulators for wired and wireless networks. NS is an object – oriented, discrete event driven network simulator which is written in C++, with an OTcl interpreter as a frontend, and is available free. It follows the layered approach, and is accompanied by a rich set of protocols.

We run two simulations, one without the attacker node and other including the attacker node. The simulation parameters are shown in TABLE1

We apply the random way-point model in ns-2 to emulate node mobility patterns with a topology of 1000m by 632m. We use UDP/CBR (Constant Bit Rate) as underlying transport protocol, and AODV protocol is used in the experiments. The maximum number of connections is set to be 10 out of which 3 nodes are malicious nodes, traffic rate is 10, the pause time between movements is 10s.These settings are typical ad-hoc settings with adequate mobility and data load overhead, and are used in all our experiments. For evaluation trace files are generated with the normal nodes and attacked nodes.

IX. Experimental Results

Fig 2 shows the designed network with 10 nodes. In this normal nodes are represented in blue color where as attack nodes are represented in red color i.e. the nodes 0 to 6 are normal nodes and nodes 7 to 9 are attacked nodes.node 7 is a black hole node where as nodes 8 and 9 are worm hole nodes.A tunnel (duplex link)is created between 8 and 9.

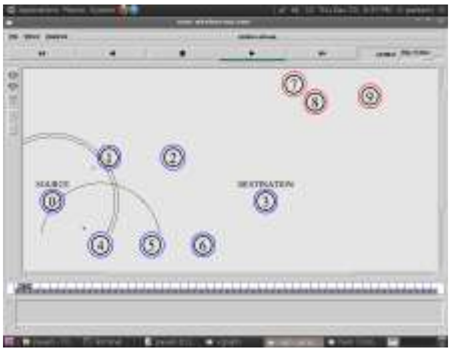


Fig 2: Network in normal condition

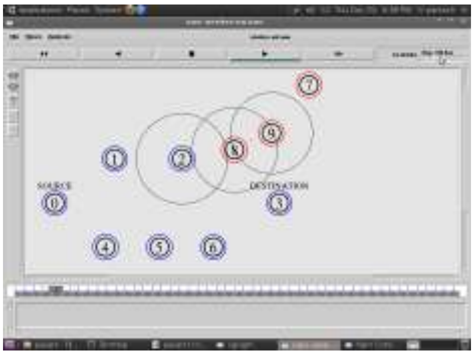
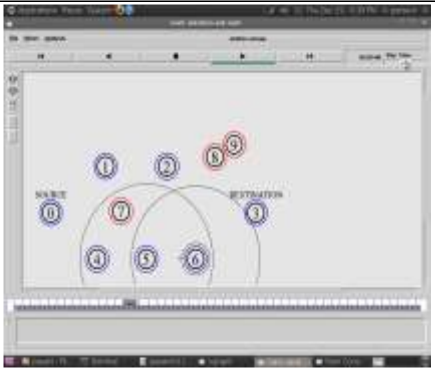


Fig 3: Network under wormhole attack

In the fig 3 a wormhole attack is created and packets are transferring from 8 to 9 instead of to 3 which is a destination node.

In fig 4 we are trying to inject a black hole attack. To implement this attack node 7 is moving nearer to source node to show the shortest distance to destination node. So the packets will transfer from source(node 0) to destination (node 3) through node 7.But node 7 as it is a black hole node drops the packets instead of sending to destination (node 3)..



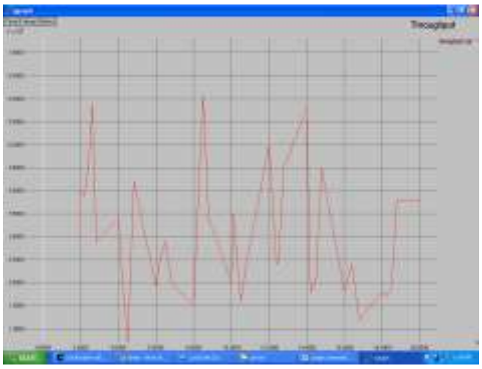


Fig 4: Network under Black hole attack   Fig 5: Graph showing Throughput

Fig 5 shows number of packets delivered i.e. throughput. In presence of attack nodes number of packets delivered gets decreased.

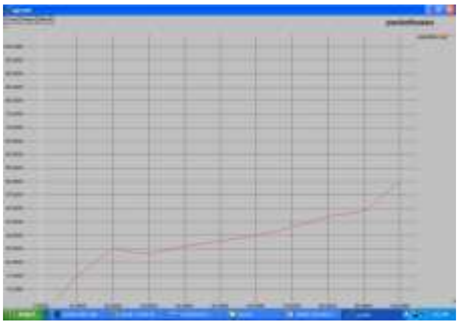


Fig 6: Impact of attacks on number of packets loss

Fig 6 shows the number of packets loss with respect to time which gradually increases as the attacks are created in network. Results also show that the network performance decreases due to the increased attacks.

X. Conclusion

The security of the Ad Hoc network routing protocols is still an open problem and deserves more research work. In this paper, we have analyzed the security threats faced in an ad hoc network. We have implemented Black hole Attack and Worm hole Attack against AODV routing protocol using Network Simulator-2.This research defines a first fruitful effort towards the definition of an attack implementation for auditing the resilience of Ad Hoc routing protocols and discovering new vulnerabilities in such communication elements. The detection and evasion of such black holes and wormholes in an ad-hoc network is still considered as future challenging task.

References

[1] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour. A Survey of Routing Attacks in Mobile Ad Hoc Networks, IEEE Wireless Communication, 14 (5), pp. 85-91,2007

[2] K. Biswas and Md. Liaqat Ali, Security threats in Mobile Ad-Hoc Network, Master Thesis, Blekinge Institute of Technology Sweden, 22nd March 2007.

[3] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad Hoc Networks, Mobicom 2000

[4] P.V.Jani, Security within Ad-Hoc Networks, Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

[5] Elizabeth M. Royer et. al. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, IEEE Personal Communication, April 1999.

[6] Yih-Chun Hu, Adrian Perrig, David B. Johnson, Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks, MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA

[7] LathaTamilselvan and Dr. V sankaranarayanan,, Prevention of Blackhole Attack in MANET, The 2nd InternationalConferenceonWirelessBroadbandand Ultra Wideband Communications, 2007, pp.21-26.

[8] Zaw Tun and Aung Htein Maw ,Wormhole Attack Detection in Wireless Sensor Networks ,World Academy of science, Engineering and Technology 46 2008.

[9] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong A New Routing Attack in Mobile Ad Hoc Networks.In the International Journal of Information Technology Vol. 11 No. 2.

[10] R.H. Khokhar, Md. A.Ngadi, S. Manda. A Review of Current Routing Attacks in Mobile Ad Hoc Networks, International. Journal of Computer Science and Security, 2 (3), pp. 18-29, 2008.

[11] http://www.isi.edu/nsnam/ns/

[12] K. Fall and e Varadhan. The ns Manual (formerly ns Notes and Documentation), 2000.

[13] NS by examplehttp://nile.wpi.edu/NS/overview.html,14 May 2006.

[14] Virtual InterNetworkTestbed, http://www.isi.edu/nsnam/vint, 14 May 2006.