Ankur Ratmele, Asst. Prof. Rajesh Dhakad / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 3, May-Jun 2013, pp.201-205

Performance Analysis of AODV under Worm Hole Attack through Use of NS2 Simulator

Ankur Ratmele[*] and Asst. Prof. Rajesh Dhakad[**]
*Research Scholar, Department of Computer Engineering, SGSITS, Indore (M.P), India.
**Asst. Prof., Department of Computer Engineering, SGSITS, Indore (M.P), India

ABSTRACT-

Wireless networks are gaining popularity to its peak from past, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Any node in mobile ad hoc networks operates not only as end terminal but both as an intermediate router and client. In this way, multi-hop communication occurs in MANETs and thus it is a difficult task to establish a secure path between source and destination. It generally works by broadcasting the information and used air as medium. Its broadcasting nature and transmission medium also help attacker, whose intention is to spy or disrupt the network. When two malicious nodes forward packet through a private "tunnel" in the network, in which one node is nearer to the source and other node is nearer to the destination and packet travelled through this malicious nodes. This type of activity is known as wormhole attack. NS2 is chosen as a simulation environment because it is one of the leading environments for network modeling and simulation.

Keywords- Mobile Ad hoc network,ns-2, Wormhole attack.

INTRODUCTION-

Mobile wireless ad hoc networks are fundamentally different from wired networks, as they use wireless medium to communicate, do not rely on fixed infrastructure and can arrange them into a network quickly and efficiently. In a Mobile Ad Hoc Network (MANET) [1], each node serves as a router for other nodes, which allows data to travel, utilizing multi-hop network paths, beyond the line of sight without relying on wired infrastructure. Security in such networks, however, is a great concern .The open nature of the wireless medium makes it easy for

Outsiders to listen to network traffic or interfere with it. Lack of centralized control authority makes Deployment of traditional centralized security mechanisms difficult, if not impossible. Lack of clear network entry points also makes it difficult to implement perimeter-based defense mechanisms such as firewalls. Finally, in a MANET nodes might be battery-powered and might have very limited resources, this may make the use of heavy-weight security solutions undesirable. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats [2].

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication [3, 4]. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

Wormhole attack is a network layer attack [5]. In a typical wormhole attack at least two colluding node in the network are located at different places that are not in direct communication range of each other i.e. one near to the source node and another near to the destination node thus bypassing information from source node to destination node and disrupting proper routing.

In this paper, we concentrate on the throughput analysis of an Ad-hoc network consisting of 16 nodes. We use Ad-hoc on demand Routing (AODV) protocol and carry out simulations to evaluate the performance of wireless ad-hoc network.

NS2[6] is selected to carry out the simulation. Ns2 provide technologies, protocols, communication devices for academic research, assessment and improvement. It is efficient robust and highly reliable which grant the user the ease of graphical interface, developing and running the simulation and validation of the results. Network Simulator (Version 2), widely known as ns-2, is simply a discrete event driven network simulation tool for studying the dynamic nature of

communication networks. It is an open source solution implemented in C++ and Otcl programming languages. ns-2 provides a highly modular platform for wired and wireless simulations supporting different network element, protocol (e.g., routing algorithms, TCP, UDP, and FTP), traffic, and routing types. In general, ns-2 provides users with a way of specifying network protocols and simulating their corresponding behaviors.

In this we investigate the throughput of wireless ad-hoc network simulation considering AODV protocol. We compare the throughput simulation results of AODV without wormhole attack and with the wormhole attack.

II.Related Work

The most commonly cited wormhole prevention mechanism is 'packet leashes' by Hu et al [7], proposed to add secure 'leash' containing timing and/or Global Positioning System (GPS) information to each packet on a hop-by-hop basis. Based on the information contained in a packet leash, a node receiving the packet would be able to determine whether the packet has traveled a distance larger than physically possible.

Hu proposed two different kinds of leashes: geographical leashes and temporal leashes. Geographic leashes require each node to have access to up-to-date GPS information, and rely on loose (in the order of ms) clock synchronization. When geographical leashes are used, a node sending a packet appends to it the time the packet is sent t_s and its location p_s. A receiving node uses its own location p_r and the time it receives a packet t_r to determine the distance the packet could have traveled. Keeping in mind maximum possible node velocity v, clock synchronization error Δ, and possible GPS distance error Δ, the distance between the sender and the receiver d_{sr} is upper-bounded by:

$$d_{sr} < \|p_s - p_r\| + 2v(t_r - t_s + \Delta) + \Delta \quad \text{……..(i)}$$

Geographical leashes should work fine when GPS coordinates are practical and available. However, modern GPS technology has significant limitations that should not be overlooked. While the price of GPS devices is going down, it remains substantial.

Finally, GPS systems are not versatile, as GPS devices do not function well inside buildings, under water, in the presence of strong magnetic radiation, etc. As opposed to geographical leashes, temporal leashes require much tighter clock synchronization (in the order of nanoseconds), but do not rely on GPS information. When temporal leashes are used, the sending node specifies the time it sends a packet t_s in a packet leash, and the receiving node uses its own packet reception time t_r for verification. In a slightly different version of temporal packet leashes, the sending node calculates an expiration time t_e after which a packet should not be accepted, and puts that information in the leash. This is to prevent a packet from traveling farther than distance L

$$t_e = t_s + L/C - \Delta, \quad \text{….(ii)}$$

where, C is the speed of light and Δ is the maximum clock.

One possible way to prevent wormholes, as used by Capkun et al[8] , Hu et al[9] , Hong et al[10] , and Korkmaz et al[11], is to measure round-trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determine whether the calculated distance is within the maximum possible communication range. The basis of all these approaches is the following. The Round Trip Travel Time (RTT) δ of a message in a wireless medium can, theoretically, is related to the distance d between nodes, assuming that the wireless signal travels with a speed of light c: $d=(\delta c) / 2$ and $\delta = 2d/c$ …….. iii)

The neighbor status of nodes is verified if d is within the radio transmission range R for R > d (d within transmission range): $R > \delta c/2$ and $\delta < 2R/c$. In essence, the use of RTT eliminates the need for tight clock synchronization required in temporal leashes: a node only uses its own clock to measure time. However, this approach, while accounting for message propagation, completely ignores message processing time. When a message is sent by one node and is acknowledged by another, the time it takes for a node to process a message and to reply to it is generally non-negligible, particularly in the context of bounding short distances using signals whose speed is similar to that of light in vacuum. After all, it takes the light less than 0.2 seconds to circle the entire Earth around the equator. Outstanding clock precision and practically nonexistent errors are required to bind distances on the order of hundreds of meters.

III. Overview of AODV Protocol

Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol for mobile ad hoc networks and other wireless ad-hoc networks. It is jointly developed in Nokia Research Centre of University of California, Santa Barbara and University of Cincinnati by C. Perkins and S. Das. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand. AODV is capable of both unicast and multicast routing. It keeps these routes as long as they are desirable by the sources. Additionally, AODV creates trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. The sequence

numbers are used by AODV to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes. AODV defines three types of control messages for route maintenance:

RREQ- A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Data packets waiting to be transmitted (i.e. the packets that initiated the RREQ). Every node maintains two separate counters: a node sequence number and a broadcast_ id. The RREQ contains the following fields.

Table1 RREQ Fields

source address	broadcast ID	Source sequence no.	destination address	destination sequence no.	Hop count

The pair <source address, broadcast ID> uniquely identifies a RREQ. Broadcast_id is incremented whenever the source issues a new RREQ.

RREP- A route reply message is unicast back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

RERR- Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a ―precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

Wormhole Attack

Wormhole attack is a network layer attack. In a typical wormhole attack at least two colluding nodes in the network are located at different places that are not in direct communication range of each other i.e. one near to the source node and another near to the destination node thus bypassing information from source node to destination node and disrupting proper routing. In Fig. 1, M1 and M2 are two colluding nodes. The malicious node M1 takes data near the source node then tunnels it to M2 placed near the destination node. Communication of data occurs via path having this low latency link all the times due to less number of hops.

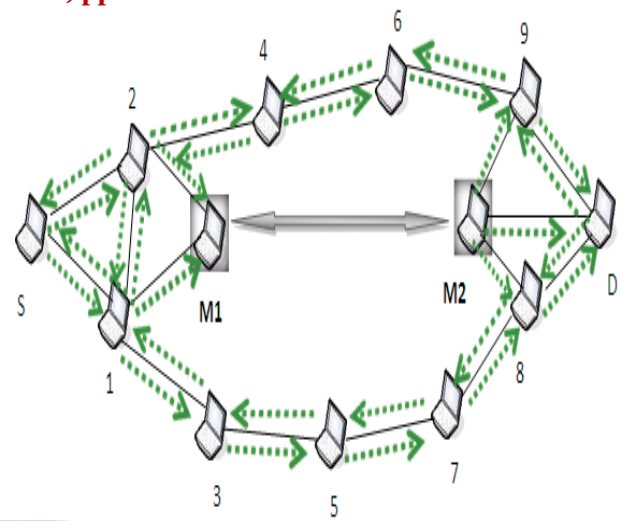

Fig.1 wormhole attack

IV. Simulation Description

The ns-2 simulator is the most popular network simulator today Ns2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (ns) contains all commonly used IP protocols. The network animator (nam) is use to visualize the simulations. Ns2 fully simulates a layered network from the physical radio transmission channel to high level applications.Ns2 is an object oriented simulator written in C++ and OTcl. The simulator supports a class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. There is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compile hierarchy.

Simulation Parameter

Parameter	Value
Mobility Model	Two Ray Ground Model
Nodes (Wifi)	16
Simulation Time	20sec
Packet Size	1000 bytes
Node Speed	10m/s
Traffic model	CBR

Simulation Scenario

Following are the simulation Scenarios in which there are 16 nodes. Node 0 is source node and node 4 is the destination node.

1. **Simulation of AODV without wormhole Attack**

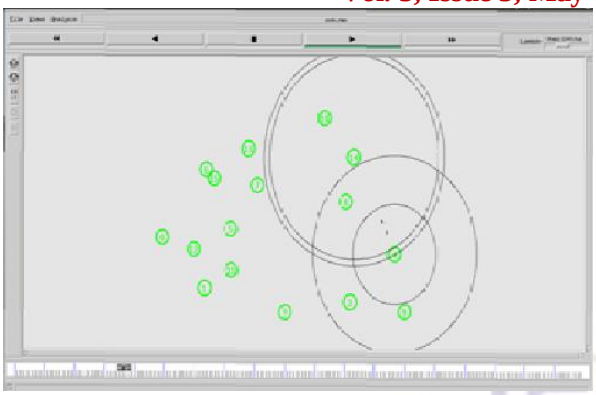

Fig.2 simulation of aodv

2. Simulation of AODV with wormhole attack

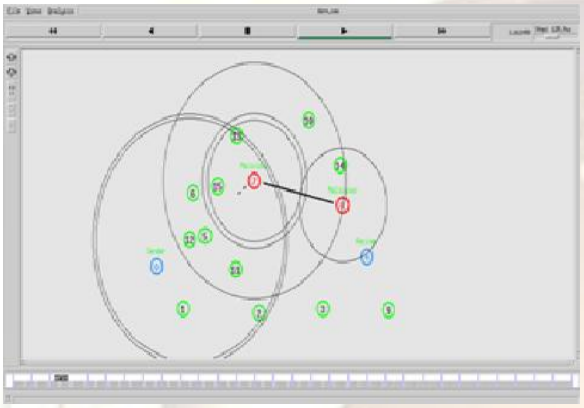

Fig.3 Simulation of attack

In this node 3 and node 4 are the malicious nodes and wormhole link is established as shown. Packet is travelled through these malicious nodes. So packets will not reach to the destination.

V. Performance Evaluation:

The following are the graphs shown below. These graphs are the throughput-time graph.

a. Throughput/Time Graph without wormhole attack

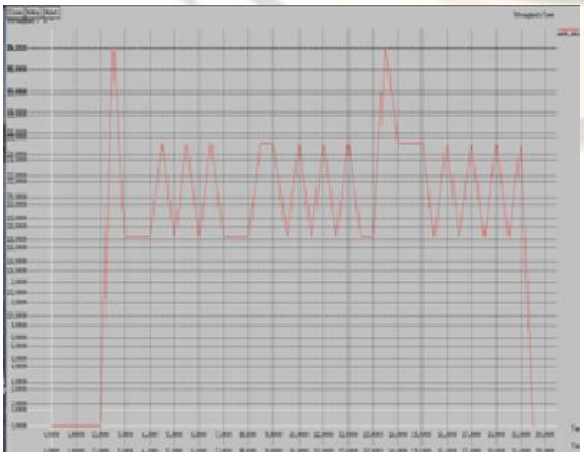

Fig.4 Graph without wormhole attack

a. Throughput/Time Graph with wormhole attack

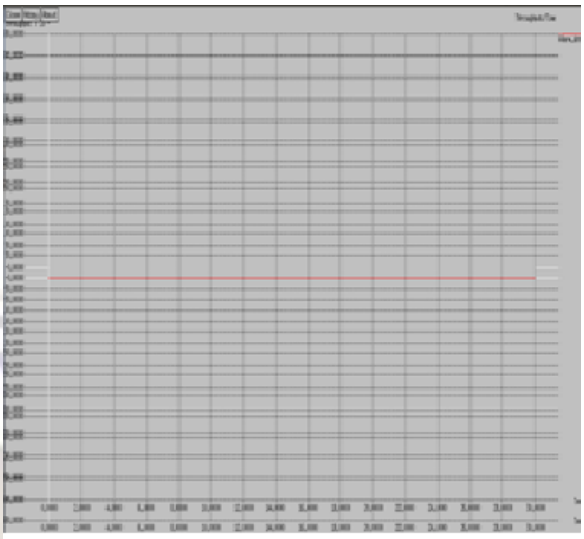

Fig.5 Graph with wormhole attack

VI. Conclusion

In this paper we carried out the simulation using ns2.We used AODV protocol. In Fig.4 shown without wormhole attack packet reached to the destination. Varying throughput with time indicate that the packet reached to the destination but in the Fig.5 shown with the wormhole attack there is constant line i.e zero throughput ,which indicate that no packet is reached to the destination because malicious node dropped all the received packet. So no packet is received at the destination.

Effects of wormhole attack

Effect of wormhole attack in the network is that packet is not reached to the destination as shown in the fig.5.

REFERNCES

[1] C.Siva Ram Murthy and B. S. Manoj. “Ad hoc wireless networks: Architecture and Protocols”. Prentice Hall Publishers, May 2004, ISBN 013147023X.

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

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

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

[5] Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad. “Chapter 30: Security in wireless ad-hoc networks, the handbook of Ad hoc wireless network”.CRC PRESS Publisher, 2003.

[6] The ns2 network simulator," http://www.isi.edu/snam/

[7] Y.-C. Hu, A. Perrig, D. B. Johnson; "Packet leashes: a defense against wormhole attacks in wireless networks"; INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, pp. 1976-1986, 2003.

[8] S.Capkun, L. Buttyan, J.-P. Hubaux; "SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks"; Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks; 2003.

[9] Y-C Hu, A. Perrig, D. Johnson; "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols"; Proc. of WISE 2003, September 19, San Diego, California, USA, 2003.

[10] Korkmaz T.; "Verifying Physical Presence of Neighbours against Replay-based Attacks in Wireless Ad Hoc Networks"; Proc. International Conference on Information Technology: Coding and Computing 2005, ITCC 2005, pp. 704-709, 2005.

[11] M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks.