Varying Number of Nodes Based Implementation of Wormhole Attack Based on Manet Using NS3

Anjali Soni[1], Shivendu Dubey[2], Jyoti Gupta[3]
[1, 2, 3] Dept of CSE
[1, 2] Gyan Ganga Institute Of Technology And Sciences, Jabalpur
[3] Kala Niketan Polytechnic College,Jabalpur

Abstract- *Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.[2] Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.*

MANETs are a kind of wireless ad hoc network (WANET) that usually has a routable networking environment on top of a link layer. ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network.

This research paper provides an overview of AODV routing protocols by presenting their characteristics, functionality, benefits and limitations and then makes their and implementation of wormhole attack in MANET using NS-3 simulator.

Keywords- MANET; routing protocol; performance; ns-3

I. INTRODUCTION

Mobile ad hoc network is a collection of wireless nodes that do not need to rely on a predefined infrastructure to keep the network connected. MANET is a self-configurable network and nodes are free to move in anywhere within the range of the network, so topology may change and this event is unpredictable. MANET participant do not need access point or base stations, and instead rely on each other to establish a temporary network; peers communicate beyond their individual transmission ranges by routing packets through intermediate nodes. According to these characteristics, routing is a critical issue and we should choose an efficient routing protocol to makes the MANET reliable . Mobile ad hoc network topology is dynamic , so due to mobility of nodes, dynamic topology of the network, lack of centralized mechanism makes MANET more vulnerable. One of the distinctive features of MANET is, each node must be able to act as a router to find out the optimal path to forward a packet.

MANET protocols are usually evaluated by means of simulation: a network of nodes is modeled and then run for a set of scenarios in a specific simulation environment. In each scenario, the set of events generated by the nodes are specified. The simulation environment may take into account the physical area in which nodes are located, the time duration of simulation, the physical characteristics of nodes, and a node mobility model [18], which defines the speed and direction of a node's movement over time and also simulation result the robustness of protocol.

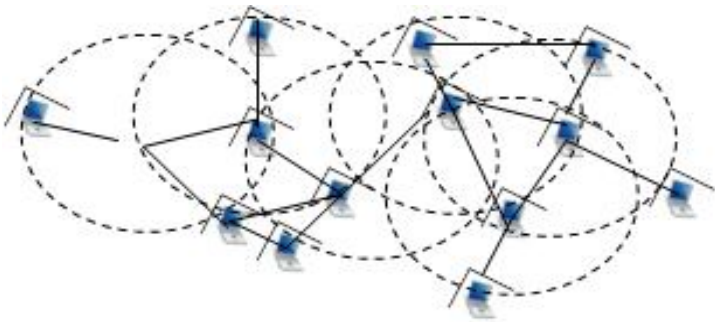

Figure 1. Architecture of MANET

1. Characteristics of MANET

MANET's node consists of wireless transmitters and receivers using antennas which are: highly directional, omni-directional or a combination of both . To enable communication within a MANET, a routing protocol is required to establish routes between participating nodes. Because of limited transmission range, multiple network hops may be needed to enable data communication between two nodes in the network. In MANETs mobile nodes share the same frequency channel thereby limiting the network capacity. Thus one of the highly desirable properties of a routing protocol for MANETs is that it should be bandwidth efficient. Since MANET is an infrastructure-less network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network .

Any protocol must efficiently handle several inherent characteristics of MANETs:

- In MANET, each node act as both host and router. That is it is autonomous in behavior.
- Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
- Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
- The nodes can join or leave the network anytime, making the network topology dynamic in nature.
- Mobile nodes are characterized with less memory, power and light weight features.
- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
- Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- High user density and large level of user mobility.
- Nodal connectivity is intermittent.

2. Advantages of MANET

- Lower getting-started costs
- no need to install base stations
- easier temporary setup
- Well suited to free unlicensed spectrum
- significant savings given typical auction prices
- Inherent scalability
- with power control & cooperative relaying, each user contributes to network capacity

3. Disadvantages of MANET

- **Security**

Wi-Fi devices in ad hoc mode offer minimal security against unwanted incoming connections. For example, ad hoc devices cannot disable SSID broadcast like infrastructure mode devices can. Attackers generally will have little difficulty connecting to your ad hoc device if they get within signal range.

- **Signal strength monitoring.**

The normal operating system software indications seen when connected in infrastructure mode are unavailable in ad hoc mode. Without the ability to monitor the strength of signals, maintaining a stable connection can be difficult, especially when the ad hoc devices change their positions.

- **Speed.**

Ad hoc mode often runs slower than infrastructure mode. Specifically, Wi-Fi networking standards like 802.11g) require only that ad hoc mode communication supports 11 Mbps connection speeds: Wi-Fi devices supporting 54 Mbps or higher in infrastructure mode will drop back to a maximum of 11 Mbps when changed to ad hoc mode.

RELATED WORK

[1] Mukaddam M, Dighe S, Varude A , Supugude A, Sangle V has studied the attack.The attack studied in this paper is wormhole attack. The choice of attack was based on the difficulty in identifying and mitigating the attack in real life scenarios. We used AODV protocol for the simulation; the most popular routing protocol used for small scale networks. Wormhole attack is a potential threat to MANETs; it involves using a two node system to route enables the attacker to manipulate packet traffic.

II. AODV (ADHOC ON DEMAND DISTANCE VECTOR ROUTING)

It reduces flooding in the network & provides low overhead as compared to proactive protocols .It causes large delays in a route discovery, also require new state information when a link gets failed & notification is sent to the affected node.

AODV uses following messages:

i. Route Request(RREQ)- RREQ is broadcasted by a node requiring a route to another node.IP address is used as a source address,when it request for a route.
ii. Route Errors(RERRs)- A message RERR is generated upon failure of any link.
iii. Route Replies (RREPs)- RERR message contains the information of nodes,which cann't access due to this failure.HELLO message are used for detecting and monitoring links to neighbors

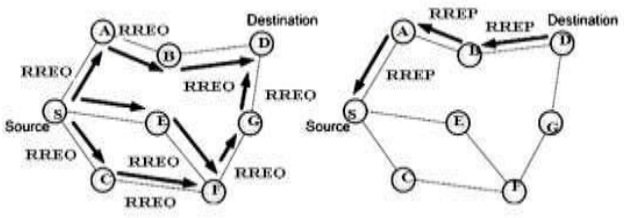

Figure 2. AODV Route Discovery Process

III. WORMHOLE ATTACK

Wormhole attack essentially creates a tunnel between two malicious nodes, thereby disrupting normal packet traffic. Figure 4.1 depicts a multi-node system, in which node S9 acts as the first end of wormhole tunnel and S2 acts as the second end of wormhole tunnel [4][5][7]. This tunnel is a direct line of communication between the two. One end will record all the packet information at one end and send it over to the other end. Needless to say, this compromises the security of the network; it also is difficult to detect being a two-node system [6]. By programming the nodes to behave maliciously for a certain time period and normally during the rest, increases the complexity of detecting such an attack. If the tunnel is created reliably, it can actually benefit the network, however that is not the intent of most malicious nodes.

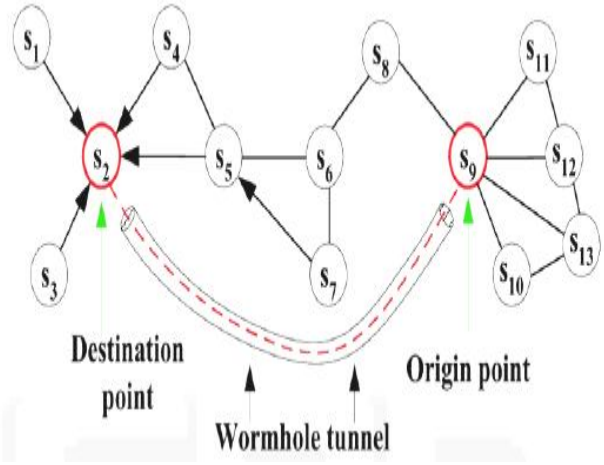

Figure 3. Wormhole attack

IV. EXPERIMENTAL SETUP & RESULTS

Table 1 the Queuing parameters of the system

Parameter	Value
Examined Protocol	AODV
Number of Nodes	15,20 and 25
Simulation Time	1000sec
Simulation Area	150mX150m
Network Traffic	CBR
Packet Size	512 Bytes
No of Malicious nodes	02
Simulator	NS 3.25

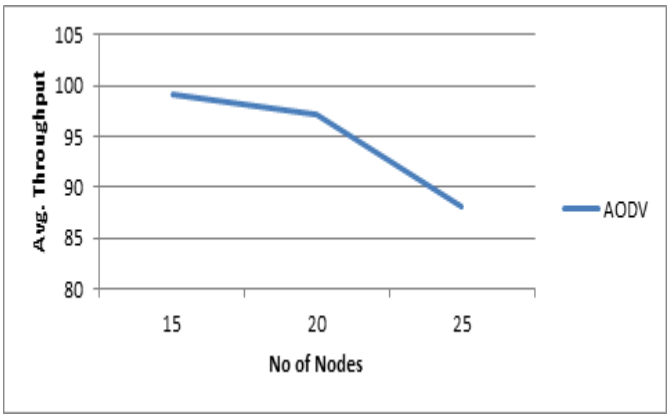

Figure 4. Average Throughput

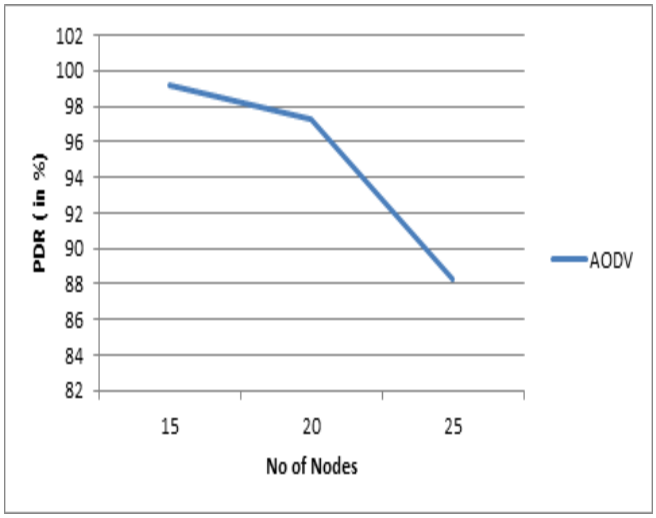

Figure 5. PDR (in %)

V. CONCLUSION

The above fig5.1 shows that the throughput decreases with increasing number of nodes. The fig. 5.2 shows that the packet delivery ratio also decreases with increasing number of nodes.

The overall results reveals that the performance of AODV decreases with increase in number of nodes when wormhole or malicious nodes are present. The routing protocol used by MANETs must be reliable, secure, efficient and scalable. Security is a growing concern over the years and these routing protocols are no exception. AODV while being extremely popular is also vulnerable to attacks that involve modified Destination sequence number and hop count like the wormhole attack. The purpose of the study was to better understand the attack to help prevent it. There is undoubtedly more scope for research in this area, for securing routing protocols to theses flaws as well as intelligent Intrusion

Detection Systems (IDS) that can weed out such attacks from the network.

REFERENCES

[1] Komala CR, Srinivas Shetty, Padmashree S., Elevarasi E., "Wireless Ad hoc Mobile Networks", National Conference on Computing Communication and Technology, pp. 168- 174, 2010

[2] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu and Jorjeta Jetcheva, "A Performance Comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols", http://www.monarch.cs.cmu.edu/

[3] Perkins C. and Royer E. Ad hoc on-demand distance vector routing, In Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100 (1999)

[4] Harris Simaremare and Riri Fitri Sari. Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious Attacks, International Journal of Computer Science and Network Security, VOL-11, June 2011, pp.6.

[5] K. Lakshmi, S.Manju Priya, A.Jeevarathinam, K.Rama and K. Thilagam. Modified AODV Protocol against Black hole Attacks in MANET, International Journal of Engineering and Technology Vol.2 (6), 2010.

[6] S Upadhyay . and B.K Chaurasia. Impact of Wormhole Attacks on MANETs, International Journal of Computer Science & Emerging Technologies, Vol. 2, Issue 1, pp. 77-82 (2011)

[7] R. Maulik and N. Chaki. A Comprehensive Review on Wormhole Attacks in MANET. In Proceedings of 9th International Conference on Computer Information Systems and Industrial Management Applications, pp. 233-238, 2010

[8] MANET Routing Protocols and Wormhole Attack against AODV, International Journal of Computer Science and Network Security, Vol.10, No.4, April 2010.