Implementation of Wormhole Attack Based on AODV Routing Protocol Using Ns-3 Simulator

Anjali Soni[1] Shivendu Dubey[2] Shuchita Mudgil[3]
[1,2,3]Department of Computer Science & Engineering
[1,2,3]GGITS, Jabalpur, Kala Niketan Polytechnic College Jabalpur (MP)

Abstract— Mobile Ad Hoc Network (MANET) is collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure. The wireless links in this network are highly error prone and can go down frequently due to mobility of nodes, interference and less infrastructure. Therefore, routing in MANET is a critical task due to highly dynamic environment. In recent years, several routing protocols have been proposed for mobile ad hoc networks and prominent among them are DSR, AODV and TORA. 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.

Key words: Manet; Routing Protocoll; Performance; Ns-3

I. INTRODUCTION AND BACKGROUND

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.

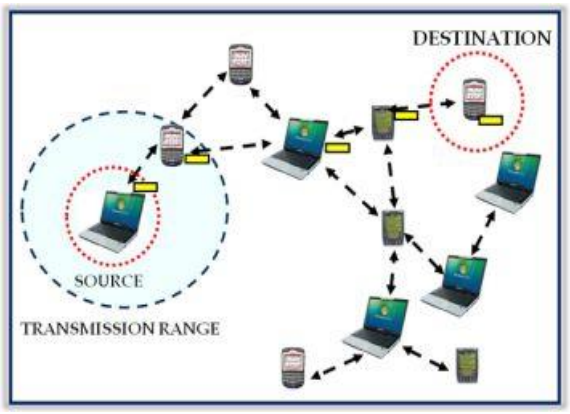

Fig. 1: Scenario of Mobile Ad hoc Network

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 , which defines the speed and direction of a node's movement over time and also simulation result the robustness of protocol.

A. 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:

1) Dynamic topology: Mobility of nodes lends to unpredictable network topology.
2) Variable capacity wireless links: The capacity of wireless-networks is significantly lesser than the hardwired systems. Considering the multiple access, fading, noise, and interference conditions, etc. and throughput of wireless networks is often much less than a radio's maximum transmission rate.
3) Power constrained operation: Power conservation is *crucial* in mobile wireless systems since these networks typically operate off power-limited sources, which dictate whether a network is operational or not.
4) Limited Physical security: Mobile networks are more vulnerable to physical security threats such as eavesdropping.

MANET routing protocol include various desirable properties. They describe following:

1) Distributed Operation: The decentralized nature of a MANET requires that any routing protocol execute in a distributed fashion.
2) On demand operation: Since a uniform traffic distribution cannot be assumed within the network, the routing algorithm must adapt to the traffic pattern on a demand or need basis, thereby utilizing power and bandwidth resources more efficiently.
3) Loop-free: To ensure proper message delivery and efficient network operation, a routing protocol must be loop-free.
4) Security: Since MANETs are more vulnerable to physical security threats, provisions for security must be

All rights reserved by *www.ijsrd.com*

made, e.g., the application of Internet Protocol (IP) security techniques.

5) Entering/Departing nodes: A routing protocol should be able to quickly adapt to entering or departing nodes in the network, without having to restructure the entire network.
6) Bidirectional/Unidirectional links: Since the condition of a MANET is dynamic, a routing protocol should be able to execute on both bidirectional and unidirectional links.
7) Sleep- period operation: Nodes of a MANET stop transmitting and receiving for some arbitrary time interval as a result of energy conservation. This property require close coupling with the link-layer protocol through a standardized interface.

B. Advantages of MANET

1) They provide access to information and services regardless of geographic position.
2) These networks can be set up at any place and time.
3) Setting up a wireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings.
4) Network can be extended to places which cannot be wired.
5) Wireless networks offer more flexibility and adapt easily to changes in the configuration of the network.

C. Disadvantages of MANET

1) Limited resources and physical security.
2) Volatile network topology makes it hard to detect malicious nodes.
3) Interference due to weather, other radio frequency devices, or obstructions like walls.
4) Security protocols for wired networks cannot work for ad hoc networks.
5) The total Throughput is affected when multiple connections exists.

II. RELATED WORK

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.

III. 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:

1) 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.
2) Route Errors (RERRs)- A message RERR is generated upon failure of any link.
3) 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

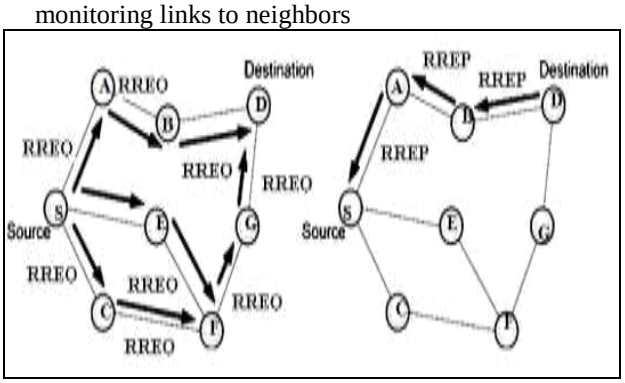

Fig. 2: AODV Route Discovery Process

IV. WORMHOLE ATTACK

A. Wormhole Attack

- Wormhole nodes fake a route that is shorter than the original one within the network; this can confuse routing mechanisms which rely on the knowledge about distance between nodes.
- It has one or more malicious nodes and a tunnel between them.
- The attacking node captures the packets from one location and transmits them to other distant located node which distributes them locally.
- A wormhole attack can easily be launched by the attacker without having knowledge of the network or compromising any legitimate nodes or cryptographic mechanisms.

The tunnel is either the wired link or a high frequency links. This creates the illusion that the two end points of the tunnel are very close to each other.

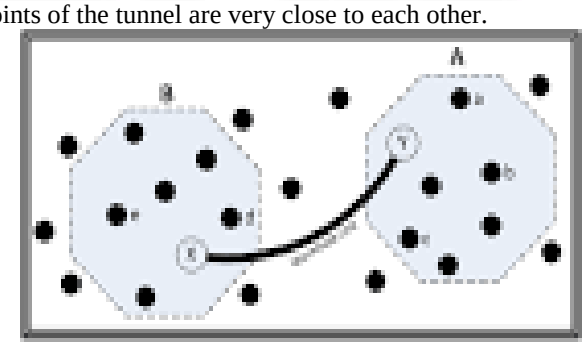

Fig. 3: Wormhole attack

V. EXPERIMENTAL SETUP & RESULTS

Parameter	Value
Examined Protocol	AODV
Number of Nodes	15,20 and 25
Simulation Time	500sec
Simulation Area	150mX150m
Network Traffic	CBR
Packet Size	512 Bytes
No of Malicious nodes	02
Simulator	NS 3.25

Table 1:

All rights reserved by *www.ijsrd.com*

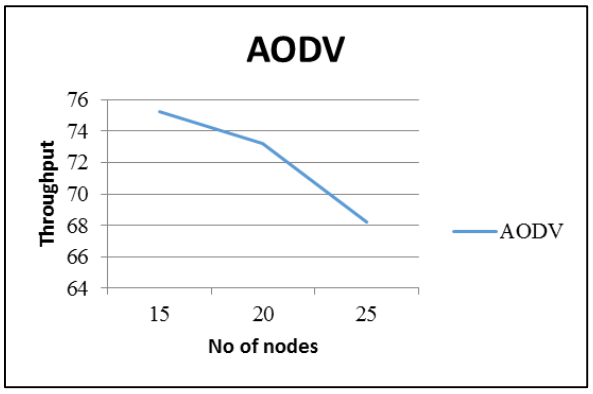

Fig. 4: Average Throughput

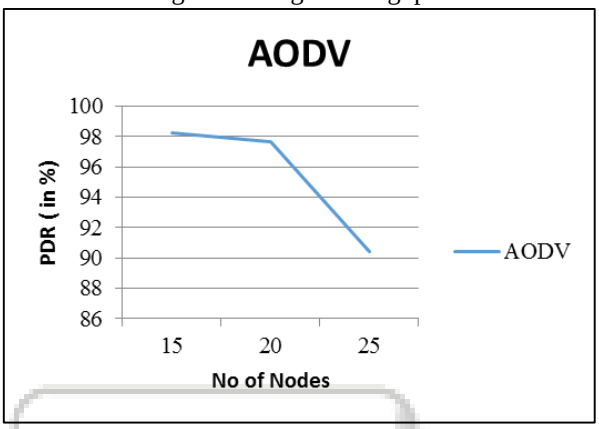

Fig. 5: PDR (in %)

VI. 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 these flaws as well as intelligent Intrusion Detection Systems (IDS) that can weed out such attacks from the network.

REFERENCES

[1] Mohseen Reeyaz Mukaddam," Simulation study of wormhole attack in ns3", IJSRD, Volume : 3, Issue : 8, 01/11/2015 Page(s): 384-387
[2] Komala CR, Srinivas Shetty, Padmashree S., Elevarasi E.,"Wireless Ad hoc Mobile Networks", National Conference on Computing Communication and Technology, pp. 168- 174, 2010
[3] 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/
[4] 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)
[5] 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.
[6] 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.
[7] 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)
[8] 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
[9] MANET Routing Protocols and Wormhole Attack against AODV, International Journal of Computer Science and Network Security, Vol.10, No.4, April 2010.

All rights reserved by *www.ijsrd.com*