Approach to Detect Prevent Wormhole Attack in MANET

Asha Mansore[1], Surbhi kaushik[2]
[1]*M.Tech DC PCST College Indore*
[2]*Asst. Prof. Electronic Dept. PCST College Indore*

Abstract - MANET has recently attracted a lot of interest in the research community due to their wide range of applications. Due to distributed nature network and deployment in remote areas, sensor networks are vulnerable to numerous security threats that can adversely affect its functioning & degrade network performance. This problem becomes more critical if it is deployed for some confidential mission i.e. military applications. So far, very little research has been done in the development of secure routing protocols. The work investigate that attacker may deploy a high power transmission node to attract all neighboring node as shortest path. Such kind of attempt is known as high power transmission node wormhole attack. By the investigating transmission power work will investigate the wormhole attack. Work will also integrate security policy and algorithms with AODV routing protocol. It will improve the throughput and packet delivery ratio and also reduce the energy consumption and improve the routing performance during security attack. At last work will compare the results between traditional AODV and modified AODV.

Keywords: MANET, AODV, WSN, Wormhole, Cluster-based.

1. INTRODUCTION

A mobile ad hoc network (MANET) is a group of devices or nodes that transmit across a wireless communication medium mainly based on radio frequency without any fixed infrastructure or centralized control. Cooperation of nodes is important to forward packets on behalf of every different once other destinations are out of their direct wireless transmission vary. There will be no centralized control or network infrastructure for a MANET to be set up, thus making its deployment quick and inexpensive. The nodes facility to move generously ensures a flexible and handy vibrant network topology which is another important feature of a MANET [2]. Some of the MANET applications includes emergency disaster relief, military operations over a battlefield (vulnerable infrastructure), and wilderness expeditions (transient networks), and community networking through health monitoring using medical sensor network (MSN).

There are numerous issues in MANETS which addresses the points some of them are IP address, radio interference, routing protocols, power Constraints, security, mobility management, bandwidth constraints, QOS, etc. As of now some hot issues in MANETS can be related to the routing protocols, routing mobility and position updates have raised lot of interest of researchers. Let us understand by it an actual scenario of ad hoc network i.e. A message sent by a node reaches all its neighboring nodes that are placed at distances up to the transmission radius. Because of the limited transmission radius, the routes between nodes are normally created through several hops in such multi-hop wireless networks. The use of the nodes' position for routing poses evident problems in terms of reliability. The accuracy of the destination's position is an important problem to consider. Here a few cases the destination is a fixed node (e.g., a monitoring centre known to all nodes, or the geographic area monitored), and some networks are static. The problem of wormhole security threat in mobile ad hoc networks appears to be more difficult than routing itself.

2. SECURITY OF NETWORK OPERATIONS

From a security point of view, there are many reasons due to which wireless ad hoc network are at danger. When unapproved node or entities disrupt the normal operation, we can say the network is under assault. When different nodes communicating with each other by a wireless medium and all this are vulnerable to connect attacks some of the links attack are:

- Submissive eavesdrop
- Dynamic snooping
- Leaking clandestine information
- Data changing
- Masquerade
- Message respond
- Message deformation

- DOS

The majority of the security necessities require not be tended to in the system or upper layers. For example, in a few remote LANs connection layer encryption is connected. Be that as it may, as a rule the security administrations are actualized in higher layers, for example, in the system layer, since numerous specially appointed systems apply IP-based steering and propose or recommend the utilization of IPSec.

The recognition of compromised node is one of the biggest problems. Frequently such nodes can be discovered by observing their behavior, but because of their unfortunate link quality sometimes other nodes misbehave as well. A complicated failure has mainly happened due to the presence of negotiating node.

3. WORMHOLE ATTACK ON AODV PROTOCOL

A Wormhole attack is used to compromise the network by capturing or introducing better communication node then existing sensor nodes to degrade the performance. There are five methods to apply wormhole attack on AODV. The attacker uses high power transmission node or high bandwidth tunnel to create illusion of shortest path among nodes. Attacker uses these quality techniques to promote itself for route discovery or data packet communication. Due to quality shortest route, neighbor gets wonder and adopt the solution for communication. Once connection establish, attacker collect data packet one end and deactivate the forwarding link

A typical wormhole attack requires two or more attackers (malicious nodes) having better communication capability and resources than other sensor nodes. The attacker creates a low-latency link (high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighboring sensor nodes take up this tunnel for their communication. The strange factor is, all data packet moves from this tunnel and attacker may collect or drop data packet respectively.

4. PROBLEM STATEMENT

In mobile ad hoc network, mobile nodes are free to move from one location to another location means that position of mobile nodes is frequently changed. Due to the mobility (rate of position change of mobile node with respect to time) of nodes and continuously changing network topologies pose several challenges. Due to this best route may no longer remain at same time instant. Security threats may use this vulnerability not only to compromise mobile nodes but also to degrade performance. So detection and prevention of security threat is slightly difficult in mobile ad hoc network.

Mobile ad hoc network uses asymmetric links, so that nodes are frequently changing their position within network. There are many problems with routing:

- **Routing overhead**: In mobile ad hoc network, nodes often change their location in network so that routing table is frequently changed. Due to this the problem is routing overhead.

- **Interference**: This is the major problem in mobile ad hoc network. Wireless links in MANET come and go depending on transmission characteristics. Interference occurs due to noise, weather etc.

- **Asymmetric links**: Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile and constantly **ever-changing** their position **among** network. For example consider a MANET (Mobile Ad-hoc Network) where node B sends a signal to node A but this does not tell anything **concerning the standard** of the **affiliation within the** reverse direction

- **Dynamic topology**: Topology is not constant in MANET, So that routing tables are frequently changed. Routing tables must reflect changes in topology.

- **Security Threats**: Due to vulnerability in routing protocols, it is prone for various security threats. Routing protocols are used to discover route among nodes. Thus vulnerable routing protocol may give option for security threats to compromise.

5. LIMITATION OF CURRENT SYSTEM

A malicious node can carry out the following attacks in AODV.

1. Source node can be impersonated by the malicious node by modifying the source address with its address in the RREQ packet.

2. To analyze the communication in the route and become a part of it, malicious node can change the other contents of

RREQ packet also such as hop count. It reduces the hop count in order to increase the chances of being selected in the route between source and destination.

3. Destination node can also be impersonated by forging the destination address by its own address in a RREP.

4. Malicious node can capture an entire network and act as a network leader by broadcasting the biggest sequence number. It can become a black hole to the entire sub network.

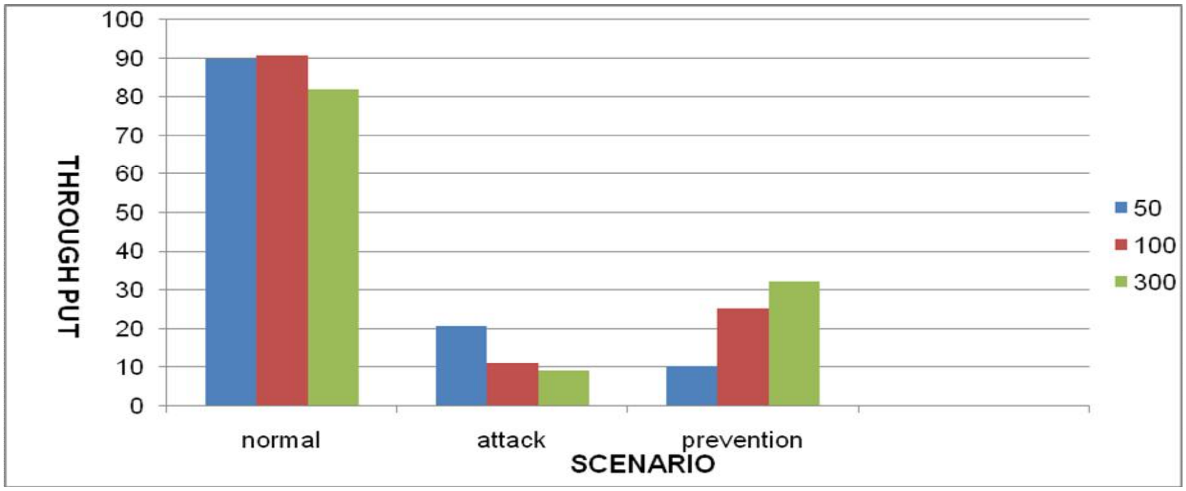
5. It can selectively forward certain RREQ packets and RREP packets and avoid other packets.

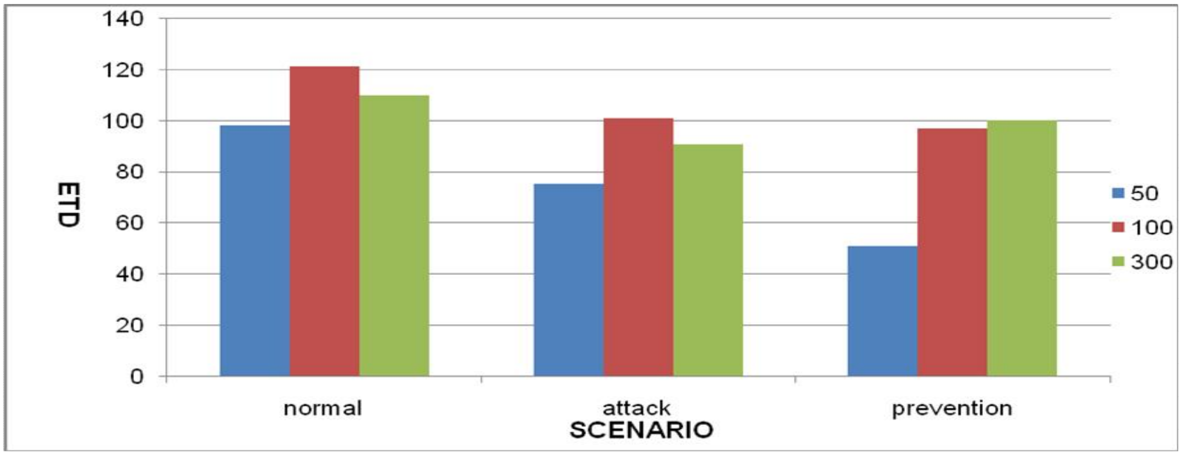
6. It can forge a RERR message and avoid further communication between nodes as they cannot reach the destination with different sequence number.

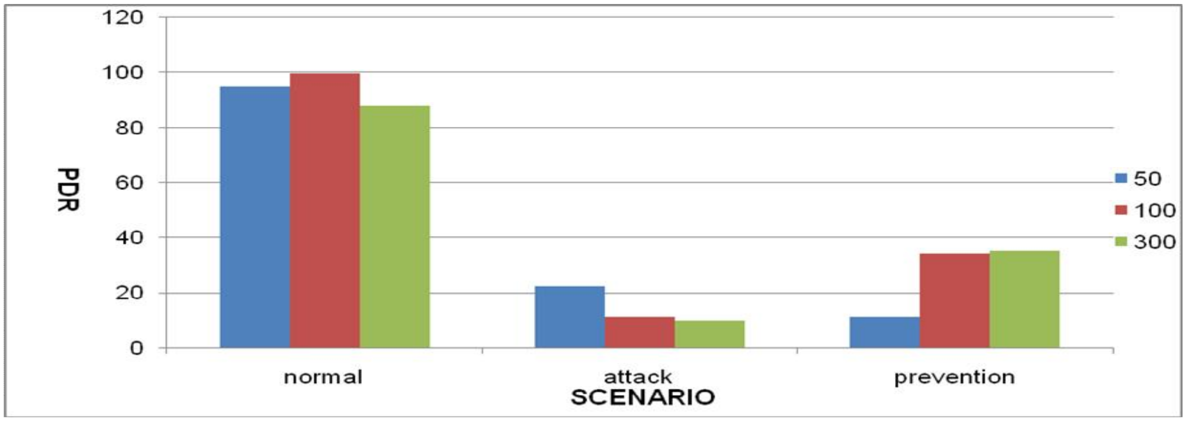
7. To create delay in the communication, malicious node can send two different RREQs to the neighboring node with different sequence numbers.

6. SOLUTION DOMAIN

Intrusion is a kind of unwanted activity occurs in the network causes its degradation. Hence it has to be detected at early stages of data transmission. There are so many intrusion prevention measures available for users to overcome such unwanted activities of intrusion. These mechanisms are encryption and authentication, which reduce and eliminate intrusions. It is must for network to deploy any live IDS with high functional requirements. Now a day's most of the IDS depend upon real-time traffic flow parse, filter, format and study, usually observer the traffic flow at switches, routers, and gateways network data monitoring .The basic parameters for a secure system are: Integrity, Confidentiality, Availability, Authentication, Non-repudiation & Scalability. Intrusion detection techniques have been traditionally classified into one of two methodologies: an anomaly detection or misuse detection detail of this is given in . In this process it is going to be executed on malicious nodes in a choice specific situation. Many nodes can transfer file at the same time with their routing topology at every node because of its mobility. In this system it lead to more security resolving option during execution.







PROPOSED WORK

The simulation of the proposed work will carried out in two scenarios. The configuration of scenarios will be based on the number of nodes are deployed and the position of the source node and destination node. Scenario-1 & Scenario-2 consists 10 nodes and 20 nodes respectively. Both scenarios will be used to test performance of proposed algorithm and wormhole attack in 4 steps.

Step 1 # Performance analysis of original AODV protocol

Step 2 # Performance analysis of AODV routing protocol with wormhole attack.

Step 3 # Detection of Wormhole attacks

Step 4 # Performance analysis of AODV with proposed preventive technique

Following results are using normal, attack and AODV (Prevention) –

7.CONCLUSION

The complete work concludes that wormhole attack is one of severe attack in MANET. It also observes that attacking technique give big impact in AODV and routing protocols. Still this technique increase end-to-end delay gives a very small impact on network performance. Improvement in end-to-end delay is expected in future work.

8. REFERENCES

[1] Gowrishankar.S , T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, "*Issues in Wireless sensor networks*" Proceedings of the World Congress on Engineering vol I, 2008.

[2] Pathan,A.S.K., Lee,H.W., Hong, C.S. "*Security in Wireless Sensor Networks: Issues and Challenges* " ICACT ISBN 89-5519-129-4, pp 1043-1048, 2006.

[3] Jaydip Sen "*A Survey on Wireless Sensor Networks Security*" In International Journal of Communication Networks and Information Security (IJCNIS) Vol.1, No. 2, August 2009, pp 55-74,

[4] Sangwan,A., Sindhu,D., Singh, K., "*A Review of various security protocols in Wireless Sensor Network*", IJCTA, ISSN:2229-6093, vol. 2 (4), july-august-2011, pp.790-797.

[5] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, Xiangke Liao "*Topological Detection on Wormhole in Wireless Ad Hoc and Sensor Networks*", IEEE/ACM Transaction on Networking, vol. 19, No. 6 December 2011, pp.1787-1796.

[6] Miss Morli Panday,Ashish Kr. Shriwastava, "*A Review on security Issues of AODV routing protocol for MANETs*", IOSR Journal of Computer Engineering(IOSR-JCE), e-ISSN:2278-0661, p-ISSN:2278-8727 vol. 14, Issue 5 (Sep. - Oct. 2013), pp.127-134.

[7] R.balakrishna, U.Rajeshwar Rao, N. Geetahanjali, "*Performance issues on AODV And AOMDV for MANETs*", International journal of Computer Science and Information (IJCSIT), vol. 1 (2), 2010,pp. 38-43.