Detection and Prevention against Wormhole Attack in AODV for Mobile Ad-Hoc Networks

Priyanka Sharma
M. Tech Student
Deptt. Of ECE, MMEC, MMU,
Mullana, Ambala, Haryana,
India

H.P. Sinha, Ph.D
Professor
Deptt. Of ECE, MMEC, MMU,
Mullana, Ambala, Haryana,
India

Abhay Bindal
Assistant Professor
Deptt. Of ECE, MMEC, MMU,
Mullana, Ambala, Haryana,
India

ABSTRACT
Security is one of the major issues in Mobile Ad-hoc Network (MANET) because of its inherent liabilities. Its infrastructure-less network with dynamic topology pose a number of challenges to security design and makes it vulnerable for different types of security attacks. In wormhole attack a pair of colluding nodes makes a tunnel using a high speed network. These colluding nodes create an illusion that the two remote nodes of a MANET are directly connected through nodes that appear to be neighbours, but are actually distant from one another. In this, a secret key is used for encryption and decryption of hello packets. Because of this, the only authentic node will remain in the network, non-authentic nodes (wormhole node) will be discarded. As a result, communication can take place only between the trusted nodes. So malicious node cannot enter into system and communication is secured.

Keywords: MANET, Ad-hoc, AODV, RREQ, RREP, Wormhole.

1. INTRODUCTION
An Ad-Hoc network is an autonomous collection of mobile nodes and wireless communication network is used to connect these mobile nodes. This type of network is known as Mobile Ad-Hoc Network (MANET). Each device in a MANET is free to move independently. MANET is an infrastructure less network with no fixed BS for communication. Intermediate mobile nodes act as router to deliver the packets between the two nodes. So, MANET is a highly dynamic network and hence more vulnerable to attack[1]. Nodes in an Ad-hoc networks are computing and communication devices, which can be laptop computers, PDAs, mobile phones, or even sensors that communicate with each other over wireless links and works in a distributed manner in order to provide the network functionality. Applications of Ad-hoc networks include military communication, emergency relief operations, commercial and educational use in remote areas, and in meetings and other situations where the networking is mission oriented and communication based.

1.1 Security Goals
Security services include the functionality required to provide a secure networking environment. The main security service can be summarized as follows:

- **Authentication:** This service verifies user's identity and assures the recipient that the message is from the source that it claims to be from. Firstly, at the time of communication initiation, the service assures that the two parties are authentic, that each entity is what it says. And next, it must assure that the third party doesn't interfere by impersonating one of the two authentic parties for the purpose of authorized transmission and reception.
- **Confidentiality:** This service ensures that the data transmitted over the network doesn't disclose to unauthorized users. Confidentiality can be achieved by using different encryption techniques.
- **Access Control:** This limits and controls the access of such a resource which can be an application or a host system.
- **Integrity:** The function of integrity control is to assure that the data is received in verbatim as sent by authorized users. The data received contains no modification, deletion or insertion.

1.2 Wormhole Attack
The wormhole attack is a severe threat against packet routing in sensor networks that is particularly challenging to prevent. In the wormhole attack, an adversary receives packets at one location in the network and tunnels them to another location in a network, where the packets are resent into the network to consume the bandwidth. The wormhole attack would involve two distant malicious nodes colluding to undertake their distance from each other by relaying the packets along an out-of-band channel which is available only to the attackers. Thus, a false route would be established by the attackers which would shorten the hop distance between any two non-malicious nodes as shown in figure 1.

Wormhole attacks can also cause Denial-of-service through unauthorized access, Data Traffic, and routing disruptions. The malicious node(s) can add itself in a route and then drop the data packets. Denial of service can prevent the discovery of legitimate routes and unauthorized access could allow access to wireless control systems that are based on physical proximity [1].

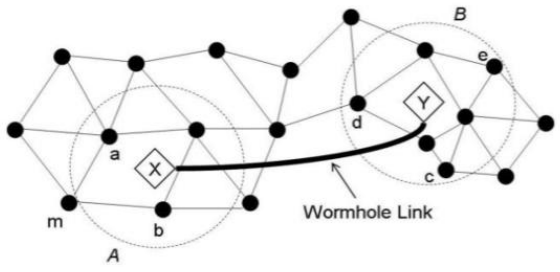

Fig 1: Wormhole Attack [1].

Figure 2 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts a RREQ to find a route to a destination node D, its

neighbours J and K for- ward the RREQ as usual. However, node A1, which received the RREQ, forwarded by node J, records and tunnels the RREQ to its colluding partner A2. Then, node A2 rebroadcasts this RREQ to its neighbour P. Since this RREQ passed through a high-speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-P-J-S to unicast a RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-J- P-D that indeed passed through A1 and A2 to send its data [13].

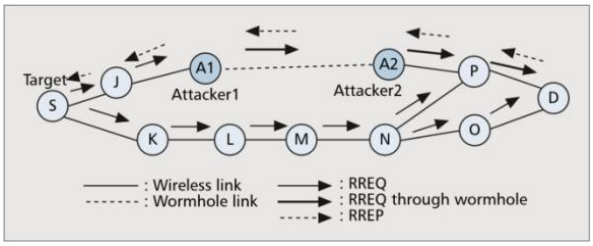

Fig 2: Example of Wormhole Attack [13].

1.3 Wormhole Attack Modes

Wormhole attacks can be achieved using several modes as follows:

- **Wormhole with high power transmission**: In this mode, when an attacker node gets a RREQ, it broadcasts the RREQ at a high power level towards the destination. By this method, the malicious mode attracts the packets to follow path passing from it.
- **Wormhole using encapsulation**: When the source node broadcast the RREQ packet, a malicious node which is at one part of the network receives the RREQ packet. Then it tunnels that packet to a second malicious node via legitimate path only, it then rebroadcasts the RREQ. When the neighbours of the second colluding party receive the RREQ, it discards all of them and the result is that the routes between source and the destination go through the two malicious nodes that will be said to have formed a wormhole or the tunnel between them. This prevents the other nodes from discovering any other legitimate path that are more than two hops away.
- **Wormhole using out of band channel**: This mode of wormhole attack involves the use of an out of band channel. In this mode, an out-of-band high bandwidth channel is placed between two end points to create a wormhole link.
- **Wormhole using Packet Relay**: In this mode also, one malicious node replays packets between two far nodes and this way fake neighbours are created[12].

1.4 Types of Wormhole Attack

Wormhole attacks are of different types namely, closed wormhole, the half open wormhole and open wormhole. Figure 3 shows these different types of wormhole attack.

- **Open wormhole attack:** In the open wormhole attack, the attackers include themselves in the RREQ packet header in the route discovery stage. Other authentic nodes are aware that the two colluding parties lie on the path, but they would think that they are direct neighbours.
- **Half open wormhole attack**: One side of the wormhole does not modify the packet, and only another side modifies the packet, following the route discovery procedure. This leads to the path S-M 1-D for the packets sent by S to D.

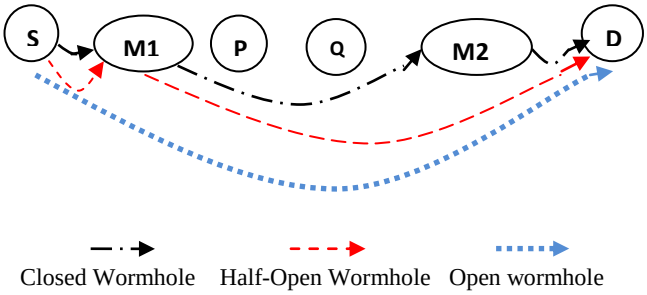

Fig 3: Types of Wormhole Attack

- **Closed wormhole attack:** The attackers do not modify the content of the packet in a route discovery. Instead, they simply tunnel the packet from one side of the wormhole to another side and it rebroadcasts the packet[7].

2. PROPOSED APPROACH

The proposed work, is about to prevent the mobile Ad-hoc network of the wormhole attack. In this, a complete work with AODV protocol is presented. To detect the wormhole node and to prevent the wormhole attack by encrypting the packet at each level by sharing the Secret Key with the neighbouring nodes and ensuring secured delivery via decrypting the packet at the neighbour node and matching the distributed Secret Key in MANET in AODV protocol environment.

3. SIMULATION ENVIORNMENT

Here, the basic parameters of the proposed approach are presented respective to the simulation environment. The approach is implemented with NS2 simulator and the Xgraph is used as the tool for the analysis.

The mobile Ad-hoc network of 36 nodes is constructed in the NS2 with the boundary area of 800m X 800m with the use of Tcl scripts. The nodes are mobile with the initial energy, speed and threshold energy as shown in the table. AODV routing protocol is used here as the protocol for the analysis.

Table 1. Simulation Parameters.

PARAMETER	VALUE
Traffic Type	TCP, UDP
Number of Nodes	36
Area Covered	800 X 800
Speed of the Node's	1,2 m/s
Simulation Time	25 Sec
Routing Approaches	AODV
Nodes Initial Energy	0.5 watts
Mobility Type	Critical Mobility
Threshold Energy of Node's	1.42681E-12

4. SIMULATION RESULTS

The simulation scenario in figure 4 shows the forwarding of the HELLO packets to its one hop nodes.

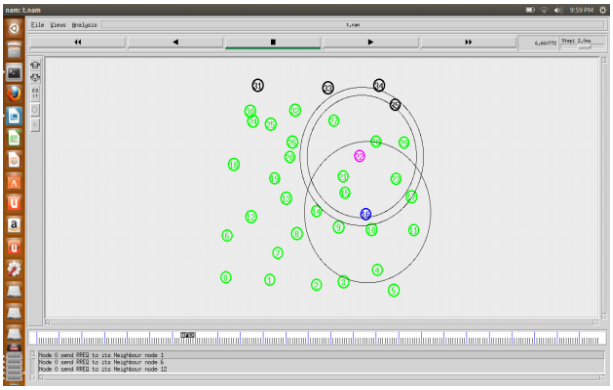

Fig 4: Forwarding of the HELLO packets to its one hop nodes.

This discovery happens when the neighbouring nodes are within the signal range of the source nodes. The HELLO packet acceptance at the one hop neighbour nodes leads to the addition of the neighbours to the routing table of the source nodes. This process continues until all the nodes are covered in the simulation scenario.

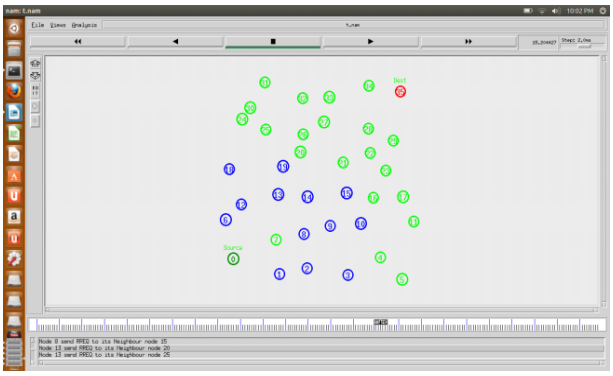

Fig 5: Sending the RREQ packet

In figure 5 the nodes are sending the RREQ packet for the route discovery of the destination after the neighbour discovery. The source sends the RREQ packet to its neighbouring nodes, which in turn, sends the packet to their neighbouring nodes, till the RREQ packet reaches the destination.

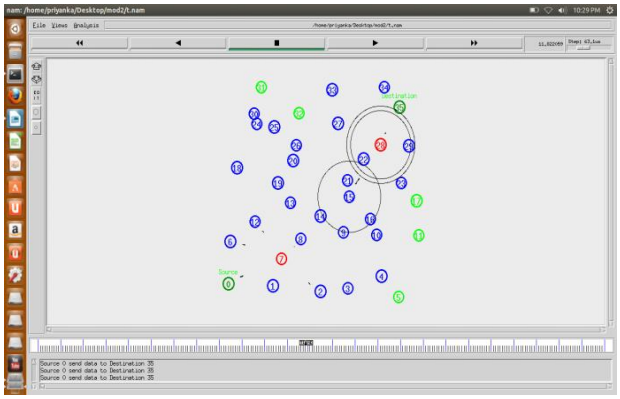

Fig 6: Tunnel created by the pair of wormhole nodes.

Figure 6 shows how the wormhole node makes it available to most of its neighbouring. The wormhole node becomes the one hop neighbours to most of its neighbouring nodes. The source node transfers data through the wormhole node to the destination. The wormhole node makes use of the tunnel to transfer the data. The tunnel created by the pair of wormhole nodes is called wormhole tunnels which causes the late delivery of the data and overall incurs the energy losses in the network.

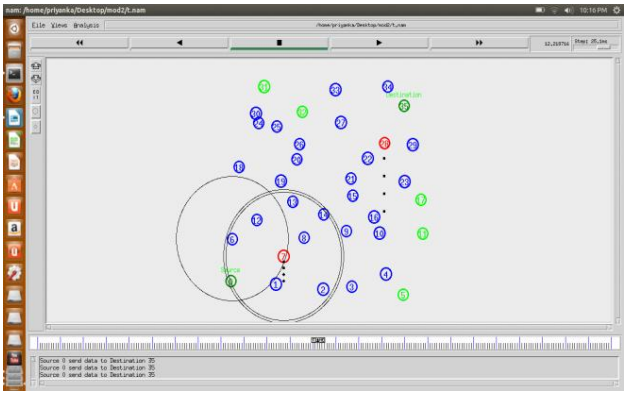

Fig 7: The wormhole node dropping the data.

The wormhole node transfers the data through the tunnel, thus, in this process it put a large number of the data packet in its queue to process the large number data and while processing all the data it drops the data packet beyond its queue size. Thus, figure 7 shows how the wormhole node drops data constantly while they are effective in the network.

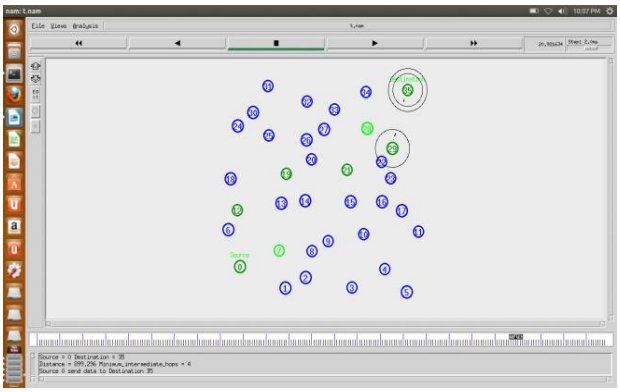

Fig 8: The node transferring the data without wormhole.

The nodes transferring data without wormhole nodes make the smooth passage of the data in the Ad-hoc network environment as shown in figure 8. The data drop in this process is very negligible. The source can easily send data without any late delivery and packet loss. This scenario is very reliable to send the data from the source to the destination nodes.

In figure 9, compared throughput are of the scenario's when there is no wormhole node present in the network, which is represented in green while the red curve represents the throughput after the intrusion in the network, i.e. the packet losses during the wormhole attack decreases the throughput of the network which is caused by the packet losses incurred on the wormhole nodes.

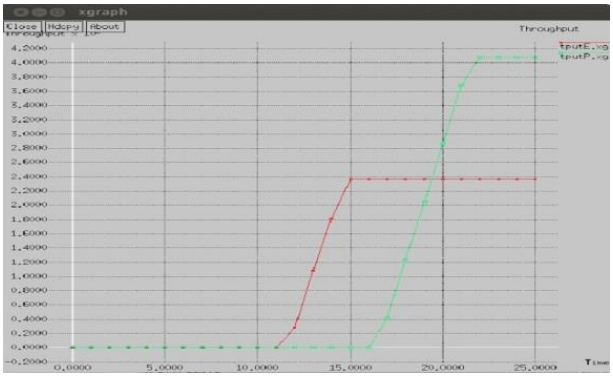

Fig 9: The comparison of the throughput.

The graph in figure 10 shows the number of packets dropped during the wormhole attack which is represented in red. The other losses in the network are very less and negligible as compared to the wormhole packet losses thus they are represented in green.

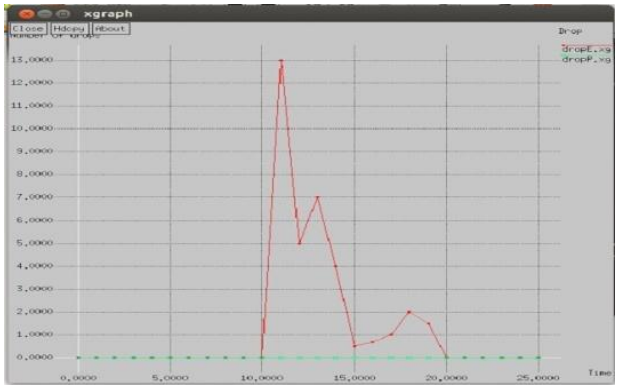

Fig 10: The comparison of the packet drop.

Figure 11 shows, the packet delivery ratio touches a new low when the wormhole nodes are effective in the network, thus, the delivery of the packets is affected when the wormhole nodes put the packets in the queue and also when it drops the packets.

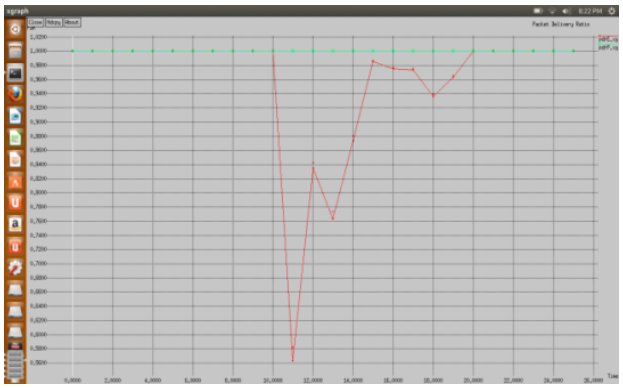

Fig 11: The comparison of the packet delivery ratio.

The following table explains the comparison of the throughput, delay and packet delivery ratio. Here the time and delay are taken in seconds, throughput and PDR in packets per second.

The comparison table explains that the efficiency of the network decreases with the effect of wormhole attack, and wormhole attack is controlled, the network has a better throughput, a PDR and a reduced amount of delay.

Time (In seconds)	Throughput with wormhole attack (Packets per Sec)	Throug-hput withou-t wormh-ole attack (Packets per Sec)	Delay with worm-hole attack (In Sec)	Delay without worm-hole attack (In Sec)	PDR with worm-hole attack (Packets per Sec)	PDR without worm-hole attack (Packets per Sec)
11	0	0	13	0	0.563	1
12	285.6	0	5	0	0.835	1
13	1077.1	0	7	0	0.763	1
14	1811.5	0	4	0	0.874	1
15	2366.4	0	0.5	0	0.985	1
16	2366.4	0	0.7	0	0.975	1
17	2366.4	416.16	1	0	0.973	1
18	2366.4	1240.3	2	0	0.936	1
19	2366.4	2056.3	1.5	0	0.963	1
20	2366.4	2864.1	0	0	1	1
21	2366.4	3680.1	0	0	1	1
22	2366.4	4080	0	0	1	1

5. CONCLUSION

With development in computing environments, the services based on ad hoc networks have been increased. However, wireless ad hoc networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. A wormhole attack is such an attack, that is, it is executed by two malicious nodes causing serious damage to networks and nodes. The detection of wormholes in ad hoc networks is still considered to be a challenging task. Here, a solution is proposed to prevent the network against wormhole attack. In this, a secret key is used for encryption and decryption of hello packets. Because of this, the only authentic node will remain in the network, non-authentic nodes (wormhole node) will be discarded. As a result, communication can take place only between the trusted nodes. So malicious node cannot enter into system and communication is secured. In this work AODV is chosen as a routing protocol for MANET, a pair of wormhole nodes is selected for performing wormhole activity. And simulation is done on NS 2.34 with 36 nodes. Simulation clearly shows that, this method is well effective in preventing the network against wormhole attack.

Here, the attackers were from outside the network. A situation may occur, if one of the authentic nodes act maliciously. In

future, it will be tried to make a system which will prevent the system from inside as well.

6. ACKNOWLEDGEMENTS

I, Priyanka Sharma, author of this paper would like to thank my College, MMEC, MMU Mullana, Haryana, India, for providing me adequate resources to make this paper. Also, I would like to thank my supervisors Dr. H.P. Sinha and Er. Abhay Bindal for their valuable suggestions.

7. REFERENCES

[1] Pravin Khandare, Prof. N. P. Kulkarni, "Public Key Encryption and 2Ack Based Approach to Defend Wormhole Attack", International Journal of Computer Trends and Technology- volume4, Issue3, 2013.

[2] Anil Kumar Fatehpuria, Sandeep Raghuwanshi, "An Efficient Wormhole Prevention in MANET Through Digital Signature", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 3, 2013.

[3] L. Sudha Rani, R. Raja Sekhar (Ph.D), " Detection And Prevention Of Wormhole Attack In Stateless Multicasting", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March 2012.

[4] Pushpendra Niranjan, Prashant Srivastava, Raj Kumar Soni, Ram Pratap, " Detection of Wormhole Attack using Hop-count and Time delay Analysis", International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012.

[5] N. S. Raote, Mr. K. N. Hande, "Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network", International Journal Of Advanced Engineering Sciences And Technologies Vol. No. 2, issue no. 2, ISSN 2230-7818, pp. 172 – 175, 2011.

[6] Nidhi Nigam, Amit Saraf, Chetan Nagar, "A Review New Thread Based Wormhole Attack Prevention Mechanism in MANET", International Journal of Electrical, Electronics & Computer Engineering, ISSN No. 2277-2626, pp: 84-87, 2011

[7] Pallavi Sharma, Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad-hoc Network Using Digital Signature", IEEE 2011.

[8] Saurabh Gupta, Subrat Kar, S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", International Conference on Innovations in Information Technology, 2011.

[9] Mariannne. A. Azer, "Wormhole Attacks Mitigation", Sixth International Conference on Availability, Reliability and Security, 2011.

[10]Rutvij H.Jhaveri, Ashish D.Patel, Jatin D. Parmar, Bhavin I. Shah, " MANET Routing Protocols and Wormhole attack against AODV", IJCSNS International Journal of Computer Sciences and Network Security,VOL.(4), April 2010.

[11] Majid Khabbazian, Hugues Mercier, and Vijay K. Bhargava, "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad-hoc Networks", IEEE Transaction On Wireless Communications, VOL.8, Issue 2, 2009.

[12] Viren Mahajan, Maitreya Natu, Adarshpal Sethi,"Analysis of Wormhole Intrusion Attack in MANETs", IEEE, 2008.

[13] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, "A Survey of Routing Attacks In Mobile Ad Hoc Networks", IEEE Wireless Communications, ISSN No. (1536-1284), pp. 85-91, October 2007.

[14]L.Lazos, R.Poovendran, C.Meadows, P. Syverson, L.W Chang, "Preventing Wormhole Attack on Wireless Ad-hoc Networks: A Graph Theoretic Approach", IEEE Communications Society IEEE, 2005.