Impact and Performance Analysis of Wormhole Attack on AODV in MANET using NS2

Manju Ojha[1], Rajendra Singh Kushwah[2]

[1]Department of Computer Science, Institute of Technology and Management, Gwalior, Madhya Pradesh, India

[2] Department of Computer Science, Institute of Technology and Management, Gwalior, Madhya Pradesh, India

Abstract: ***An ad-hoc network is a infrastructure less network i.e. there is no fix infrastructure. Each node is a mobile node and can act as a router, a source or a base station. There is no central coordinator. AODV is a well known on-demand routing protocol and is prone to WORMHOLE attack. Wormhole attack is one of the most common and harmful attack in MANET. In this paper we analyze and compare the performance of AODV before and under WORMHOLE attack on different AODV parameters. For this NS2 simulator has been used to study the performance of AODV on different number of nodes.***

Keywords: MANET, AODV, Wormhole attack, tunnel, DelPhi

1. Introduction

Wormhole Attack- Wormhole is a type of DoS attack. In this type of attack an attacker obtains the packet from source or neighbor node and transfer it to other malicious node(another attacker). Wormhole attack is a tunneling attack in which 2 or more colluding nodes participate. One malicious node sends route packet to another malicious node through a secret channel. Various types of malicious activities are carried out in this secret channel like sniffing, drop, selective-drop of data packets etc.

In wormhole attack malicious node m1 first captures routing message from neighbor or source node and propagates this message to another malicious node, say m2, by means of a secret path.m2 then sends this message to the desired destination.

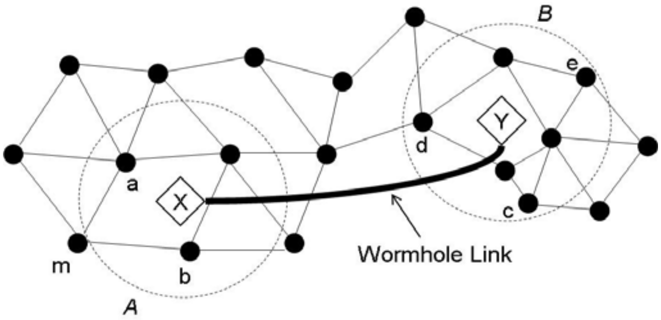

Figure 1: wormhole attack

Above is the example of Wormhole Attack with two malicious node X and Y. In this way a tunnel like channel is formed between two malicious node.

1.1 Wormhole Implementation Method

Wormhole attack can be implemented by 2 methods:

1. In-band channel:- In this mode malicious node consider some other neighbors for packet transfer along them.
2. Out-band channel:- This method does not involve participation of any other neighbor node except wormhole node and transfer packets through themselves only. Hence not letting hop count value to increase by more than one.

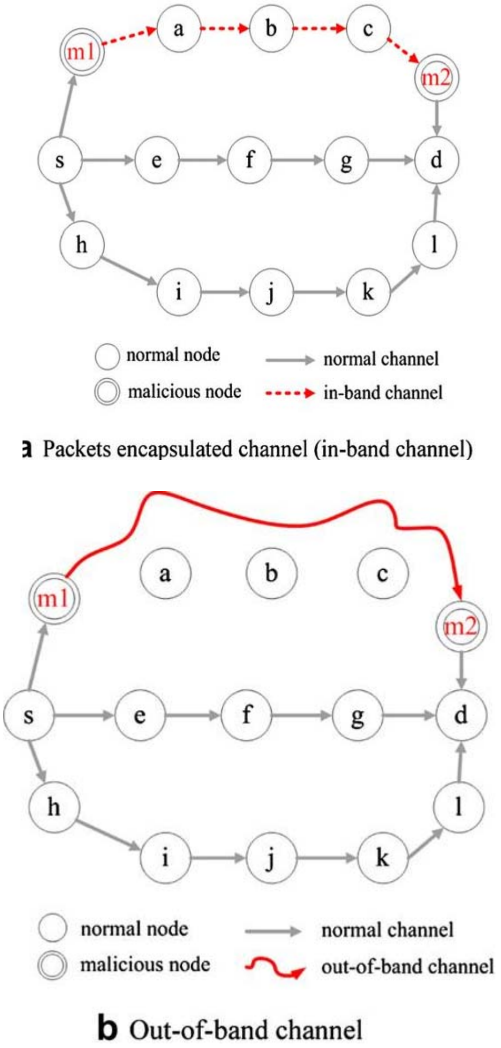

Figure 2: Implementation method of wormhole attack

1.2 Various proposed Wormhole detection And prevention methods

2. Song al. proposed a modified DSR to defend against wormhole attack by adopting a multi-path routing protocol.

3. Chin and Lui proposed an AODV based routing protocol named DelPHI. This method also applied multi-path approach and records the delay and hop count.
4. Su and Boppana proposed a routing protocol to alleviate wormhole attacks. This method can only defend against in-band –channel of wormhole attack.
5. Nail-Abdesselam used four message exchanges to defend against wormhole attack in OLSR. This method used Hello and ACK message to confirm the delay.

2. Working of AODV Protocol

AODV is on-demand distance vector routing protocol. In AODV each node maintains a routing table which gets updated on receiving a routing message. When a source wants to send a packet, it broadcast a route request packet(RREQ) to the whole network. Each node on receiving a route request packet will first check if the corresponding route exit. It will also check whether the request received is a fresh or a repeated one. If the request is repeated on it will simply discard the packet.

If not, then it will accept the request. If the node itself is a destination it will accept the packet else will broadcast it further to its intermediate nodes. Again, the intermediate nodes will check the content of this entry in its routing table. If it has a path to destination node, it will send a route reply packet (RREP) to the originator of a message choosing a proper reverse route. Route request Packet can be broadcast or a unicast but Route Reply Packet is always a unicast message.

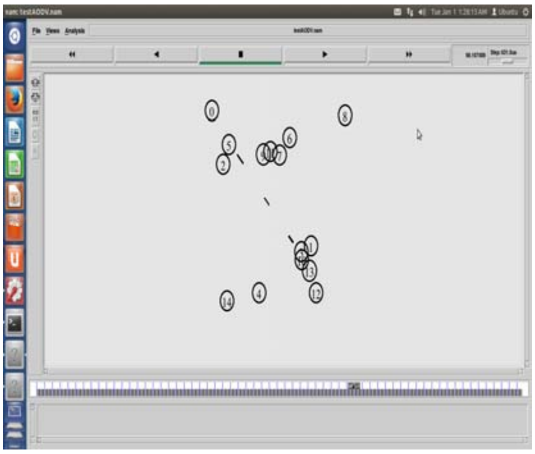

Figure 3: simulation of AODV

Above figure shows the working of AODV with 15 nodes having node 5 and node 13 as source and destination node respectively. Node 2 and node 11 are the wormhole nodes. Packets delivered from node 5 are traveled via node 2 and node 11 to destination node 13. The simulation of AODV protocol is done using NS2 simulator.

2.1 Working of Wormhole Attack on AODV:-

Suppose a node S(source node) wants to communicate to node D(destination node), it will broadcast the RRQ to every other node . Since wormhole nodes consist of high speed bus, it will give a quick response to S by sending RREP, assuring source node that it has the shortest path to the destination node.

3. Proposed Work

In this paper we will analyze the performance of AODV before and under wormhole node. We will check the AODV throughput using different number of mobile nodes. The number of wormhole node used in this paper will be 2.

Adding a malicious node to AODV:-
First of all, we need to insert two malicious node as wormhole node to see the operation of wormhole attack. Adding a malicious node is ns2 using aodv protocol. The node which is declared as malicious will simply drop the router packet (DROP_RTR_ROUTE).[4]
Two files have to be modified.
1. aodv.h
2. aodv.cc

aodv.h file changes
Declare a boolean variable malicious as shown below in the protected scope in the class AODV bool malicious;

aodv.cc file changes

1. Initialize the malicious node variable with a value "false". Declare inside the constructor as shown below

```
AODV::AODV(nsaddr_tid):Agent(PT_AODV)...
{
.......
malicious=false;
}
```

2. Add the following statement to the aodv.cc file in the "if(argc==2)"statment.

```
if(strcmp(argv[1],"malicious")==0)
{
 malicious=true;
 returnTCL_OK;
}
```

3. Implement the behavior of the malicious node by setting the following code in the rt_resolve(Packet *p) function. The malicious node will simply drop the packet as indicated below.

```
if(malicious==true)
{
drop(p,DROP_RTR_ROUTE);
}
```

4. Performance Evaluation

Table1: Effect of wormhole attack on AODV

Parameters of AODV	*AODV with no Attack*	*AODV under wormhole attack*
Avg. number of hopes per route	Normal	Low
Avg. delay in sec.	Normal	Low
Avg. route discovery time	High	Low
Avg. throughput	High	Low
Avg. retransmission rate	Low	High
Avg. data dropped	High	Low
Avg. traffic received	Low	High

4.1 Route Discovery Time

Due to wormhole attack route discovery time will decrease from average route discovery time of AODV. This will happen because each time a packet is delivered, wormhole affected path is choosen by wormhole nodes. Whereas when there is no attack, the entire route path is first checked to find optimum route. So route discovery time of AODV is higher under wormhole Attack.

4.2 Throughput

Efficiency of AODV decreases under wormhole attack than under normal working of AODV. Here green line shows the throughput of AODV without attack and red line shows throughput of AODV under wormhole attack. It can be clearly seen there is a huge decrease in the performance of AODV in the presence of Wormhole nodes.

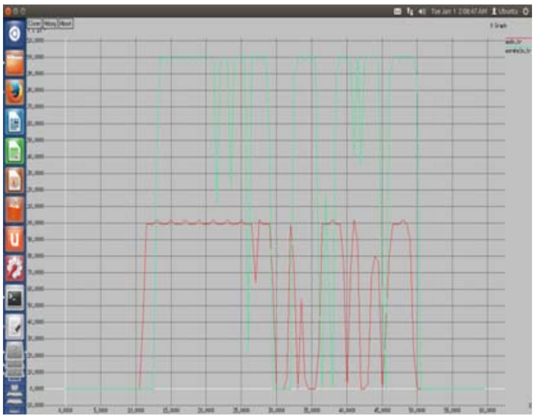

Figure 4: Graph showing Throughput of AODV before and under Wormhole attack

4.3 Delay

Here x-axis represents number of packet sent and y-axis represent delay in seconds "aodv"

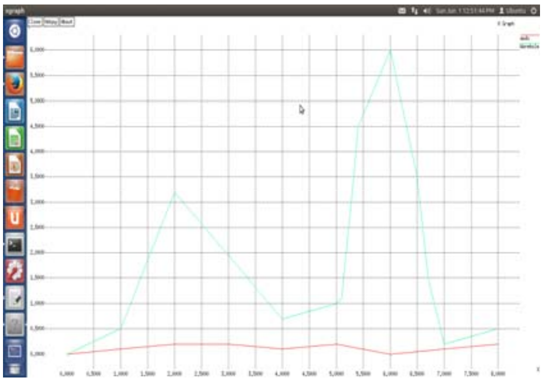

Figure 5: Graph showing packet Delay in AODV before and under Wormhole attack

4.4 Packet Loss

Here x-axis represents time in sec. and y-axis represent packet loss percent due to wormhole nodes.

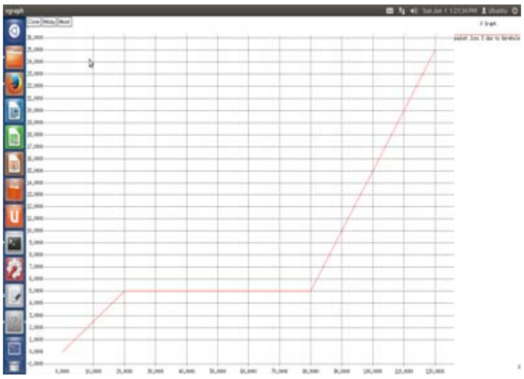

Figure 6: Graph showing packet loss % of AODV under Wormhole attack

5. Conclusion and Future Work

Wormhole path can be the efficient path in AODV unless and until wormhole nodes perform any malicious activities on route packets. As wormhole node participate in the routing network by posing themselves as authenticate member of that network, hence it becomes difficult to identify them as attackers, Thus considered as most harmful attack. This paper consist of complete analysis of AODV protocol under wormhole nodes which will help researchers to find more accurate or better Wormhole avoidance or prevention techniques. The table above gives the brief description of various AODV parameters that are affected by wormhole attack. Using this information, different techniques to eliminate wormhole from AODV along with maintaining the performance of AODV can be used as future work which will help in achieving better efficiency of AODV.

References

[1] Xia Wang and Johnny Wong, An end-to-end detection of wormhole attack in wireless ad-hoc networks. In the proceedings of the 31st annual international computer software and applications conference (COMPSAC); 2007
[2] Xu Su and Rajendra V. Boppana. On mitigating in-band wormhole attacks in mobile ad hoc networks. In the

proceedings of the IEEE international conference on communications; 2007.

[3] Securing MANET against Wormhole Attack using Neighbor Node Analysis. International Journal of Computer Applications 81(18):44-48, November 2013

[4] http://www.nsnam.com/2014/02/adding-malicious-node-in-ns2-in-aodv.html

[5] A Wormhole Avoidance Routing Protocol by Anomaly Detection in Mobile Ad Hoc Networks", Computers & Security, vol. 29, pp. 208-224, March 2010

[6] Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 "Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks", Twenty-Second ANNUAL Joint Conference of IEEE Computer and Communications , pp. 267-279.

[7] Y.-C. Hu, A. Perrig, A Survey of Secure Wireless Ad Hoc Routing Security and Privacy Magazine, IEEE, vol. 2, issue 3,pp. 28-39, May

[8] Routing Protocol by Anomaly Detection in Mobile Ad Hoc Networks", Computers & Security, Elsevier vol. 29, pp. 208-224, March 2010.

[9] Samir R. Das, Charles E. Perkins and Elizabeth M. Royer, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks"

Author Profile

Manju Ojha has done B.E from NRIITM, Gwalior, MP, India and is a GATE scholar and is persuing M.tech from Computer Science from ITM Universe, Gwalior, MP, India.

Dr. Rajerdra Singh Kushwah has done his Ph.D and is currently the Head of Department (HoD) of Computer Science/IT Dept., ITM Universe, Gwalior, MP, India.