Volume: 04 Issue: 04 Pages: 1652-1656 (2013) ISSN : 0975-0290

Evaluation of Impact of Wormhole Attack on AODV

Vandana C.P
Department of Information Science Engineering, Oxford College of Engineering, Bangalore, India
Email: vandana.hareesh@gmail.com
Dr. A. Francis Saviour Devaraj
Department of Information Science Engineering, Oxford College of Engineering, Bangalore, India
Email: saviodev@gmail.com

----------**ABSTRACT**----------

Mobile Adhoc Networks (MANET) are self organizing, decentralized networks and possess dynamic topology, which make them attractive for routing attacks. Wormhole attack is a network layer attack observed in MANET, which completely disrupts the communication channel. This paper focuses on study of wormhole attack , its behavior and the performance impact of wormhole attack on Adhoc On Demand Distance Vector (AODV) routing protocol. The NS2 network simulator is used to evaluate the wormhole attack impact on AODV.

Keywords – **AODV, MANET, Routing attack, Tunnel, Wormhole attack**

Date of Submission: January 04, 2013 Date of Acceptance: January 21, 2013

1. INTRODUCTION

A Mobile Adhoc network (MANET) [1] is composed of a collection of independent mobile hosts connected by wireless links without any fixed or centralized administration. MANET is characterized by its dynamic topology, multi hop routing, energy limited operations and network scalability. Malicious nodes carry out both active and passive attacks [2] due to the open and adhoc nature of MANET. Basic routing protocols [3] used in MANET, table-driven/proactive, demand-driven /reactive or hybrid variants, have not met the security requirements such as confidentiality, availability, integrity, authentication and non repudiation.

Wormhole attack [4] is a network layer attack launched by malicious nodes by creating a tunnel through which the packets are replayed to malicious nodes disrupting the communication channel and corrupting the routing process. Wormhole tunnel is created by any two malicious nodes (generally at distant location) which collude together to create an illusion that they are one hop away causing the routing of packets to happen through them as neighbor nodes. Once wormhole peers establish the tunnel successfully, they can tamper the packets, replay, drop the packets or selectively forward them.

This paper aims at studying the wormhole attack behavior and its performance impact on Adhoc On demand Distance Vector (AODV) [5] routing protocol using ns2 [16] network simulator. Rest of the paper is organized as follows: Section 2 describes how wormhole attack is launched in AODV routing protocol, Section 3 reviews the related work done to detect and prevent wormhole attack in MANET, Section 4 deals with simulation study of wormhole attack in AODV, its result analysis and section 5 explains the conclusion and future work.

2. WORMHOLE ATTACK IN AODV ROUTING PROTOCOL

AODV [5] is an on demand routing protocol, which creates the routes on demand. During the route discovery phase, the route request message, RREQ are broadcasted to its immediate neighbors. This process is repeated till the RREQ message reaches the destination. Upon receiving the first RREQ at destination, reply message RREP is sent back by destination to the source following the reverse path. All intermediate nodes set up forward route entries in their table. Route error message are forwarded upon detecting an error in link. Periodic hello messages check for the neighbor node link connectivity.

Wormhole attack [6] is launched in AODV. The colluding nodes create a high speed tunnel, emulating as one hop neighbor, hence causing the RREQ to reach the destination at a faster rate compared to usual path. According to AODV protocol, destination discards all the later RREQ packets received, even though they are from authenticated node. The destination then chooses the false wormhole tunnel infected path to send the RREP causing the inclusion of wormhole tunnel in the data flow route.

Wormhole attack can be launched in hidden mode and exposed mode. In hidden modes, network is unaware of the presence of malicious nodes as packets are not modified by attackers, and in exposed mode, network is aware about of the presence of malicious nodes but can't identify the malicious peers. The tunnel [4] can be created in one of the four ways, namely: packet encapsulation, creation of out of band link using specialized hardware channel, packet relay approach and usage of high power transmission.

3. RELATED WORK

Various wormhole detection mechanisms have been devised. In wormhole attack detection mechanism [7], the

Volume: 04 Issue: 04 Pages: 1652-1656 (2013) ISSN : 0975-0290

fact that the transmission time between two wormhole nodes is much longer than that between two legitimate neighbours which are close together is considered. Wormhole attack creates an illusion that the malicious nodes are one hop neighbours and are the best route to be taken in on demand routing protocols by exhibiting low hop count. But this approach can have high false positive rate since the link latency may go exceptionally high due to congestion in certain cases.

Delphi (Delay Per Hop Indicator) [8] detects both hidden and exposed wormhole attack. Every possible disjoint path between sender and receiver is found. Delay per Hop value is used to detect wormhole. LITEWORP [9] is wormhole countermeasure based on monitoring local traffic monitoring systems but is applicable to only stationary networks. In MOBIWORP [10] neighbour discovery process confirms the presence of wormhole attack.

WORMEROS [11] technique considers round trip time between source node and destination node for detecting wormhole link based on high latency. In WAP [12] approach, the relative frequency of each link appearance in a set in multi-path routing is considered for detection of wormhole attack.

Trust and Reputation based approaches exploit the packet drop property of wormhole nodes. TARF [13] a trust aware routing framework computes the trust level of each neighbour node and the lowest trust levels are considered to be wormhole nodes. In this approach, threat model includes the energy level of malicious nodes to be always high to lure the packets.

4. SIMULATION STUDY

4.1 Scope of study

In this work, wormhole attack is simulated in ns2 [14] by using encapsulation of packet approach in AODV routing protocol. At one end of the wormhole tunnel, the packets are encapsulated and at the other ending end of tunnel, packets are decapsulated. Here, wormhole peers are far apart but this tunnel creates an illusion that wormhole peers are one hop count apart as shown in Fig. 1. However the latency of the wormhole link is very high. Once wormhole tunnel is created, wormhole peer nodes would drop the packets.

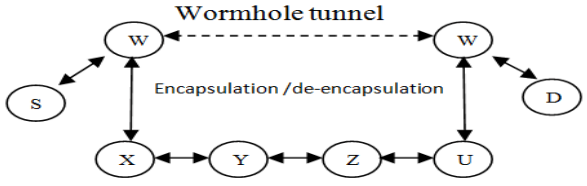

Fig 1. Wormhole tunnel creation by packet encapsulation

A new wormhole aodv agent is created and attached to the wormhole peer nodes via the front end Otcl of the ns2. The actual tunnelling (encapsulation and decapsulation) of the packet is done in the AODV protocol implementation (aodv.cc and aodv.h). The encap_packet() and the decap_packet() methods of Encapsulator.h are overridden in aodv.cc and are invoked in rt_resolve(), recvPacket(), recvRequest(), recvReply() methods of aodv.cc for creation of wormhole tunnel.

4.2 Simulation Environment

The parameters shown in Table 1 are configured in ns2 [14]. Random way point mobility [15] model is used for simulating the node mobility in MANET due to its simplicity and flexibility to provide pause time in mobility pattern.

Table1. Parameters used for simulation

PARAMETER	VALUE
Area	1000 m * 1000m
Simulation Time	200 seconds
Number of nodes	50
Traffic Model	CBR
Mobility model	Random Way Point
Number of wormhole tunnels	1/2/3/4/5 (upto 10 wormhole peers maximum)
Number of network connections	1/2/3/4/5
Mac protocol	802.11
Data rate	2 Mbps
Data Packets	512 bytes/packet

4.3 Simulation Result Analysis

Performance of AODV routing protocol with and without wormhole attack is analyzed in terms of network throughput, packet delivery ratio, packet drop rate and average end to end delay. Also a scenario, with increasing number of wormhole tunnels is simulated to capture the above mentioned parameters.

4.3.1 Network Throughput

Network throughput is measured as the total number of packets received at the destination over a period of time and is expressed in kbps. In the first scenario, 50 node MANET is considered with a wormhole link (two wormhole peers) simulated and number of network connections is increased from 0 to 5. The throughput comparison for this first scenario is depicted in Fig 2.As shown in Fig 2, the AODV throughput decreases when the wormhole link is present compared to normal AODV throughput. Maximum throughput difference observed between normal AODV and wormhole infected AODV is around 40kbps. In the Table 2, the throughput observed in normal AODV and wormhole infected AODV is represented. Also the percentage of decrease in AODV throughput due to the presence of one wormhole link is depicted. The simulated second scenario involves increasing the wormhole links from 1 to 5; total 10 wormhole malicious nodes are present. Again the network throughput is calculated in this scenario and depicted in Fig3.

Volume: 04 Issue: 04 Pages: 1652-1656 (2013) ISSN : 0975-0290

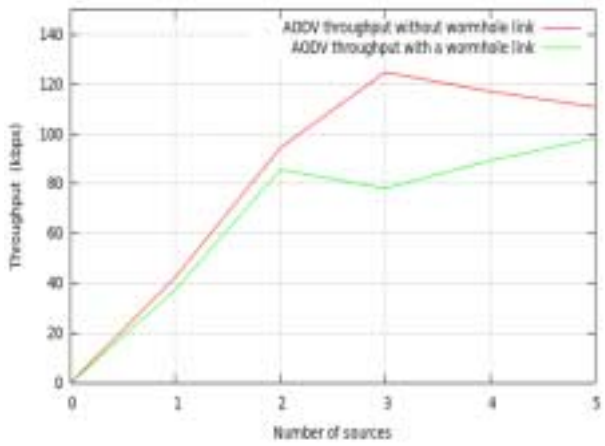

Fig 2. AODV throughput decrease when a wormhole link is present.

Table2. Throughput in kbps

Number of connections	Throughput in normal AODV	Throughput in wormhole AODV	Percentage decrease in Throughput
1	42.495641	37.466132	5%
2	94.532151	85.799677	9%
3	124.932287	78.189349	46%
4	117.170742	89.422096	28%
5	110.947987	98.367258	13%

In Fig. 3, a steady decrease in throughput is observed, until the fifth wormhole tunnel is introduced in the network of 50 nodes with 5 sources. This behaviour may be due to node mobility, possibly the packets are not getting routed through wormhole links for certain duration, hence steady decrease in throughput is not observed when fifth wormhole tunnel is introduced and the AODV throughput finally decreases to the value of 37.453kbps.

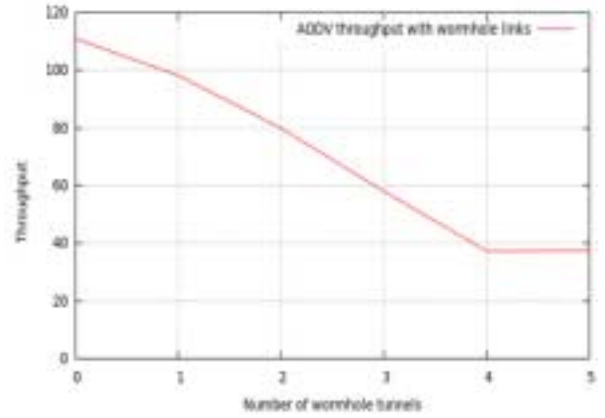

Fig 3. Throughput decrease when number of wormhole tunnels increase.

4.3.2 Average end to end delay

It is the total time taken for the packet to reach from source to destination and measured in seconds. In Fig. 4, the time taken for packets to reach destination is high when a wormhole link is present as the link latency is more for wormhole link. Increase in end to end delay in presence of a wormhole link in AODV is shown in Table 3.

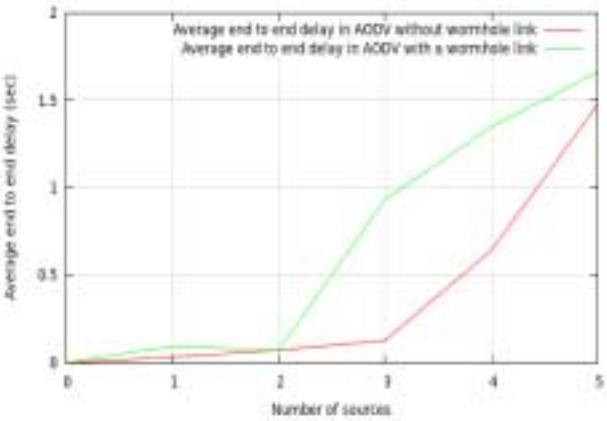

Fig 4. Average end to end delay higher for wormhole infected AODV compared to normal AODV.

Table3. Average End to end delay in sec

Number of connections	End to end delay in normal AODV	End to end delay in wormhole AODV	Percentage increase in end to end delay
1	0.032438	0.095283	6.2%
2	0.070926	0.070858	0.6%
3	0.127620	0.932756	80%
4	0.641664	1.349955	70.8%
5	1.477801	1.664211	18%

In Fig. 5, the wormhole tunnels are increased from 1 to 5 and average end to end delay reaches the maximum value 4.296241 when all the 10 womehole peers are active.

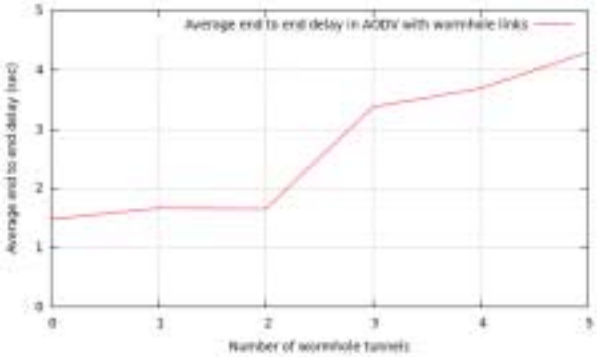

Fig 5. Average end to end delay increases with increase in wormhole tunnels.

4.3.3 Packet delivery ratio (PDR)

PDR is the ratio of number of packets received at destination node to that of number of packets sent by source node.Here it is expressed in percentage. In Fig 6, it is observed that the PDR has maximum reduction by 32%

Volume: 04 Issue: 04 Pages: 1652-1656 (2013) ISSN : 0975-0290

when a wormhole link is present compared to normal AODV's PDR value.This behaviour is due to the reduction in number of packets reaching destination because of dropping of packets by wormhole peers. Table 4 shows the decrease in PDR when one wormhole link is present.

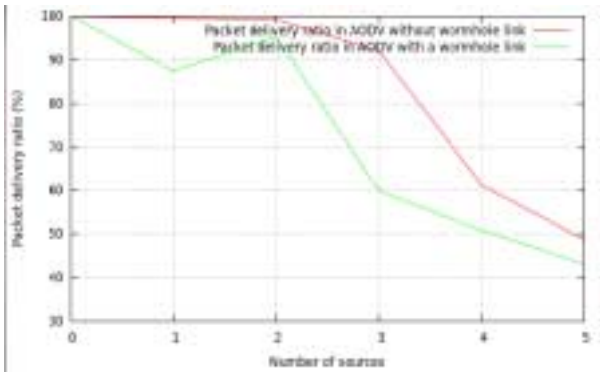

Fig 6. PDR is higher for normal AODV compared to wormhole infected AODV.

Table 4. Packet delivery ratio (PDR) in (%)

Number of connections	Packet delivery ratio in AODV	PDR in wormhole AODV	Percentage decrease in PDR
1	99.579390	87.381703	12%
2	99.211356	95.320715	4%
3	91.973361	59.866807	32%
4	61.251314	50.841220	10.4%
5	48.643533	43.028391	6%

According to the second simulated scenario wherethe number of wormhole links are increased from 1 to 5 leading to the presence of 10 wormhole malicious nodes finally. In Fig.7, when number of wormhole tunnels are increased from 1 to 5, packet delivery ratio decreases to 14.468980 as more packet drop is observed at the wormhole nodes.It is observed that when all the 5 wormhole links are present, the packet delivery ratio is minimum.Maximum number of packets get routed through the wormhole tunnels, hence the wormhole peers node buffer may overflow leading to drop of packets , hence reducing the packet delivery ratio further.

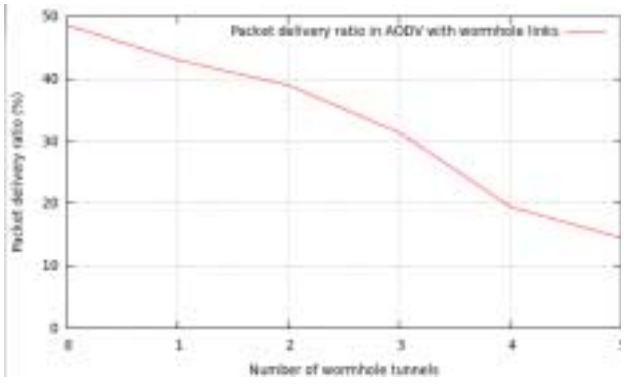

Fig 7. Steady decrease in PDR with increase in wormhole tunnels.

4.3.4 Packet drop rate

Drop rate is the ratio of number of packets dropped during transmission to that of number of packets sent by the source node. Here it is expressed in percentage. Number of packets dropped is the differnce between number of packets send by source node and number of packets received at destination node.In figure 8, the drop rate is higher for wormhole infected AODV.In figure 9, drop rate increases with increase in wormhole tunnels from 1 to 5. Drop rate is maximum with value 85.531020% when all 10 wormhole peers are present in 50 node network.Table 4 shows the increase in packet drop when one wormhole link is present.

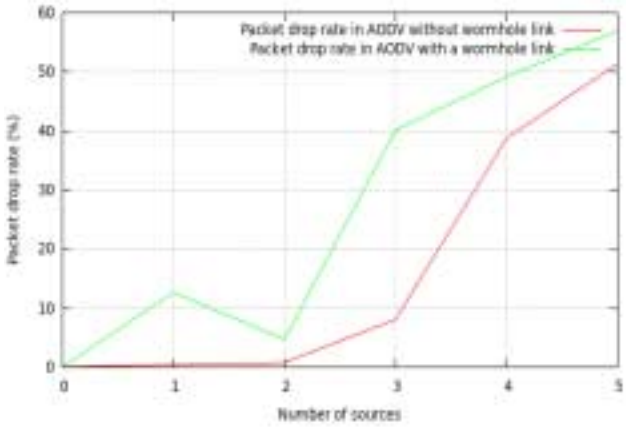

Fig 8. Packet drop rate higher for wormhole infected AODV.

Table 5. Packet drop rate in (%)

Number of connections	Packet drop rate in normal AODV	Packet drop rate in wormhole AODV	Percentage increase in packet drop rate
1	0.420610	12.618297	12%
2	0.788644	4.679285	3.9%
3	8.026639	40.133193	32%
4	38.748686	49.158780	10%
5	51.356467	56.971609	5.6%

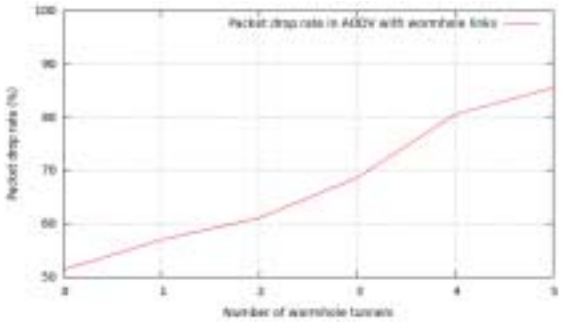

Fig 9. Increase in drop rate with increase in wormhole tunnels.

Volume: 04 Issue: 04 Pages: 1652-1656 (2013) ISSN : 0975-0290

5. CONCLUSION AND FUTURE WORK

In this paper, the study of wormhole attack launched in AODV routing protocol in MANET is conducted and the simulation study depicts the performance degradation in terms of parameters like network throughput, average end to end delay, packet delivery ratio, drop rate.

In future, a novel multi layer approach to detect wormhole attack in MANET would be proposed and the simulation results for same would be captured to show the effectiveness of the proposed detection mechanism.

REFERENCES

[1] C.Sivaram Murthy and B.S Manoj, *Ad Hoc wireless Networks* (Pearson Education, Second Edition India,2001).

[2] R.H. Khokhar, Md. A.Ngadi, S. Manda, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Science and Security, 2 (3)*, pp. 18-29, 2008.

[3] Toh, C-K, *Ad Hoc Mobile Wireless Networks: Protocols and Systems* (Prentice Hall, 2002).

[4] Jhaveri, R.H., Parmar, J.D., Patel, A.D., and Shah, B.I, "MANET Routing Protocols and Wormhole Attack against AODV", *International Journal of Computer Science and Network Security*, 10 (4).

[5] C. E. Perkins and E. M. Royer, "The ad hoc on-demand distance vector protocol", in *Ad hoc Networking, Addison-Wesley*, pp. 173–219, 2000.

[6] Reshmi Maulik and Nabendu Chaki, "A Study on Wormhole Attacks in MANET", *International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3* (2011) pp. 271-279

[7] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Heejo Lee,Sungyoung Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", *Wireless Sensor Network Track at IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, USA, Jan 11-13, 2007.

[8] Hon Su Dr A Francis Saviour HI: Wormhole Detectic Devaraj has done his B.Sc Hoc Wireless Networ and M.Sc in Computer *on Wireless Pervasi* Science from St.Xavier's

[9] Issa K College, M.E (Computer s B. Shroff, "LITEV Science & Engineering) easure for the Wormh from Anna Universitv. ss Networks", *International Conference on Dependable Systems and Networks DSN*,2005

[10] Lijun Qian, Ning Song, and Xiangfang Li, "MOBIWORP Detecting and locating wormhole attacks in Wireless Ad Hoc Networks through statistical analysis of multi-path", *IEEE Wireless Communications and Networking Conference - WCNC* ,2005.

[11] H. Vu, A. Kulkarni, K. Sarac, N. Mittal, "WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks", *In Proceedings of International Conference on Wireless Algorithms Systems and Applications*, LNCS 5258, pp. 491-502, 2008.

[12] S. Choi, D. Kim, D. Lee, J. Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", *In International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing*, pp. 343-348, 2008.

[13] Guoxing Zhan, Weisong Shi, Julia Deng, "Design and Implementation of TARF:A Trust-Aware Routing Framework for WSNs", *IEEE Transactions on dependable and secure computing*, pp 1545-5971(2012)

[14] TheNetworkSimulator http://www.isi.edu/nsnam/ns/

[15] Geetha Jayakumar, Gopinath Ganapathi, "Reference Point Group Mobility and Random Waypoint Models in Performance Evaluation of MANET Routing Protocols", *Journal of Computer Systems, Networks, and Communications*, 2008.

Authors Biography

Vandana C.P is currently perusing her M.Tech in computer networks under VTU University. She has 6 years of software industry experience in telecom domain mainly on network management systems (NMS) and storage area networks (SAN) domain. Her networks (SAN) domain. Her research interest includes security issues in MANET, network management systems and functionalities.

Dr A Francis Saviour Devaraj has done his B.Sc and M.Sc in Computer Science from St.Xavier's College, M.E (Computer Science & Engineering) from Anna University. He has obtained his PhD in Computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has also obtained certification in CCNA. He is a life member in technical societies like CSI, ISTE, CRSI, and ISOC. He has around eleven years of teaching experience in leading educational institutions in India and abroad. He has authored/co-authored research papers at the national and international levels. He has attended/conducted national and international level workshops/ seminars/conferences.