Advances in Wireless and Mobile Communications.
ISSN 0973-6972 Volume 10, Number 5 (2017), pp. 1197-1206

http://www.ripublication.com

Analysis of Wormhole and Packet Drop Attack Using AODV protocol in MANET using NS3

Ashutosh Kispotta[1], Er. Navendu Nitin[2], Er. Neelesh Agrawal[3], Prof. A.K Jaiswal[4]

SAM Higginbottom University of Agriculture and Technology Sciences, Allahabad-211008, India.

Abstract

Wireless networks are picking up fame to its top today, as the client's needs remote availability independent of their geographic location. Due to the fact that MANET (mobile ad hoc network) is infrastructure-less based network with wireless links there are some genuine problem faced by it. The way that Ad-hoc systems (MANET) need settled foundation and utilize remote connection for correspondence makes them exceptionally defenseless to an enemy's malignant attacks [7]. The following paper presents the study of simulation and the survey regarding the scenarios of packet drop and wormhole attack in Mobile Ad-hoc Network (MANET). We have used AODV for simulating this attacks using NS3 and as for any network the packet delivery ratio and throughput are main parameter so here we are analyzing the throughput and PDR of the network. The protocols are analyzed and simulated on network simulator. The simulator used is network simulator version 3.25 i.e. NS-3.25.

Index Terms: Network Simulator 3.25, Wormhole Attack, Packet drop Attack, AODV protocol, MANET

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is shaped by the group of various wireless nodes which are communicating to each other without having any basic administrator to control their activities. The wireless networks are capable of connecting nodes

wirelessly without considering their nodes in a straight line or outside the area of transmission of the wireless antenna. [5] Recently, ad hoc networks have been gaining popularity for applications requiring quick deployment. Researchers have tried to propose protocols that will improve the quality of service for ad hoc networks in the hostile wireless environments. [1] It is troublesome to constantly maintain the traffic while creating a MANET structured network. The Wormhole and Packet drop are two most severe threats which are faced by the MANET network. [2] In Packet drop attack the nodes discards all the packets that were meant to transmit from one node to another node across the network. Due to which there is a situation of packet loss in the network. In wormhole attack when two far away nodes get synchronized via wireless network they behave like neighboring nodes, then the incoming packets are received at a location 'tunneled' (wormhole tunnel) to a different location in the network. [10]

Simulation and study of such attacks has become necessary in order to defend them. The remaining paper consist of following sections: Section II contains the routing protocols used. Simulation Environment is discussed in section III. Section IV contains the Simulation Results. It also describes throughput and Packet delivery ratio analysis for different node scenarios respectively. Section V presents conclusions.

II. ROUTING PROTOCOL

The presence of wireless network forms immensely challenging conditions to form a better Ad-hoc Network. [1] There are two types of dynamic routing protocol:

1. DSDV i.e. table driven
2. AODV i.e. reactive protocol

Since the MANET is dynamic in attributes so it considers AODV as a protocol which helps to maintain the stability between the nodes in the MANET network.

Ad hoc On Demand Distance Vector Routing (AODV)

Ad-hoc On-demand Distance Vector Routing Protocol is also known as reactive table driven routing protocol which is descendent of DSDV. [2] It uses routing table for the route analysis and also uses messages like RREQ, RREP for route request and route reply respectively. It can also receive multiple RREP, Route failure and RERR. The route expires after route life time uses hello messages for local connectivity maintenance. [19]

Packet Drop Attack

Packet drop attack occurs when all the packets gets dropped and discarded instead of getting transmitted to the destination. [25] It is basically Denial of Service attack, here the node itself ingurgitate all data packets, as similar as a hole which absorbs everything. This phenomenon creates a situation of packet loss in the network. The Network layer of MANET is involved by the threats of Packet drop attack. [14]

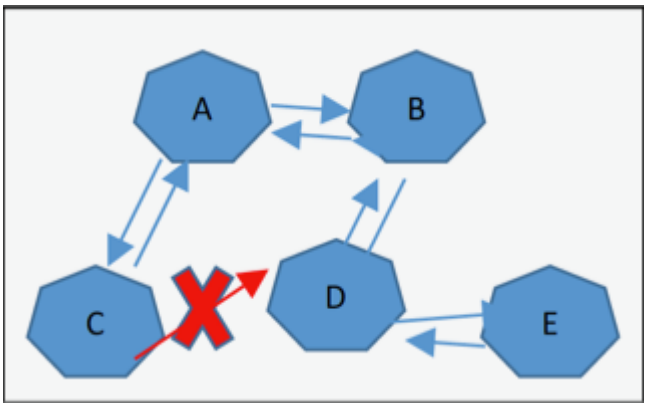

Figure (i): Packet drop Attack

From Figure (i) it is illustrated that in a MANET with nodes A, B, C, D, E. Node 'A' is a source node and node 'E' is destination. [11] Here node 'C' is a malicious node, when source node 'A' wants to transmits the packet to destination 'E' it starts a route discovery process, but as soon as this process starts the node 'C' i.e. malicious node calls that it has active route to the destination node 'E'. Immediately node 'C' accepts the RREQ packets and sends a reply to node "A" before any other node. Due to which source node 'A' consider it as active route and completes its route discovery process by ignoring all the other enquires. Hence node 'A' starts sending packets to malicious node 'C'. As a result, the data packet is assumed to be lost or discarded. [8]

Wormhole Attack

The wormhole attacks standout amongst the most serious security threat which disturbs the communication across the network. [9] Wormhole nodes fake a course that is shorter than the first one inside the network; this can befuddle routing mechanisms which depend on the learning about separation between nodes. It has one or more malicious nodes and a tunnel between them. [15] The attacking node catches the bundles from one area and transmits them to other far off found hub which conveys them locally. [24] A wormhole attack can undoubtedly be propelled by the attacker without having knowledge of the network or trading off any genuine nodes. This attack is a vulnerable attack which can be performed only if two nodes are

compromised. [20]

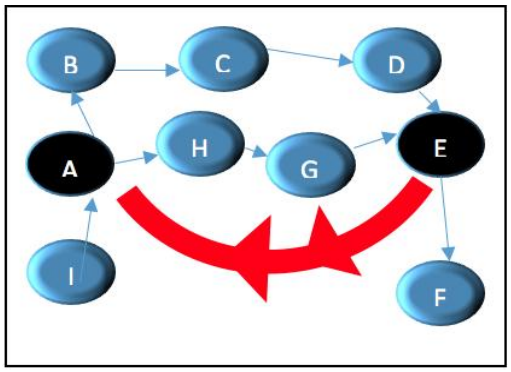

Figure (ii): Wormhole Attack

Illustrated example of the effect of a wormhole on routing protocol is provided in Figure (ii). The attacker builds a wormhole link between nodes A and E, with low-latency link. When node 'A' broadcasts its routing table as in AODV protocols, node E hears the broadcast via the wormhole and assumes it is one hop away from node 'E'. Furthermore, the neighboring nodes of 'E' adjust its own routing tables and route to reach any of the nodes 'D' and 'F'. [21]

III. SIMULATION ENVIRONMENT

In this proposed work, Network Simulator (NS-3) software version 3.25 has been used because of its open source simplicity and free accessibility.

Table 1. Simulation Parameters

Channel	Wireless
Routing protocol	AODV
NS Version	3.25
No. of Nodes	5, 10
Simulation Area Size	720 * 520
CBR Packet Size	512 bytes
Simulation Durations	34 second
Mobility Model	Constant Position
Traffic Pattern	CBR Sessions

IV. SIMULATION RESULTS

A. Throughput

Throughput is the amount of data transferred successfully on a communication network or network link over the period of time. Throughput is calculated in bytes/sec or bits/second (bps).

$$\text{Throughput} = \frac{\text{Total No of Received Packets at Destination}}{\text{Total Simulation Time}}$$

The following graphs show comparison results of Packet drop and wormhole attacks on AODV and their detection techniques

B. Packet delivery ratio

The Packet Delivery Ratio is the ratio of packets that are effectively conveyed to a destination comparing the number of packets that have been sent out by the sender.

It is a proportion of number of packets delivered against the number of packets sent. Packet delivery ratio shows the total number of data packets that is delivered to the destination successfully.

$$\text{PDR} = \frac{\text{Total No of Packets Delivered}}{\text{Total No of Packets Sent}}$$

Higher the packet delivery ratio higher protocol performance.

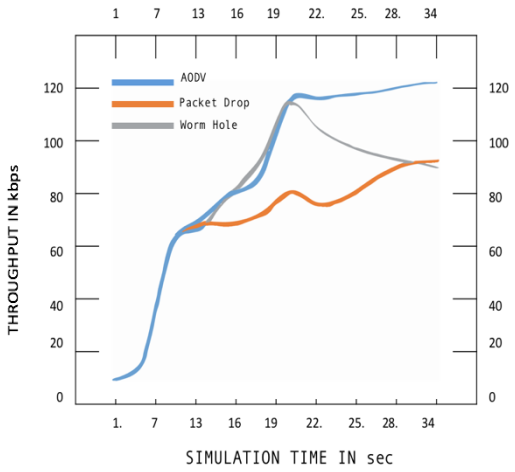

*Figure (iii)**Throughput Comparison for 5-node Scenario***

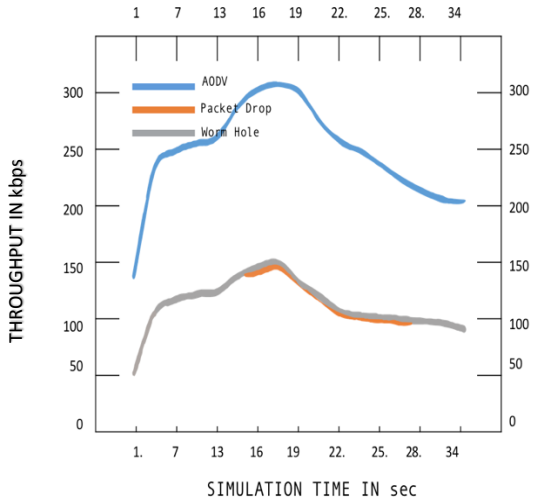

Figure (iv): ***Throughput Comparison for 10-node Scenario***

The following figure (iii) and (iv) depicts the graphs of throughput vs simulation time for AODV under attack and normal AODV protocols. From figure (iii) it is satisfied that throughput of normal AODV is greater than AODV under attacks. The AODV under worm hole attack is having less throughput than normal AODV protocol. AODV under Packet drop attack throughput is least because here the malicious node discards the packet instead sending them to the destination. Figure (iv) determines that throughput of normal AODV is greater than that of AODV under Packet drop attack and wormhole attacks. The throughput of AODV under Packet drop and wormhole attack are almost similar.

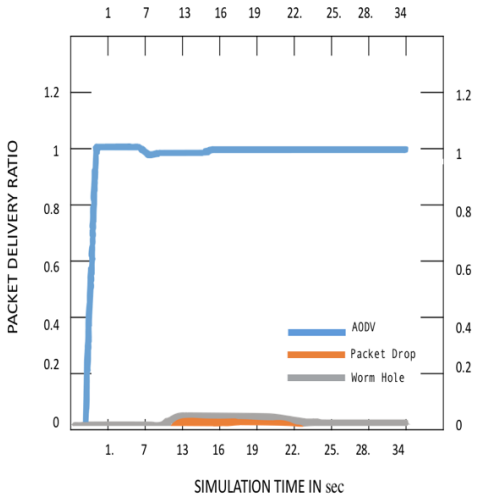

Figure (v): ***Packet delivery ratio Comparison for 5-node Scenario***

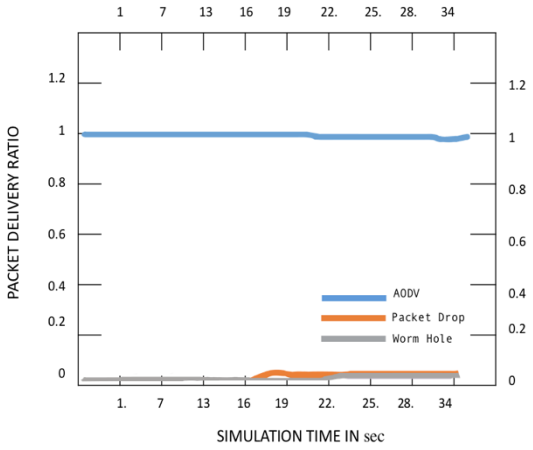

Figure (vi): ***Packet delivery ratio Comparison for 10-node Scenario***

The following figure (v) and (vi) is showing the Packet delivery ratio vs simulation time graphs. The figures (v) and (vi) determines the Packet delivery ratio vs Time graph for AODV under Packet drop, AODV under wormhole and normal AODV protocols.

From figure (v) it is satisfied that Packet delivery ratio of normal AODV is greater and optimal than that AODV under wormhole attack and AODV under Packet drop but here wormhole attacks is more vulnerable than packet drop. The figure (vi) determines that Packet delivery ratio of normal AODV is greater than that of AODV under Packet drop attack and AODV under worm hole attack. And in this scenario also the Packet delivery ratio of AODV is influenced by worm hole attack more than packet drop attack

V. CONCLUSIONS

This paper as a whole analyses Packet drop and Wormhole attack which is associated to AODV protocol. The presented work emphasizes the impact of wormhole and Packet drop attack on AODV protocol in term of security. The MANET resemble as multicast network, due to which the packet loss occurs hence hectic communication takes place over the network, resulting in the form of attacks. The proposed work is to observe the throughput and Packet delivery ratio over the network. The simulation of the two attacks is done by network simulator. This simulation shows that Worm hole attack behaves more effectively than the packet drop attack.

Thus, it comes to our vision that overall network connectivity gets affected by the behavior of these attacks over AODV and existence of these attacks can only be identified when there is some sort of data loss.

REFERENCES

[1] **Babakhouya, Y. Challal, and A. Bouabdallah (2008)** "A Simulation Analysis of Routing Misbehavior in Mobile Ad Hoc Networks", Second International Conference on Next Generation Mobile Applications, Services, and Technologies.

[2] **C. Wu, J. Chen, J. Wu and M. Cardei (2006)**, "A Survey on Attacks and Countenneasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer.

[3] **Dipali Koshti (2011)** "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", IJSCE

[4] **D.Johnson, Y. Hu, and D. Maltz (2007),** "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4" The IETF Trust.

[5] **Elizabeth M. Royer, and Chai-Keong Toh (1999)** "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications.

[6] **Fei Xing Wenye Wang (2006),** "Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks", IEEE Communications Magazine.

[7] **H. Deng, W. Li and D. P. Agrawal (2002)** "Routing Security in Wireless Ad Hoc Networks", Telecommunications Network Security, IEEE Communications Magazine.

[8] **H. L. Nguyen and U. T. Nguyen (2008)**, "A study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Networks, Science Direct

[9] **L. Hu and D. Evans (2004)**, "Using Directional Antennas to detect Wormhole Attacks", In Network and Distributed System Security Symposium (NDSS 2004), San Diego, California, USA.

[10] **L. Qian, N. Song and X. Li (2005)**, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path", IEEE Wireless Communications and Networking Conference, Vol. 4, pp 2106-2111,2005.

[11] **M. Medadian, A. Mebadi and E. Shahri (2009)** "Combat with Packet Drop Attack in AODV Routing Protocol", in the Proceedings of the 2009 IEEE 9 Malaysia International Conference on Communications, 2009.

[12] **M. Y. Su, K. L. Chiang and W. C. Liao (2010)** "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks", International Symposium on Parallel and Distributed Processing with Applications, Parallel and Distributed Processing with Applications (ISPA), IEEE Computer Society, 2010.

[13] **M. Meghdadi, S. Ozdemir and I. Guier (2011)**, "A Survey of Wonnhole-based Attacks and their Countermeasures in Wireless Sensor Networks", IETE Technical Review, V01.28

[14] **Mieso K. Denko**," Detection of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme", IEEE Communications Magazine.

[15] **P. V. Tran, L. X. Hung, Y. K. Lee, S. Lee and H. Lee (2007)**, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks" IEEE Communications Magazine.

[16] **P. Sankareswary, R. Suganthi, G. Sumathi (2010)** "Impact of selfish nodes in multicast Ad hoc on demand Distance Vector Protocol", in Wireless Communication and Sensor Computing, 2010

[17] **S. Vuppala, A. Bandyopadhyay, P. Choudhury, Tanmay De (2010),** "A Simulation Analysis of Node Selfishness in MANET using NS-3" Int. J. of Recent Trends in Engineering and Technology, Vol. 4, No. 1

[18] **Suma R, Sridevi K N, Mozil M, Mungara J.Nπ, Sethi P (2011),** "Random-Cast: An Energy-Efficient Communication Scheme for Mobile Ad Hoc Networks," European Journal of Scientific Research, 2011

[19] **Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker (2000)** "Mitigating routing misbehavior in mobile ad hoc networks", International Conference on Mobile Computing and Networking, Proceedings of the 6th annual international conference on Mobile computing and networking, 2000, Boston, Massachusetts

[20] **T. V. Phuong,N. T. Canh, Y.K. Lee, S. Lee and H. Lee (2007)**, "Transmission Time-based Mechanism to Detect Wormhole Attacks", IEEE Asia-Paci c Services Computing Conference,IEEE Computer Society,pp 172- 178,2007.

[21] **V. Mahajan, M. Natu, A. Sethi (2008).** "Analysis of wormhole intrusion attacks in MANETS". In IEEE Military Communications Conference (MILCOM) 2008

[22] **V. Gupta, S. Krishnamurthy, and M. Faloutsos (2002)** Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks in IEEE MILCOM "02, 2002

[23] **X. Su and R. V. Boppana (2007),** "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks", in Proceedings of IEEE Communications Society, ICC.

[24] **Y.c. Hu, A. Perrig and D. B. Johnson (2006)**, "Wormhole attacks in wireless networks", IEEE journal on selected areas in communications, Vol. 24, 2006.

[25] **Y. F. Alem and Z. C. Xuan (2010)**, "Detecting Packet Drop Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2nd International Conference on Future Computer and Communication, IEEE, Vol. 3, pp 672-676.