Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 6, June -2015

Performance Evaluation of Wormhole and Sybil Attacks in AODV

Samuel Jacob, Dr. P. N. Nemade***
**Lecturer, Electronics Department, AtharvaCollege of Engineering, Malad (W),Mumbai, India*
*** Director, AtharvaCollege of Engineering, Malad (W),Mumbai, India*

ABSTRACT: *The Mobile Ad hoc Networks (MANETs) is a collection of wireless nodes which interact with each other by sending packets to one another or on behalf of another node, with the absence of any central network infrastructure to control data routing. The nodes cooperatively forward data packets to other nodes in network by using the routing protocol. These routing protocols are, however,insecure, thus, the MANET becomes open to malicious attacks. Some malicious attacks commonly observed in MANET environment are wormhole and Sybil attacks. The objective of this work is to analyze the performance parameters of throughput, delay and packet loss in AODV with the existence of such attacks. It has been observed from simulation results that the performance parameters are affected very much when there is an attack due to wormholes and Sybil.*

Keywords- *Wormhole, MANET, AODV etc*

I. INTRODUCTION

Advancement of mobile device technology has led to a huge use of wireless networks. Thus, always-on communicating capability and information access are granted to mobile users. A collection of mobile nodes enabling users to communicate without any physical infrastructure regardless of their location geographically is known as Mobile Ad-hoc Networks (MANET). A MANET has a dynamic network topology due to the fact that the nodes are mobile in nature. It has the potential of being affected by attacks due to the non-static nature of nodes, threats due to compromised nodes andthe absence of centralized management.

MANETs can be broadly classified as table-driven/proactive or on-demand/reactive. Table driven protocols exchange routing information periodically, thus they are called proactive protocols. Thus, routes are created prior to their being required, resulting in an increase in overhead. Reactive protocols create routes only when connection is required to be established. An example of reactive protocol for MANETs is AdhocOn Demand Distance Vector (AODV).

In this paper we analyze the throughput, delay and packet loss parameters of AODV protocol in a MANET in the presence of wormhole attack. The impact of wormhole and Sybil attacks on AODV protocol in a MANET is obtained from simulation results.

II. MANETs SECURITY ISSUES

MANETsare quite more susceptible than the wired networks to attacks due to the following major issues:

ii.i De-centralized management

MANET does not have any centralized management control. Since management control is unavailable in MANET, attacks detection is difficult because it is not easy to monitor the traffic in a highly dynamic and large ad-hoc network. Trust management for nodes is broken due to lack of centralized management.

ii.ii Unavailability of Resources

Resource availability is another issue in MANETs. The achievement of secure communication in such a dynamic environment as well as protection against specific threats and attacks has kindled development of a number of security schemes and architectures.

ii.iii Ever-changing topology

In MANETs, nodes can join and leave the network dynamically and can move independently. This nature of nodes leads to an ever-changing topology in MANETs. Moreover, nodes do not remain static. The trust relationship existing among nodes could be disturbed by the above factors.

The trust may also be impeded if some nodes are found to be compromised. This dynamic behaviour can be better protected with distributed and adaptive security mechanisms.

ii.iv Lack of scalability

Due to mobility of nodes, the ad-hoc network scale can change and may not remain constant always. Thus, scalability becomes a major concern concerning security. The employed mechanism of security must be capable of handling large as well as small networks equally well.

ii.v Limited Power Supply

The nodes in mobile ad-hoc network do not have access to unlimited power supply. Also, a node may behave in a selfish manner when it observes that power supply is restricted.

ii.vi Lack of Cooperation

MANET Routing algorithms usually assume that all the nodes are cooperative and contribute actively for secure communication. But, in practice, some nodes become malicious nodes. As a result, they easily become important routing agents and disrupt secure network operation by refusing to comply with all the routing protocol specifications.

III. WORKING PRINCIPLE

iii.i Adhoc On Demand Distance Vector (AODV) Routing Protocol

Adhoc On Demand Distance Vector (AODV) protocol, designed for a mobile ad hoc network, is a very efficient, simple and effective reactive routing protocol. In AODV, paths are found only when required. AODV discovers and maintains a route between source and destination nodes only when the two need to communicate or when the former node is offering its services as an intermediate forwarding station to maintain connectivity between two other nodes. AODV employs the following control message types:

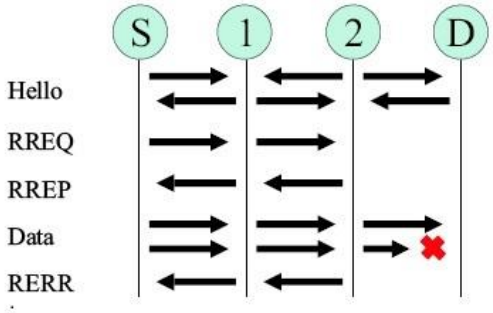

Fig. 1. AODV Message types

When a data packet is to be sent by a source node S to a destination node D and node S does not have a route to node D, the route discovery process begins by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors on receiving this RREQ rebroadcast the same RREQ to their neighbors. Forwarding of this RREQ is carried out until the destination node or until an intermediate node with a "fresh enough" route to the destination is located. As soon as the first arrived RREQ is received, the destination node or a node with a route to the destination sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. If the destination node obtains the same RREQ later, it will be ignored. AODV also permits intermediate nodes having sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node.In case if a node realizes that the route is damaged or broken it transmits a route error (RERR) message to the source and destination nodes separately.

AODV assumes that all the nodes in the network are trusted nodes. However, this is not true all the time. Some node may pose as a malicious node and may break trust by indulging in various types of attacks, thus adversely affecting AODV performance characteristics. Some types of attacks could be used to compromise AODV but in this paper the focus is only on Wormhole and Sybil attack.

iii.ii Wormhole Attack

The attacks can be categorized based upon the source of the attacks as Internal or External, and as Passive or Active attack depending on the behavior of the attack. A pair of nodes that are connected together in some way is employed by an attacker for a wormhole attack. A request packet may be tunneled directly by an attacker to the destination node without increasing the hop-count value. Two colluding nodes that are not close to each other are linked by a high speed tunnel thus giving an illusion of being neighbors. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node through the newly created tunnel which will then replay it into the network. These nodes advertise that they have the shortest path through them and that the RREQ packet through them reaches the destination faster compared to usual path by using this tunnel. AODV routing protocol is susceptible to be affected by wormhole attack.Wormhole could be classified as in-band or out-band, and self-sufficient or extended wormhole.

iii.ii Sybil Attack

A Sybil attack is underway when a malicious node behaves like two or more nodes instead of just a node. An unfamiliar or malicious entity creates more than one identity. Thus, false identities, imitations or impersonation of MANET nodes create Sybil nodes. These additional node identities could be represented by one physical device. The attacker behaves as several different identities or nodes rather than one.

IV. EXPERIMENTAL SETUP

We have taken 60 nodes and the traffic model taken is CBR (constant Bit Rate). The simulation parameters used in this paper are listed in table given below:

Parameter	Value
Simulator	Ns-2(ver.2.35)
Number of Nodes	60
Simulation time	30 seconds
Traffic Type	Constant Bit Rate
Packet Size	512
Routing Protocol	AODV

TABLE 1. SIMULATION PARAMETERS

V. RESULTS

v.i Packet Delivery Ratio

It is the ratio of number of packets at destination node to the number of packets sent by source node. The network PDR of AODV with 60 nodes is illustrated below. In the figures, the x-axis denotes time in seconds and the y-axis PDR. Packet delivery ratio is lower in case of Wormhole and Sybil attacks as shown below:

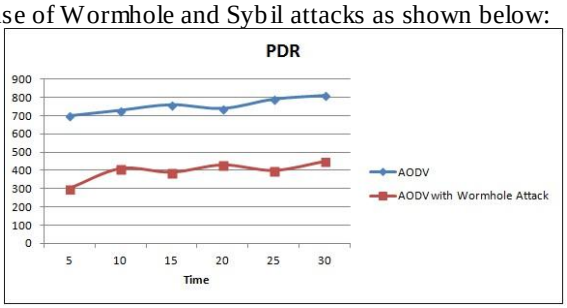

Fig. 2. PDR Vs. timewith Wormhole attack

PDR in case of Sybil attack is shown below:

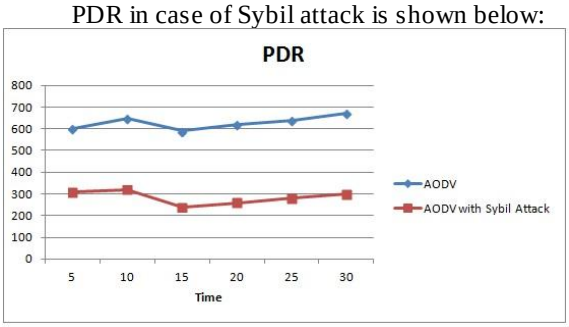

Fig. 3. PDR Vs. time with Sybil attack

v.ii Throughput

The network throughput gives the fraction of the channel capacity used for useful transmission of data. It is measured in bits per second. The network throughput of AODV with 60 nodes is illustrated below. In the figures below, the x-axis denotes time in seconds and the y-axis throughput. Throughput is lower in case of wormhole and Sybil attacks as shown below:

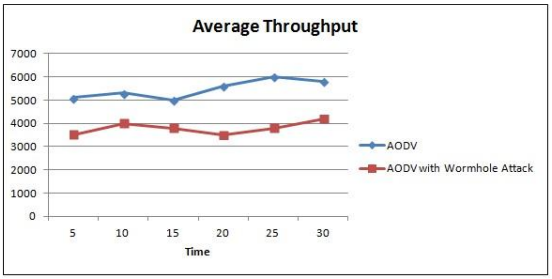

Fig. 4. Throughput Vs. time with Wormhole attack

Throughput in case of Sybil attack is shown below:

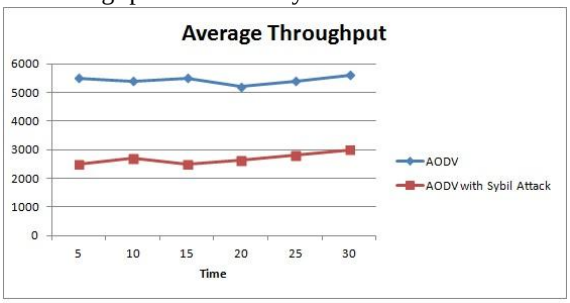

Fig. 5. Throughput Vs. time with Sybil attack

v.iii End to End Delay

This parameter indicates the average time taken for a data packet to reach destination. It is measured in seconds. The network delay of AODV with 60 nodes is illustrated below. In the figures below, the x-axis denotes time in seconds and the y-axis end-to-end-delay. The End-to-End-delay is higher in case of wormhole and Sybil attacks as shown below:

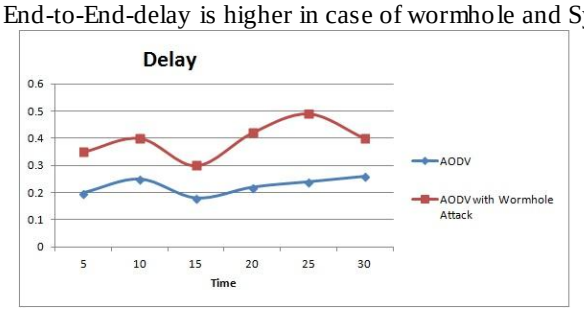

Fig. 6. Delay Vs. time with Wormhole attack

Delay in case of Sybil attack is shown below:

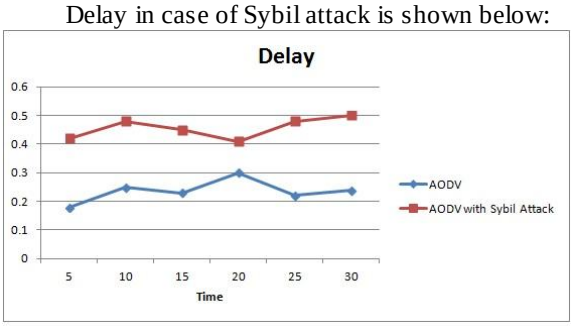

Fig. 7. Delay Vs. time with Sybil attack

VI. CONCLUSION

The performance of an on- demand routing protocol i.e. AODV (Ad hoc on demand distance vector routing) is evaluated with and without wormhole and Sybil attacks. Three parameters of performance i.e packet delivery ratio, throughput, and average end to end delay have been considered. Results show that AODV performance gets badly affected by the wormhole and Sybil attacks.

REFERENCES

[1] Priyanka Goyal, SahilBatra, Ajit Singh, A Literature Review of Security Attack in Mobile Ad-hoc Networks, *International Journal of Computer Applications,9(12)*, 2010, 0975–8887.

[2] Akshai Aggarwal, NirbhayChaubey,KeyurbhaiJani, A simulation study of malicious activities under various scenarios in Mobile Ad hoc Networks (MANETs), *International Conference on Automation, Computing, Communication, Control and Compressed Sensing*, 2013, 827-834.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A.Jamalipour, A survey of routing attacks in mobile ad hoc networks, *Security in wireless mobile ad hoc and sensor networks*,2007, 85-91.

[4] C. Perkins, M Royer, Ad-hoc On-Demand Distance Vector Routing, *International Conferenceon Mobile Computing Systemsand Applications*, February 1999

[5] R. Ahuja, A.B. Ahuja, P. Ahuja, Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack, *IEEE Second International Conference on Image Information Processing (ICIIP)*, 2013, 699-702.

[6] Kevin Fall and Kannan Varadhan (Eds.), The ns Manual,2006, *http://www mash.cs.berkeley.edu/ns/*

[7] M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, *International Journal of Modelling and Simulation*, 1998, 827-83

[8] Shah, R.H.J.A.D.P.J.D.P.B.I., MANET Routing Protocols and Wormhole Attack against AODV, *International Journal of Computer Science and Network Security, 10(4)*, 2010.

[9] Maulik, R.C., N., A comprehensive review on wormhole attacks in MANET, *International Conference on Computer Information Systems and Industrial Management Applications (CISIM)*,2010.

[10] Nirmal Patel and Pratik Modi, Detecting Sybil Attack using AODV in MANET, *International Journal of Advance Engineering and Research Development (IJAERD)*, May 2014.

[11] ZolidahKasiran and Juliza Mohamad, Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV, *International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, 2014, 81-84.

[12] ManjunathaT.N.,SushmaM.D.,Shivakumar K. M, Security Concepts and Sybil Attack Detection in Wireless Sensor Networks, *International Journal of Emerging Trends andTechnology in Computer Science (IJETTCS)*, 2013, 383-390.

[13] KanniSelvam R., Karthikeyan C. M. E., Identifying theSybilnode byusing LightweightschemeinMobileAdhoc Network Detection in Wireless Sensor Networks, *International Journal of AdvancedResearch in Electronics and CommunicationEngineering (IJARECE)*, 2014, 602-607.

[14] Yu-sen, G.J.-j., Z.T.Z., Modeling and Analyzing the Sybil Attack to Ad-hoc RoutingProtocols, *International Conferenceon Multimedia Technology(ICMT)*, 2010.

[15] HimadriNathSaha, D.B.P.K.B.,Semi- Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack,*InternationalJournal of Computer Science & EmergingTechnologies*, 2010.

[16] Navneet, Rakesh G, Sybil Attack Detection and Prevention using AODV in VANET, *International Journal of Computer Science & Management Studies (IJCSMS*,September 2013, 333-339.

