ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 4, Issue 4, April 2017

# Enhance Performance of AODV Protocol During Blackhole Attack in MANET

[1] Chetan C. Dhulkotiya, [2] Sandip Toshniwal
[1] [2] Department of Electronics and Communication
[1] [2] Kautliya Institute of Technology and Engineering

***Abstract*— Mobile Ad Hoc Networks are an appealing branch of wireless networking due to benefits of having communication without need of infrastructure, ease of deployment, etc. AODV (Ad Hoc on demand Distance vector Routing) is one of the protocols used for facilitating communication in MANET. The nodes in the network work on mutual trust basis. Due to this nature of MANET, it is vulnerable to network layer attacks such as blackhole attack, wormhole attack, grayhole attack etc. These attacks are launched by malicious nodes. Significant decrease in performance is observed when multiple malicious nodes launch attack in the network. The aim of this paper is to study the effects of collaborative blackhole attack launched by multiple malicious nodes in the network taking the performance of AODV protocol into account***

***Index Terms*— MANET, Selfish nodes, AODV, Blackhole Attack, Collaborative Blackhole Attack.**

## I.INTRODUCTION

Ad hoc networks are formed by autonomous systems communicating to each other mostly through wireless links.

Each device in the network is known as a node. The nodes are peers; every device in the network has similar privileges. The devices in an Ad Hoc Network function as a client and server interchangeably during the course of communication period. In latin, 'ad hoc' means 'for a specific purpose'. The concept of Ad Hoc Networks has been further extended to incorporate the nodes when they are moving. This concept is known as Mobile Ad Hoc Network [1] [2] also known by the acronym MANET [1] [6]. Mobile Ad Hoc networks are formed by devices communicating without the need of wired connection as well as infrasturcture. MANETs do not rely on any base stations or access points for its functioning.

Nodes co-operate to forward data to each other in the network [1] [2] assuming the nodes to be trustworthy. This property of nodes in MANETs is exploited to launch a blackhole attack. Blackhole attack is a network layer denial of service attack [3] [4] in which an adversary node drops all the data packets generated by other nodes in the network by attracting the traffic towards itself. A variant of this attack is the collaborative blackhole attack [5] in which multiple nodes launch a blackhole attack together. These nodes may launch the blackhole attack simultaneously or at different times. These types of nodes are called blackhole nodes or malicious nodes. Simulation results in further chapters show that a single blackhole attack degrades the performance of the network greatly therefore a launch of collaborative blackhole attack would render the network useless for relay of sensitive information. It is therefore necessary to impede this attack. The aim of this paper is to study the performance of AODV protocol during blackhole and collaborative blackhole attack. The rest of the paper is organized as follows: Section II elaborates the protocols for MANET concentrating on the AODV protocol, then, the blackhole and collaborative blackhole attack are explained. Section III gives the simulation results for implementation of AODV protocol, and its performance during blackhole and collaborative blackhole attack using metrics throughput, packet delivery ratio and end to end delay. Then the conclusion and references follow.

## II. AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

The protocols in MANET can be broadly categorized as proactive (table driven) and reactive (On demand) [1] . The nodes communicating using the proactive protocols periodically exchange the routing information through the network. Examples of proactive protocols are Destination Sequenced Distance Vector (DSDV) and Wireless Routing Protocol (WRP). On the other hand, the nodes using reactive protocols exchange routing information when required to forward data or to find routes to the destination. Protocols like AODV, DSR, etc use the reactive approach. The advantages of proactive and reactive protocols are combined in the hybrid routing protocol called Zone Routing Protocol (ZRP). The following subsection explains the AODV protocol.

A. AODV protocol:

The Ad hoc On Demand Vector [1] [2] protocol finds routes on demand by using control packets RREQ (Route Request), RREP (Route Reply) and RERR (Route Error). When any node wants to find a destination node, it would first send an RREQ control packet. Now, when any intermediate node receives the RREQ it checks whether the RREQ has been repeated, if yes then the RREQ is discarded, otherwise, it is processed and rebroadcasted. A route generates an RREP if it itself is a destination node or it has a route existing towards the destination node. When the RREP is generated, the node copies the Destination IP address and the originating sequence number from the RREQ message into the corresponding field of the RREP message. The intermediate node and the destination node process the RREQ differently and make the RREP. The RERR packet is sent when the link break causes one or more of the destinations to become unreachable from some of the node's neighbors. Thus the network information is maintained in this way by AODV protocol.

## III. BLACKHOLE ATTACK IN MANET

MANETs are also exposed to security attacks because of an inherent setback of mutual trust between the nodes. The nodes so not foresee the latent presence of an attacker and therefore any node; either from among the nodes of the network or a node joining the network remotely can launch attacks on the network. The nodes which launch any attack are termed as selfish or misbehaving node. This corrupts the performance of the network. The messages cannot be relayed and sensitive information can be modified or lost. One of the attacks in a MANET is the blackhole attack under the influence of which a node in the network attracts all the data packets towards itself by advertising a fresh enough route to the destination to the other nodes in the network. Once the packets are forwarded to the node, it drops all the packets which it receives. The variant of this blackhole attack is the collaborative blackhole attack which is explained in the next subsection:

### *A.Methods of launching blackhole attack:*

The blackhole attack [7] can be launched by fabrication of the control messages i.e. RREQ and RREP messages RREQ falsification is the process in which the RREQ is modified where the malicious node increases the destination sequence number of the RREQ received from the source but doesn't increment the hop count. When the destination or the intermediate node receives the RREQ with smaller hop count but higher sequence number, it chooses the route via the malicious node and then, the malicious node launches the blackhole attack. The blackhole attack by RREP falsification is much simpler. The malicious node replies to the RREQ message immediately when it receives the RREQ. The source node thinks it as the fresh enough route and replies to it immediately and disregards the legitimate RREP received from the genuine node.

### *B.Collaborative blackhole attack [5]:*

Collaborative blackhole attack [5] is the phenomena in which a number of selfish nodes launch a blackhole attack together. The nodes may or may not collude to commence an attack. In case of collusion of nodes, the blackhole attack can be called co-operative blackhole attack [10]. The concept of collaborative blackhole attack is explained in the next figure.

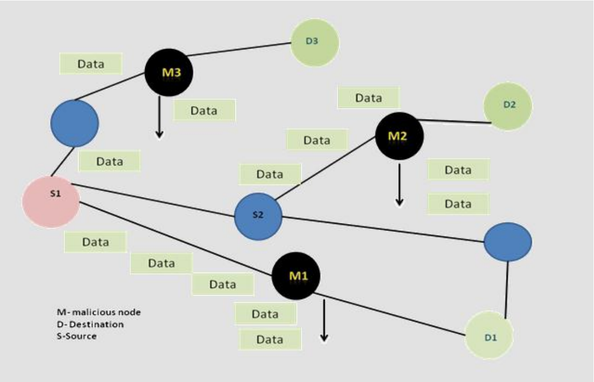

*Figure 2. Collaborative Blackhole Attack*

## IV. PROPOSED WORK

Trusted Routing Operations in TAODV: Routing Table Extensions: We add three new fields into each node's original routing table: positive events, negative events and opinion. Positive events are the successful communication times between two nodes. Similarly negative events are the failed communication ones. Opinion means this node's belief towards another node's trustworthiness as defined before. Routing Message Extensions: We extend the original AODV routing messages by appending some trust information fields. Two main types of extended messages are TRREQ (Trusted Routing REQuest) and TRREP (Trusted Routing REPly). In trusted routing discovery procedures, every routing request and reply carries trust information, including opinions towards originator node S and destination node D, which will be employed to calculate the credibility of S and D. When a node is required to provide its certificate information, it will fill the fields of trust information with its own signature, as proposed by some traditional security solutions for MANETs.

Trust Updating Policies: Initially we assign trust value 10 to each nodes. Opinions among nodes change dynamically with the increase of successful or failed communication times. When and how to update trust opinions among nodes will follow some policies, which are derived as follows:

a. Each time a positive event occurs from node A to node B, B’s number of successful events in A’s routing table will be increased trust by 1.

b. Each time a negative event occurs from node A to node B, B’s number of failed events in A’s routing table will be increased by 1.

c. Each time when the field of the successful or failed events changes, the corresponding value of opinion will be recalculated using the evidence space to the opinion space.

d. Each time when the new opinion has been obtained through combination, the corresponding number of successful or failed events will be mapped back using the opinion space to the evidence space. e. The positive events include successful data or routing packets forwarding, keeping message integrity, and passing cryptographic verification, and so on

### V. PERFORMANCE OF AODV ROUTING PROTOCOL DURING COLLABORATIVE BLACKHOLE ATTACK

The purview of this paper is to monitor the performance of AODV protocol during blackhole attack in presence of single and multiple malicious nodes. The performance metrics are given as follows:

- Throughput: The difference between the sent and received packets in a given unit of time is called throughput. Here the throughput is measured in kilobits per second (kbps).
- Packet delivery ratio or (pdr): The number of data packets delivered to the destination.
- End to end delay: Average time taken by data packet to arrive to the destination.

| Packet Delivery Ratio (%) | | |
|---|---|---|
| Nodes | AODV under attack | AODV |
| 50 | 48 | 99.51 |
| 100 | 67.64 | 91.77 |
| 150 | 47.74 | 95.23 |
| 250 | 80.94 | 99.32 |
| 350 | 47.24 | 99.22 |
| 450 | 57.5 | 99.9 |

The performance of AODV protocol without the presence of malicious nodes, in presence of a single malicious node and in presence of multiple malicious nodes is given as follows:

*Table 1. parameters*

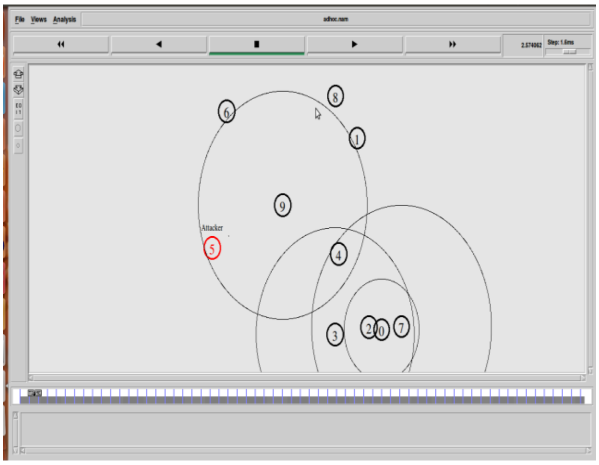

*Figure 3. Implementation of single blackhole node*

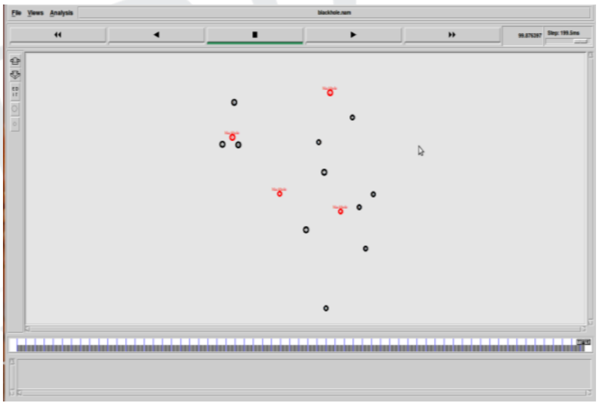

*Figure 4. Implementation of multiple malicious nodes*

| Throughput (kbps) | | |
|---|---|---|
| Nodes | AODV | AODV under Attack |
| 50 | 44.48 | 21.55 |
| 100 | 40.93 | 30.26 |
| 150 | 43.62 | 21.23 |
| 250 | 44.8 | 36.44 |
| 350 | 44.53 | 20.99 |
| 450 | 44.48 | 25.5 |

*Table 2. Simulation results for throughput in presence of single malicious node*

| Parameters | Values |
|---|---|
| Terrain Area | 500 X 500 |
| Protocol | AODV |
| Traffic | cbr (UDP) |
| Antenna | Omni directional |
| Packet size | 512 bytes |
| Performance Parameters | Throughput, packet delivery ratio and end to end delay |
| No. of nodes | 50, 100, 150, 250, 350,450 |
| No. of malicious nodes | 3, 4, 5, 10, 15 |
| Simulation time | 100 sec |

*Table 3. Simulation results for packet delivery ratio in presence of single malicious node*

| End to End delay | | |
|---|---|---|
| **Nodes** | **AODV under attack** | **AODV** |
| 50 | 25.6 | 41.24 |
| 100 | 23.19 | 583.738 |
| 150 | 153.415 | 303.51 |
| 250 | 10.61 | 14.198 |
| 350 | 28.96 | 17.42 |
| 450 | 10.27 | 26.37 |

*Table 4. Simulation results for end to end delay in presence of single malicious node*

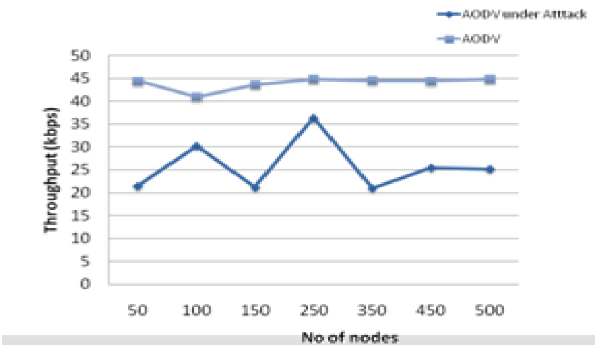

*Figure 5. Graph for throughput of network with varying number of nodes in presence of a single malicious node*

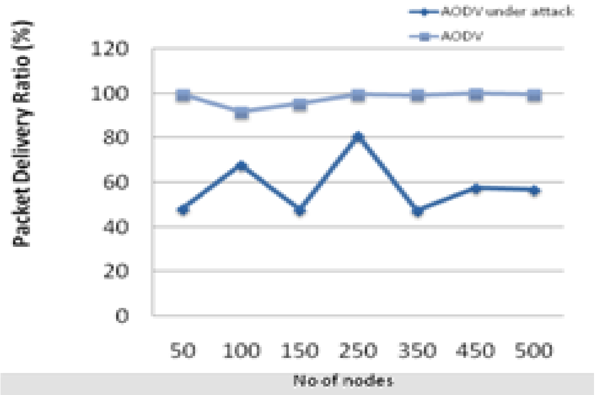

*Figure 6. Graph for pdr of network with varying number of nodes in presence of a single malicious node*

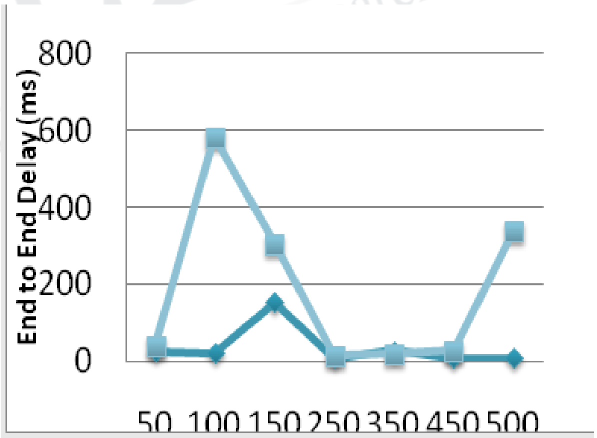

*Figure 7. Graph for end to end delay of network with varying number of nodes in presence of a single malicious node*

The simulation results shown above explain that a single malicious node can bring a significant drop in the performance of the network. But when multiple malicious nodes launch an attack on the network, its functioning is rendered almost useless. To study this, simulation was carried out using multiple malicious nodes in a network, the number of nodes ranged from 3 to 15. To compare it with the normal working of AODV, a reading for AODV without presence of malicious nodes is included.

| No. of malicious nodes | Throughput (kbps) | Packet delivery ratio (%) | End to end delay (ms) |
|---|---|---|---|
| 0 | 99.82 | 99.00 | 10.08 |
| 3 | 17.35 | 31.31 | 6.12 |
| 4 | 17.35 | 31.13 | 6.12 |
| 5 | 17.11 | 30.77 | 6.09 |
| 10 | 17.47 | 31.45 | 5.99 |

*Table 5. Simulation results for collaborative blackhole attack*

Simulation results show that the performance of the network is degraded due to collaborative blackhole attack launched by several malicious nodes.

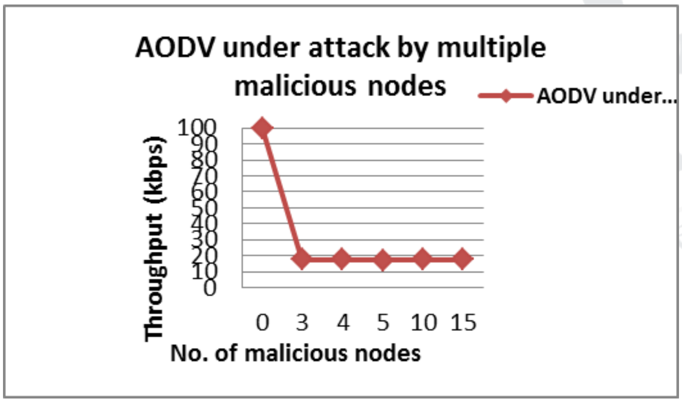

*Figure 8. Graph of throughput during collaborative blackhole attack*

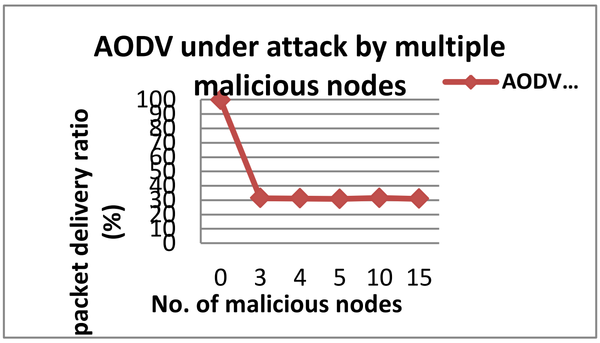

*Figure 9. Graph of packet delivery ratio during collaborative blackhole attack*

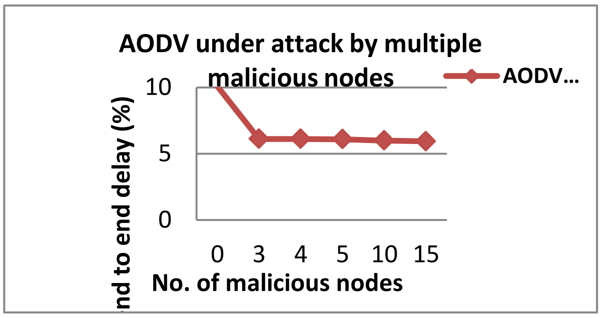

*Figure 10. Graph of end to end delay during collaborative blackhole attack*

## VI. CONCLUSION

Mobile Ad hoc Networks are formed by autonomous nodes communicating with the help of wireless links. The nodes in the network work on mutual trust basis. This property of the network is abused by a malevolent node to launch blackhole attack. Blackhole attack can be launched by fabrication of RREQ and RREP control messages. A variant of blackhole attack is the collaborative blackhole attack which is an attack launched by multiple malicious nodes. The study of single and collaborative blackhole attack has been carried out and the review has been presented in the paper. Simulation results show major degradation in the performance of the network in terms of parameters like throughput, packet delivery ratio. The end to end delay is found to decrease. The reason is that no processing is done on the data packets, so the end to end delay is decreased. The future course of study includes the identification and removal of the collaborative blackhole nodes.

## VII. REFERENCES

1. Perkins, C.; Belding-Royer, E.; Das, S. (July 2003). Ad hoc On-Demand Distance Vector (AODV) Routing. IETF. RFC 3561. Retrieved 2010-06-18.

2. Ivan Stojmenovic, Handbook of Wireless Networks and Mobile Computing; 5th Edition; Wiley India Edition, New Delhi, 2001, pp 536.

3. Heisri Weerasinghe and Huirong Fu, “Preventing Co-operative Blackhole Attacks in Mobile Ad Hoc Networks: Simulation, Implementation and Evaluation”, International Journal of Software Engineering and its Appplications, vol. 2, No. 3, July 2008, pp.39-54.

4. Moumita Deb, “A Co-operative Blackhole Node Detection Mechanism for ADHOC Networks ”, WCECS 2008, Sanfransisco, USA, 2008.

5. Fan-Hsun Tseng, Li-Der Chou and Han-Cheih Chao, “A Survey of Blackhole Attacks in Wireless Mobile Ad Hoc Networks ”, Human- centric Computing and Information Sciences, a Springer Open Journal, 2011, pp. 1-16.

6. Mohit Kumar, Rashmi Mishra, “An Overview of MANET: History, Challenges and Applications”, Indian Journal of Computer Science and engineering, (IJCSE), Vol. 3 No. 1 Feb-Mar 2012, pp. 121-125.

7. Hoang Lan Nguyen; Uyen Trang Nguyen, "A study of different types of attacks in mobile ad hoc networks," Electrical & Computer Engineering (CCECE), 2012 pp.1-6.

8. Ehsan, H.; Khan, F.A., "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs," Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE vol., no., pp.1181,1187, 25-27.

9. C.K. Nagpal, Chirag Kumar, Bharat Bhushan, Shailender Gupta, “A Study of Blackhole Attack on MANET Performance ”, I.J. Mordern Education And Computer Science, 2012, vol. 8, pp 47-53.

10. Latha Tamilselvan, Dr. V Shankaranarayanan, “Prevention of Co-operative Blackhole Attack in MANET”, Journal of Networks, vol. 3, No. 5, May 2008, pp. 13 – 20.