ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Enhancing QoS of AODV Routing Protocol by Preventing Black-hole Attack over Mobile Ad-hoc Network

Dipali Sheth[1], Sunera Kargathara[2], Sunil Lavadiya[3]

Student of M.E, Department of E.C., MEFGI, Rajkot, Gujarat, India[1]

Assistant Professor, Department of E.C., MEFGI, Rajkot, Gujarat, India [2]

Assistant Professor, Department of E.C., MEFGI, Rajkot, Gujarat, India[3]

ABSTRACT: Dynamic nature of Mobile Ad-hoc networks (MANET) challenges the quality of service (QoS) because route failure probability is increased in MANET due to the mobility of nodes. Lack of fixed infrastructure, wireless shared medium and dynamic topology makes MANET prone to different types of attacks. Ad-hoc On-Demand Distance Vector (AODV) routing protocol in MANETs which is vulnerable to a variety of security threats in ad-hoc networks. Blackhole attack is an attack that drop considerable number of packets by performing packet forwarding misbehaviour and violate the security to cause Denial of Service in Mobile Ad-hoc Networks (MANETs). In our solution, additional cache table is introduced. When a node detects unusual routing information while receiving route reply from misbehaving neighbour node, it detect and isolate that multiple malicious node during route reply process and propose an improved AODV for better performance of wireless network. We examine the proposed AODV algorithm and evaluate its performance using NS-2.35 under various network parameters.

KEYWORDS: MANETs; AODV; Blackhole Attack.

I. INTRODUCTION

An ad-hoc network [1] is a group of wireless mobile nodes forming a network without the help of any stand-alone infrastructure. As Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks, the structure changes dynamically. This is mainly due to the mobile nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in such a manner to engaging themselves in multi-hop fashion. The node in the network acts as both hosts as well as routers.

Each device in a MANET [2] is free to move independently in any direction, and will therefore change its paths to other devices frequently. Each must forward traffic unrelated to its use, and thus the router. Routing has been a challenging task for the ad-hoc network as there is the constant change in network topology because of high degree of mobile nodes. To accomplish this task number of protocols has been introduced.

AODV [11] is reactive routing protocol in MANET, which creates route from source to destination. In AODV source broadcast RREQ packet to its neighbours to find route to its destination. After receiving RREP from the neighbours' source, select optimum route to its destination and sends data packets through it.

MANETs are liable to different active and passive attacks on the network layer. DoS attacks are the attacks that badly disrupt fundamental functionalities of an ad-hoc network. Wormhole attack, Sinkhole attack, Blackhole attack are major DoS attacks in MANETs. Here we concentrate on Blackhole attack that degrades performance of network by packet forwarding misbehaviour during data transmission phase.

In Blackhole attack, the malicious node generates and propagates fictitious routing information and advertises itself as having a valid shortest route to the destination node. If the malicious node replies to the requesting node before the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

genuine node, a stale route will be created. As a result, packets do not reach to the specific destination node; instead, the malicious node intercepts the packets and drops them. Thus, the network traffic is absorbed. In this paper, a mechanism to detect and remove this attack is proposed using AODV.

Here we are improving QoS of AODV, which greatly increases reliability of detection and isolation of multiple malicious nodes during route discovery process and discovers a short and secure route towards destination. To eliminate existing problem of blackhole attack, we put an effort to improve in AODV protocol by analyze the algorithm theoretically and evaluate it practically using NS-2.35.

The remaining of this paper is organized as follows. Section 2 explains AODV routing protocol, and also Blackhole attack on AODV routing protocol. Section 3 describes the work had done previously. Our proposed scheme is introduced in Section 5. The simulation results using NS-2.35 are analysed in Section 6. The last section is the conclusions.

II. THEORETICAL BACKGROUND

2.1 Ad-hoc On-Demand Distance Vector (AODV) Routing

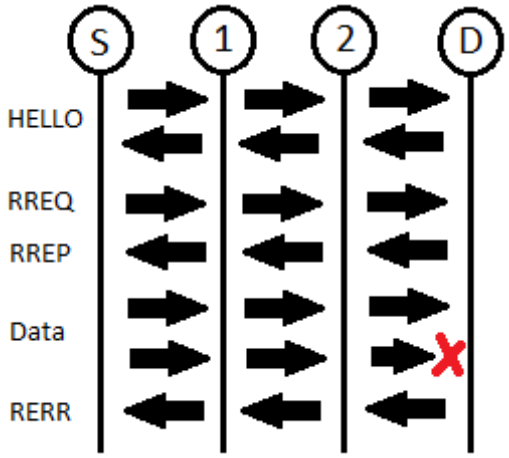

Fig. 1 AODV Protocol Messaging

The AODV routing protocol is a reactive routing protocol; therefore, routes are discovered only when needed. Figure 1 shows the message exchange takes place in AODV protocol. Hello messages are used to detect and observe links to neighbours. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbours accept. As nodes periodically send Hello messages, if a node fails to receive some Hello messages from a neighbour, a link break is found.

When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received, a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is uni-cast in a hop-by-hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. As data flows from the source to the destination, each node along the route updates the timers associated with the routes to the source and destination, maintaining the routes in the routing table. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently, the node removes the route from its routing table. If data is flowing and a link break is detected, a Route Error (RERR) is sent to the source of the data in a hop-by-hop fashion. As the RERR propagates towards the source, each intermediate node in validates routes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

to any unreachable destinations. When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery if necessary.

2.2 Blackhole Attack

In a Blackhole attack, a malicious node sends fake routing information, claiming that it has an optimal route and causes other good quality nodes to route data packets through the malicious one. Source node considered it as a fresher path and then false route will be created. The effect generated is Blackhole absorbs traffic and start to drop the data packet forwarded through it to destination.

In case of AODV, the attacker can send a fake RREP (including a fake destination sequence number that is to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a suitably fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

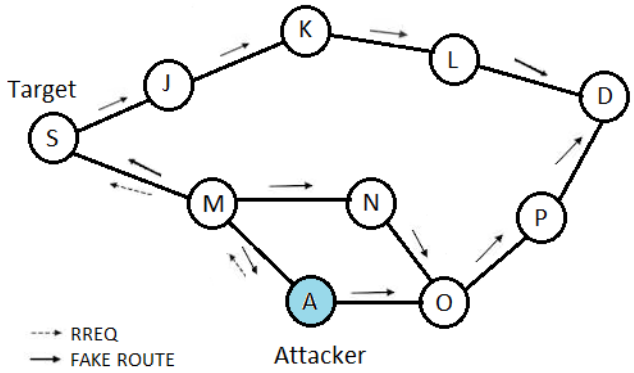

Fig. 2 Example of a blackhole attack

Figure 2 shows an example of a blackhole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a suitable route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A.

III. RELATED WORK

Marti et.al [3] proposed a mechanism with Watchdog/Pathrater to detect malicious node. Promiscuous mode is used to listen to the next hop nodes transmission where a node confirms next hop node has indeed forwarded the packet. If the node finds next hop node not forwarding packet within specific time, it is accused as a malicious node. Using results of Watchdog, Pathrater algorithm rates paths and highest rating path is chosen. The drawbacks of this mechanism are that the watchdog algorithm may accuse good nodes as malicious nodes and it does not consider partial dropping and ambiguous collisions; also, exchanging ratings in Pathrater algorithm lead to blackmail attack.

DPRAODV protocol suggested by Payal et.al [4] periodically calculates the difference of destination sequence number of RREP and that of routing table entry and compares it with threshold value; for greater difference than threshold the node sending RREP is marked as a malicious node. Node detecting the malicious node broadcasts an ALARM packet to inform neighbour nodes about existence of a malicious node. The protocol, though, adds overhead in generating the ALARM packet and broadcasting it leads to higher routing overhead.

Nital et.al [5] provided a modification in AODV called MOSAODV that uses heuristic approach to calculate MOS_WAIT_TIME which is the amount of time source node waits after first RREP received for other RREPs; a table Cmg_RREP_Tab is used to store all RREPs. Out of all RREPs source node discards RREPs with higher sequence number considering those from malicious nodes. Limitation of this solution is that selecting the value of sequence

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

number to detect malicious reply is presumed; also, the solution adds overhead in terms of MOS_WAIT_TIME and Cmg_RREP_Tab.

Rutvij et.al [6] introduce Reliable-AODV (R-AODV), which modifies the structures of basic RREQ and basic RREP and adds a extra fields in the routing table of AODV. In R-AODV, in the presence of an attacker, in route discovery phase, S appends a MALICIOUS_NODE_LIST to RREQ if it has one or more MALICIOUS_NODE entries in the routing table. Every intermediate node receiving the RREQ updates its routing table with MALICIOUS_NODE entries. An IN receiving RREP with sequence number higher than the calculated PEAK value from malicious node MN marks it as DO_NOT_CONSIDER and the node consider that RREP as MALICIOUS_NODE node in routing table. After that RREP updates routing table with MALICIOUS_NODE entry of MN of INs and source node. When S broadcasts RREQ in future, it appends a MALICIOUS_NODE_LIST in RREQ to notify other nodes about the presence of MN along with other recorded malicious nodes. As a result, replies from MN and other malicious nodes remain unconsidered and they remain isolated from genuine nodes.

Rutvij et.al [7] introduce MR-AODV in which when a node detects a malicious node, it update the routing table with malicious node entry and discards the RREP; it is neither forwarded on the reverse path nor requires a DO_NOT_CONSIDER flag; so all RREPs reaching to the source node will be sent by genuine nodes only; the RREP indicating shortest fresher path will be chosen for data transmission by the source node. Thus, MR-AODV attempts to reduce routing overhead by not forwarding RREP after detection of misbehaviour.

Hesiri et.al [8] uses Data Routing Information (DRI) table for each node that has two fields called 'from' and 'through'. 'From' means that from this node gets a routing message and 'through' means that from current node sends a message to that node or not. In this first, source tries to discover a route from source to destination. Source sends RREQ packets to destination. If destination returns RREP, source trust its answer. If an intermediate node returns RREP, that node should also send its DRI table and ID of next node in the route to source. Node is trustable if source previously sent a message to that node and source starts sending data packets through that to destination. If source does not identify that node, it sends a packet to its next node and asks it for DRI table and also ID of its next node. The same process is done on the next node until source receives a DRI table of a trustable node and then stops this process and checks DRI table of both neighbour nodes to find maliciousness by checking 'from' and 'through' field of them. If source finds any differences in two neighbours' DRI tables announces all the nodes in the network regarding maliciousness.

IV. PROPOSED ALGORITHM

Here we proposed enhanced and modify AODV routing protocol named A_AODV (Authentic AODV) for efficient throughput, end and packet delivery ratio. Algorithm uses cache table mechanism stored at every node.

This cache table contains four fields in which three fields are of RREQ that is destination sequence number, destination ip, time stamp and one additional field called processing node id PN_ID.

Thus, in our work we modify RREQ message and add one more parameters with source sequence number, destination sequence number, hop count, source node id, destination node id and PROCESS_NODE_ID.

During Routing process source node Broadcast RREQ message, neighbour node process this RREQ if 1) it is not originator 2) not previously received from other node. Neighbour node verifies destination address and send back M-RREQ. This process continues until last node reach.

By receiving M-RREQ, every node generates cache table with updated entries. Thus, every node generate cache table of its next node. Here originator nodes and previously received RREQ node maintain cache table and store destination sequence number, destination id, time stamps, process node id. This cache table maintain by all nodes over network during routing process.

After complete routing process when node receive RREP from destination, first each node verifies time stamps and Destination sequence number, if Destination sequence number it too high compare to cache Destination sequence number then processing node simply discard RREP message and not entertain this node during routing process. On the other hand if destination sequence number matches with cache table then packet data is delivered to destination.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

In blackhole attack, attacker adds high Destination sequence number so it will not participate during routing process and simply bypass it. In A_AODV we just make simple change in routing process and through this we can get improve result of throughput and pdf over attacker scenario.

V. SIMULATION RESULTS

5.1 Simulation Environment

Our simulations are performed using ns-2 network simulator (Ver.-2.35) [10] which is network simulation tool that provides implementations of a different routing protocols. We are using random way point model for generating various network scenarios; cbrgen and setdest utilities are used to generate connection patterns and mobility models respectively. In order to implement Black hole attack, malicious node puts higher sequence number in RREP than in received RREQ. We fixed 50 nodes in the area of 500m x 500m for the simulation time of 100 seconds where number of malicious nodes are varying from 1 to 5. We use UDP at the transport layer. We vary following network parameters in our simulations:

Network Size: Number of mobile nodes in given network.

Number of Attackers: Number of Blackhole nodes in given network.

Table 1. Simulation Parameters

Channel Type	Wireless
Simulator	NS – 2.35
Terrain Area	500 mtr. X 500 mtr.
Simulation Time	100 Sec.
Traffic Type	CBR (UDP)
Routing Protocol	AODV
Data Payload	512 Bytes / Packet
Pause Time	1 Sec.
Maximum Speed	4 mtr. / sec.
No. of Nodes	10 to 50
No. of Malicious Nodes	1 to 5

5.2 Simulation Results and Analysis

We evaluate the performance of our protocol A_AODV under Blackhole attack and compare it with AODV under attack by varying different network parameters. We compare AODV under attack and A-AODV for different metrics.

Many solutions exist that may not perform well when multiple malicious nodes are present or when a node has more number of malicious nodes as neighbours than number of genuine nodes. But, A_AODV performs much better even if number of malicious nodes is present in the network. Moreover, A_AODV proves its reliability when network has malicious nodes; when node detects its neighbour node behaving maliciously, it do not propagate their information further. The performance of A-AODV under multiple malicious nodes with network size of 50 nodes, pause time of 1.0 sec is evaluated in **Figure 3**.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

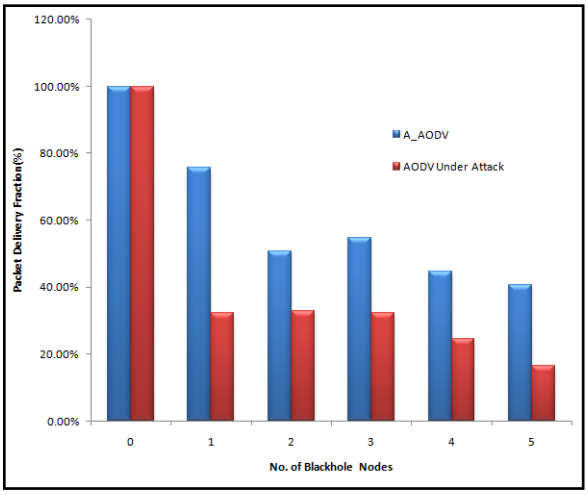

Fig. 3(a) Packet Delivery Fraction

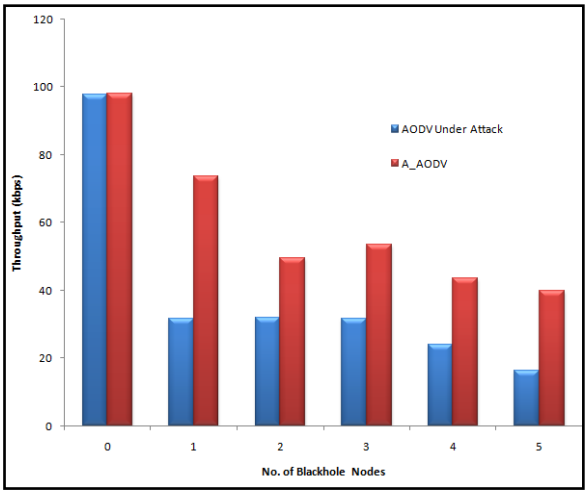

Fig. 3 (b) Throughput

PDF of AODV under Blackhole attack drops from nearly 32% to 16% as the number of malicious nodes increases from 1 to 5 as shown in **Figure 3(a).** On the other hand, A_AODV isolates multiple malicious nodes and gives more PDF than AODV under attack for all five cases. Throughput of A_AODV gives better results as compared to AODV under attack. However, it decreases as number of black hole nodes increases. It decreases from 97% to 39% as shown in **Figure 3(b).**

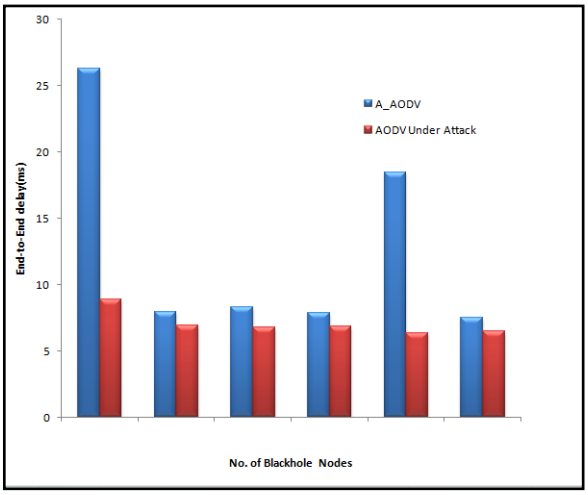

Fig. 3 (c) End-to-End Delay

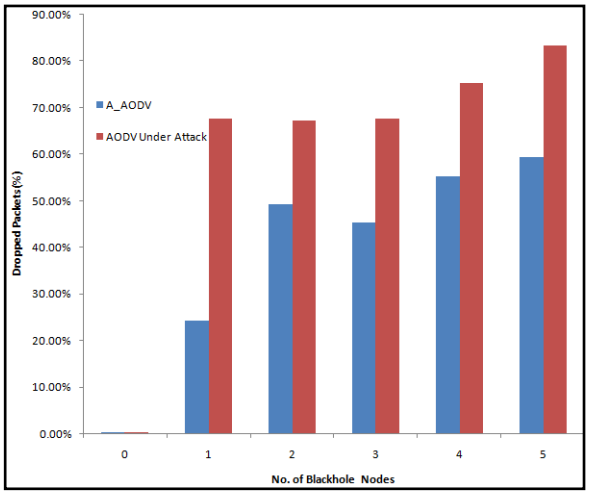

Fig. 3 (d) Percentage Dropped Packet

AODV under attack gives less End-to-End delay as compared to A_AODV as under attack because node chooses fake route to transfer data which takes less time to reach to the fake destination. Although, it stay within acceptable range as shown in **Figure 3(c)**. Ratio of number of packets dropped is less than AODV under attack in case of A_AODV as shown in **Figure 3(d)**. However, packet drop is increased as malicious nodes increases in both the cases. In A_AODV, it increases from 0.27% to 59%.

Figure 4 shows the performance comparison of AODV under attack and A_AODV under attack by varying network size between 10 to 50 and keeping pause time as 1.0 sec and maximum speed as 4 m/sec. As Blackhole node intercepts and drops all packets, PDF of AODV under attack drops significantly.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

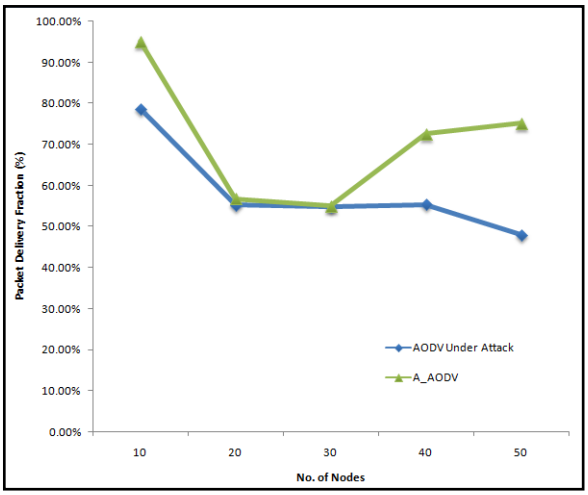

Fig. 4(a) Packet Delivery Fraction

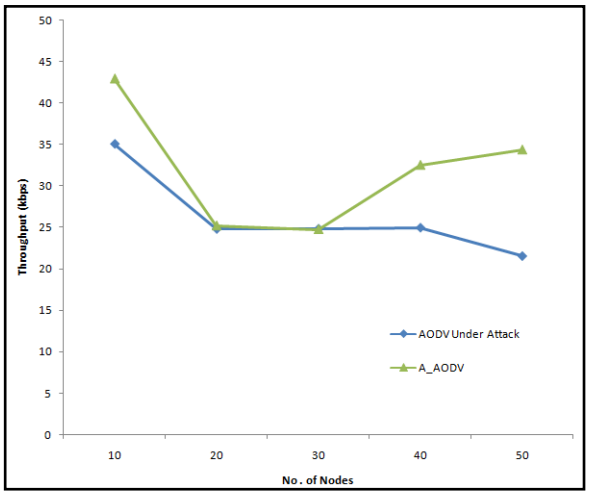

Fig. 4(b) Throughput

As Blackhole node intercepts and drops all packets, PDF of AODV under attack drops significantly. PDF drops from 95 to 75 percent as network size increases in case of A_AODV. As number of nodes increases packets are dropped due to collision. A_AODV isolates misbehaving nodes and gives better PDF as compared to attack as shown in **Figure 4(a)**. Throughput drops from 42 to 34 as network size increases in case of A_AODV. We can see visible difference from the **Figure 4(b)** that A_AODV gives much better performance with attack. A_AODV isolates misbehaving nodes and gives better throughput.

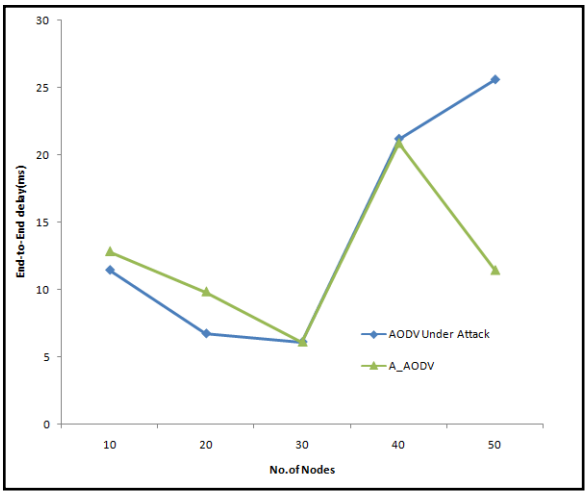

Fig. 4 (c) End-to-End Delay

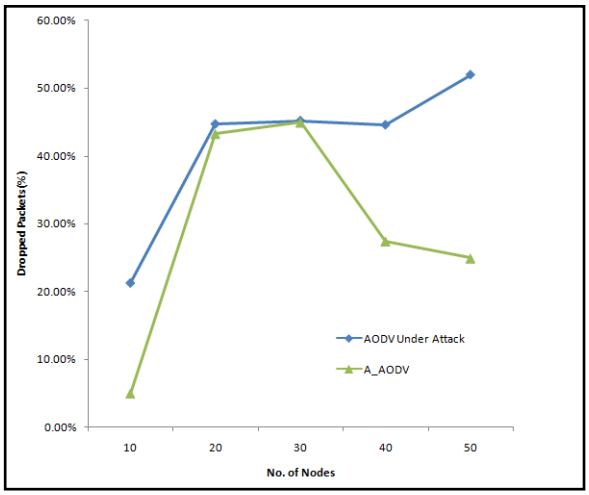

Fig. 4 (d) Percentage Dropped Packet

For AODV with attack, as the number of mobile nodes increases, average delay increases. Delay for A_AODV starts staying in acceptable range than that of AODV under attack initially and with increase in network size, it starts staying below. Average delay is varying between 12 to 11 ms in case of A_AODV in case of **Figure 4(c)**. Ratio of number of packets dropped is less than AODV under attack in case of A_AODV. However, packet drop is increased as number of nodes increases in both the cases. In A_AODV, it increases from 4% to 24% as shown in **Figure 4(d)**.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

VI. CONCLUSION AND FUTURE WORK

Ad hoc networks are an increasingly promising area of research with practical applications, but they are vulnerable in many settings to nodes that misbehave. For the sake of robustness of un-trusted environment, it is necessary to resist such routing behaviour. Black hole attacks are the most important security problems in MANET. Black hole starts in route discovery phase. We mentioned some of the proposed methods in detecting Black hole attacks. Most of these algorithms suffer from overload and low speed which degrade the QoS. As from the graphs, we can easily infer that the performance of the normal AODV drops significantly under presence of Black hole attack. In this paper, we analyse cache table mechanism to mitigate the effect of routing misbehaviour in ad-hoc networks. Result shows that A_AODV is a reliable solution which gives significant improvement in PDF and throughput with acceptable average end-to-end delay under various network parameters and traffic conditions.

REFERENCES

[1] C. S. R. Murphy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols. New Jersey: Prentice Hall PTR, May 24, 2004.
[2] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Mobile Ad hoc Networking. Hoboken, John Wiley, 2004.
[3] Marti, S., Giuli, T. J., Lai, K., and Baker, "Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of the 6th Annual International Conference on MOBICOM, Boston, Massachusetts, United States, 255-265, 2000.
[4] Payal N. Raj, Prashant B. Swadas. "DPRAODV: A Dyanamic Learning System Against Blackhole Attack In AODV Based Manet." In: International Journal of Computer Science Issues,Vol.2, pp 54-59, 2009.
[5] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri : "Improving AODV Protocol against Black hole Attacks" In proceeding of International Multiconference of Engineering and Computer Science, March 17, 2010.
[6] RUTVIJ H. JHAVERI, SANKITA J. PATEL, DEVESH C. JINWALA, "Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs", INFOCOMP, v. 11, no. 1, p. 01-12, March-2012.
[7] Rutvij H. Jhaveri, "MR-AODV : A solution to mitigate blackhole and grayhole attacks in AODV based MANETs", Third international conference on advance computing and communication technologies, 2013.
[8] Hesiri W. and Huirong Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks". International Journal of Software Engineering and its Applications, Vol. 2, No. 3, July-2008.
[9] Biswas, K., and Liakat Ali, Security Threats in Mobile Ad Hoc Network. Thesis no: MCS-2007:07. , Blekinge Institute of Technology, 2007.
[10] Fall, K. and Varadhan, K. The ns manual. *http://www.isi.edu/nsnam/ns/doc/*, 2010.
[11] C. Perkins, E. Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF, RFC 3561, 2003.