ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Impact of Collaborative Attacks on Performance of Reactive Routing Protocols in MANET

Prof. M. Nagendra[1], B.Kondaiah[2]

Research Supervisor, Dept. of Computer Science & Technology, S.K. University, Anantapur, India[1]

Research Scholar, Dept. of Computer Science & Technology, S.K. University, Anantapur, India [2]

ABSTRACT: Mobile Ad hoc Network (MANET) is a self configuring network of mobile nodes connected by wireless links and considered as network without infrastructure. The security in MANET has become a significant and active topic within the research community. Some attacks involving multiple nodes still receive little attention. Furthermore, it may also have to do with the fact that no survey or taxonomy has been done to clarify the characteristics of different multiple node attacks. In this paper we discuss collaborative attacks against MANET from the various multiple node attacks found. Simulation using NS2 was used to investigate the performance impact of a collaborative blackhole, wormhole and grayhole attacks on AODV and DSR routing protocol in mobile ad hoc network. We implemented four performance metrics are used in our result analysis. Finally we have shown the performance of AODV and DSR with collaborative attacks in MANET.

KEYWORDS*:* MANET, AODV, DSR, Collaborative attacks, NS2

I. INTRODUCTION

Mobile Ad-hoc networks are collectively composed of autonomous nodes, which are self managed and hold a dynamic topology such that nodes can easily join or leave the network at any instant time. Without relying on any fixed infrastructure, they are organized in decentralized manner means no central authority, self-configuring, self managing networks and also capable of modeling a communication network. Packets forwarded from one node to another that means each Node in the network have to trust one another because they participate in routing the traffic or acts like a mediator for routing. Some attributes in mobile ad-hoc networks makes routing additionally more complex are moderate bandwidth and limited battery power. Various types of attack target the network, therefore requirement of security protocols truly demanded. Many security protocols were already developed to attempt some of the attacks. But if talk about two or more attacks harmonized simultaneously in the network, knows as collaborative attacks where each and every attack is launched by a specialized expertise.

II. RELATED WORK

In this Section, we discuss different types of collaborative attacks that are proposed in the recent years by various researchers working on the areas of attacks over MANETs with their detection methods. MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalability. Despite the fact of the popularity of MANET, these networks are very much exposed to attacks. The network security attack can be broadly classified in two categories i.e. passive and active attacks. A passive attack does not disrupt the operation of the network except for snooping the data. The requirement of the confidentiality is dishonored if the attacker is able to interpret the data. Since the network operation is not affected, it is very difficult to detect this kind of attack. In contrast active attack tries to alter or destroy the data being exchanged and disrupts the normal operation of the network. Active attack can be further classified as external and internal attacks. External attack is committed by external nodes and internal attack is done by nodes which are part of the MANET having shortages of resources like battery power and

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

bandwidth etc. It is very difficult to separate these nodes. Different kinds of attacks have been analyzed in MANET and their affect on the network.

In the black hole attack, attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An attacker use the flooding based protocol for listing the request for a route from the initiator, then attacker create a reply message he has the shortest path to the receiver. As this message from the attacker reached to the initiator before the reply from the actual node, then initiator assume that it is the shortest path to the receiver. So that a fake route is create. Once the attacker has been able to insert himself between the communications node, then attacker may able to do anything with the packet which is send by the initiator for the receiver. Worm-hole attack which is also known as the tunneling attack, is possible even if the attacker has not compromised any other legitimate nodes and even if all communication provides authenticity and confidentiality.

A gray-hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later. In this attack, an attacker drops all data packets but it lets control messages to route through it. Sybil attack refers to the multiple copies of malicious nodes. It can be happen, if the malicious node shares its secret key with other malicious nodes. This way the number of malicious node is increased in the network and the probability of the attack is also increased. This paper focuses on the study the different collaborative attacks in MANET and compares the major cause of these attacks on the performances of different MANET applications.

III. CLASSIFICATION OF ROUTING PROTOCOL IN MANET

Classification of routing protocol [1] in MANET depends on routing strategy and network structure. According to the routing strategy the routing protocols can be categorized as Table-driven and Source initiated, while depending on the network structure these are classified as flat routing, hierarchical routing and geographic position assisted routing [2]. Both the Table-driven and source initiated protocols come under the Flat routing. The classification of Ad hoc routing protocols is shown in the Figure.1.

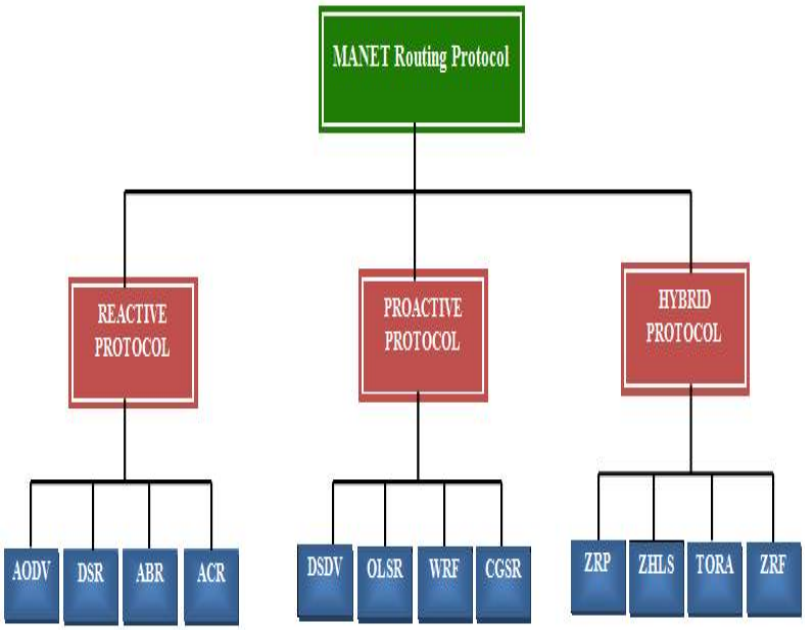

Figure 1: Classification of Routing Protocols in MANET

On Demand Routing Protocols (Reactive):

These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network.

Ad Hoc on-Demand Distance Vector (AODV)

AODV [3] shares DSR [4] on-demand characteristics in that it also discovers routes on an as-needed basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate a RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine the freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers. An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries.

A routing table entry is expired if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs. Route error propagation in AODV can be visualized conceptually as a tree who roots is the node at the point of failure and all sources using the failed link as the leaves. Inconsistency

Dynamic Source Routing (DSR)

The key distinguishing feature of DSR [4] is the use of source routing. That is, the sender knows the complete hop-by-hop route to the destination. These routes are stored in a route cache. The data packets carry the source route in the packet header. When a node in the adhoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a route discovery process to dynamically determine such a route. Route discovery works by flooding the network with route request (RREQ) packets. Each node receiving an RREQ re-broadcasts it, unless it is the destination or it has a route to the destination in its route cache. Such a node replies to the RREQ with a route reply (RREP) packet that is routed back to the original source. RREQ and RREP packets are also source routed. The RREQ builds up the path traversed across the network. The RREP routes back itself to the source by traversing this path backward.

The route carried back by the RREP packet is cached at the source for future use. If any link on a source route is broken, the source node is notified using a route error (RERR) packet. The source removes any route using this link from its cache. A new route discovery process must be initiated by the source if this route is still needed. DSR makes very aggressive use of source routing and route caching. No special mechanism to detect routing loops is needed. Also, any forwarding node caches the source route in a packet it forwards for possible future use.

IV. COLLABORATIVE ATTACKS

A collaborative attack in MANET is a homogeneous attack (i.e. blackhole, wormhole or grayhole attack), involving two or more colluding nodes; classified as internal active attack that can be processed using wired or wireless link and triggered by single or multiple attackers. It can also be referred to as the first level of attack, in which the adversary only interests in disrupting the foundation mechanism of the ad hoc network, for instance routing protocol, which is crucial for proper MANET operation [5].

Black hole Attacks

A blackhole attack occurs when a malicious node impersonates the destination node or forging route reply message that is sent to the source node, with no effective route to the destination [5]. The malicious node may generate unwanted traffics and usually discards packets received in the network [6]. When this malicious node (blackhole node) has effects on one or more nodes, making them malicious as well, then this kind of attack can be referred to as multiple node attack or collaborative attack.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

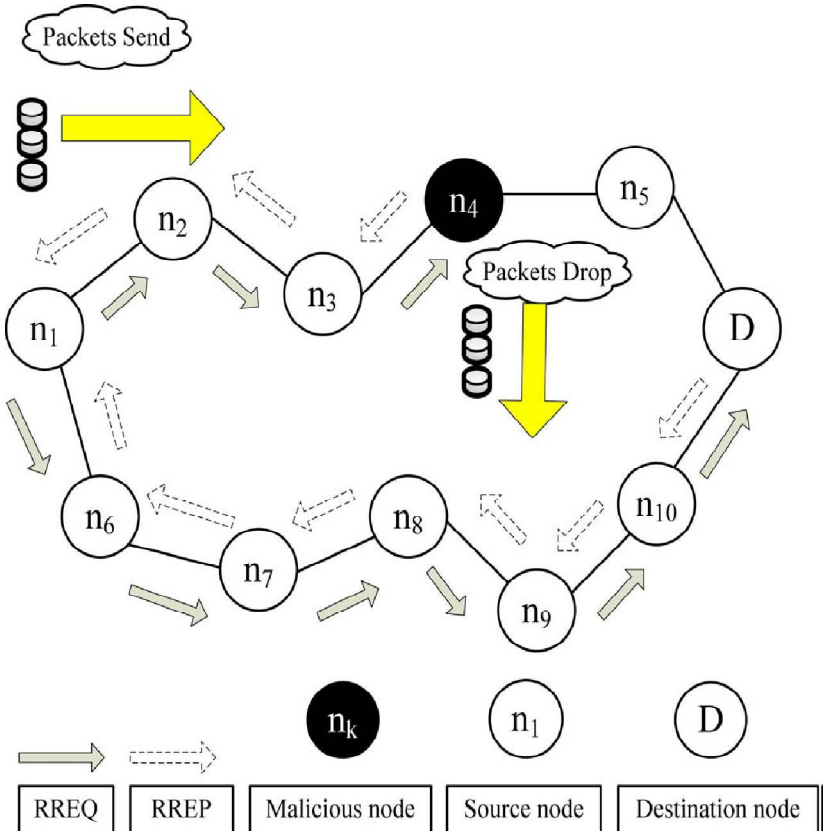

Fig. 2. Blackhole attack–node n_4 drops all the data packets

In blackhole attacks (see Fig. 2.), a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. In this case, a malicious node (so-called blackhole node) can attract all packets by using forged Route Reply (RREP) packet to falsely claim that "fake" shortest route to the destination and then discard these packets without forwarding them to the destination[7].

Wormhole Attack

In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious nodes is referred to as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. Attackers use wormholes in the network to make their nodes appear more attractive so that more data is routed through their nodes [8][9].

When the wormhole attacks are used by attacker in routing protocol such as DSR and AODV, the attack could prevent the discovery of any routes other than through the wormhole[10]. If there is no defense mechanism are introduced in the network along with routing protocols, than existing routing protocols are not suitable to discover valid routes.

In fig.3, the nodes "X" and "Y" are malicious node that forms the tunnel in network. The source node "S" when initiate the RREQ message to find the route to node "D" destination node[11]. The immediate neighbour node of source node "S", namely "2" and "1" forwards the RREQ message to their respective neighbours "5" and "X". The node "X" when receive the RREQ it immediately share with it "Y" and later it initiate RREQ to its neighbor node "8", through which the RREQ is delivered to the destination node "D". Due to high speed link, it forces the source node to select route <S-1-8-D> for destination. It results in "D" ignores RREQ that arrives at a later time and thus, invalidates the legitimate route <S-2-5-7-D>

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

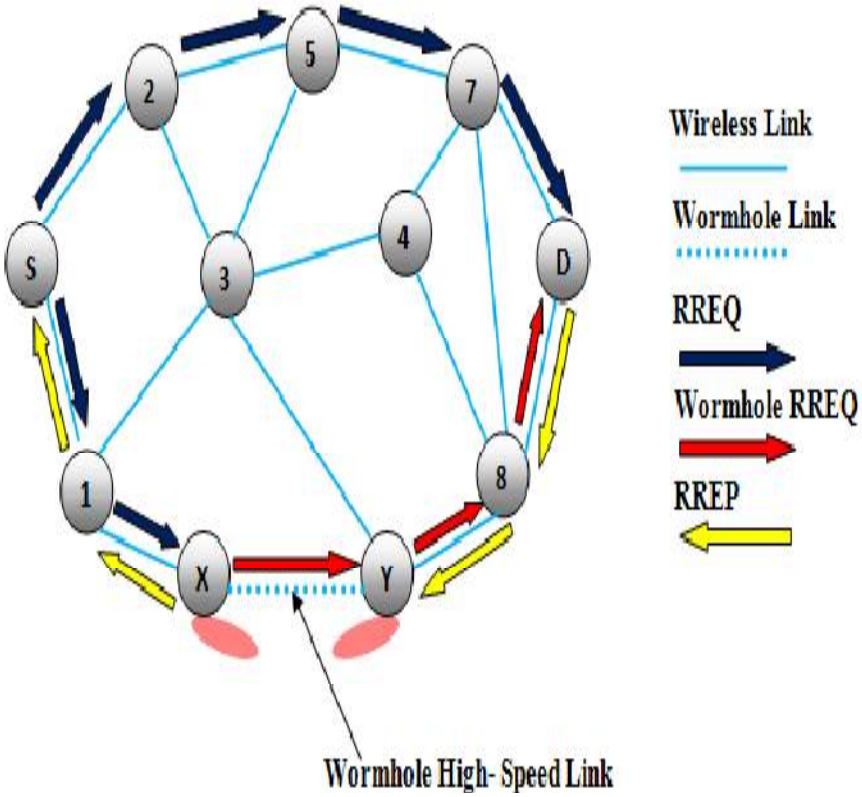

Fig 3: Wormhole Attack

Gray hole Attack

A Grayhole attack is an active attack which takes place at the network layer in the MANET. This type of attack cause damage or interrupt the network functionality by dropping the data packets which are being transmitted. Grayhole is a node that selectively drops the packet and after sometime it will start forwarding the packets normally like any other nodes in the network[7].

Grayhole attack takes place in two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a shortest route to the destination, with the intention of intercepting the packets. But in actual there is no such short route to the destination exists. In the second phase, after trapping the source node maliciously, Grayhole will receive the packets from the source node and eventually start dropping the packets. As per its default nature, Grayhole attack will drop the data packets selectively without any certainty. Due to such nature, it becomes hard to detect the Grayhole as it can act both as a normal node as well as a malicious node.

V. PERFORMANCE EVALUATION

Simulation setup

Ns2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (ns) contains all commonly used IP protocols. The network animator (nam) is use to visualize the simulations. Ns2 fully simulates a layered network from the physical radio transmission channel to high-level applications.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

TABLE 1
SIMULATION PARAMETERS

Parameter	Value
Application Traffic	10 CBR
Transmission rate	4 packets/s
Radio Range	250m
Routing protocol	DSR, AODV
Packet Size	512 bytes
Channel data rate	11 Mbps
Pause time	0s
Maximum Speed	20 (ms)
Simulation time	800s
Number of nodes	50
Area	700m*700m
Malicious nodes	0% 40%
Threshold	Dynamic Threshold

Performance Metrics

We have compared the AODV and DSR routing protocols with collaborative attacks.

Packet Delivery Ratio

This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. Here, $pktd_i$ is the number of packets received by the destination node in the i^{th} application, and $pkts_i$ is the number of packets sent by the source node in the i^{th} application. The average packet delivery ratio of the application traffic n, which is denoted by PDR, is obtained as

$$PDR = \frac{1}{n}\sum_{i=1}^{n}\frac{pktd_i}{pkts_i}.$$

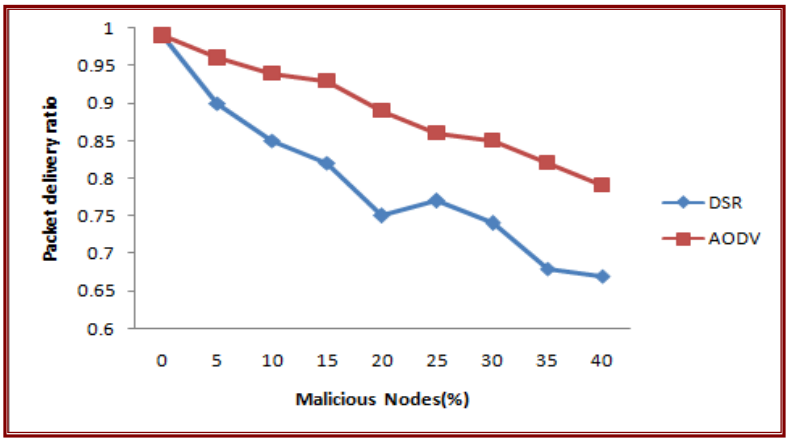

Fig.4. Effect of the malicious nodes on Packet delivery ratio

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

In the above fig.4, we compared AODV and DSR in terms of Packet delivery ratio against malicious nodes are increased from 0% to 40% with a fixed speed. It is observed that, the DSR heavily suffered more than AODV. Moreover AODV shows the highest packet delivery ratio when compared to DSR.

Routing Overhead

This metric represents the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. Here, cpk_i is the number of control packets transmitted in the i^{th} application traffic, and pkt_i is the number of data packets transmitted in the i^{th} application traffic. The average routing overhead of the application traffic n, which is denoted by RO, is obtained as

$$RO = \frac{1}{n}\sum_{i=1}^{n}\frac{cpk_i}{pkt_i}.$$

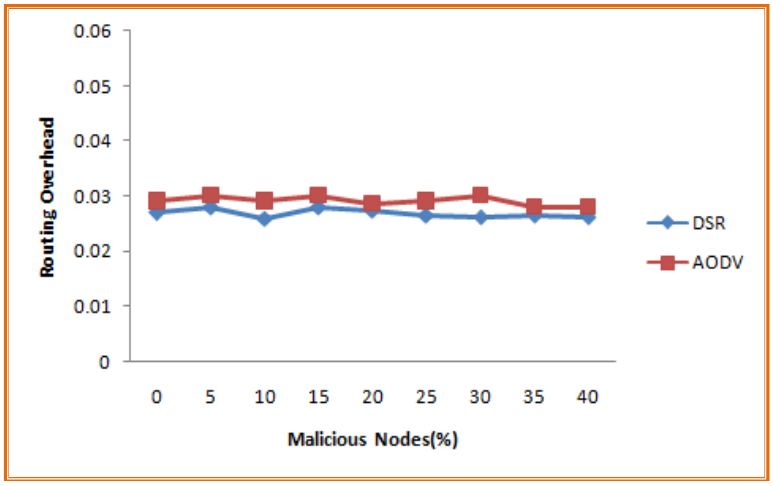

Fig.5. Effect of the malicious nodes on Routing Overhead

In above fig.5, we compared AODV and DSR in terms of routing overhead against malicious nodes are increases from 0% to 40% with a fixed speed. It is observed that, the AODV produces slightly highest routing overhead than DSR. Moreover DSR has shown lowest routing overhead, when compared to AODV.

Average End-to-End Delay

This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is d_i, and the number of packets received by the destination node is $pktd_i$. The average end-to-end delay of the application traffic n, which is denoted by E, is obtained as

$$E = \frac{1}{n}\sum_{i=1}^{n}\frac{d_i}{pktd_i}.$$

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

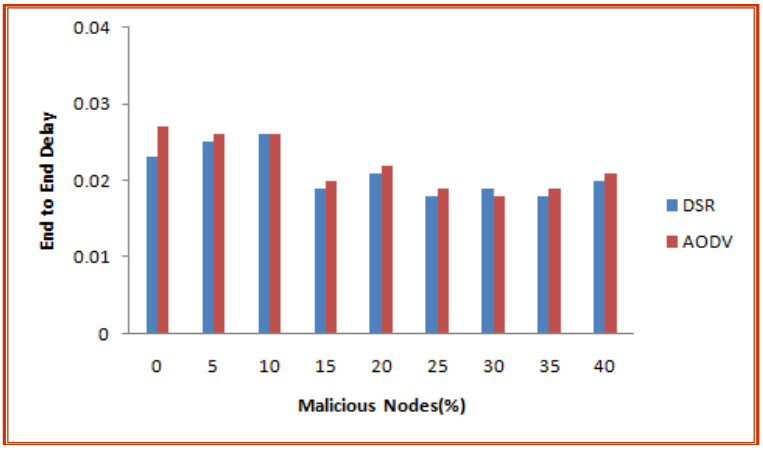

Fig.6 Effect of the malicious nodes on End to End Delay

In the above Fig.6, show that DSR proves a minimum end to end delay rather than the AODV. DSR takes the least time to deliver a packet from one end to the other i.e., 0.020 to 0.023 seconds. AODV takes 0.021 to 0.027 milliseconds to deliver packets from one end to the other. The comparison of end-to-end delay analysis of data packets reaches a minimum time in DSR method when compared with AODV.

Throughput

This is defined as the total amount of data (b_i) that the destination receives them from the source divided by the time (t_i) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput of the application traffic n, which is denoted by T, is obtained as

$$T = \frac{1}{n} \sum_{i=1}^{n} \frac{b_i}{t_i}.$$

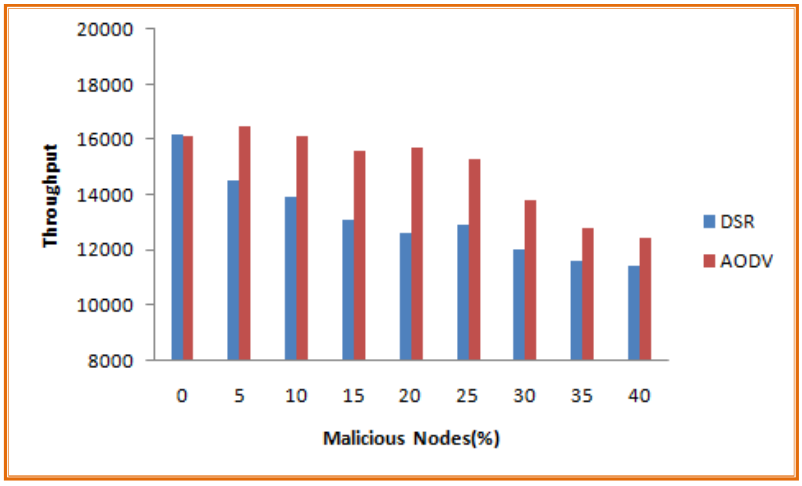

Fig.7. Effect of the malicious nodes on Throughput

The results are captured in Fig.7. It is observed that, the DSR is more suffering than AODV when the percentages of malicious nodes are increased from 0% to 40% with a fixed speed. The AODV experimental results shows, it is higher throughput compared with DSR.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

VI. CONCLUSION

The entire theme of this chapter is on performance evaluation of AODV with collaborative attacks such as blackhole, wormhole and grayhole. The impact of collaborative attacks on AODV is measured by comparing with the DSR. The experimental result obtained through AODV and DSR with two scenarios. Each scenario has the four performance metrics such as packet delivery ratio, routing overhead, end-to-end delay and throughput are effectively studied. Each performance metrics of AODV is effectively compared with existing method known as DSR routing method. As future scope, we intended to investigate and implement the integrated security schemes for defending against collaborative attacks.

REFERENCES

[1] Gorantala, K. (2006). Routing Protocol in Mobile Ad-hoc Networks. Technical report Department of Computer Science from UMEA University.
[2] Hong, X.; Xu, Kaixin and Gerla, Mario (2002). Scalable routing protocols for mobile ad hoc networks. IEEE Network Magazine, pp 11-21.
[3] Perkins, C. E.; Das, S. R. and Royer, E. (2000). Ad-hoc Demand Distance Vector (AODV). Mobile AdHoc Networking Working Group, IETF Internet Draft, online available: http://www.ietf.org/internet-draft/draft-ietf-manet-aodv-05.txt.
[4] Johnson, David B. and Maltz, Dravid A. (1996). Dynamic Source Routing in AdHoc Wireless networks.Technical report, Carneigie Mellon University.
[5] Aditya Bakshi, A.K.Sharma, Atul Mishra, ―Significance of Mobile AD-HOC Networks (MANETS)‖ International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-4, March 2013.
[6] Dr.V.Egaiarasu, D.Kailashchandra, ―Detection of Black Hole and Worm Whole Attacks in MANETS, SSRG International Journal of Mobile Computing & Application (SSRG- IJMCA) – volume 2 Issue 3 May to June 2015.
[7] V. K and A. J PAUL, "Detection and Removal of CooperativeBlack/Gray hole attack in Mobile Ad Hoc Networks," 2010 International Journal of Computer Applications, Vol. 1, No.22, 2010.
[8] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak, "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks", IEEE Third International Conference on Advanced Computing & Communication Technologies, 2013.
[9] Weichao Wang, Bharat Bhargava, Yi Lu, Xiaoxin Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Conference of Wiley Journal Wireless Communications and Mobile Computing (WCMC), 2010 .
[10]Amol A. Bhosle, Tushar P. Thosar and SnehalMehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Volume- 2,issue- 1, pp 325-331, February 2012.
[11] Ms. N.S.Raote, Mr.K.N.Hande, "Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network", International Journal Of Advanced Engineering Sciences And Technologies Volume- 2, Issue- 2, pp 172 – 175, 2010.