Analyzing the Impact of Jellyfish attack on Reactive Routing Protocols in MANET

[1] Er. Pankaj,[2] Shikha Verma
Department of Electronics and Communication
LRIET,Solan, HP, India.

Department of Electronics and Communication
LRIET, SOLAN,HP, INDIA

Abstract: JFDV attack causes delayed ACK and sender assumes that packet has been lost and begins to retransmit the packet leading to congestion in the network. Routing protocols specifies the ways to establish the route from source to destination. The established route belongs to reactive and proactive category. AODV and DSR fall under the category of reactive routing protocol or on demand routing protocol. The AODV routing protocol is based on DSDV and DSR. In AODV, each packet carries the destination path, whereas in DSR each packet carries full routing information. Moreover AODV is adaptive to highly dynamic network. The present work has been implemented on network simulator, NS 2.35. It is a discrete set of terms and protocol settings for network lay-outing and configurations. The present work has taken 2-routing protocols AODV and DSR; on which JFDV attack has been implemented. The impact of varying number of jellyfish attacker nodes 1, 3, 6 and 9 has been compared in both the protocols. AODV outperforms DSR protocol for several performance parameters, which include "*Throughput*" and "*End to End Delay*" with JFDV detection algorithm. The Algorithm provides better identification and removal in AODV protocol.

Keywords: JFDV, AODV,DSR, ACK.

I. INTRODUCTION

Now-a-days gadgets are becoming compact, less expensive and easier to understand. Mobile ad-hoc network is composed by series of fast moving wireless nodes. Because of the absence of the organization and the versatility of nodes, every node in the network contributes in directing operation by being aware of network connectivity and topology changes. MANETs are self-framing and self-recuperating, empowering peer-level communication between mobile nodes without dependence on infrastructure and centralized device. In MANET, every node can act as router to forward the packet throughout the specific network. These attributes enable MANETs to deliver significant benefits in virtually any situation that includes a cadre of highly mobile users or platforms, a strong need to share IP-based information, and a atmosphere in which fixed network infrastructure is impractical, impaired, or impossible. Four core functions of manet are Path Generation, Path Selection, Data Forwarding and Path Maintenance [2]. Key applications of Ad-hoc networks include disaster recovery, heavy manufacture, mining, transportation, defense, and special event management.

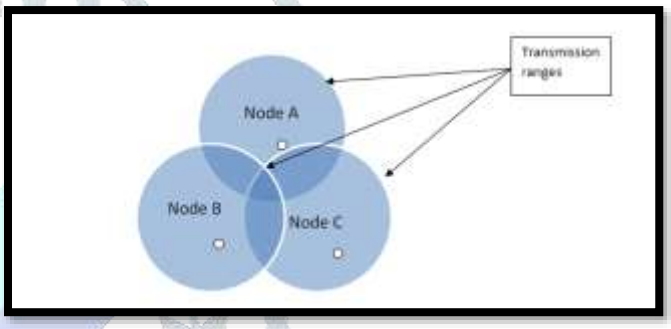

Fig.1 Mobile Ad-Hoc network

1.1.1 Classification of Ad-hoc Routing Protocols

Based on the delivery of packets from sender to receiver, Classification of routing protocols can be done as Unicast and Multicast routing protocols. In unicast routing protocol single source and single destination is involved for communication forming one-to-one relationship. In multicast routing protocols, info or data is delivered to group of destinations simultaneously using the most convenient and efficient strategy. Further routing protocols are classified as Table-driven routing protocol, On-demand routing protocol and Hybrid routing protocol

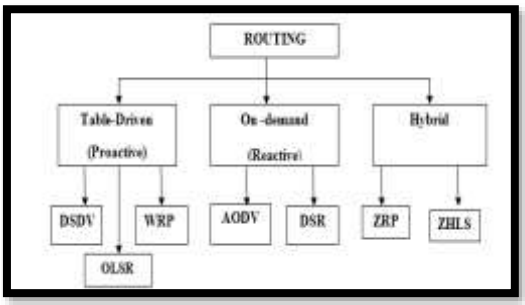

Fig. 2. Routing Protocols

1.1.1.1 Proactive (Table Driven) Routing Protocol

In proactive routing protocols routes are computed prior to request. Periodic updation and distribution of routing info takes place in it. Proactive protocols consume more bandwidth as it holds a routing table throughout the

transmission. The Advantage of proactive protocol is that a route can be selected immediately without waiting for hold up but maintaining large amount of data for routing information with higher bandwidth and slow reaction on failures and attacks are major setbacks. Ex: DSDV, OLSR, WRP.

- **DSDV (Destination Sequence Distance Vector Routing):** In DSDV, each mobile node in a network maintains a table. Each routing table maintains a list of all possible routes and hop count to reach the destinations. These tables are update either periodically or driven by an event. Each node advertises its own routing table to the neighboring nodes by broadcasting or multicasting. The routing updates could be set in two ways. One is called as full dump and another is known as incremental.
- **WRP (Wireless Routing Protocol):** WRP maintains a Distance table, a Routing table, a Link Cost table and a message retransmission for the purpose of routing. WRP reduces the number of cases in which routing loop get established. It uses periodic update message transmission to the neighboring nodes. The nodes in the response list send acknowledgements. If there is no change with the last update, then nodes in response list sends idle hello message to ensure connectivity.
- **OLSR (Optimized Link State Routing):** OLSR protocol is an optimization of pure link state routing protocols for MANETs. Firstly, it declares only a subset of link with its neighbors instead if all links thus reducing the size of control packets with the use of multipoint relay selectors. Secondly, it minimizes the flooding of traffic by using selected nodes called multipoint relays, to send messages in the network. It uses hello and Topology Control (TC) messages to get and then spread link state info throughout the network.

1.1.1.2 Reactive (On Demand) Routing Protocol

Routes are discovered, when demanded by flooding route request in reactive routing protocols. There is no need of distribution of routing information. Reactive routing protocols ensure less bandwidth and effective in route maintenance but require high time route discovery and sometimes excessive flooding may lead to network congestion. Ex: AODV, DSR.

- **AODV (Ad hoc On Demand Distance Vector):** AODV is a routing protocol intended for remote and portable computer systems. This protocol sets up routes to goals on request and backings both unicast and multicast routing. The AODV protocol was created by Nokia Research Center, the University of California, Santa e Barbara and the University of Cincinnati in 1991. AODV (Ad hoc on demand distance vector routing), an on-request calculation and does not make any additional movement for correspondence along links. The routes are kept up as long as they are required by the sources. In AODV, systems are quiet until the point when associations are set up. System nodes that need associations communicate a request for association. The rest of the AODV nodes forward the message and record the node that requested an association. In this way, they make a progression of brief routes back to the requesting node.
- **DSR (Dynamic Source Routing):** The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes.DSR represents on-Demand routing using source-route. DSR allows the network to be wholly self-organizing and self-configuring, without the need for any existing network infrastructure or administration.DSR is an on demand source routing protocol which indicates that the data packets contain a list of nodes representing the route to be followed and routes are created whenever a source node requests to send data to the destination node [3]. By using source routing, packet routing is allowed to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use.

1.2 JELLYFISH ATTACK

Jellyfish attack maintains acceptance with both scenarios like control and data protocols. Because it acts compliant to both data and control protocol which make it difficult to detect and prevent. Therefore Jellyfish attacker is difficult to detect until after the sting [21]. The jellyfish attacker firstly implements the rushing attacks to gain access to the routing mesh. If become successful, it then delays all the packets by a random period of time [22]. As there is no functional distinction among mobile nodes in MANETs, an intermediate node can introduce a critical vulnerability for TCP congestion Control mechanism. There are various variant of the jelly fish type of attack.

1.2.1 Jelly Fish Reordering Attack

As name implies, attacker node reorders some of the packets before being forwarded to the immediate next node in its neighbor. As ACKs of some of the reordered packets are not received in time, the sender will considers that these packets have been dropped in the network and will re-forward them. Receiver will receive the packets again and their will re-generation of the Ack. frame. This results in the formation of more than one ACK for single packet. TCP initiate its flow control to control these duplicate ACK packets, when these ACK packets exceed the threshold. The reordering packets can be performed in two ways. First is by reordering packets in batches of k packets each. This procedure is performed in three basic steps. 1. Reorder current batch of k packets. 2. Forward the reordered batch. 3. Wait for next batch. Second is by reordering is done using sliding window of k size and each time a packet is sent, this window is grown by one packet. Reordering is initiated on available k

packets each time a packet is about to leave the reordering buffer [23].

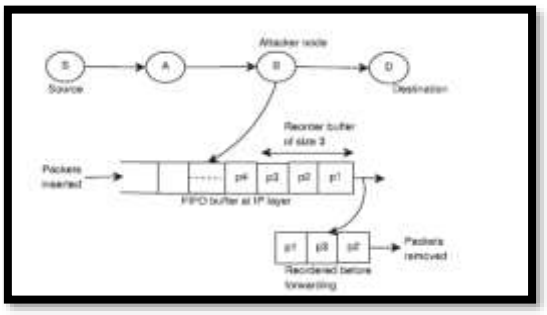

Fig. 3. Reordering Attack[16]

1.2.2 Jelly Fish Periodic Dropping Attack.

In this attack, a JF node randomly discards some packets received over the specific period of time. JF attacker node may drop a fraction of packets or all the packets in a specified time. For example if 5 percent packets, then it has received 100 packets it will drops the 5 packets. This dropping of the packets can be the indication of congestion in the network. TCP will try to control the disturbed flow in specific period of time. Later on jellyfish attacker node chooses another time period to starts dropping the packets which will again disturb the flow. That means this type of exercise is performed after certain period of time resulting in decreased network performance.

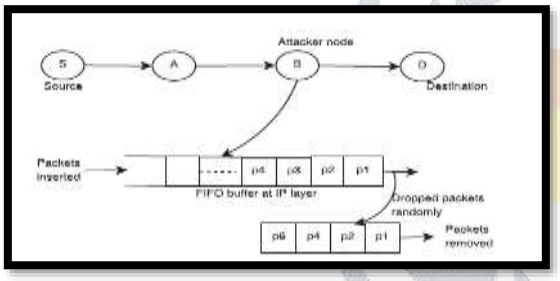

Fig. 4. Periodic dropping attack [16]

1.2.3 Jelly Fish Delay Variance attack

Jellyfish delay variance attack is the one which follows all protocol rules and hence difficult to detect. Jellyfish is a passive attack as the attacker disrupts the network from within. JF attacker becomes the part of routing mesh and introduces some amount of delay before forwarding the packets. When ACK is delayed then the sender will not receive the acknowledgement within specified amount of time. Source node will assume that packets are lost and start retransmitting the packets. It leads to increased congestion and reduced throughput. Jellyfish attack targets closed loop flows because of which flow is affected by packet loss and delay [9]

II. RELATED WORK

Mohammad Wazid et al., (2012), gives Cluster based Intrusion Detection and prevention techniques for JF reorder attack(CBIDPT) and Super cluster based Intrusion detection and prevention technique for reorder attack(SCBIDPT) are two techniques proposed for jellyfish reorder attack. Cluster head elect on the basis of fairness and efficiency of the participating. In CBIDPT, source node and intermediate nodes make entry into FIFO buffer. The Buffer forwards the data packet to its neighbor node. Source node and intermediate node sends same FIFO buffer to cluster head also. Sequence number of FIFO buffer and is compared with the sequence numbers of all intermediate nodes. If any reordering is found in forwarding data packet, cluster head automatically omits that intruder node on the basis of their ID which is already stored in cluster head. Then cluster head searches for other optimum route which has not any type of intruder node. However, in SCBIDPT, super cluster is build by collecting multiple clusters. SCBIDPT is used to find and remove the fake cluster head from the network [12]

Mohammad Wazid et al., (2013), explained that Jellyfish delay variance attack delays the data packet during forwarding the data packet to the destination. Due to the delay in packet forwarding, ACK is also delayed and sender assumes that the packet has been lost. Sender assumes that packet has been lost and starts retransmission, leading to congestion in the network. If the cluster head time is equal to intermediate node buffer entry tie then efficient TCP otherwise not. Efficient TCP protocol prevents JFDV attack by disabling fast transmission of malicious data packets and enabling selective ACK. As the network performance was improved, therefore named as Efficient-TCP [13].

Sanjay Kumar et al., (2016), proposed a procedure for AODV routing protocol, to detect jellyfish delay variant attacker node. Sending time and sequence number is noted before sending the packets. When the packet reaches the destination and ACK is received, then difference between the previous values of time and ACK receiving time of all the nodes was compared to the ideal time taken by all the nodes. When the value was greater than the maximum value then the receiver was assumed to be a Jelly Fish attacker node and flag value was set to 1. This maximum value is based on the propagation delay, link delay etc. This process continued for every node until it was known that which node caused delay of the packet. Once the jellyfish attacker was identified, no path will use these attacker nodes has been explained in this work [14]

III. ALGORITHM

In MANET, nodes communicate with each other and on the hop-by-hop basis. In the attacker node detection and removal technique, every node broadcasts packet to its neighbor nodes with Time to Live(TTL)=1 and neighboring node IP address as destination IP address after a fixed time interval and timer is set to keep track of delayed packets. A counter is used to avoid false decisions and each node is twice given a chance not be marked as attacker incorrectly. Timer is set in a way that it takes threshold value. Threshold delay value selected depends on the packet delivery time

P: Broadcast packet
Count=2
T: Timer
For each node
{

Create a packet P
Broadcast the packet to its neighboring nodes
}
For each node
{
If (P received) {
If (T expired) {
Jellyfish attacker suspected
Count= Count -1
If (Count < 0) {
Node is a jellyfish
node
}}}}
For each node
{
While (route discovery)
{
If (RREP from jellyfish attacker)
{
Reject RREP
}}}

IV. RESULTS AND ANALYSIS

4.1 Performance Parameters

The analysis of routing protocols is done using two important performance metrics named as throughput and end to end delay.

- **Average End-to-End Delay**: It is the average time taken by a data packet to arrive at the destination. It includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC and propagation transfer times.

  D=Σ (Tr-Ts) / Σ No. of Connections

  Where Tr is received time and Ts is sent time.
- **Throughput:** It is the average rate of successful message delivery over a communication channel. It is also called as packet sent per unit interval of time. The throughput is usually measured in bits per second or data packets per time slot.

  Throughput=Total packet received / Total time

4.2 Network Configuration

SIMULATION PARAMETERS	
COVERAGE AREA	1000m x 1000m
PROTOCOLS	AODV,DSR
NUMBER OF NODES	50
SIMULATION TIME	100 seconds
TRANSMISSION RANGE	250m
MOBILITY MODEL	RANDOM WAY POINT MODEL
LOAD	5 Kb-UDP Packets
MOBILITY SPEED(variable)	(80,90.100,150)Seconds
TRAFFIC TYPE	CBR,UDP,FTP,TCP
PACKET SIZE	512 Kbps
PAUSE TIME	10 ms

4.3 PERFORMANCE ANALYSIS

The performance of routing protocols is analyzed using NS2 simulator. Firstly, behavior of AODV under jellyfish attacker node is studied. Then DSR routing protocol is taken and analyzed. Further comparison of AODV and DSR is done on the basis of performance parameters such as throughput and end to end delay

4.4 AODV

In this section End to End delay and Throughput is calculated for AODV routing protocol under the impact of Jellyfish attack

4.4.1 End to End Delay for AODV

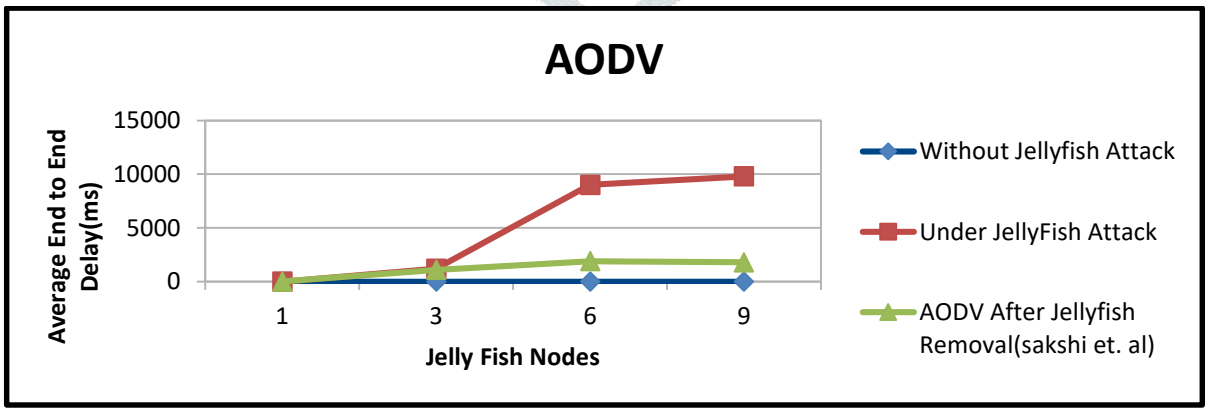

Fig.5. AODV E2E Delay

Average End to End delay for network under AODV routing protocol is taken to understand the effect of jellyfish attack. Three scenarios are taken with varying number of nodes as 1, 3, 6 and 9. Firstly simple AODV protocol is implemented without any attack. It is noted that there is no delay in transmission. In second case, behavior of AODV is seen under varying jellyfish attacker nodes. As the number of attacker nodes increases, End to End delay keeps on increasing. Afterwards, the attacker identification

and removal algorithm is applied to the network and results are shown in Figure 4.06. It is seen that the performance in terms of End to End delay improves substantially especially at higher number of attacker nodes.

4.4.2 Throughput for AODV

Throughput under AODV routing protocol is analyzed under the impact of jellyfish attack. Three scenarios are used with varying number of attacker nodes as 1, 3, 6 and 9. In the first scenario, AODV gives maximum throughput as no attacker is present in this case. Afterwards throughput decreases significantly with increasing number of attacker nodes, when the protocol got affected by jellyfish attackers. Further after the implementation of the attacker detection and removal algorithm, significant increase in throughput is observed. The following figure represents the behavior of AODV routing protocol.

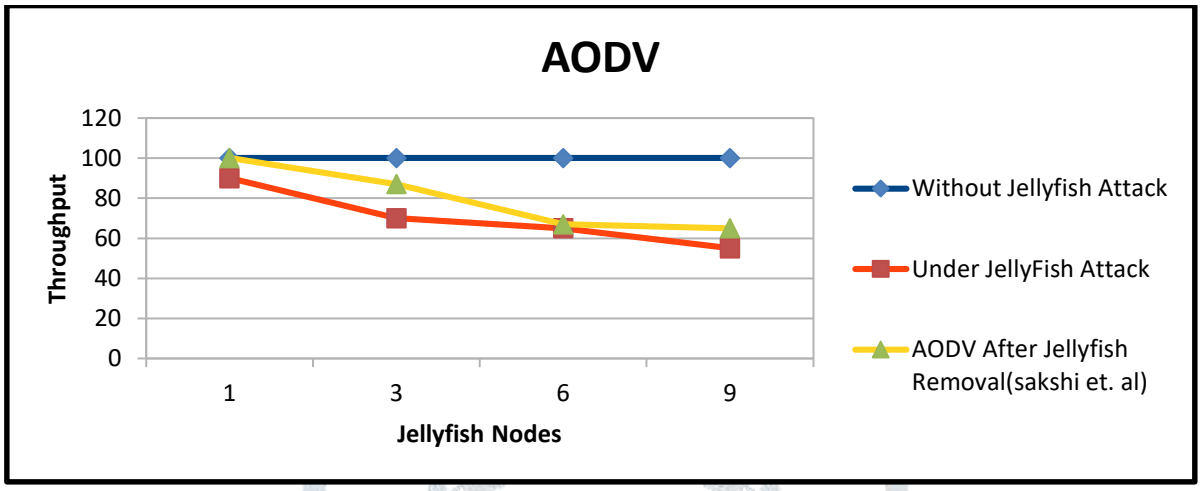

Fig. 6.AODV Throughput

4.5 DSR

In the section, End to End delay and Throughput is calculated for DSR routing protocol under the impact of jellyfish attack

4.5.1 End to End Delay for DSR

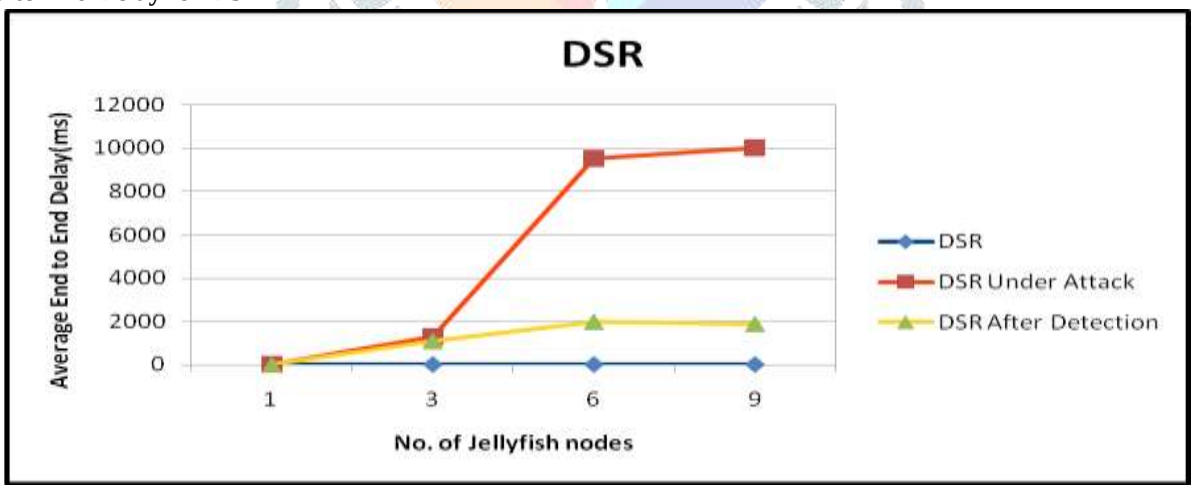

Fig.7.DSR E2E Delay

Average End to End Delay (ms) for network in DSR protocol under the impact of jellyfish attack is shown in the figure. The framework includes three cases under varying attacker nodes as 1, 3, 6 and 9. There is no delay in simple DSR. The behavior of DSR protocol changes as the number of attacker nodes increases from 1 to 9.The average end to end delay got increases substantially under the affect of jellyfish attack. Further after the execution of attacker detection and removal technique, End to End delay decreases.

4.5.2 Throughput for DSR

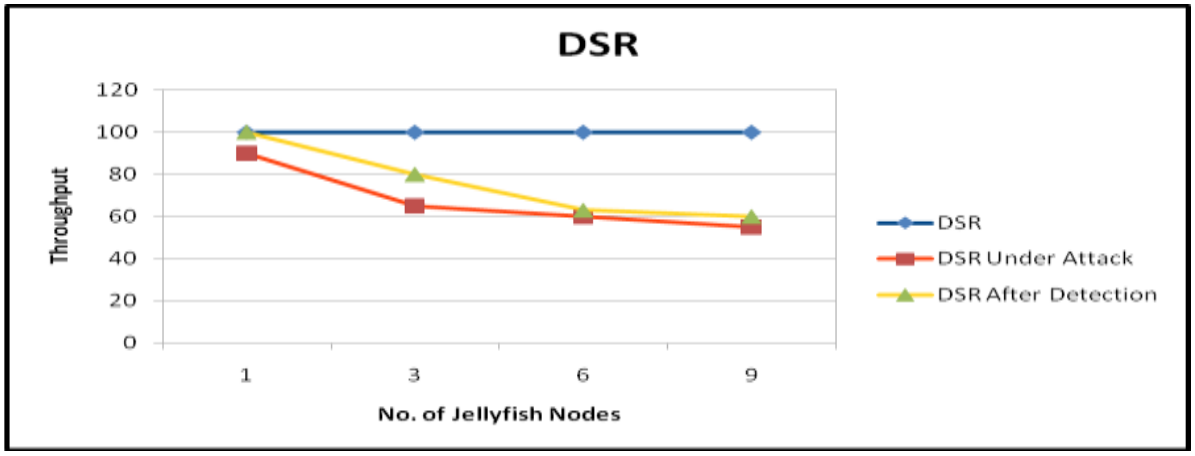

Fig.8. DSR Throughput

Throughput in DSR routing protocol is studied under the impact of jellyfish attack. Three Scenarios are shown by this figure with varying attacker nodes 1, 3, 6 and 9. Throughput is highest under the absence of attacker nodes. As the attacker nodes increase, throughput decreases significantly. Further after the implementation of attacker detection and removal technique, performance got improved in terms of throughput.

V. CONCLUSION

Major conclusions drawn on the basis of simulation results on NS-2 platform are-

- Jellyfish attacker node considerably affect the performance (Throughput and end-to-end delay) of both AODV and DSR routing protocols.
- Algorithm used for detection and removal of JF attacker nodes can significantly improves the performance of routing protocols.
- Throughput of AODV routing protocol is better able to sustain itself in comparison to that for DSR in the presence of JF attacker nodes. Further, after the detection and removal of attacker node, AODV routing protocol shows higher improvements than DSR.
- End-to-End delay has smaller value in AODV routing protocol than DSR. Moreover, after the detection and removal of jellyfish attacker node, AODV routing protocol shows better results than DSR in terms of end-to-end delay.

VI. FUTURE WORK

This research can be extended by studying the other two types of jellyfish attacks namely Jellyfish periodic dropping attack and Jellyfish reorder attack. This work can also be improved by considering other proactive protocols like OLSR, WRP and hybrid category of protocols like ZRP and ZLSR.

REFERENCES

[1] Mojgan Kamali, Luigia Petre, "Comparing routing protocols", 20th IEEE International Conference on Engineering of Complex Computer System (ICECCS), Gold Coast, Australia, 9-12 Dec-2015

[2] Sd Salman Ali, Dr. G Manoj Someswar, "Mobile Adhoc Network Routing Protocols under Analytical study", IOSR Journal of Computer Engineering, Vol. 10, Issue 4, March-2013 (ISSN: 2278-8727)

[3] Mohamed A. Abdelshafy, Peter J.B. King, "Dynamic source routing under attacks", 7th IEEE International Workshop on Reliable Networks Design and Modeling (RNDM), Munich, Germany, 5-7 Oct-2015

[4] Devesh Tedia, Umesh Kumar Lilhore, "Various attacks including Jellyfish attack along with Security issues in MANET", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 4, Issue 7, July-2016. ISSN: 2321-9653

[5] Manjot Kaur, Malti Rani, Anand Nayar, "A Comprehensive study of Jellyfish attack in Mobile Adhoc networks", International Journal of Computer Science and Mobile Computing(IJCSMC), Vol. 3, Issue 4, pg. 199-203, April-2014, ISSN: 2320-088X

[6] Bhawna Singla, A.K Verma, L.R. Raheja, "An Evaluation on selfish behaviour attack and jellyfish attacks under AODV routing protocol", International Journal in Foundations of Computer Science & Technology, Vol. 7, No. 2, pg. 15-28, March-2017

[7] Ming Yu, "A Secure routing protocol against byzantine attack for MANETs in adversarial environments", IEEE Transactions on Vehicular Technology, Vol. 58, No.1, Jan-2009, ISSN: 0018-9545

[8] Sohail Abbas, Madjid Merabati, David Llewellyn-Jones and Kashif Kifayat, "Lightweight Sybil attack detection in MANETs", IEEE System Journal, 2012, ISSN: 1932-8184

[9] Nitika Gupta and Shailendra Narayan Singh, "Wormhole attack in MANET", 6th International

Conference on Cloud Computing and Big Data Engineering, Noida, India, 14-15 Jan-2016

[10] Ahmed M.Abd El-Halan and Ihas A.Ali, "TRIUMF: Trust based routing protocol with controlled degree of selfishness for securing MANET against packet dropping attack", International Journal of Computer Systems, Vol. 8, Issue 4, July-2011, ISSN: 1694-0814

[11] Jaydip Sen, Girish Chandra,Harihara S.G, Harsh Reddy and P. Balamuralidhar, "Mobile Ad-hoc Networks", 7th International Symposium on Communication and Information Technologies, Sydney, NSW, Australia, 17-19 Oct-2007

[12] Mohammad Wazid, Vipin Kumar, RH Goudar, "Comparative Performance Analysis of Routing Protocols in Mobile Ad Hoc Networks under JellyFish Attack", 2nd IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, 6-8 Dec-2012

[13] Mohammad Wazid, Avita Katal, Roshan Singh Sachan, R H Goudar, "E-TCP for Efficient Performance of MANET under JF Delay Variance Attack", Proceedings of IEEE Conference on Information and Communication Technologies, Thuckalay, Tamil Nadu, India, 11-12 April-2013

[14] Sanjay Kumar, "Detection and Prevention of Jellyfish Attack in AODV Routing protocol in MANET", International Journal of Science Technology & Engineering, Vol. 3, Issue 6, Dec-2016, ISSN-2349-784X

[15] Sakshi Garg, Satish Chand, "Enhanced AODV protocol for defense against Jellyfish Attack on MANETs", IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), Greater Noida, India, 24-27 Sept-2014, ISBN; 978-1-4799-3080-7

[15] Vijay Laxmi, Chhagan Lal, M.S Gaur, Deepanshu Mehta, "Jellyfish attack: Analysis Detection and Counter measure in TCP-based MANET" Journal of Information Security and Applications (JISA), Elsevier 2014

[16] Sakshi Sachdeva, Parneet Kaur, "Detection and Analysis of Jellyfish Attack in MANETs", IEEE International Conference on Inventive Computation Technology (ICICT), Coimbatore, India, 26-27 Aug-2016