International Journal for ReseaArch in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

Mitigation of Jellyfish Attack in AODV

Kamna Sharma[1,] Harish Saini[2]
[1,2] Computer Science and Engineering Department, GNI, Mullana, Haryana, India

Abstract: The rapid proliferation of wireless networks, deployment of many mobile computing devices and applications has changed the shape of network security. One such field which needs more security in comparison to wired networks is the mobile ad hoc network (MANET). The term "ad hoc" means self-organized nodes without any centralized infrastructure. In Jellyfish packet dropping attack, the attacking node attracts more data traffic by advertising themselves having the best path to other destinations in the network. Further, these jellyfish nodes selectively drop data packets degrading network throughput. This paper mainly focuses on jellyfish packet dropping attack, its consequences and proposes mechanism for detection & prevention of it in the context of AODV routing protocol. The simulations are carried on NS-2 simulator and performance is evaluated in terms of packet delivery ratio, throughput and routing overhead.
Keywords: Jellyfish attack, Detection, MANET, Security

I. INTRODUCTION

A mobile ad hoc network is a collection of mobile nodes communicating with the help of wireless links without any underlying centralized infrastructure or base station [2]. It is an adaptive self-configurable network so the mobile nodes can be deployed quickly. These networks are very useful in situations where infrastructure is not available or costly to establish, its installation is difficult or has been destroyed [10]. Application set of MANETs is very divergent. MANETs can be applied in military, voting systems, automated battlefields, rescue systems, mobile offices, electronic payments, and virtual classrooms, other emergency and disastrous situations [5]. The characteristics of MANETs pose many issues such as the power constraint of nodes and security issues because of lack of trust relationship among nodes, lack of centralized authority, dynamic topology. The wireless channel is accessible by both legitimate users as well as malicious nodes and there is no clear boundary separating inside network from outside world [1].

Security is major aspect in MANETs, there is need to heal performance of attack affected networks. Jellyfish attack is one such attack that affects network throughput to a great extent. Jellyfish attack selectively drops the packet in network and leads to decreased throughput; thus degrades network performance. In this paper, we will study impact of Jellyfish attack in reactive adhoc routing protocol and a suitable mechanism will be proposed to detect the attack and remove it from the forwarding path created during the route discovery.

II. RELATED WORK

Wazid et al. [3] proposed Cluster Based Intrusion Detection and Prevention Technique (CBIDPT) and Super Cluster Based Intrusion Detection and Prevention Technique (SCBIDPT) for detection and prevention of JF reorder attack. CBIDPT performs well in case of intermediate node acting maliciously and fails when cluster head behaves maliciously whereas SCBIDPT performs well in presence of malicious cluster head also. Cluster head compares all sequence numbers of packets stored in its buffer to the sequence numbers of packets stored in buffer of all intermediate nodes to detect misbehaving node. Ukey et al. proposed I-2ACK [6] for preventing routing misbehaviour and detecting malicious nodes by sending acknowledgement packets back as data packets are received and using simple rating mechanism for counting the number of data packets such that it overcomes the problem of misbehaving nodes. If data packets received are below threshold value, then a misbehaving node is detected. Simulations were performed on NS-2 and results proved that I-2ACK performed better in terms of throughput, packet delivery ratio and data packets dropped in the presence of misbehaving nodes.

Shakshuki et al. proposed an intrusion detection system, namely, EAACK (Enhanced Adaptive Acknowledgment) [7] which utilizes digital signature to prevent an attacker from forging acknowledgment packets. EAACK includes three components: Acknowledge (ACK), Secure-Acknowledge (S-ACK) and Misbehaviour Report Authentication (MRA). EAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report. S-ACK mode makes every three consecutive nodes to work in collusion to detect misbehaving nodes in the presence of receiver collision or limited transmission power. It assumed that nodes are connected by bi-directional links and source node and the destination node are not malicious. Garg and chand [8] proposed enhanced AODV which detects jellyfish delay variance attack on the basis of threshold value. Poongodi and Bose [11] proposed novel IDS based on

trust evaluation for the flooding attack. The proposed TEB-SOT-FCN IDS combines the existing Firecol-based security procedures [4] with Dynamic Growing Self-Organizing Tree Algorithm [9] in the trust evaluation-based environment.
Sharma et al. [13] analyzed various security threats that MANET have suffered and presented the some novel approache for preventing the Jellyfish attacks that are found mostly in TCP based environment. Various variants of the Jellyfish attacks have also been described along with the way how they are affecting the performance of the MANET. Ns-2 is used for simulation the the performance of the proposed work was evaluated in respect to three of the parameters: Packet Delivery Ratio, Throughput and Drop of Packets. Anjugam and Muthupriya [14] proposed a light-weight Direct Trust-based Detection (DTD) algorithm and Monitor, Detect, Rehabilitate (MrDR) technique to detect a JellyFish node from an innovative transmission route. They analyzed the effects of three JF (Jelly-Fish) attack variants: JF-reorder, JF-delay and JF-drop over TCP-SACK.

III. PROPOSED ALGORITHM AGAINST JELLYFISH PACKET DROPPING ATTACK

In Jellyfish attack, attacker intends to minimise throughput of network by either reordering the packet sequence, dropping or delaying the packets [12]. In this attack, attacker node became a part of network after getting access of it. It is similar to blackhole attack with dissimilarity in terms of dropping the packets, blackhole attack drops all the packets but jellyfish (JF) attacker drops periodically.
In our proposed algorithm, secure route is selected using Fuzzy based IDS against jellyfish packet dropping attack. The proposed algorithm takes into consideration two parameters packet delivery rate and average destination sequence number to create fuzzy rule base. In this, each node maintains packet delivery rate and average destination sequence number for each neighbouring node in neighbour table. Every node has to work in the promiscuous mode to listen to the network traffic of its neighbouring node for collecting the input for fuzzy system. Packet delivery ratio is the ratio of number of data packets forwarded to number of packets received. The destination node inserts updated sequence number in RREP packet of AODV The sequence number of any node depends upon its connectivity within the network. A highly connected node will have high destination sequence number and is treated as more reliable node. A malicious node in the network will falsely insert very high value of its destination sequence number in RREP packet in order to be a part of route. So, if a node is jellyfish node, it will transmit highest destination sequence number. In order to check the variation in the sequence numbers, we have calculated average of the difference of destination sequence number between the previous sequence number in the neighbour list and RREP packet received in each time slot. This average destination sequence number is calculated as soon as a node transmits a RREP packet.
In this scenario, a number of combinations of these factors are monitored and a fuzzy rule base is prepared, which yields proper justification to all the participating nodes. Different combinations of the parameters are assigned different trust factors. The nodes with less trust value are treated as jellyfish node and they are further isolated from the network by sending alarm signals to other nodes which in turn discard their control and data packets. Data packets are re-routed via alternate paths which are free from jellyfish nodes.

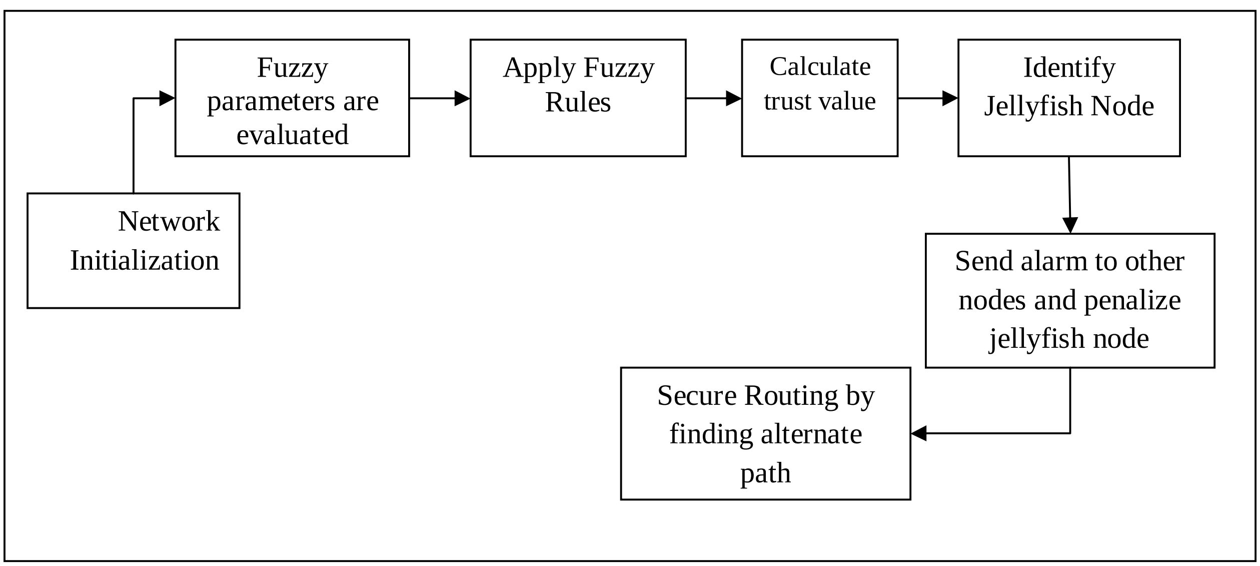

Figure 1 Fuzzy based IDS for secure routing in AODV

Basically, fuzzy logic is a multi-valued logic that enables transitional values to be classified between conventional yes/no like evaluations. Fuzzy logic systems target the approximation and ambiguity of input and output variables by defining fuzzy numbers and fuzzy sets that can be expressed in linguistic variables. A linguistic fuzzy rule is just an "If Then construct" that can be expressed in following way: If X is A Then Y is B.

The average of difference in sequence number is an important factor in a filtering based approach. A malicious node will have high average value. In proposed rule base, High value of this attribute means high probability of being jellyfish node. Low value of packet delivery rate means a node is jellyfish as it is dropping packets. Combinations of different linguistic rules corresponding to Low (L), medium (M) and high (H) levels of the attributes have been used. Next, on the basis of these linguistic rules, a "Trust Value" is assigned with levels: very high, high, medium, low, very low that varies between 0 and 1. Different combinations of these linguistic rules have assigned different trust values. A low trust value means the node may be a attacker and it should be blacklisted. Any control or data packet from a blacklisted node will be ignored and no processing will be performed. This way effect of Jellyfish packet dropping attack can be minimized. Fuzzy logic based algorithm for trust has been devised and it is applied to the calculated trust value of the nodes. These values are treated as fuzzy input variables and the Fuzzy logic based algorithm marks the nodes as either trusted or malicious. The overall flow for secure routing in proposed algorithm is given in Figure 2.

```
Initialize a network with N number of nodes with S as source node and D as destination
node
Set S as current_node
While current_node != D
{
        Identify the list of neighboring nodes to current_node say (NB1, NB2, .......NBm)
        For each neighboring node i=1 to m
        {
                Identify the fuzzy parameters Packet delivery rate and destination
                sequence number for RREP packet
        }
}
Fuzzify these rules under the fuzzification process
Detect the jellyfish nodes
```

Figure 2 Secure routing in AODV

After finding the values of packet delivery rate, the Rule based method assign values (HIGH, MEDIEM , LOW) to the nodes and then assign trust values in the range of [0, 1]. If the assigned trust value of a node is less than threshold value say 0.6, then it is treated as jellyfish node and all other nodes drop packets from attacker for fixed time and then after every fixed time interval repeat the process for getting new values and then again assigning trust value to the nodes and compare again with threshold.

Table 1 Fuzzy Parameters

Packet Delivery rate	Average Destination Sequence Number	Trust factor
Low	High	Low
Low	Medium	Low
Low	Low	Low
Medium	High	Medium
Medium	Medium	Medium
Medium	Low	High
High	High	High
High	Medium	High
High	Low	High

Table 2 Fuzzy discrimination

Fuzzy levels	Trust Values	Semantics
High	0.8 to 1	Benign
Medium	0.8 to 0.6	Benign
Low	0.6 to 0	Jellyfish node

IV. SIMULATION ENVIRONMENT AND RESULTS

This section presents the topology and different parameters used in the simulation process. This simulation process considered a wireless network of nodes which are placed within a 1000m X 1000m area. CBR (constant bit rate) traffic is generated among the nodes. The simulation runs for 100 seconds.

Table 3 Simulation Parameters

Parameter	Value
Simulation time	100 Sec
Simulation area	1000m x 1000m
Antenna	Omni antenna
No. of nodes	10, 20, 30, 40
Speed	5, 10, 15, 20
Pause Time	1, 2, 5, 10
Packet size	512 Bytes
Max queue length	50
Traffic	CBR (Constant bit rate)
Routing protocol	AODV
Transport Layer	UDP
Data Rate	2Mbps

A. Effect of jellyfish attack and proposed algorithm on PDR

It is clear from Figure 3 and 4 that PDR of AODV is drastically affected by the presence of jellyfish nodes in the network where as PDR of proposed algorithm is immune to it. The graphs confirm that AODV under proposed algorithm is secure against jellyfish nodes and AODV is not. PDF drops from 86.98% to 39.58% in presence of jellyfish attack and with our scheme it improves by 83.45% in presence of single jellyfish node. As malicious node increases in Figure 4, more packets are dropped so PDF further drops to 22% and with our scheme it regains back to 78.11%.

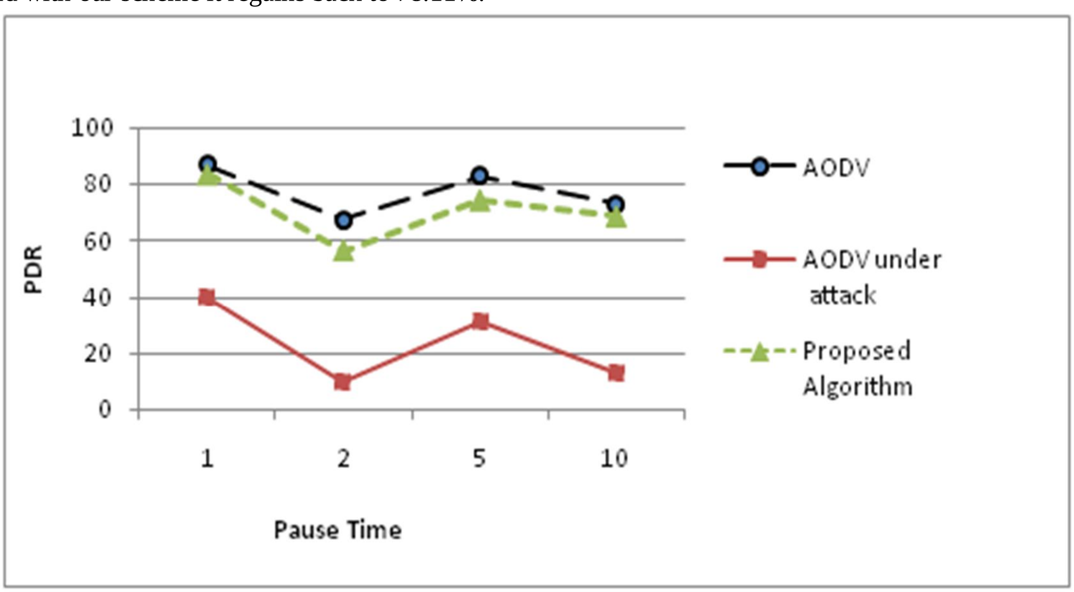

Figure 3 PDR vs Pause time in presence of single malicious node

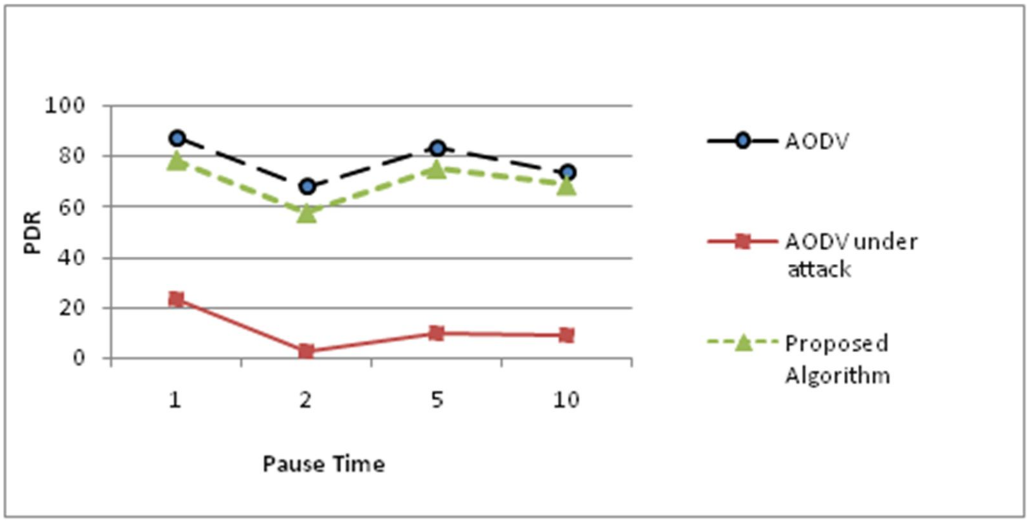

Figure 4 PDR vs Pause time in presence of two malicious nodes

B. Effect of jellyfish attack and proposed algorithm on routing overhead

In Figure 5 and 6, it is observed that there is slight increase in routing overhead of our scheme, which is quite negligible. The routing overhead increases by just 1.01% with proposed algorithm which is tolerable.

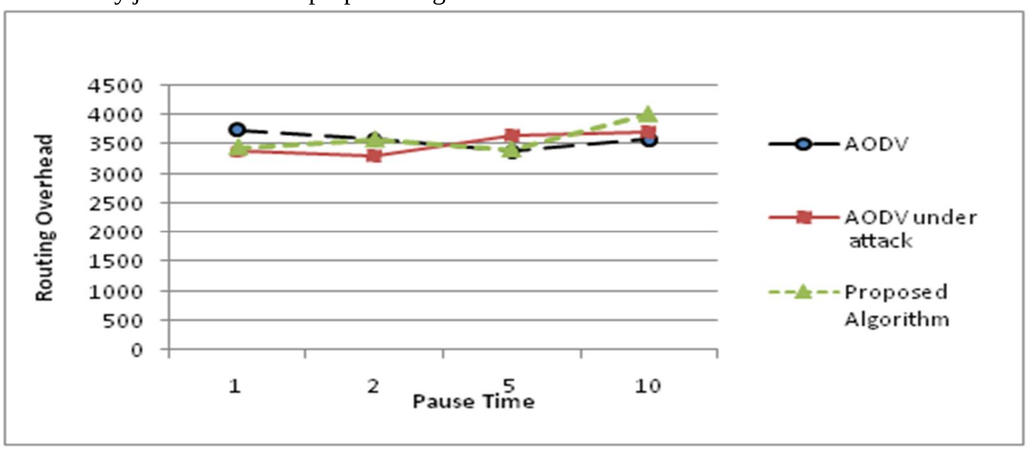

Figure 5 Routing Overhead vs Pause time in presence of single malicious node

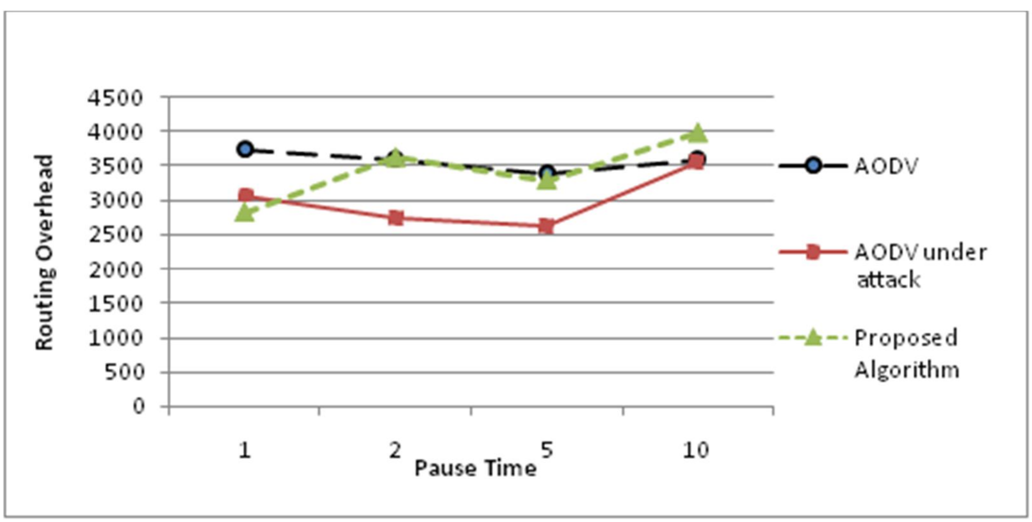

Figure 6 Routing Overhead vs Pause time in presence of two malicious nodes

C. Effect of jellyfish attack and proposed algorithm on throughput

Figure 7 and 8 shows the effect of pause time on the throughput. There is huge difference between the throughput for AODV and AODV under attack. High pause time means less mobility and more stable network but when pause time increases then the node will not move and throughput decreases. With AODV, without attack, its throughput is higher than in the case with under attack because of the packets dropped by jellyfish node.

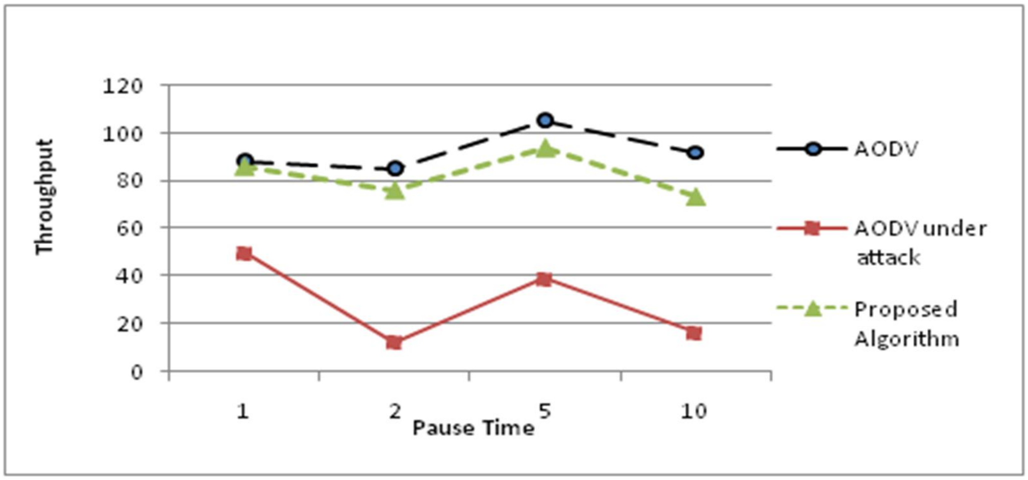

Figure 7 Throughput vs Pause time in presence of single malicious node

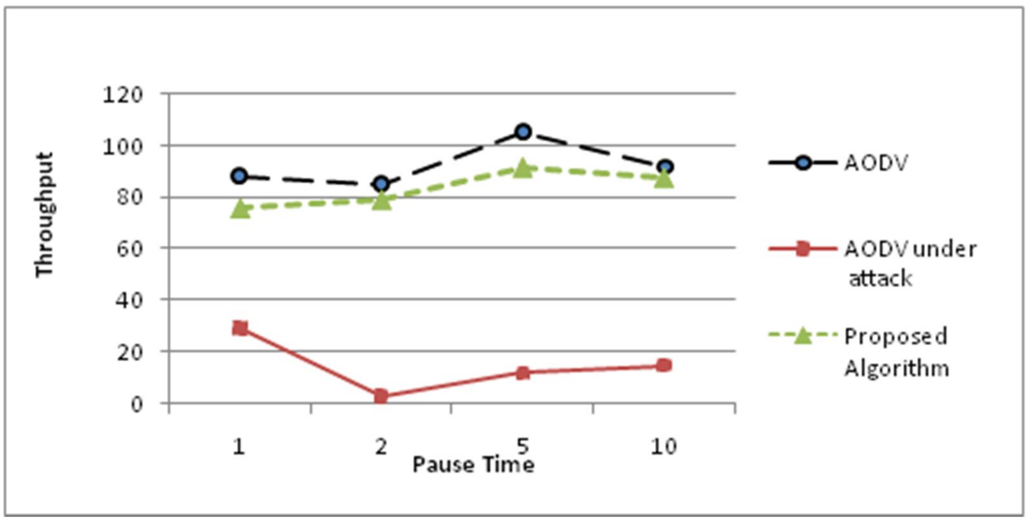

Figure 8 Throughput vs Pause time in presence of two malicious nodes

As throughput is the ratio of the data received from source to the time taken by the receiver. As the jellyfish nodes immediately send fake route reply and thereafter drops data packets, the network throughput is much lower. The throughput of network drops by 43% with single jellyfish node and throughput rises by 92% with our proposed algorithm. The throughput of network drops by 67.02% in presence of two malicious nodes which increases by 85% with proposed algorithm.

V. CONCLUSION AND FUTURE WORK

In this paper, we emphasized over the Jellyfish packet dropping attack in MANET. We simulated the jellyfish packet dropping attack in the ad-hoc networks and investigated its affects. Having simulated the jellyfish attack, we saw that the packet loss is increased. Simulation results show significant difference between the number of packets lost in the network with and without jellyfish attack. We also proposed an algorithm based on fuzzy rule base and demonstrated the result outcomes in the form of graphs. Results presented here clearly demonstrate the performance in terms of PDR, routing overhead and throughput. Future enhancement of this approach may include some other fuzzy parameters for better detection. The mitigation algorithm can also be modified to thwart other routing attacks such as blackhole, Sybil, wormhole etc in the future.

REFERENCES

[1] Yang H., Luo H., Ye F., Lu S., and Zhang L., "Security in mobile ad hoc networks: challenges and solutions." Wireless Communications, IEEE, vol. 11, no. 1, pp. 38-47, 2004.

[2] Nguyen H.L and Nguyen U.T, “A study of different types of attacks on multicast in mobile ad hoc networks”, Ad Hoc Networks, vol. 6, no. 1, pp. 32-46, 2008.

[3] Wazid, M., A. Katal, and R. H. Goudar, "Cluster and super cluster based intrusion detection and prevention techniques for JellyFish Reorder Attack."Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on. IEEE, 2012.

[4] François, J.; Aib, I.; Boutaba, R.: FireCol: a collaborative protection network for the detection of flooding DDoS attacks. IEEE/ACM Trans. Netw. 20(6), 1828–1841 (2012)

[5] Bhatia, T. and Verma, A.K., 2013. Security issues in MANET: a survey on attacks and defense mechanisms. International Journal of Advanced Research in Computer Science and Software Engineering, 3(6), pp. 1382-1394.

[6] Ukey, A.S.A., Chawla, M. and Singh, V.P., 2013. I-2ACK: Preventing Routing Misbehavior in Mobile Ad hoc Networks. International Journal of Computer Applications, 62(12), pp. 34-39.

[7] Shakshuki, E.M., Kang, N. and Sheltami, T.R., 2013. EAACK—a secure intrusion-detection system for MANETs. Industrial Electronics, IEEE Transactions on, 60(3), pp.1089-1098.

[8] Garg, Sakshi, and Satish Chand, "Enhanced AODV protocol for defence against JellyFish Attack on MANETs." Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014.

[9] Poongodi, M.; Bose, S.: A firegroup mechanism to provide intrusion detection and prevention system against DDoS attack in collaborative clustered networks. Int. J. Inf. Secur. Priv. 8(2), 1– 15 (2014).

[10] Kaur Harvaneet, “A Survey on Manet Routing Protocols”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, 2015

[11] Poongodi, M., & Bose, S. (2015). A Novel Intrusion Detection System Based on Trust Evaluation to Defend Against DDoS Attack in MANET. Arabian Journal for Science & Engineering (Springer Science & Business Media BV), 40(12).

[12] H.P. Chatar and S.Waghmare, "Vehicular Ad Hoc Networks (VANETS): Attacks and Challenges: A Survey," International Journal of Electronics, Electrical and Computational System (IJEECS), vol. 4, no. 4, pp. 60-64, 2015.

[13] Sharma, P., Rai, K., Jain, D. and Rai, B.L., Hybrid Method for MANET Security against Jelly Fish, Blackhole and DoS. International Journal of Computer Applications Volume 139 – No.11, April 2016pp. 20-24.

[14] Anjugam, S., & Muthupriya, V. “Direct Trust-Based Detection and Recovery Process of Jellyfish Attack in Manet”. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) Volume 22 Issue 2 – MAY 2016, pp. 32-38