Detection and Prevention of Jelly Fish Attack

Shina Karwal[1]

[1,2]*GGS College, Kharar*

Abstract*— Mobile ad hoc networks (MANETs) are vulnerable to various types of attacks due to inherently insecure wireless communication medium and multihop routing communication process. In this research, we analyze the behavior and impact of JellyFish attack over MANETs. We implement and evaluate all three variants of JellyFish attack namely JF-reorder, JF-delay and JF-drop through simulation processes. These attacks exploit the behavior of closed loop protocols such as TCP and disturb the communication process without disobeying any protocol rules, thus the detection process becomes difficult. Consequently, traffic is disrupted leading to degradation in network throughput. Through extensive simulation results that are obtained using an industry standard scalable network simulator called MATLAB, impact of these attacks in terms of network throughput, overhead incurred and end-to-end delay is analyzed and used for devising detection and countermeasure. We propose a light-weight direct trust-based detection (DTD) algorithm which detect and remove a JellyFish node from an active communication route. Simulation results are provided, showing that in the presence of malicious-node attacks, the CBDS outperforms the existing and compared with proposed JF detection scheme in terms of packet delivery ratio and routing overhead.

***Keywords*—**

I. INTRODUCTION

Mobile Ad Hoc Network is an autonomous system of mobile nodes, which are connected by various wireless links and in which each node behaves as a router, So as to forward the packet data to the neighboring node. Principle of Mobile Ad Hoc Network is that nodes are free to join and leave the network and there is no central administration. This is the infrastructure less network. This type of networks experiences the dynamic topology.

There are lots of unsolved problems in ad hoc networks; securing the network being one of the major concerns. Ad hoc networks are vulnerable to attacks due to many reasons; amongest them are lack of secure boundaries, threats from compromised nodes within the network, lack of centralized management facility, restricted power supply, scalability[1]. Mobile Adhoc Networks have various flaws which make it more vulnerable to attacks[5].

Attackers are always trying to modify messages or generate false messages and thus take down the network's operations which cause denial of service in MANETs..Tremendous progress has been made in order to ad hoc networks by developing secure routing protocols that ensure different security concepts such as authentication and data integrity. Moreover, intrusion detection and trust-based systems have been developed to protect MANETs against misbehaviors such as rushing attack, query flood attacks, and selfish behaviors. Yet, most of the defense mechanisms are not able to detect a set of protocol compliant attacks called jellyfish (JF) attacks. Jelly fish attack is one of the denials of service attack and also a type of passive attack, which is difficult to detect. It produces delay before the transmission and reception of data packets in the network. Applications such as HTTP, FTP and video conferencing are provided by TCP and UDP. This attack disturbs the performance of both protocols. It is same as black hole attack but the difference is that the black hole attacker node drops all the data packets but jelly fish attacker node produces delay during forwarding packets. Attackers can also scramble packet ordering before delivering packets to the destination node. ACK based flow control mechanism generates duplicate ACK packets in the network. Jellyfish attack is primarily targeted towards closed loop flows with the ultimate goal to disrupt normal operation of the network by packet dropping.The goal of jellyfish node is to diminish the good put, which can be achieved by dropping some of packets. When a malicious nodes launches forwarding rejection attacks it also may comply with all routing procedures. A malicious node launching Jellyfish attacks may keep active in both route discovering and packet. In the existing approach the Jelly Fish node is hard to locate so the network is always prone to attack. In the existing approach the false alarm is an issue. False alarm is a parameter in which the attack is not simulated but the technique pretends as attack is simulated. In order to avoid these problems of Jelly Fish attack,we proposed the Fuzzy based APD_JFAD technique in this research

II. JELLY FISH ATTACK

Jellyfish attack comes under the classification of passive attack and is regarded as a type of Denial of Service (DoS) attack. It maintains complete compliance with control and data protocols for making detection and prevention highly challenging tasks to work upon. Jellyfish attack introduces delay in network before any sort of transmission and receipt of packets happen between the communicating nodes. Jellyfish attack degrades the performance of both TCP and UDP packets and performs in the same manner like Blackhole attack. The only difference is that, in black hole attack, the infected node drops all the packets whereas Jellyfish malicious node introduces delay during packet forwarding. Attackers can also scramble packet ordering before delivering packets to the destination node. ACK based flow control mechanism generates duplicate ACK packets in the network. Jellyfish attack is primarily targeted towards closed loop flows with the ultimate goal to disrupt normal operation of the network by packet dropping. Jellyfish attack is highly vulnerable in TCP traffic in which cooperative nodes can hardly distinguish between attacks from network congestion.

Attackers are always trying to modify messages or generate false messages and thus take down the network's operations which cause denial of service in MANETs. In this section we summary introduce JELLY FISH Attack. Tremendous progress has been made in order to ad hoc networks by developing secure routing protocols that ensure different security concepts such as authentication and data integrity. Moreover, intrusion detection and trust-based systems have been developed to protect MANETs against misbehaviors such as rushing attack, query flood attacks, and selfish behaviors. Yet, most of the defense mechanisms are not able to detect a set of protocol compliant attacks called jellyfish (JF) attacks. Jelly fish attack is one of the denials of service attack and also a type of passive attack which is difficult to detect. It produces delay before the transmission and reception of data packets in the network. Applications such as HTTP, FTP and video conferencing are provided by TCP and UDP. Jelly fish attack disturbs the performance of both protocols. It is same as black hole attack but the difference is that the black hole attacker node drops all the data packets but jelly fish attacker node produces delay during forwarding packets. Jelly fish attacks are targeted against closed loop flows. TCP has well known vulnerabilities to delay, drop and mis-order the packets. Due to this, nodes can change the sequence of the packets also drop some of the data packets. The jelly fish attacker nodes fully obeys protocol rules, hence this attack is called as passive attack [3]. Jelly fish attacks are targeted against closed-loop flows. The goal of jellyfish node is to diminish the good put, which can be achieved by dropping some of packets. When a malicious nodes launches forwarding rejection attacks it also may comply with all routing procedures. The Jellyfish attack is one of those kinds. A malicious node launching Jellyfish attacks may keep active in both route discovering and packet forwarding in order to prevent it from detection and diagnosis, but the malicious node can attack the traffic via itself by r eordering packets, dropping packets periodically, or increasing jitters. The Jellyfish attack is especially harmful to TCP traffic in that cooperative nodes can hardly differentiate these attacks from the network congestion. Reference also described that malicious nodes may even abuse directional antenna and dynamic power techniques to avoid upstream nodes to detect their misbehaviors of dropping packets. This attack mainly targets closed-loop flows as such flows respond to network conditions like packet loss and packet delay. It targets TCP's congestion control mechanism. The main goal of the Jellyfish nodes is to reduce the good put of all the flows to near-zero by either reordering the packets or dropping a small fraction of packets. [4] These forwarding mechanisms are variants of Jellyfish attack.

III. JELLYFISH ATTACK CLASSIFICATION

Jellyfish attack is further classified into three sub categories Jellyfish recorder attack, Jellyfish periodic dropping attack and Jellyfish Delay variance attack.

Jellyfish Reorder Attack Jelly Fish Reorder attack is possible due to well known vulnerability of TCP. Jelly fish attacker uses this vulnerability to record packets. This is possible because of factors such as route changes or the use of multi path routing.

Jellyfish Periodic Dropping Attack Periodic dropping is possible because of sarcastically chosen period by the mischievous node. This kind of periodic dropping is possible at relay nodes. Suppose that congestion losses force a node to drop α% of packets. Now consider that the node drops α% of packets periodically then TCPs throughput may be reduced to near zero even for small values.

Jellyfish Delay Variance Attack In this type of attack, the malicious node randomly delays packet without changing the order of the packets.

Effects of Jelly Fish Attack This attack compliance with all data and control protocols as a result its detection and diagnosis is quite difficult to dete ct. This attacks effects mainly closed- loop flows as such these flows respond to network conditions like packet loss and packet delay

IV. APD JFAD

APD-JFAD study defines a novel method for detecting and combating Jellyfish attack in MANET called the Accurate Prevention and Detection of Jellyfish Attack Detection (APD-JFAD). MANETs is surrounded by tons of different attacks, each with different behavior and aftermaths. The Jellyfish attack is regarded as one of the most difficult attack to detect and degrades the overall network performance. In the APD-JFAD, node property based hierarchical trust evaluation was carried out so that only trusted nodes are selected for route path construction.[1] Support Vector Machine was used to perform packet forwarding learning. The proposed technique was validated using NS-2 simulator and compared with 3 other existing techniques i.e. ABC, MABC and AR-AIDF-GFRS algorithms by various parameters such as throughput, PDR, dropped packet ratio and delay.[1]

In the existing approach the Jelly Fish node is hard to locate so the network is always prone to attack.

In the existing approach the false alarm is an issue. False alarm is a parameter in which the attack is not simulated but the technique pretends as attack is simulated. So in the proposed approach the accuracy of attack detection is to be improved by which the false alarm will be reduced.

Malicious node generates tremendous amount of junk packets in the network preventing legitimate nodes from gaining access to the communication channel for transmission of data or control messages.

Malicious node generates control packets carrying incorrect topological information leading to false entries in other nodes' routing table.

After receiving control messages, a malicious node can delay the dissemination process. As a result, the information in these control messages might become incorrect as it may not correspond to recent change in the network topology.

V. RELATED WORK

In this section, we have a tendency to summarize and discuss connected authentication ways employed in follow or

projected within the literature to boost positive identification authentication on the net and gift their limits.

Doss, S.; et al. [1] proposed a novel technique called accurate prevention and detection of jelly fish attack detection (APD-JFAD) to combat Jellyfish attack in MANETs. It is a fusion of authenticated routing-based framework for detecting attacks and support vector machine (SVM). SVM is utilized for learning packet forwarding behavior. The proposed technique chooses trusted nodes in the network for performing routing of packets on the basis of hierarchical trust evaluation property of nodes. The technique is tested using NS-2 simulator against other existing techniques, i.e., ABC, MABC, and AR-AIDF-GFRS algorithms by various parameters such as throughput, PDR, dropped packet ratio, and delay. One of the serious attacks that affect the normal working of MANETs is DoS attack. A sort of DoS attack is Jellyfish attack, which is quite hard because of its foraging behavior.

Sajjad, M. et al. [2] analyzed the performance of Dynamic Source Routing (DSR) routing protocol in the presence of Jellyfish attack. To evaluate the performance we have created different scenarios having various number of Jellyfish attacks in MANETs environment. From the simulation result, it has been observed that Jellyfish attack significantly degrades the performance of DSR protocol in terms of end to end delay, throughput and packet delivery ratio. Moreover it has also been observed that when the number of Jellyfish attacks increases in the network then the performance is further degraded.

Bhawsar, D. and Suryavanshi, A. [3] developed a prevention scheme against the jellyfish attack in MANET environment. Simulation is done in NS2. Here the performance is evaluated on the basis of number of attacker nodes identify in the network along with number of infected packets injected in the network by the attacker nodes to degrade the performance of the network along with the routing overhead of the network. Mobile Ad-Hoc Networks (MANET) are group of mobile adhoc nodes which could correspond with one to another by using multihop links which are wireless. MANETs are very frequently deployed in various those environments, where there is no centralized management and fixed infrastructure.

Bhalsagar, S.S.; et al. [4] given overview of some conventional protocols such as AODV, DSDV and DSR protocols. Different types of malicious attacks such as Black hole, Gray hole, Jellyfish and Wormhole Attack are studied. In this paper, how trust based scheme will help in overcoming the adverse effects due to the presence of malicious nodes is given. The trust based schemes are introduced in a protocol in order to avoid addition of a malicious node in the route by assigning it a trust value. Also a comparative analysis has been done between the preventive Trust Based Protocols that ensure high security and minimize the effects of these malicious attacks. The DSR protocol under Black hole attack is implemented and the performance is analysed with respect to Packet Delivery Ratio, Throughput, Number of Received Packets and Average End-toend Delay. The improvement in these factors of a protocol will make it more secure and reliable. Thus, it will be applicable to be employed in the fields where security is of utmost importance.

Batra, J. and Krishna, C.R. [5] presented a machine learning approach that is Feed Forward Back Propagation Neural Network (FFBPNN) as a classifier and Ad hoc On-Demand Distance Vector(AODV) routing protocol for route discovery to shield the network from Distributed Denial of Service (DDoS) attack. The MANET is trained using FFBPNN. Therefore, when malicious node appears in the network, the node is identified on the basis of the node properties like energy consumption and delay. The route is changed by discarding the malicious nodes from the route and hence the network is protected. In the existing work, it has been found that the researchers have utilized Support Vector Machine (SVM) and fuzzy logic as a classification algorithm to identify the DoS attack in MANET. The problem with SVM and Fuzzy logic is that they are more complex and more time consuming mechanism to detect attackers

Kaur, M. et al. [6] gave an overview that Jellyfish attack has gained its name recently in attack scenario in Mobile Ad hoc networks. JellyFish Attack exploits the end to end congestion control mechanism of Transmission Control Protocol (TCP). Mobile Adhoc Networks have become a part and parcel of technology advancements due to its working as autonomous system. MANET networks are vulnerable to various types of attacks and threats due to its unique characteristics like dynamic topology, Shared physical medium, distributed operations and many more. There are many attacks which effect the functioning of MANETS' such as denial of service which is most commonly used to affect the network is one of the types of attacks in MANETS.

Subramanian, P.; [7] proposed a lightweight direct trust-based detection (DTD) algorithm which detect and remove a Jellyfish node from an active communication route. Simulation results are provided, showing that in the presence of malicious-node attacks, the IDS outperforms the existing and compared with proposed JF detection scheme in terms of packet delivery ratio and routing overhead and analyze the behavior and impact of Jellyfish attack over MANETs. We have implemented and evaluated all three variants of Jellyfish attack namely JF-reorder, JF-delay and JF-drop through simulation processes. These attacks exploit the behavior of closed loop protocols such as TCP and disturb the communication process without disobeying any protocol rules, thus the detection process becomes difficult. Consequently, traffic is disrupted leading to degradation in network throughput.

Mamatha, C. R. and Ramakrishna, M.; [8] proposed open areas in which the performance of the network may be improved by considering energy-efficient networks, achieving stability in the network and finding better routes. The nodes are independent and communicated with each other by self-organizing among those nodes to provide the global network functionality. It draws more attention in recent years because of enormous applications and its cost-effective implementation. The communication among these nodes

entirely depends on the routing path and battery power. Many researches have concentrated only on finding the shortest path and throughput in this area. The energy-efficient routing has a lot of scope and important factor to be considered for routing in MANET's.

VI. PROPOSED WORK

During preliminary study, it has been studied that for creating any network some assumptions are taken into account. There are a number of parameters that are assumed before the simulation like Frame Duration, frequency Bandwidth, Mode of transmission, network size etc. The area taken into consideration is 100*100m and the simulation time to be considered is 300sec. For the implementation of coverage techniques in WSN, simulation parameters used are shown in Table 1:

Table 1 Simulation Parameters for Jellyfish attack detection

Simulation parameters	Value
Frame duration	1ms
Frequency bandwidth	25MHZ
Mode of transmission	TDD
Number of mobile stations	20, 40, 60, 80, 100
Packet size	5kb
Simulation grid size	100m*100m
Rounds	3000
Initial Energy	0.5J
Energy for transmission	50*0.000000001J
Energy for reception	50*0.000000001J
Energy for Amplification	0.0013*0.000000000001J
Energy for Data Aggregation	5*0.000000001J

In this research we define 5 scenario in which 20, 40, 60, 80 and 100 nodes are deployed so that the scalability of the proposed algorithm can be verified.

In the fig 1 flow of work is defined in which following steps are involved.

First of all Manet nodes are deployed and routing schemes are applied to transfer packets. For routing of packets AODV routing protocol is used. After packet transmission jelly fish attack is simulated on the MANeT to perform attack simulation.

Now existing scheme that is APD-JFAD (Accurate Prevention and Detection of Jelly Fish Attack) is applied on network so that attack can be detected and prevented. But this approach did not get the jelly fish node i.e. attacker node so to prevent the node from attacking network proposed model is applied in which the existing protocol APD-JFAD is optimized and attacker node is blacklisted so that the network can be saved from attack and Jelly fish attack can be mitigated.

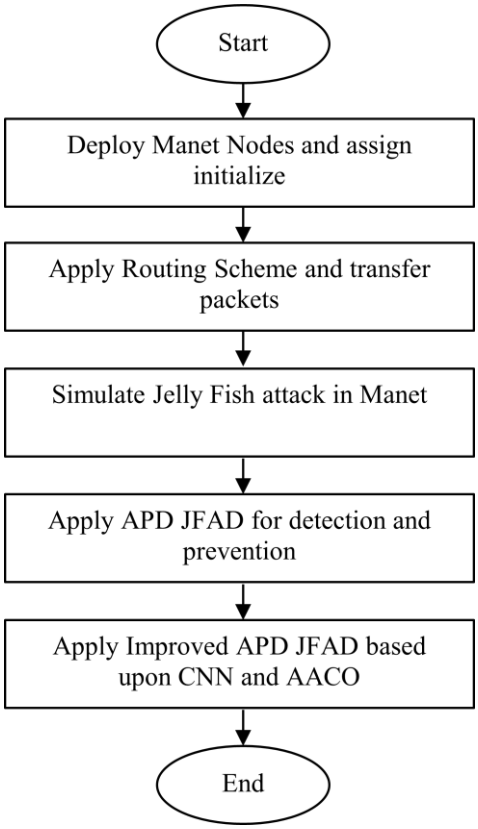

Fig 1: Flow Chart

At the end results are generated and then compare it with APD-JFAD

VII. RESULTS AND DISCUSSION

In this research various performance metrics are improved by using the optimization schemes that is ant colony optimization and adaptive ant colony optimization. The effect on various QoS parameters such as Packet Delivery Ratio, Overheads, Average End-to-End Delay, Throughput, Average Energy Consumption have been observed by varying the no. of nodes i.e. 20,40,60.80 and 100 nodes at the constant speed of 100m/s by taking constant twenty number of rounds. Firstly by taking the 20 number of nodes the values are plotted against packet delivery ratio. Then the mean of that ten values are taken and we get one value. The whole process is repeated for 40, 60, 80, 100 no. of nodes. Similarly the values are plotted against throughput, overhead, average energy consumption and average end-to-end delay.

Packet Delivery Ratio

Figure 2 shows the PDR in APD-JFAD(existing technique) and Fuzzy based APD-JFAD (proposed technique) the values are plotted against no. of nodes and packet delivery ratio on abscissa and ordinate. Fuzzy based APD-JFAD shows better results as compared to the APD-JFAD. From the graph shown below it may be defined that the average value of Packet Delivery Rate in APD-JFAD is least i.e. 0.68 whereas in case of Fuzzy based APD-JFAD it is quite better and it is 0.8. According to this figure the proposed results shows 12.5%

improvement in packet delivery ratio. If there is link breakage or there is a dead node in a network due to more energy dissipation; then we use the reciprocal path generated by AACO, as a result of which losses are reduced thus the packet drop is reduced so packet delivery ratio is improved in Fuzzy based APD-JFAD.

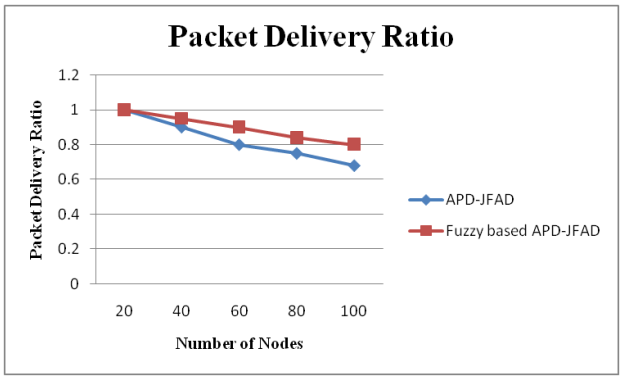

Fig 2: Comparison of PDR in APD-JFAD (Existing) and Fuzzy based APD-JFAD (Proposed)

Average End-to-End Delay

Figure 3 shows the Average End-to-End Delay in APD-JFAD(Existing technique) and Fuzzy based APD-JFAD (Proposed technique) the values are plotted against no. of nodes and delay on abscissa and ordinate. The values are plotted against the varying nodes. From the graph it may be seen that the value of Average End-to-End Delay in APD-JFAD is most i.e. 0.25 sec whereas in case of Fuzzy based APD-JFAD it is quite better and it is 0.135 sec. According to this figure the proposed results shows 4.5% improvement in average end to end delay. If there is a link down in the network; that energy of any node goes below the desired level then message will not reach to the destination in time. Due to which the messages are delayed in order to reduce this delay the message packets are forwarded to the new path that is generated by the AACO optimization technique. Hence Fuzzy based APD-JFAD will show better results than other two.

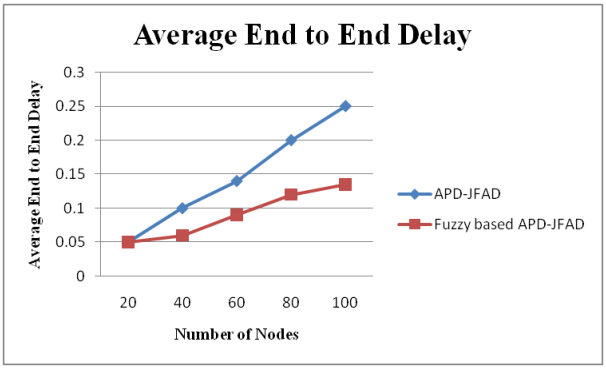

Fig 3: Comparison of Average End-to-end delay in APD-JFAD (Existing) and Fuzzy based APD-JFAD (Proposed)

Overhead:

Figure 4 compares the overhead in APD-JFAD (Existing technique) and Fuzzy based APD-JFAD (Propsoed technique). The result is plotted against the overhead bitts and number of varying nodes. From the graph it may be defined that the average value of overheads in APD-JFAD is most i.e. 1.1 whereas in case of Fuzzy based APD-JFAD it is quite better and it is 0.8. According to this figure the proposed results shows 27% improvement in overheads. As the packet drop is reduced due to new path generation the packet delivery ratio is improved; all the packets are delivered in time as the result of which overhead is reduced in Fuzzy based APD-JFAD.

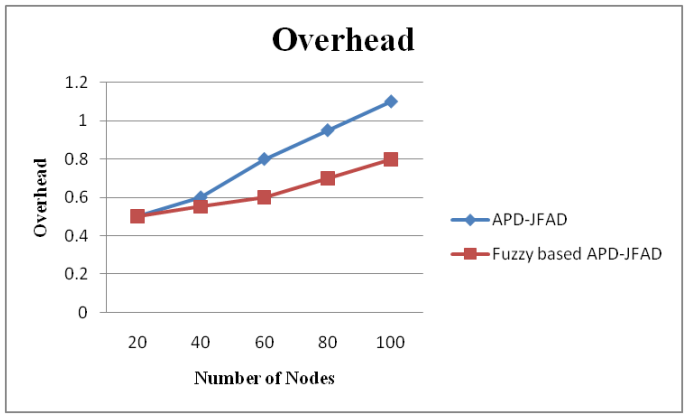

Fig 4: Comparison of Overhead in APD-JFAD (Existing) and Fuzzy based APD-JFAD (Proposed)

Throughput

Figure 5 represented the relation between APD-JFAD (Existing technique) and Fuzzy based APD-JFAD (Proposed technique). Fuzzy based APD-JFAD shows better results as compared to the existing protocol. From the graph it may be defined that the average value of throughput in APD-JFAD is least i.e. 1000 bits whereas in case of Fuzzy based APD-JFAD it is quite better and it is 1200 bits. According to this figure the proposed results shows 20% improvement in throughput. As the packets will take the reciprocal path more no. of packets will reach to the destination without any loss; which means maximum number of data bits will reach successfully to the sink hence throughput of Fuzzy based APD-JFAD is improved than the other two.

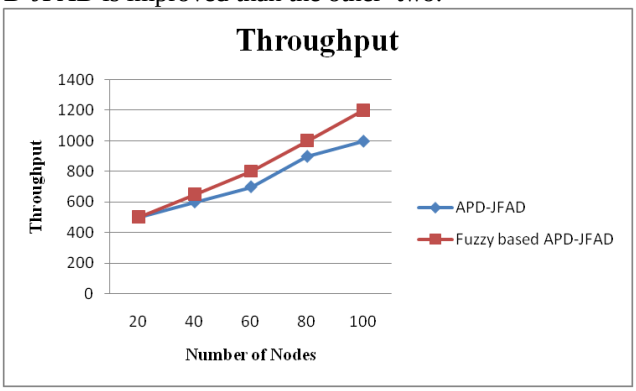

Fig 5: Comparison of Throughput in APD-JFAD (Existing) and Fuzzy based APD-JFAD (Proposed)

Average Energy Consumption:

Figure 6 shows that there is less energy consumption in Fuzzy based ADP-JFAD (Proposed technique). From the graph it may be defined that the average value of Average Energy consumption in APD-JFAD is more i.e. 0.0015 joule .whereas in case of Fuzzy based APD-JFAD it is quite better and it is

0.001 joule. According to this figure the proposed results shows 12.5% improvement in average energy consumption. As the packet drop is less; the re-transmission attempts for sending the message to receiver are less. So as a result of which there is less energy dissipation and hence there is less energy consumption in optimized scheme as compared to the existing protocol.

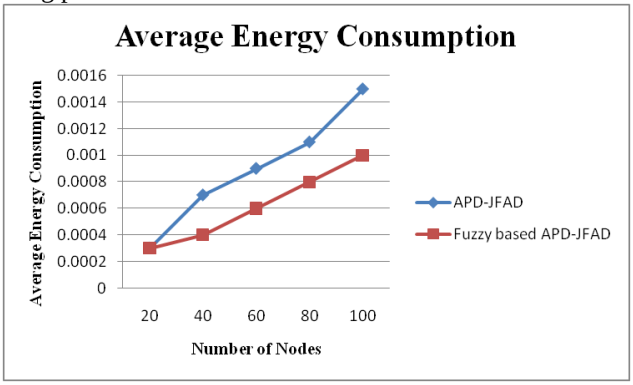

Fig 6: Average Energy Consumption in APD-JFAD (Existing) and Fuzzy APD-JFAD (Proposed)

Table 1: Comparative study for APD-JFAD and Fuzzy based APD-JFAD

Technique / Parameters	APD-JFAD (Existing)	Fuzzy Based APD-JFAD (Proposed)
Packet delivery ratio	.76	0.9
Average end-to-end delay(sec)	.14	.25
Overheads(bits)	1.1	0.6
Throughput(bits)	1000	1200
Average energy consumption(joule)	.0011	.0013

Tabular comparison of existing protocol parameters and protocol with optimization scheme is shown in table 1. We compare two techniques APD-JFAD(existing) and Fuzzy based APD-JFAD(proposed) in this table along with diffent-2 parameters. The values of all the performance metrics packet deliver ratio, overhead, throughput, average end-o-end delay, average energy consumption is shown in the following table against the number varying nodes that is 20, 40, 60, 80, 100 nodes.

VIII. CONCLUSION

In this research, a detailed performance evaluation of Jelly Fish attack (JF-reorder, JF-delay and JF-drop) over AODV based MANETs is presented. Based on the simulation results generated over various MANET scenarios with varying number of attackers, intermediate hops and attack parameters, it has been observed that Jelly Fish attack causes network performance degradation in terms of network throughput, end-to-end delay and control overhead.

There is analysis of performance of AODV protocol without jellyfish attack, with jellyfish attack and the proposed prevention scheme against jellyfish attack. Ad-hoc network play very critical role in many fields ranging from military applications to other house hold applications. It is very vital to handle security in data transmission in such cases which is very much challenging due to their infrastructure less behavior. It is very much clear that the performance of the proposed work — Defending against Intrusion and Prevention of Jellyfish Attack Approach for Detecting Malicious Node in MANET performs better.

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.

IX. REFERENCES

[1]. Doss, S.; Nayyar, A.; Suseendran, G.; Tanwar, S.; Khanna, A.; Son, L.H.; Thong, P.H.; "APD-JFAD: Accurate Prevention and Detection of Jelly Fish Attack in MANET", IEEE, vol: 6, 2018, pp: 56954-56965

[2]. Sajjad, M.; Saeed, K.; Hussain, T.; Abbas, A.W.; Khalil, I.; Ali, I.; Gul, N.; "Impact of Jelly Fish Attackonthe Performance of DSR Routing Protocol in MANETs", Journal Of Mechanics Of Continua And Mathematical Sciences, vol: 14, 2019, pp: 132-140

[3]. Bhawsar, D.; Suryavanshi, A.; "Collaborative Intrusion Detection and Prevention against Jellyfish Attack in MANET", International Journal of Computer Applications, vol: 129, 2015, pp: 1-6

[4]. Bhalsagar, S.S.; Chawhan, M.D.; Suryawanshi, Y.; Taksande, V.K.; "Performance Evaluation Of Routing Protocol Under Black hole Attack In Manet And Suggested Security Enhancement Mechanisms", International Journal of Innovative Technology and Exploring Engineering, vol: 8, 2019, pp: 1-7

[5]. Batra, J.; Krishna, C.R.; "Ddos Attack Detection and Prevention using Aodv Routing Mechanism and Ffbp Neural Network in a Manet", International Journal of Recent Technology and Engineering, vol: 8, 2019, pp: 4136-4142

[6]. Kaur, M.; Rani, M.; Nayyar, A.; "A Comprehensive Study of Jelly Fish Attack in Mobile Ad hoc Networks", International Journal of Computer Science and Mobile Computing, vol: 3, 2014, pp: 199-203

[7]. Subramanian, P.; "An Efficient Trust-Based Detection System for Defending Intrusion and JF Attack in MANET", International Journal of Multidisciplinary Research Transactions, vol: 1, 2019, pp: 13-21

[8]. Mamatha, C. R.; Ramakrishna, M.; "An Assessment on Energy Efficient Protocols for MANETS", International Journal of Engineering and Advanced Technology, vol: 9, 2019, pp: 1556-1561