Survey on Delay Based Jellyfish Attack

[1]Mr. Ankit M Vaghela, [2]Prof. Mayank Gour, [3]Prof. Ashish Patel
[2]Assistant Professor, [3]Assistant Professor
[1, 2, 3]Computer Engineering Department,
[1, 2, 3]Silver Oak College of Engineering & Technology, Ahmedabad, Gujarat, India

Abstract— Mobile ad-hoc network (MANET) is more vulnerable to different types of attacks due to its insecure communication medium, no centralize administration and dynamic forming topology. Jellyfish is a new type of DOS attack, which is focus on closed loop protocols like TCP and it, create problem in the communication process without violating any protocols rules thus, detection of this type of attack become quite difficult. A main target of this attack is to decrease the throughput and increase the end-to-end delays, which drastically affect the network, which leads to degrade the overall performance of network. In our research, we are going to analyze behaviour and impact of Jellyfish attack over a TCP based MANET under the AODV protocol and propose a new technique, which can be used to detect and mitigate the Jellyfish delay variance (JFDV) attack using Network Simulation 2(NS2).

Index Terms— Jellyfish attack, JFDV, Jellyfish Delay Variance attack, MANET, DOS attacks, AODV, E2E delay, and Jitter.

I. INTRODUCTION

All A mobile ad hoc network is a self-organizing network of mobile nodes that communicate with each other using wireless links with no fixed infrastructure or centralized administrations. In addition, nodes in a MANET act as both hosts as well as router to forward packets to other in a multi-hop fashion. MANETs are used for applications in which no infrastructure exist such as military battlefield, emergency rescue, vehicular communications and mining operations.[1]There are lots of open research issues available in MANET due to its open medium. Among all the research issues, security is an essential requirement in MANET environments. Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority, lack of trust relationships between mobile nodes, easy eavesdropping because of shared wireless medium, dynamic network topology, low bandwidth, and battery and memory constraints of mobile devices [1].

In this paper, we present a study the effects of different types of attacks in MANETs. We study how the number of attackers and their positions affect the performance of a connection in terms of packet delivery ratio, throughput, end-to-end delay, and delay jitter. In our literature review, we used AODV (Ad hoc On-demand Distance Vector) [2] as the routing protocol due to its popularity. The existing studies considered only one performance metric, namely the packet delivery ratio (PDR). We, on the other hand, provide a comprehensive study by examining several other important metrics such as throughput, end-to-end delay and delay jitter, which are critical to many real-time applications. We consider many common types of attacks, namely black-hole attack, jellyfish attack etc. out of them we focus on Jellyfish attack because of its passive nature and it is quite difficult to detect this attack. We divided our work into two sections. First we analyze the behavior of DOS attacks after that we discuss the effect of jellyfish attack on MANET and types of Jellyfish attacks. In second section, we proposed a new technique which going to detect the jellyfish delay variance attack and measure the some network parameters such as throughput, end-to-end delay, jitter etc.

DOS ATTACKS [13]

A Denial of Service attack is a special type of attack on network, which disturb or shutdown the network by flooding it with lots of useless traffic. Following are the types of DOS attacks [3].

A. Blackhole Attack[13]

Blackhole attack target the AODV routing protocol in which a malicious node publicizes itself as having the shortest path to the destination. If the reply sent by malicious node reaches the requesting node before the reply packet sent by the actual node then a malicious route is created and this results in packets not being forwarded to actual destination, which allows the malicious node to intercept the packets and drop them.

B. Wormhole Attack[13]

The Worm Hole attacker creates a tunnel in order to record the ongoing communication and traffic at one node and channels it to another node in the network [4].

C. Grayhole Attack[13]

The attacker node drops some selective packets t hat pass through it [4] [13].

D. Jellyfish Attack [4]

This attack is due to the vulnerability of TCP.. Jellyfish attack is a type of passive attack which is difficult to detect because the attacker disobey any of the protocol rules. Cutting down the good put of the traffic to minimum or zero either by dropping the data packets or by changing the order of the data packets. It is similar to blackhole attack, the only means by which it is different from blackhole attack is that in blackhole attack the attacker node drops the data packets but in jellyfish attack packets are delayed before transmission of packets and after reception of packets in the network[4][13]. It has three types, Jellyfish delay variance attacks, Periodic dropping attacks and jellyfish reorder attack.

E. Rushing Attack[13]

A node required a route to a destination and its floods the network with ROUTE REQUEST packets in an attempt to find a route to destination. To limit the overhead of this flood, each node typically forwards only one ROUTE REQUEST originating from any Route Discovery.

F. Selfish Node Misbehaving[13]

A node refusing to forward packets in order to conserve its limited resources is termed a 'selfish node'. This behavior causes network and traffic disruptions [4][13].

AODV PROTOCOL [6][7]

AODV is described in RFC 3561 [15]. When a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network. There are three types of control messages in AODV which are discussed below.

- **Route Request Message (RREQ) [6]:** Source node that needs to communicate with another node in the network transmits RREQ Message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.
- **Route Reply Message (RREP)[6]:** A node having a requested identity or any intermediate node that has a route to the requested Node generates a route reply RREP message back to the originator node.
- **Route Error Message (RERR)[6]:** Every node in the network keeps monitoring the link status to its neighbour's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.
- **Route Discovery Mechanism in AODV[6]:** When a node "A" wants to initiate transmission with another node "G" as shown in the Figure 1, it will generate a route request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forwarded to the neighbour's, and those nodes forward the control message to their neighbour's nodes. This process of finding destination node goes on until it finds a node that has fresh enough routes to the destination or destination node is located itself. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is established between "A" and "G", node "A" and "G" can communicate with each other. Figure 1 depicts the exchange of control messages between source node and destination node.

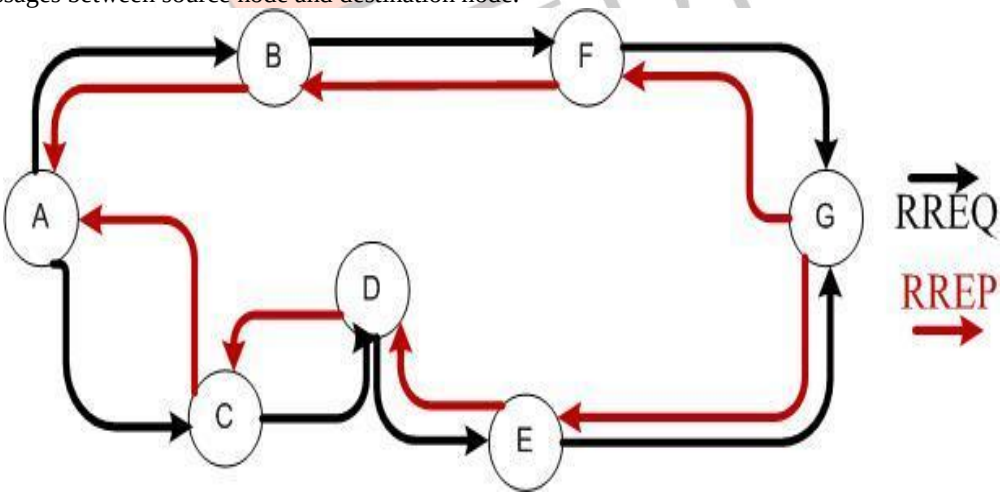

Figure 1 AODV Route Discovery [14]

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbours nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating the destination node i.e. from the node "A" to the neighbours nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error, where "A" is source node and "G" is the destination node. The scheme is shown in the Figure 2 below.

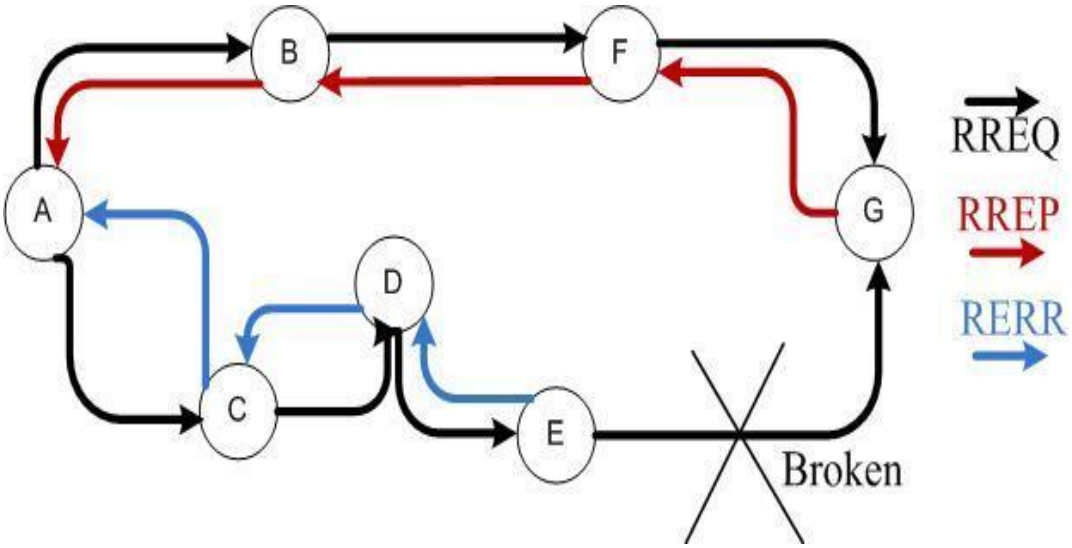

Fig. 2 Route Error Message in AODV [14]

II. JELLYFISH ATTACKS [6][12]

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 reordering packets, dropping packets periodically, or increasing jitters [3].The Jellyfish attack is especially harmful to TCP traffic in that cooperative nodes can hardly differentiate these attacks from the network congestion. As shown in Figure-2, node JF is a Jellyfish, and node S starts to communicate with node D after a path via the Jellyfish node is established. Then the DoS attacks launched by node JF will cause packet loss and break off the communications between nodes S and D eventually [3][6].

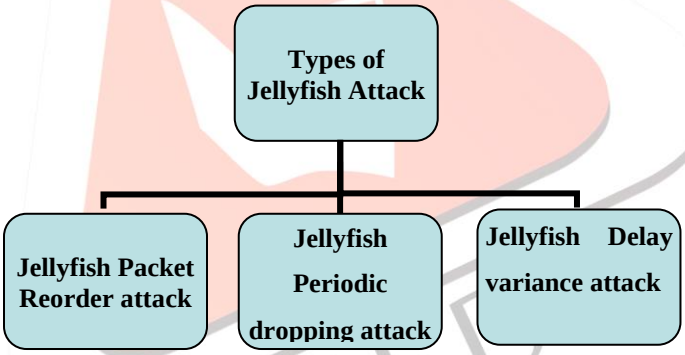

Fig. 3 Types of Jellyfish attacks [5]

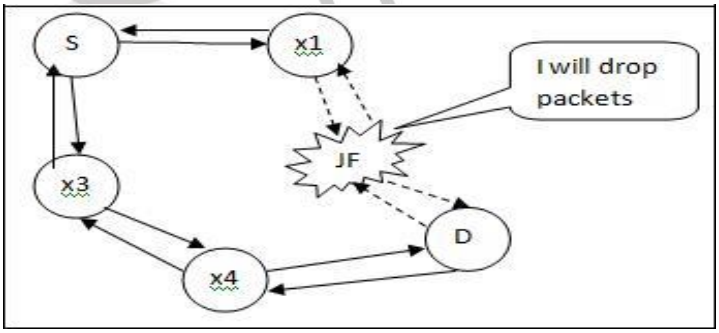

Fig. 4 Jellyfish attack scenario [3]

Jellyfish Packet Reorder attack [6]

In this type of attack, malicious nodes forward the packets in random order from the queue, instead of forwarding them in FIFO order. Packets can be placed in a random buffer in place of FIFO buffer [2]. Diagram of JF reorder attack is shown in figure 4. Buffer is reordered by jellyfish node and packets are sent from the buffer. At the destination side, when packets do not arrive in actual order, duplicate acknowledgement is sent to the sender. If three duplicate acknowledgements are received at the sender side, retransmission of packets is started without waiting for retransmission timeout. Even if the packet has reached the destination side, sender still believes that packet is lost and may keep retransmitting the packet [2].

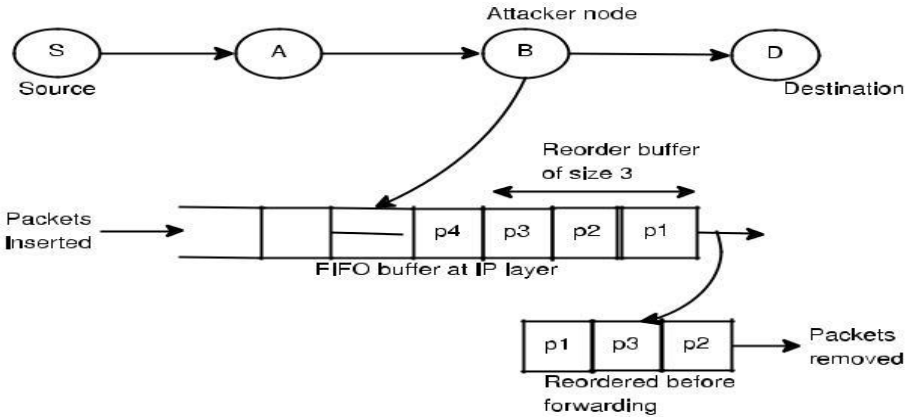

Fig. 5 Jellyfish Reorder attack [4]

Jellyfish Periodic dropping attack [6]

Periodic dropping attack is usually possible at relay nodes. Due to congestion, a node is forced to drop packets and if node drops packets periodically then TCP throughput will reduce to zero [2].

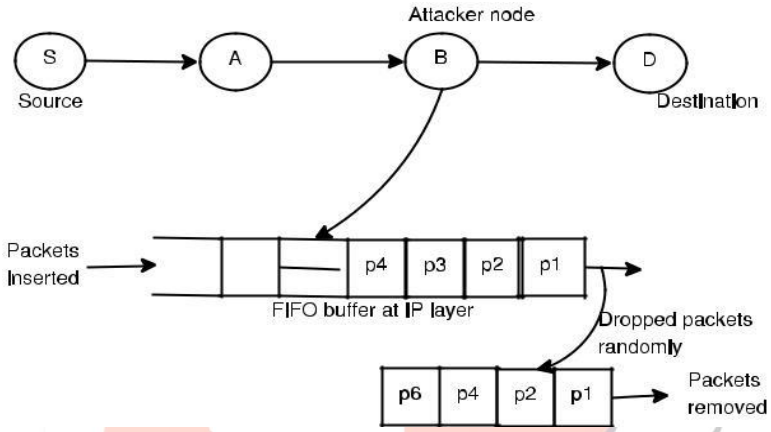

Fig. 6 Periodic dropping attack [4]

Jellyfish Delay variance attack [6][12]

In this attack, order of packets is not altered but packets are delayed in random manner. Malicious node has to acquire access to the routing paths and after that all the packets it receives are delayed before forwarding [2].

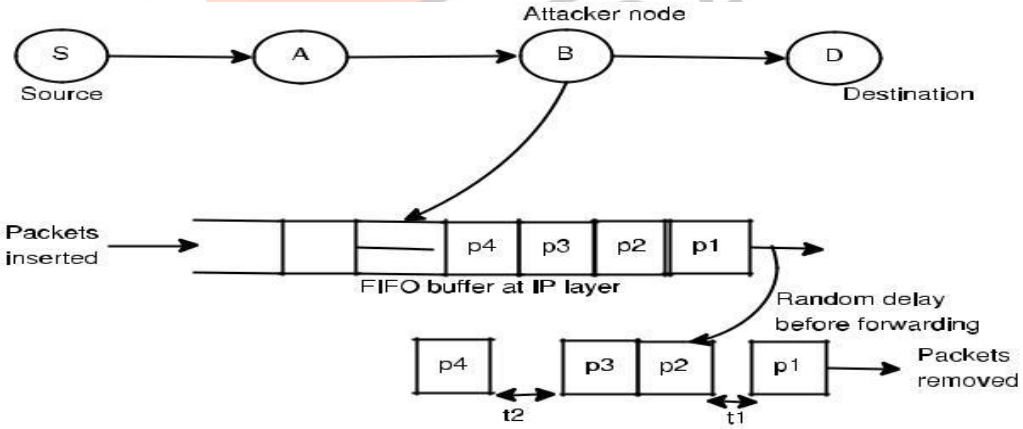

Fig. 7 Jellyfish Delay variance attack [4]

Some Existing Technique to Detect and Prevent Jellyfish attack

- Cluster Based Intrusion Detection and Prevention Technique (CBIDPT)[2[9]].
- Super Cluster Based Intrusion Detection and Prevention Technique (SCBIDPT)[2][9].
- Detection of jellyfish reorder attack using parameters like displacement frequency and reorder density [2].
- Detecting jellyfish delay variance attack using E-TCP [2][10].
- A Time Space Cryptography Hashing Solution for Prevention Jellyfish Reordering Attack in Wireless Ad hoc Networks[5].
- Enhanced AODV protocol[8]
- Secure Link establishment method to prevent Jelly Fish Attack [11].

III. IMPLEMENTATION STRATEGIES

As shown in below figure First we will install the NS2(Network Simulator 2) and learn the basic command of NS 2. In the second step, we will move on MANTE in which we will create one Mobile Ad hoc Network using AODV routing protocols. Then after we will analyze the behavior of Network without Jellyfish attack and with more than two Jellyfish node measure the End to End delay, Jitter, Packet delivery ratio, etc. Lastly using some network parameters such as Jitter, E2E delay, we will detect the jellyfish attack.

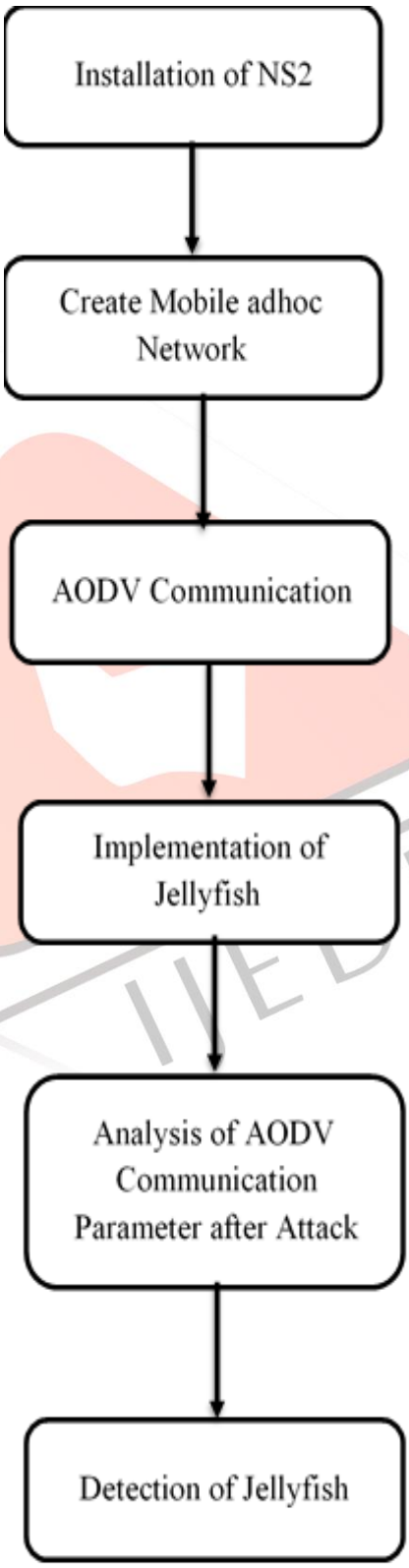

Fig. 8 Implementation Strategy

IV. CONCLUSIONS AND FUTURE WORK

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Hence Security of MANET is one of the important features for its deployment. In this paper we have analysed the behaviour and challenges of security threats in MANET and also discussed the few of DOS attacks out of them our main focus is on jellyfish attack because it's a new kind of DOS attacks and it is a Protocol variant attack. Although many solutions have been proposed but still those are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it may not be applicable in case of multiple malicious nodes. Survey includes the analysis the effect of jellyfish attack on performance of network and at the still more research required in Jellyfish Attack.

In our next paper we will present implementation details of Jellyfish attacks. First, we will create the MANET network under the AODV protocol and measure performance parameter like throughput, end to end delay, Packet dropping ration(PDR) etc. using NS2. Then after we will implement jellyfish delay variance attack (JFDV) in normal network and measure the performance parameters and at the last we will detect the jellyfish attack using one of the Network parameter which is still not used by anyone and compare simulation result with the normal network simulation result.

V. ACKNOWLEDGMENT

I am sincerely thankful to my Guides, Prof**. Ashish Patel** and **Prof. Mayank Gour for** their constant encouragement, valuable guidance and constructive suggestion during all the stages of the literature review and other faculty members who have directly or indirectly helped me whenever it was required by me.

REFERENCES

[1] Mr. Hoang Lan Nguyen, Mr. Uyen Trang Nguyen, "A Study of different types of attack in Mobile Ad hoc Network", IEEE 2012.

[2] Mr. Simranpreet Kaur, Mr. Rupinderdeep kaur, Mr. A.K. Verma, "Jellyfish attack in MANETs: A Review", IEEE 2015.

[3] Nidhi Purohit, Richa Sinha and Khushbu Maurya, "Simulation study of Black hole and Jellyfish attack on MANET using NS3" IEEE 2011.

[4] Vijay Laxmi, Chhagan Lal*, M.S. Gaur, Deepanshu Mehta, "Jellyfish attack: Analyze, detection and countermeasure in TCP based MANET", Science Direct 2014.

[5] Hetal P. Patel, Prof. M.B.Chaudhari, "A Time Space Cryptography Hashing Solution for Prevention Jellyfish Reordering Attack in Wireless Ad hoc Networks", IEEE 2013.

[6] Mohammad Wazid,Vipin Kumar,R H Gaudar, "Comparative Performance Analysis Of Routing Protocols in Mobile Ad Hoc Networks Under Jellyfish Attack," International Conference On Parallel, Distributed and Grid Computing On IEEE, 2012.

[7] Sunil J Soni, Suketu D Nayak, "Enhancing Security Features & Performance Of AODV Protocol Under Attack For MANET", 2013 International Conference On Intelligent Systems And Signal Processing IEEE, 2013.

[8] Sakshi Garg, Satish Chand, "Enhanced AODV protocol for defense against Jellyfish Attack on MANETs", IEEE, 2014.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[9] Avita Katal, R HGoudar, Mohammad Wazid "Cluster and Super Cluster Based Intrusion Detection and Prevention Techniques for Jellyfish Reorder Attack", 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, IEEE 2012.

[10] Roshan Singh Sachan, Avita Katal, R HGoudar, Mohammad Wazid, "E-TCP for Efficient Performance of MANET under JF Delay Variance Attack", Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013), IEEE 2013.

[11] Ashish Thomas, Vijay Kr. Sharma, Gaurav Singhal, "Secure Link establishment method to prevent Jellyfish Attack in MANET" International Conference on Computational Intelligence and Communication Networks, 2015.

[12] Avani Sharma, Rajbir Kaur, Purnendu Karmakar, "JFDV Attack: Influence on Workability of Mobile Ad- hoc Networks", Sixth International Conference on Computational Intelligence, Communication Systems and Networks, IEEE 2014.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[13] Ankit Agrawal, Dr .A.K.Verma,"A review & impact of Trust Schemes in MANET", ACM 2016.

[14] P. Kuppusamy, Dr. K.Thirunavukkarasu, Dr. B Kalaavathi "A Study and Comparison of OLSR, AODV and TORA", On IEEE 2011.

[15] Manjot Kaur, Malti Rani, Anandnayyar, "Acomprehensive Study of Jelly Fish Attack in Mobile Ad Hoc Networks", IJCSMC, Vol. 3, Issue. 4, April 2014.