Mitigation and Detection of Jellyfish Delay Variance Attack in MANET

Ankit M. Vaghela[1], Prof. Ashish Patel[2]
Department of Computer Engineering
[1,2] Silver Oak College of Engineering and Technology

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 delay which drastically affects 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 proposes a new technique which can be used to detect and mitigate the Jellyfish delay variance (JFDV) attack using Network Simulation 2(NS2).*

Keywords- Jellyfish attack, JFDV, Jellyfish Delay Variance attack, MANET, DOS attacks, AODV, E2E delay, and Jitter.

I. INTRODUCTION

The mobile Ad-hoc network (MANET) is an infrastructure less network under wireless communication. It is transfer information without the central administration. [7]. Arbitrary nodes move in random motions so that each node must therefore be intelligent and every node acts as a router and processor and transmit a packet to other nodes. If the receiving node outside the communication ranges then send node send the packets to intermediate node [12]. Due to the open medium and high mobility the network topology may change randomly and unpredictably [4] [5].

MANET widely used in, commercial sector, Military War, LAN, Personal Area Network, (PAN), and the hybrid network.

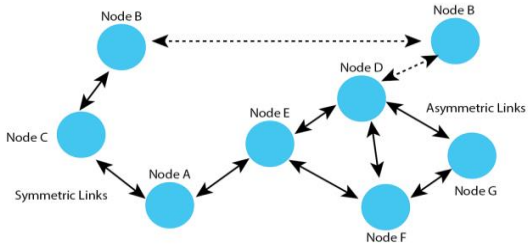

Fig. 1: Mobile Ad hoc Network

As shown in figure if Node F is within a communication range of node G then we can say that communication channel is Symmetric.

Due to the open Medium any node can join or leave the network chances of intruders are more so security is one of the most important mechanisms, these mechanisms are used to detect and respond to security attacks [6]. Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The confidentiality, integrity, availability of network services can be achieved by assuring that security issues have been met. MANET is highly vulnerable to security threats and attacks because of its features like dynamic topology, open medium, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism [6].

In this paper, first the extensive literature review is presented regarding the Mobile Ad hoc Network and their different security issues. Second, Define Security goal and taxonomy of Security attacks. Third, discuss about the types of jellyfish attacks and their effects on networks. Then after discussed about proposed work, Research Methodology, and Simulation tools. Last we implemented jellyfish node and observed the behavior of network with 25,50 and 75 normal nodes. At the end we conclude our thesis and discuss the future scope of our work.

II. RELATED WORKS

In the [01] paper authors discussed important Security issues of MANET and types of Denial of service attacks like Wormhole, Black hole, Jellyfish etc. Then after they explained Jellyfish attack in details like how it affects the network. And end authors discussed some existing Technique for Detection and Prevention of Jellyfish attack like Cluster and Super Cluster based Intrusion Detection and Prevention techniques. The Paper [02] discussed Networking model and TCP flow and congestion control. Also paper proposed light weight direct trust based detection (DTD) algorithm which first detect and prevent jellyfish node from the established communication path. Authors implemented DTD algorithm and shown the result that jellyfish node is detected and prevented from

communication route. In the Paper [03] authors explained DOS attacks in details and assessed the behavior of Jellyfish attack and Black hole attack they also proposed countermeasure of these attacks. Authors also studied these attacks in variety of settings and they have provided quantification of the damage they can inflict. In the Paper [04] author done the comparative protocols performance analysis of AODV, DSR, and TORA and authors also provided the protocols works best in under Jellyfish attack. Last they provided the real time application of this experiment. Paper [5] showed the some modification in AODV protocols for detection and prevention of jellyfish attack without the knowledge malicious node. A Paper [06] shown the Simulation study of Jellyfish attack and Black hole attack and shown the how these attacks damage the throughput of the network. In the paper [07] authors made and analyzed the impact of jellyfish re-orders attack and proposed a protocol for MANET. They also showed the simulation result of Throughput, Average E2E delay, Mobility etc. The paper [08] provided efficient TCP protocol which works best under the jellyfish attack. As per the result shown in paper end to end delay is reduced and throughput is increased by doing some modification in TCP. In the paper [09] author discussed Jellyfish Packet Reorder attack in detail and shown its effect on MANET for that they have done the scheme uses time space cryptography and edited SHA-1 (mSHA-1) hash function for verifying whether the packets are reorder or not. In the paper [10] author presented a results of network performance under the Jellyfish attack with reactive (AODV) and proactive protocols (DSDV and OSLR). Also they have presented the comparison of these protocols and shown the AODV is more vulnerable to JFDV attack compared to DSDV and OSLR. Paper [11] proposed new security technique in order to provide security to AODV routing protocol. In this paper authors merged digital signature and hash chain to secured AODV protocol which is able to defend against malicious node and unauthorized node with marginal performance difference. In the paper [13] authors presented comparative study of different routing protocol like TORA, AODV, DSDV, etc. In the paper [14] provided simulation result of Jellyfish reorder effect on Delay, Throughput etc. In the paper [15] author presents results on the Network QoS parameters like Routing Load, Delay, Throughput, PDR for application of MANET in big network and small network also showed comparison between protocols under large and small scale networks. In the paper [16] authors shown the comparison between routing protocols.

III. PROBLEM STATEMENT

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. In MANET there is no centralized authority available hence it can easily deploy whenever we required . Due to the open Medium any node can join or leave the network any times therefore chances of intruders are more. Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The confidentiality, integrity, availability of network services can be achieved by assuring that security issues have been met. MANET is highly vulnerable to security threats and attacks because of its features like dynamic topology, open medium, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism [6]. Hence Security of MANET is one of the important features for its deployment as well as smooth functionality of network. As we seen in the literature review there are so many types of attacks available which affect the network drastically and it's also compromise the security of network. So. It is necessary to provide clear defence mechanism in order to protect network from attacks and security threats. 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. Still more research required in Jellyfish attack as per our literature review because it impact the network drastically.

IV. PROPOSED METHODOLOGY

As shown in proposed flowchart, First we choose one node that wish to send data, So selected node send a route request packet(RREQ) to all its neighbors and wait for the reply packet(RREP).If reply is arrived within a time then we consider route is secure and we can send the data over selected route. If reply is not received within a time then we consider a something went wrong and send the RERR packet to source node and choose an alternative route. Perhaps, in case of link failure we can also send RERR packet because in wireless network nodes are continuously moving so its link failure is the normal problem in wireless network. Here we used a AODV protocol for routing.

While data transmitting we continuously measure the QOS parameters and checking that any drastic changes found or not. If there is drastic variance found in QOS parameters then we can consider that something malicious happening inside the network. Thus, we stop the data transmission on that route and must choose an alternative route.

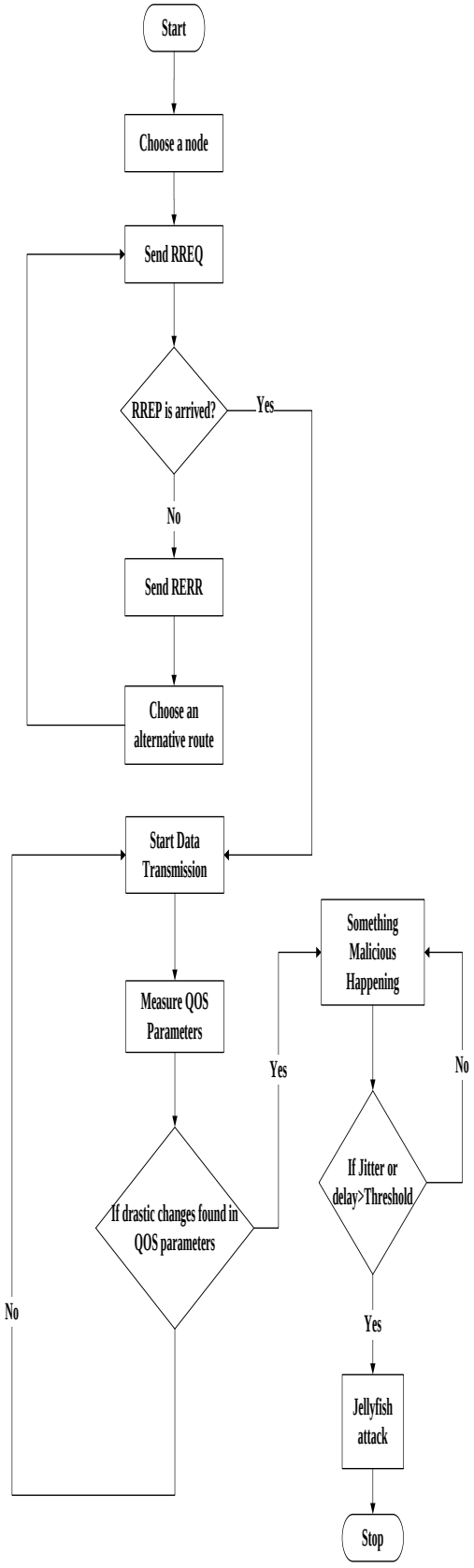

Fig.2 Proposed Methodology

Up to now AODV works, now we check that what the exact problem in network is. So we check each parameter and verify its result with normal network. If high delay variance in End to End to delay or Jitter is found then we conclude that Jellyfish attack is presence inside the network.

V. IMPLEMENTATION

Table 1 Common Parameters used in Simulation

Parameter	Value
Platform	Windows 10
Simulator	Ns2
Area	1*1 KM (FIX)
Node size	25 node(FIX)
Mobility model	Random
Traffic type	FTP
Simulation time	1 minute
Address mode	IPV4
Protocol	AODV
AODV Parameters	Default
Jellyfish Attacker	Zero for Normal flow Five for attacking flow

Table 2 MANET Traffic Generation Parameters used in Simulation

Parameters	Value
Start time(ms)	0.1ms
Packet arrival time	Exponential
Packet size	Constant(1024)
Destination IP add	Random
Stop time	End of Simulation

For the proposed work we are using the following methodology:

Here we are tacking three scenario for different node density E.g 25 nodes,50 nodes, 75 nodes

Table 3 MANET Traffic Generation Parameters used in Simulation

Parameter	Value
BSS Identifier	Auto Assigned
Physical characteristic	Direct Sequence
Data rate	0.1 Mbps
Channel setting	Auto Assigned

Transmit power	0.005
Threshold	Phase 1 - 1ms

Following table shows the analysis for 25 nodes network.

Above table shows relationship between numbers of malicious node density and its associate end to end delay this results shows that as numbers of malicious nodes increase amount of end to end delay increase which is our detection factor

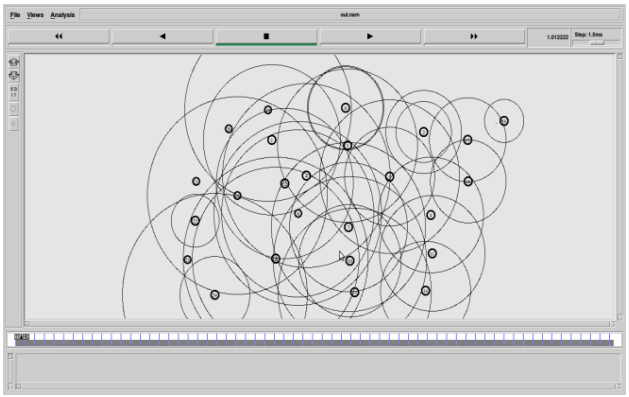

Fig.3 AODV Communication Animation

For experimental purpose we have simulated a Mobile Ad Hoc Network under delay variance JF attack using NS2 simulator. We are using the above simulation scenarios in this paper:

In figure 1 we use 25 mobile nodes and build a scenario without any JF attacker. It's a normal flow of traffic.

In figure 2 we use 25 mobile nodes and build a scenario with four JF attackers. JF attackers are shown in red label i.e. attacker1, attacker2 etc.

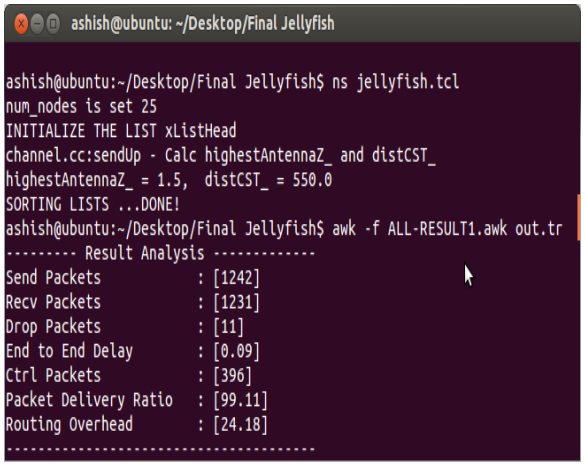

Fig.4 AODV Communication result

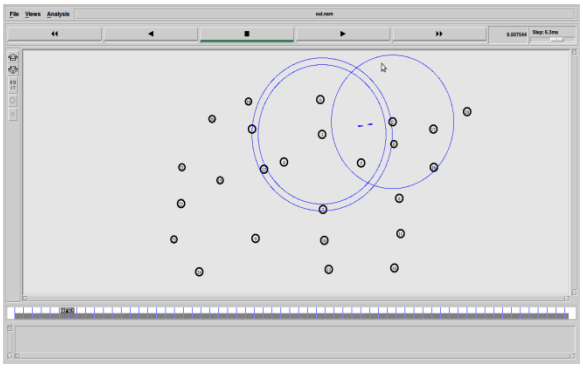

Fig.5 AODV under attack

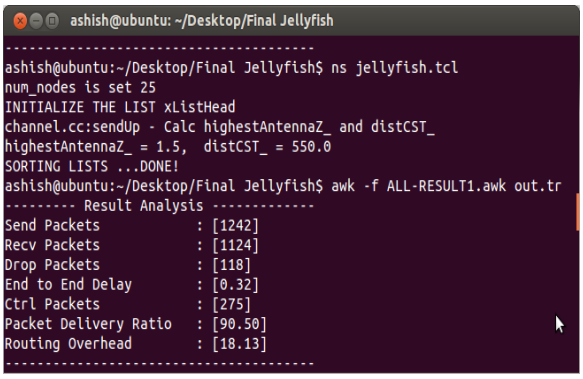

Fig.6 AODV with one node infected

Here, end to end delay increased with one node is JF node and also drastic packet drops as occurred more.

Packet End-to-End Delay

Packet end-to-end delay in case of Jellyfish attack and without attack depends on the Protocol routing procedure and number of nodes involved. In Figure 7.1, delay in case of 25 Nodes for AODV.

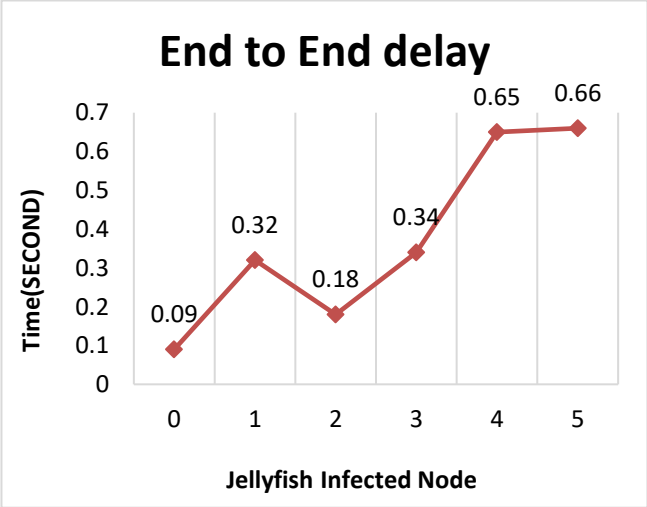

Fig.7 Analysis of End to End Delay

Table 4 Analysis Table of End to End Delay

Jellyfish Infected Node	End to End delay(sec)
0	0.09
1	0.32
2	0.18
3	0.34
4	0.65
5	0.66

Throughput

Throughput without jellyfish attack is high as per graph shown but once we increase the malicious nodes it will decrease the throughput drastically and affect the network.

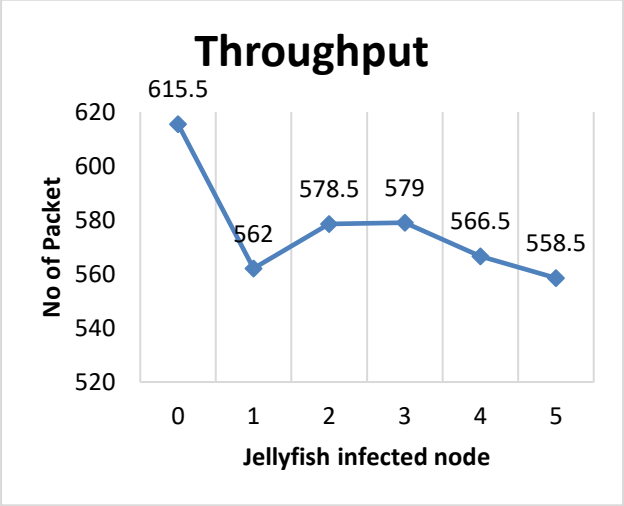

Fig.8 Throughput Analysis

Table 5 Analysis Table of Throughput

Jellyfish Infected Node	Throughput (kbps)
0	615.5
1	562.0
2	578.5
3	579.0
4	566.5
5	558.5

Routing Load

The Routing load graph of AODV with and without presence of a malicious node has been shown in the Figure. The Routing load is decrease when malicious node affect on AODV.

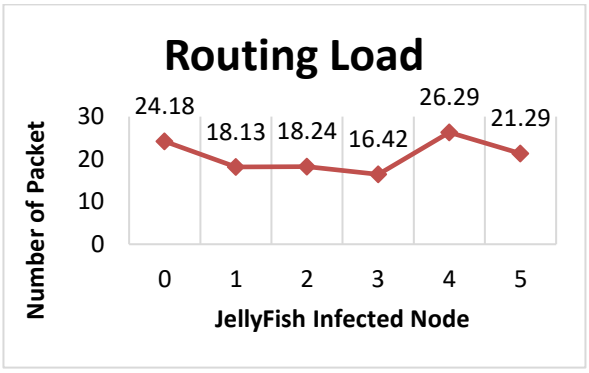

Fig.9 Routing Load Analysis

Table 6 Analysis Table of Routing Load

Jellyfish Infected Node	Routing Load (kbps)
0	24.18
1	18.13
2	18.24
3	16.42
4	26.29
5	21.29

Send, Receive, Drop, Control Packet Results

There is no of packet send, receive, drop, and control in wireless network. Here the scenario of without attack and with attack when number of infected jellyfish nodes increase so what the behavioral changes occurred which is shown in the graph.

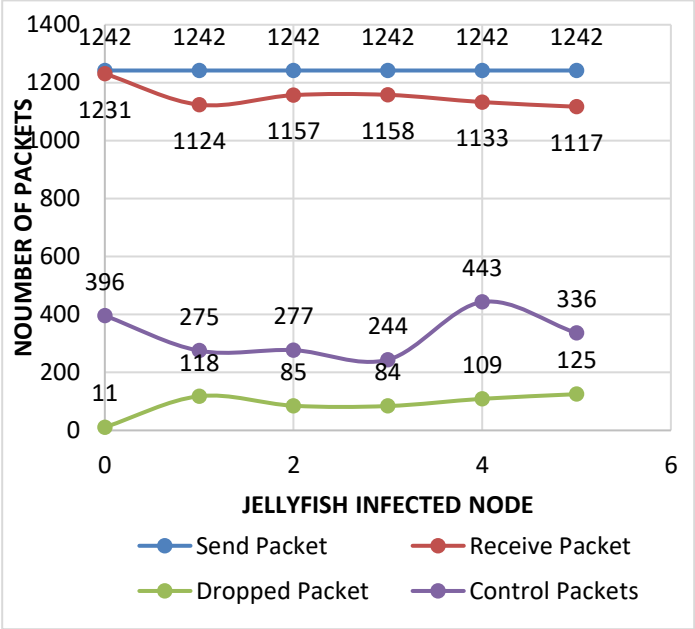

Fig.10 Send, Receive, Drop, Control Packet Analysis

Table 7 Analysis Table of Packet (Send, Receive, Drop, Control)

Jellyfish Infected Node	Send Packet	Receive Packet	Dropped Packet	Control Packets
0	1242	1231	11	396
1	1242	1124	118	275
2	1242	1157	85	277
3	1242	1158	84	244
4	1242	1133	109	443
5	1242	1117	125	336

VI. CONCLUSION

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 our thesis, we have analysed the behaviour and challenges of security threats in MANET with solutions. 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. Research includes the analysis the effect of jellyfish attack on performance of network and at the still more research required in Jellyfish attack.We have created MANET network with 25 nodes and analysed the behaviour of AODV protocol. Also we also analysed the behaviour of Network under the jellyfish attacks.

We have analyzed behaviour of |Jellyfish attack under 50 nodes MANET and 75 nodes network in which we found that this attack has high impact on network as it drastically reduce the performance of large network. Last but not least we flooded the packet to other nodes and informed them about Jellyfish attack is occurred basis on the high end to end delay and Jitter parameters, so that all the node break the current path and find the alternate route for data transmission. Using this method we may be reduce the effect of jellyfish attack.

ACKNOWLEDGEMENT

I hereby, take an opportunity to convey my gratitude for the generous assistance and cooperation that I received from the PG Coordinator, Prof. Vikas Tulshyan. I am sincerely thankful to my Guides, Prof. Ashish Patel and Prof. Mayank Gour for their constant encouragement, valuable guidance and constructive suggestions during all the stages of the literature review. Last but not least indebted to my friends without whose help I would have had a hard time managing everything on my own.

REFERENCES

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

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

[3] Jean-Pierre Hubaux, Edward W. Knightly, “Impact of Denial of Service Attacks Ad hoc Network ", Networking, IEEE 2008.

[4] Mohammad Wazid, Vipin Kumar, R H Goudar, “Comparative Performance Analysis of Routing Protocols in Mobile Ad Hoc Networks under Jellyfish Attack”, IEEE 2012

[5] Sakshi Giarg, Satish Chand, “Enhanced AODV protocol for defence against Jellyfish Attack on MANETs”, IEEE 2014

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

[7] Ashish Thomas, Vijay Kr Sharma, Gaurav Singhal, “Secure Link establishment method to prevent Jelly Fish Attack in MANET ”, IEEE 2015

[8] Mohammad Wazid, Avita katal, Roshan Singh Sachan, R H Goudar, “E-TCP for Efficient Performance of MANET under JF Delay Variance”, ICT, IEEE 2013

[9] Hetal P. Patel, Prof. M.B.Chaudhari, “A Time Space Cryptography Hashing Solution for Prevention Jellyfish Reordering Attack in Wireless Ad hoc Networks”, 4th ICCCNT IEEE 2013

[10] Avani Sharma, Rajbir Kaur, Purnendu Karmakar, “JFDV Attack: Influence on workability of Mobile Ad-hoc Network”, IEEE 2014

[11] 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 On IEEE, 2013.

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

[13] P.Kuppusamy, Dr.K.Thirunavukkarasu, Dr.B.Kalaavathi “A Study and Comparison of OlSR, AODV and TORA”, On IEEE 2011.

[14] Manjot Kaur, Malti Sarangal, Anand Nayyar “Simulation of Jellyfish Periodic attack in Mobile Ad hoc Network”,International Journal of Computer Trends and Technology Vol 15 Number 1 – Sep 2014

[15] Vahid Ayatollahi Tafti, Abolfazl Gandomi, "Performance of QoS Parameters in MANET Application Traffics in Large Scale Scenarios", World Academy of Science, Engineering and Technology 2010.
[16] Ispita Panda, "A Survey on Routing Protocols of MANETs by Using QoS Metrics", International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X Volume 2, Issue 10, October 2012.

WEB SITE

[17] Jianli Pan, Prof. Raj Jain, "A Survey of Network Simulation Tools: Current Status and Future Developments", Nov 24 2008, http://www.cse.wustl.edu/~jain/cse567-08/ftp/simtools/
[18] Mobile Ad hoc Network http://www.wikipedia.org/wiki/Mobile_ad_hoc_network
[19] Research Methodology http://www.smartdraw.com/flowcharts

BOOK

[20] Stefano Basagni, Marco Conti, Silvia Giordano, and Ivan Stojmenovic "Mobile Ad hoc Networking", 2nd Edition; Wiley Publication, Hoboken, New Jersey 1993
[21] Yang Xiao, Xuemin Shen, And Ding-Zhu Du, " A Wireless Network", Springer 2007.