Collaborative Intrusion Detection and Prevention against Jellyfish Attack in MANET

Deepika Bhawsar
Samrat Ashok Technological Institute,
Department of Information Technology,
Vidisha, India

Anil Suryavanshi
Samrat Ashok Technological Institute,
Department of Information Technology,
Vidisha, India

ABSTRACT
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. Here have 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.

Keywords
MANET, AODV, Jellyfish Attack

1. INTRODUCTION
Ad-hoc Network [1] is the wireless networks of various mobile devices of computing. This is not required any intervention of any fix infrastructure or in other words can say, without any centralized point of access e.g. base station. The various mobile nodes in an environment of MANET are self-organize and this happens in some arbitrary way. A MANET refers to as an autonomous collection having various mobile users, which interacts over sufficient bandwidth over wireless links. As the nodes are movable, the network topology might start varying fast and which is not predictable with respect to the time. Such networks could be functional among various human beings or among various vehicles in areas that are depleted of fixed-centralized infrastructure. In this, two nodes could straight away talk with each other if and only if that belongs to radio range of one another. Suppose those nodes are not under the range of one another, in that case those nodes talk with one another via third or fourth or any number of nodes by the technique of multihop routing.

Most venerable aspect of any wireless communication is its wireless medium of communication itself. This venerability's main reason is the mobility of these nodes and this will become reason to break the communication among various mobile nodes. One of the critical issues with the mobile adhoc network is their power backup. IT has very limited power backup. As there is no centralized controlling authority in any MANET, which makes it more critical. MANET is getting renown in several application areas, such as when a group of soldiers in enemy territory wants to interact by their available devices to get the report or any command of their situations. Emergency operations like search and rescue, commando operations, security scenarios, and collaborative research group are other examples of applications using MANET. Among all these applications security refer as very necessary, but basically all of them requires a distinct level of its security. Advantages of MANET are it can be set up at any place at any time and they provide access to services and information in any geographic areas. Disadvantages of MANET are limited resources leads to limited security and its time varying topology makes it unable to detect the attacker node.

2. MANET
The ad-hoc network is wireless network which recognize through the deficiency of constant infrastructures that permits the implementation of such type of network in some special circumstances, like as disastrous events, the decrement or elimination of its wiring costs & the information exchange with it users separately from its environment. The primary challenge in building a MANET is adorning each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. The device associated with a network should be able to transmit and receive data packets & to manage every functions of that network in a distributing order as routing of the packets, security, Quality of Service (QoS) etc. so these are terminals and sometimes become sheer nodes too. These devices possess wireless interface and having movable system of several sorts by such general ones such as PDA to notebooks.

A MANET refers to as a self-organizing network having mobile routers (and associated hosts) attached with wireless links—the union creates an arbitrary topology. The routers have the liberty to move randomly and make themselves arbitrarily. There are many applications of manet such as disaster management operations, battle field communication, data sharing in conference halls, etc [2].One problem in this kind of networks is performance level- in a dynamically varying topology; the nodes are desired to be power-aware because of bandwidth in that network. Another problem like as networks security concern- The motive of confidentiality, integrity, authenticity, availability and non-reputability are much hard to obtain in MANET as every node participates in the operation of that network equally and attacker nodes are hard to detect. The additional security layers attach with performance level overhead drastically.

Some of the applications of MANET are

1. Military or police exercises.
2. Disaster relief operations.
3. Mine site operations.
4. Urgent business meetings
5. Personal area network

3. MANET: AODV PROTOCOL & JELLYFISH ATTACK

A routing protocol is used to transmit a packet to a destination via number of nodes and various routing protocols have been put forward for such kind of ad-hoc networks [3]. These protocols find a route for packet delivery and to the correct destination. Basically, routing protocols can be widely classified into two types as, as shown in fig 1:

a) Proactive protocols

When a network using a proactive routing protocol, all node maintain one or more than one tables presenting the whole topology of that network. These tables are being updated every day for maintaining the date routing information from its every node to next other node. To update the routing information, topology information requires to be shared among the node which in turn leads to comparatively high load on the network. The advantage is that routes will always be available on request.

b) Reactive protocols

Reactive protocols don't make the nodes start a route discovery process till a route is not needed. This results in high latency as compare to proactive protocols, but low overhead.

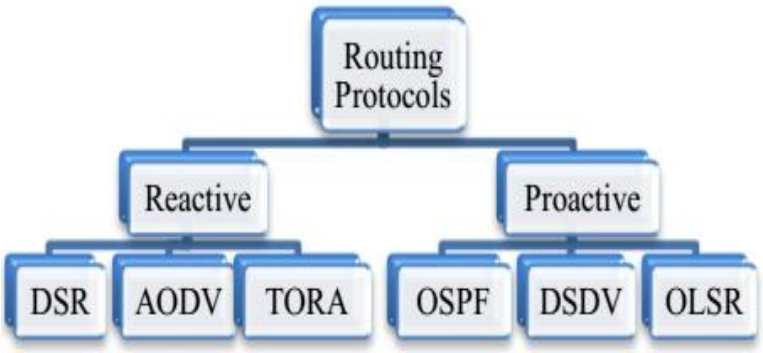

Fig 1: Nature of MANET Protocol

3.1 Ad hoc On-Demand Distance Vector (AODV)

In this protocol, the route detection is done with the help of the control message route request (RREQ) and route reply (RREP) [4]. Here in AODV all the route are obtained by flooding its network with the RREQ packets, which somehow don't receive the list of the all hops, where the traversed node of the mobile keeps the various information of the source, destination and also mobile node from which RREQ is obtained. The past information stuff is taken to generate the reciprocal path back to the source. When RREQ get to the mobile node, that node is aware of the correct route to the destination. The mobile node react with its source in packet (RREP) , whose having backward path generated by RREQ, This allows the forward route to move from source to destination ,To overlook the overloading of mobiles having their route and other route information have been deactivated and released their information at the time of the times up , when any node start moving route error (RERR) is transfer to its source node which is affected by the attack, when the source node obtain the RERR , then they can restart the route detection if they desire for, The neighbor information is obtained by the application of the hello packets [5].Here 2 techniques are used for maintaining the routes 1) ACK message in MAC level or b) HELLO message in network layer , the major benefit of such type of protocol is route are established at the time of need on time and destination series number are taken to search the new routes, this makes it a rapid process, the drawback of this technique the linked up nodes causes inconsistent route when the source sequence number is old but the linked nodes have higher but not new destination sequence number [6]. The multiple RREP packets reacts with the one RREQ packet causes huge control overhead, One more drawback of AODV is that the continuous signaling cause unwanted bandwidth usage.

3.2 Jellyfish Attack in Mobile Ad Hoc Networks

The initial JF attack referred as packet reordering attack. TCP has a good tendency for reordered packets because of the elements like as route changes or implementing multipath routing, and various TCP modifications are being introduced for improving resistance to disordering also have TCP Stack and reorder robust TCP. Moreover, no TCP variant is tough enough to prevent those malicious and persistent reordering as used through JF disordering attack. The process that jellyfish node implements for attack made up of sending all received packets, but in a mixed order through placing them in buffer unlike in a canonical FIFO order that is JF nodes maliciously reorder packets. Consequently, such persistent re-ordering of those packets leads to close zero good put, despite having all transmitted packets delivered [7].

There are mainly three types of jellyfish attacks: jellyfish reorder attack, jellyfish delay variance attack and jellyfish periodic dropping attack, as shown in fig 2. The paper [7] focuses on the first type of jellyfish attack. In this attack, the jellyfish node delivers all the packets to the destination node but instead of forwarding them in FIFO order, it forwards them in random order from the queue. When all the data are clubbed at the destination, garbled data will be obtained. Jellyfish delay variance attack misestimates available bandwidth. It also causes TCP to transmit traffic in bursts because of "self-clocking" leading to increased collisions and loss. The main drawback of periodic dropping jellyfish attack is that packet loss occurs periodically and end to end throughput becomes nearly zero.

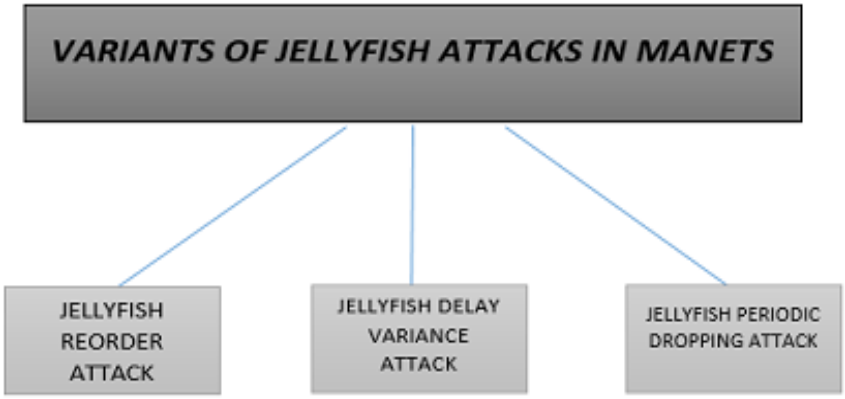

Fig 2: Variants of Jellyfish Attack

Jellyfish attacks work on MANET that use protocols with congestion control techniques, such as the Transmission Control Protocol (TCP), in the transport layer [8]. JF attacker enters without any invitation into those forwarding group & after that enhance the forwarding time interval of the mobile packets. Because of JF attack, great finish to finish occurs in that network. So the performance of network (i.e. throughput etc) drops considerably.

Jellyfish attack is related to transport layer of MANET. The JF attacker disrupts the TCP connection which is established for communication. Due to JF attack, high point to point delay is introduced in the network resulting in poor performance of the network. Various applications like as file transfer, messaging, and need to be dependable, congestion controlled delivery as offered by protocols like as TCP. JF attacker disrupts the whole functionality of TCP. As a result of which performance of real time applications becomes worse. JF attack is further divided into three categories i.e. JF Reorder Attack, JF Periodic Dropping Attack, and JF Delay Variance Attack [9].

4. LITERATURE REVIEW

In paper [10], MANETs are extremely susceptible as around is no occurrence of confidential integrated consultant and vibrant network topology. Due to such properties of adhoc network numerous type of attacks are likely to be possible. Jellyfish is a latest category of DoS attack. The main aim of jellyfish the node is to shrink the noble one put that could be accomplished by reducing few of packets. Authors have projected a secure technique in TORA protocol by the means of selective node contribution approach.

It also covers impact of jellyfish attack on adhoc network by normal TORA and by using the selective node participation method. The discussed approach decreases the influence of jellyfish attack in adhoc network by disabling the jellyfish nodes to contribute in the DAG. Still, it preserves the complete truthfulness of the DAG. It decided that the performance of adhoc network enhanced by selective node participation in the sense of terms of terminal to terminal delay, packet delivery ratio as well as throughput of the network.

In paper [11], Empirical result illustrate that the performance of a routing protocol differs widely across various mobility models and hence the results of one model can't be applied to the other model. Hence have to consider the mobility of an application while choosing a routing protocol. DSR gives better performance for highly mobile networks than DSDV. DSR is faster in discovering new route to the destination when the old route is broken as it invokes route repair mechanism locally whereas in DSDV there is no route repair mechanism. In DSDV, if no route is found to the destination, the packets are dropped.

Future study should be done to compare protocols in limited mobility environment where routes are not broken too often. Proactive protocols may give better performance for nearly stable environment. Performance of other routing protocol can be calculated over various mobility models taking in to consideration the number of average paths connected to gain greater insights into the relationship between them. The scenarios which portray real world applications more accurately can be designed through in-depth study of the application.

In paper [12], it talked about many kinds of attacks. Mainly rushing attack has been defined comprehensively. Rushing attack in contradiction of AODV protocol. It offers a do sin contradiction of the ad-hoc routing have been defined exhaustively and rushing attack in contradiction of AODV protocol. It offers a do sin contradiction of the ad-hoc routing protocol.

The attackers overflow the network with false appeal and raise the traffic flow and therefore the reply time of nodes rises thus by means of duplicate dominance mechanism achievement admission to information. In this paper a method projected of RAP (Rushing attack prevention) in that an edge price established to a level for the reply time. This method additionally can be improved by brink value and average time calculation to classify the source of false requests.

In paper [13], MANET is an important aspect of any wireless networks. No ropes and immovable routers are used in these kinds of network. It is not external network; it is the provisional network. Nodes have the competence to self arrange in themselves and it trails infrastructure less system. Network is shaped by number of nodes roaming in an unpredictable manner. They do not create any fix topology. Every nodes additional performance as routers which handovers packet from one node to additional node. Security is main issues in MANET. From previous some year security problems in MANETs are getting so much attention. As there are several security susceptibilities in MANET and that is the reason via it is not harmless from attacks. There are various kind of MANET like VANET (Vehicular Ad-hoc Network), IMANET (Internet based MANET), SPANs (Smart Phone Ad-Hoc Networks), Tactical MANET.

Now everybody has laptops, PDA's and users want to

communicate to one another via these electronics devices with others device. This all happen because by this they can exchange data and MANET is the single answer to it. It is provisional network that is agreed on the momentary foundation and separated when the task has been got over. It is improved for minor area only. It has unlimited requests in the arena of military, hospitals, education, emergency. Sensors are very tiny device that are organized in a specific are for sensing information.

In paper [14], a direct trust-based detection (DTD) algorithm is proposed which recognize and abolish a jellyfish node from an active communication route. Here in proposed DTD algorithm, each node uses locally calculated trust values which are collected over a time period to recognize whether its neighbor node is a JF node or not.

A detailed performance evaluation of Jellyfish attack (JF-reorder, JF-delay and JF-drop) over TCP based MANETs is presented. Based on the proposed work simulation results generated over various MANET scenarios with varying number of attackers, intermediate hops and attack parameters, it has been observed that Jellyfish attack causes network performance degradation in terms of network throughput, point-to-point delay and control overhead.

In paper [15], the focus is on the effects of jelly fish attack on MANET's routing protocols. Here four protocols AODV, DSR, TORA and GRP are used. Performance of the network has been evaluated in terms of Data dropped (buffer overflow), Data dropped (retry threshold exceeded), Load, Media access delay, Retransmission attempts.

If good time services and no loss of information needs then have to choose TORA and if want low delay produced during transmission and reception of information and data then go for AODV. GRP is used as optional at the place of AODV. As compare to other three protocols the performance of DSR is poor. If increasing node density, forwarding rate of packets, use different protocol and introduced JF periodic dropping attack the performance may vary.

5. COLLABORATIVE INTRUSION DETECTION AND PREVENTION APPROACH AGAINST JELLYFISH ATTACK

This work is made for Ad-hoc network. In adhoc network, there are lot and lots of mobile nodes. These mobile nodes are shown in fig 3.

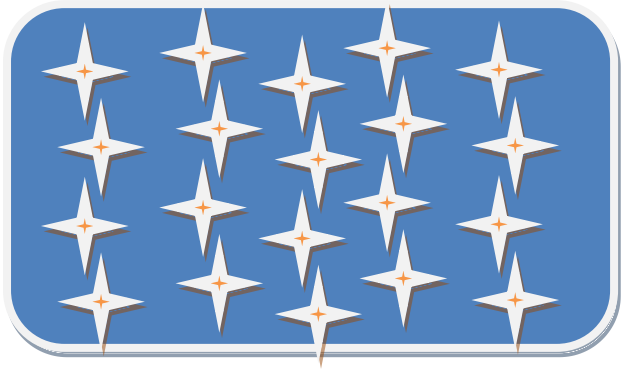

Fig 3: Mobile Adhoc network

The architecture of the proposed work "Collaborative Intrusion Detection and Prevention Approach against Jellyfish Attack in MANET" is shown in fig 4.

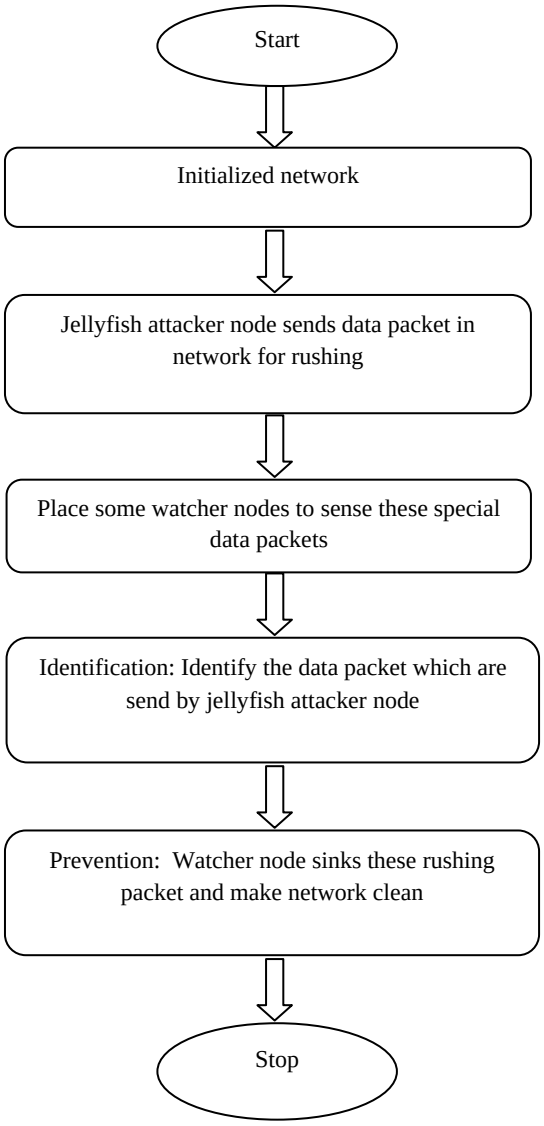

Fig 4: Proposed work architecture

6. SIMULATION AND RESULT ANALYSIS

Here have used NS-2 (Network Simulator) [16] for simulating various aspects of Jellyfish Attacks, effects and preventions. The simulation area of the whole MANET is 800 m×600 m. various properties with their values are shown in following table:

Table 1: Simulation Parameters

Property	Values
set val(chan)	Channel/WirelessChannel
set val(prop)	Propagation/TwoRayGround
set val(netif)	Phy/WirelessPhy

set val(mac)	Mac/802_11
set val(ifq)	Queue/DropTail/PriQueue
set val(ll)	LL
set val(ant)	Antenna/OmniAntenna
set val(ifqlen)	50
set val(nn)	51
set val(rp)	AODV
set val(x)	800
set val(y)	600
set val(stop)	50

Figure 5, 6 and 7 shows the ultimate result for which researchers have done all exercise. This result shows the clear cut picture of the proposed work over base paper work.

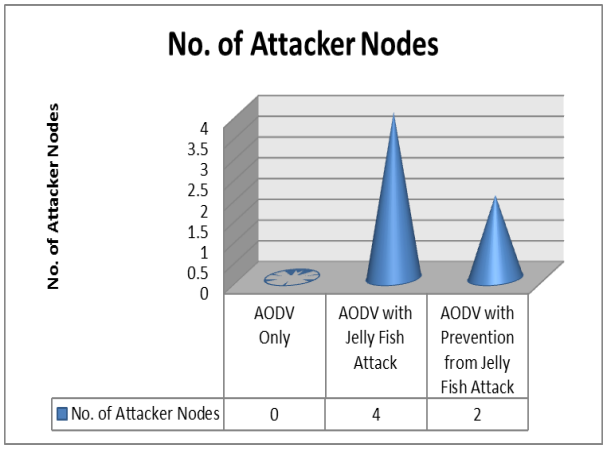

Fig5: Analysis of Number of attacking nodes in network.

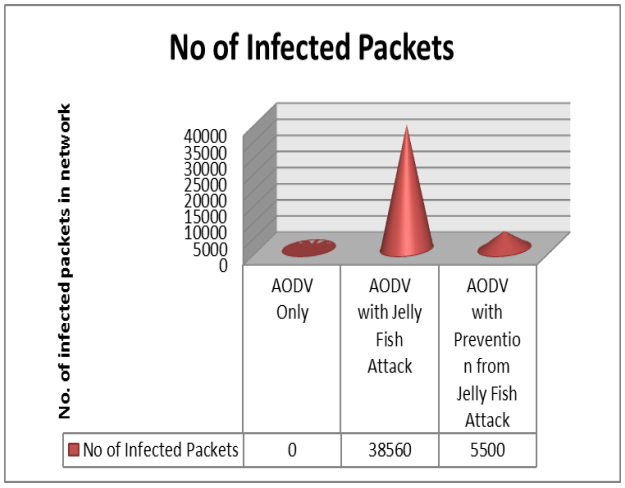

Fig 6: Analysis of Number of Infected Packets in network

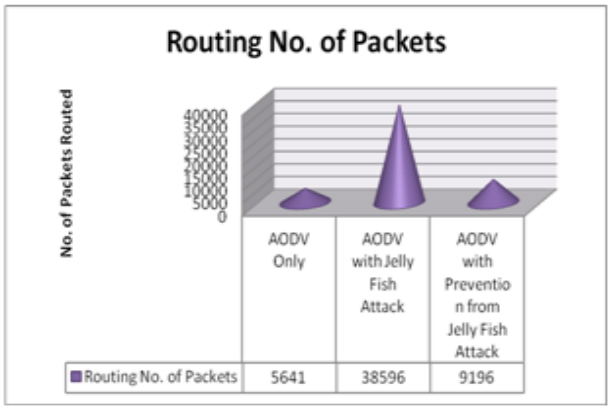

Fig 7: Analysis of Number of Packets Routed in network

Graphical Representation of the proposed work is shown in figure 8.

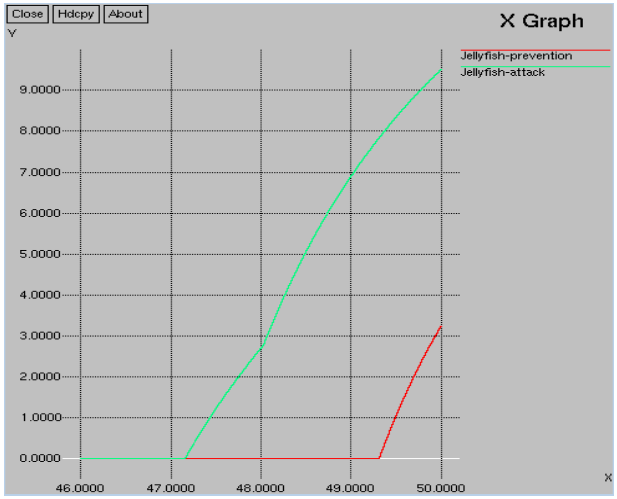

Fig 8: Representation of Jellyfish Attack and its Prevention

7. CONCLUSION AND FUTURE SCOPE

In this paper, 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. From the fig 5, 6 and 7, it is very much clear that the performance of the proposed work "Collaborative Intrusion Detection and Prevention Approach against Jellyfish Attack in MANET" performs better.

In the future research work effort will be made to put forward a solution for routing in Ad Hoc networks by tackling the core issues of security in routing. Hopefully, the output of this study can be used as reference for future work. It is proposed to compare all other routing protocols which consider the same simulation parameters so that an exhaustive comparison of various routing protocols can be made. The future work is to compare simulator for different protocols.

For the future work, this area will investigate not only the comparison between AODV and DSR routing protocols in grid but more on the vast areas. In this work other network parameters such as number of mobile nodes, traffic type-CBR, simulation scenarios. It would be interesting to observe the

behavior of these two protocols by varying these network parameters. This work can be enhanced by analyzing the other MANET protocols under different mobility model and different type of traffic sources with respect to other performance metrics.

8. REFERENCES

[1] RFC 2501, http://www.faqs.org/rfcs/rfc2501.html.

[2] N.H. Saeed, M.F. Abbod, H.S. Al-Raweshidy, "Modeling MANET Utilizing Artificial Intelligent," Second UKSIM European Symposium on Computer Modeling and Simulation, 2008, pp. 117-122.

[3] Shrikant Upadhyay, Pankaj Joshi, Neha Gandotra and Aditi Kumari, "Comparison and performance analysis of reactive type DSR, AODV and proactive type DSDV routing protocol for wireless mobile ad-hoc network using NS-2 simulator", Journal of Engineering and Computer Innovations Vol. 2(10), pp. 36-47, March 2012.

[4] Anuj K. Gupta , Harsh Sadawarti and Anil K. Verma, "Implementation Of Dymo Routing Protocol", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol.1, No.2, May 2013.

[5] C. Perkins, E Royer and S. Das "Ad hoc On-demand Distance Vector (AODV) Routing," RFC 3561 , July 2003.

[6] S. Karthik, A. Kowshika and C. Maheswari, "An Enhanced Packet Forwarding Scheme Using Random Way Point Mobility Model With AODV in Mobile Ad-hoc Network**",** Research Journal of Applied sciences,2010,Volume 5, Issue 2.

[7] Imran Raza, S.A.Hussian, Amjad Ali, Muhammad Hassan Raza"Persistant packet reordering attack in TCP based Ad-hoc wireless network", IEEE, 978-1-4244-8003- 6/10-2010.

[8] J. von Mulert et al.,"Security threats and solutions in MANETs: A case study using AODV and SAODV", Journal of Network and Computer Applications 35 (2012) 1249–1259.

[9] Syed Atiya Begum, L.Mohan, B.Ranjitha, " Techniques for Resilience of Denial of Service Attacks in Mobile Ad Hoc Networks", Proceedings published by International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X National Conference on Research Trends in Computer Science and Technology – 2012.

[10] Arminder Kaur and Dr. Tanu Preet Singh,"Securing MANET from jellyfish attack using selective node participation approach,"International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-4, April 2015.

[11] Bhavyesh Divecha, Ajith Abraham, Crina Grosan and Sugata Sanyal,"Impact of Node Mobility on MANET Routing Protocols Models", in 2005.

[12] Gajendra Singh Chandel and RajulChowksi,"Study of Rushing Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 79 – No10, October 2013.

[13] Pooja Chahal, Gaurav Kumar Tak and Anurag Singh Tomar,"Comparative Analysis of Various Attacks on MANET", International Journal of Computer Applications (0975 – 8887) Volume 111 – No 12, February 2015.

[14] Laxmi V, et al.," Jellyfish attack: Analysis, detection and countermeasure in TCP-based MANET", Journal of Information Security and Applications (2014), http://dx.doi.org/10.1016/j.jisa.2014.09.003

[15] Amandeep Kaur et al.," Effects of Jelly Fish Attack on Mobile Ad-Hoc Network's Routing Protocols", International Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013.

[16] Thenetwork simulator ns-2 http://www.isi.edu/nsnam/ns/