International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 6 June 2015

An Efficient Approach against Rushing Attack in MANET

Ankita Rathore[1], Dr. Rajiv Srivastava[2]
M.Tech. Scholar, Department of Computer Science,SIRT-E, RGPV Bhopal, MP 462033,India[1]
Director, SIRT-E BHOPAL,MP 462033,India[2]
ankita.rathore21@yahoo.com[1], drrajiv_sri@yahoo.com[2]

***Abstract**: Mobile Ad hoc Network (MANET) is a network of mobile nodes that nodes link to each other for a period of time to exchange information. MANET can be creating anywhere because there is no requirement of infrastructure prepared the nodes to organize them into a network and establish routes for a communication. Rushing attack comes under the category of reactive routing protocol. They divert the route discovery process to another route, attacker quickly forwards the route request before the other nodes, and data firstly reach to the destination node forwarded by attacker node. In this research we provide a mechanism which is helpful to prevent the network from rushing attack as well as to detect the rushing attack on Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocol. The network parameters like number of hops per route, route discovery time and routing traffic sent and received.*
***Keywords:** AODV, DSR, MANETs and Rushing Attack.*

1. Introduction

An Ad Hoc network is a wireless network characterized by the absence of a centralized and fixed infrastructure. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. We refer to an Ad Hoc network with mobile nodes as a Mobile Ad Hoc Network (MANET). A MANET is a collection of mobile nodes that connects to each other via wireless link. In MANET some nodes are directly connected to each other they directly exchanging there information when there is no direct connection between two nodes they communicate via intermediate nodes and transfer their data through intermediate nodes.

MANET is an autonomous system of mobile stations connected by multi-hop wireless links to form a network capable of operating without any fixed infrastructure s and more popular because of their important applications such as ranging from emergency rescue operation, mining operations, sensor networks commercial use like exhibitions and military applications [5]. Dynamic topology, limited physical security, bandwidth limited, complex routing are the major constraints, that makes the ad hoc networks vulnerable to different types of attacks [5]. First of all the dictionary meaning of 'RUSHING ATTACK' is a "sudden attack," [5].

Fig.1 shows a simple mobile ad-hoc network. Node A and node C are not within range of each other; however the node B can be used to forward packets between node A and node C. The node B will act as a router. In such a scenario, if A and C want to exchange their data packets then an onward transmission from A to B and B to C would be required.

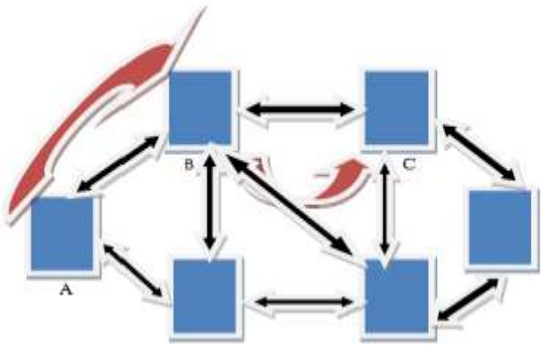

Fig.1 Example of Mobile Ad Hoc Network

Rushing attack is a new attack that results in denial of service attack when used against all previously published on-demand ad hoc network routing protocols [2]. Specifically, the rushing attack prevents previously published secure on-demand routing protocols to find routes longer than two- hops. In on-demand routing protocol are based on a property of forwarding only the first route request (RREQ) for each route discovery

request query. This 'vulnerability' of the on-demand routing protocols is exploited to mount the rushing attack. The source discovers a route to a destination and if the attacker is able to reach first to the neighbor of target node, before arrival of other RREQ [4]. In an on-demand protocol, a node needing a route to a destination floods the network with RREQ packets in an attempt to find a route to the destination [3].

This paper is organized as follows: Section II we explained in details the rushing attack. Section III the overview of routing protocols and Section IV covers the related work. Section V proposed solution defined in details and Section VI studied the performance factors in the developed protocols and analyzed the results. Finally we conclude the paper in section VII.

2. Rushing Attack

Rushing attack comes under the category of reactive routing protocols. Rushing attack diverts the route discovery process to another route, attacker node receives a RREQ packet from the source node and it broadcast the packet more quickly throughout the network before the legitimate nodes.

When source node wants to send a RREQ packet to another node in the network, if another node as an attacker they will accept the RREQ packet and send the packet to its neighbor with high speed as compared to other nodes in the network, packet forwarded by the attacker will reach first to the destination node because of high transmission speed. Destination node will accept this RREQ packet and discard those RREQ packets reached later. For further communication same route is used because receiver found this route is valid route, attacker will successfully gain access in the network.

Fig. 2, source S starts a route discovery process to the destination node D by sending a RREQ. Source node sends the RREQ to node A, B and C. Attacker node A quickly forwards the RREQ to its neighbor F and then to the destination. Request forwarded by the attacker node is reached first to the destination as compared to the other nodes. Destination node accepts the rush request and discard the other requests.

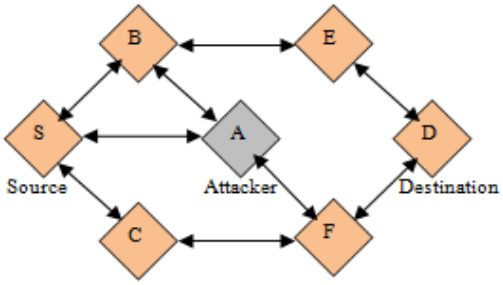

Fig. 2 Rushing Attack Formation

3. Overview of Routing Protocols

Routing protocols for ad hoc network [5] is classified in following three categories are proactive, reactive and hybrid routing protocol. Proactive routing protocol is also called 'Table driven routing protocol'. Proactive routing protocols play a role before any node want to send a packet in the network. Every node maintains a one or more routing tables to representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node in the network. Thus, when there is a need for a route to a destination, such route information is available immediately. Examples of proactive routing protocols are OLSR, DSDV, and GSR. Reactive routing protocol is also called 'on-demand routing protocol'. The reactive routing protocols play a role only when nodes want to send a data packet to a destination. Examples of reactive routing protocols are AODV, DSR and TORA [5]. Hybrid routing protocol is the combination of proactive and reactive. Example of Hybrid routing protocol is ZRP.

3.1 Ad Hoc on Demand Distance Vector

AODV routing protocol described in [11] when any source node wants to send a packet to a destination, it broadcasts a RREQ packet to its neighbors and that neighbor forward the RREQ to their neighbor and so on until the packet reaches to the destination. AODV uses destination sequence numbers to ensure that all routes are loop-free and contain the most recent route information. Each node maintains its own sequence number as well as its broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies an RREQ along with its sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose

corresponding destination sequence number is greater than or equal to that contained in the RREQ.
During the process of forwarding the RREQ, intermediate nodes record in their route tables the address of neighbors from which the first copy of the broadcast packet was received, there by establishing a reverse path. If additional copies of same RREQ are later received, these packets are silently discarded. Once the RREQ has reached the destination or an intermediate node with a route reply (RREP) with a "fresh enough," route, the destination/intermediate node responds by unicasting RREP packet back to the neighbor from which it first received the RREQ. As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables that point to the node from which the RREP came. These forward route entries indicate the active forward route. Because RREP is forwarded along the path established by an RREQ, AODV only supports the use of symmetric links [11]
In AODV, routes are maintained as follows: If a source node moves, it has to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its upstream neighbor notices the move propagates a link failure notification message (an RREP with an infinite metric) to each of its active upstream neighbors to inform them of the erasure of that part of the route [7].
These nodes in turn propagate the link failure notification to their upstream neighbors, and so on, until the source node is reached. The source node may then choose to reinitiate route discovery for that destination if a route is still desired [11].
An additional aspect of the protocol is the use of hello messages which are periodic local broadcasts made by a node to inform each mobile node of other nodes in its neighborhood. Hello messages can be used to maintain the local connectivity of a node [11].
However, the use of hello message is not required. Nodes listen for retransmission is not heard, the node may use any one of a number of techniques, including the reception of hello messages. Hello messages may list the other nodes from which mobile have heard, there by yielding a greater knowledge of network connectivity [11].

3.2 Dynamic Source Routing

The Dynamic Source Routing (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure. Network nodes cooperate to forward packets for each other to allow communication over multiple "Hops" between nodes not directly within transmission range of one another. As nodes in the network move about or join or leave the network and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by DSR. Because the number or sequence of intermediate hops needed to reach any destination may change at any time, the resulting network topology may be quite rich and rapidly changing [6]. DSR contains two phases: Route Discovery and Route Maintenance.

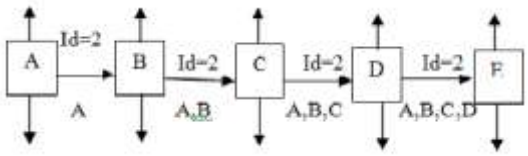

Fig. 3Route Discovery [6]

The Route Discovery process is started [8]:

Authors should consider the following points:

1) Node A sends a RREQ packet by flooding the Network.
2) If node B has recently seen another RREQ form the same target or if the address of node B is already listed in the Route Record, Then node B discards the request.
3) If node B is the target of the Route Discovery, It returns a RREP to the initiator. The Route RREP contains a list of the "best" path from the initiator to the target. When the initiator receives this RREP, it caches this route in its Route Cache for use in sending subsequent packets to this destination.
4) Otherwise node B isn't the target and its forwards the RREQ to its neighbours.

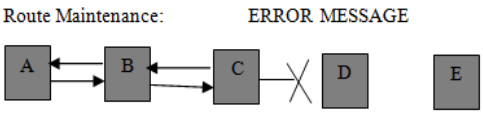

Fig. 4 Route Maintenance [6]

If node C does not receive an acknowledgement from node D after some number of requests, it returns a Route Error tothe initiator A. As soon as node receives the Route Error message, it deletes the broken-link-route. If A has another route to E, it sends the packet using the new route [6].

4. Related Work

Y. C. Hu et al. [2]developed a new component is called

rushing attack prevention (RAP) for secure route discovery. To resist the rushing attack by rushing attack prevention (RAP) protocol, that protocol can be applied on any on-demand routing protocol. They described a various mechanism such as Secure Neighbor detection, Secure Route Delegation, Randomized RREQ Forwarding and Secure Route Discovery that together applied to defend against the rushing attack. No cost for RAP protocol unless the other protocol fails to find a working route. RAP provides security properties against the rushing attack.

AL Shahrani and Abdullah Saad [1] proposed two solutions for the prevention of rushing attack in MANET on Secure Dynamic Source Routing (SDSR) routing protocol. Firstly, to address the rushing attack and introduced a simple concept is called as safe neighbors. The attacker can be modified in three lists such as the white list, the black list and the gray list. Secondly, prevent the network by randomized message forwarding technique some nodes have random choice. Randomized message forwarding technique collect and hold the packet for a particular time, then randomly selected one packet and forward that packet to the other nodes which requires extra time.

L. Tamilselvan et al. [3]provided a solution to counter the rushing attack and focused on the security of DSR protocol for the prevention of rushing attack. It is noticed that on the basis of their simulation study, the new protocol is successful in preventing the rushing attack and provides security against the rushing attack. In rushing attack, attacker node forwards the first received request to its neighbor to overcome this attack. They introduced a solution for the rushing attack such as each node collect the request from different nodes and randomly select a request to forward; the chance of rushing attack is minimized. Also in their new protocol it is seen that the SDSR protocol not only enhances the security but also enhances the basic properties of DSR, so that the throughput and packet delivery ratio is increased during data transmission.

Sushant Kumar and BibhudattaSahoo**[5]** worked on DSR protocol. They defined DSR routing protocol and analyzed the impact of rushing attack on the route discovery and route mechanisms. Discuss the cause and effect of rushing attack on both mechanisms such as route discovery and route maintenance of the DSR protocol which is also applicable to other on-demand routing protocols in the similar manner.

Anil Rawat et al. [4]discussed the functioning of Secure Routing Protocol (SRP) and described rushing attack variants. Also, analyze the behavior of rushing attack under the condition of rushing attack. In this paper, attempt has been made to evaluate the possibility of Denial of Service using rushing attack on SRP, which has been found to be ineffective and SRP can withstand the rushing attack. They also discussed various scenarios in which the attacker can attempt to disrupt the route discovery process.

V. Palansamy et al. [13**]** proposed the best position to launch the rushing attack is at three conditions. The goal of the project is to draw the graph based on the rushing position in the network. Rushing attack is at near the receiver have high success rate, rushing attack is at near receiver have low success rate and attack is at anywhere in the network have least success rate.

RushaNandy and Debdutta Barman Roy [8] presented how rushing attack works on DSR protocol. Self organized clustering technique schemes have been proposed. A parameter k has been defined for number of hop away from the cluster head. Thus the hop forms the cluster with its cluster head and routing is performed by transferring data within the cluster or between the clusters. A rushing attack detection technique have been suggested in which the cluster examine the nodes of cluster. If the RREQ transmission frequency is greater than normal frequency, node is malicious and hence removed from the cluster.

5. Proposed Solution

In rushing attack, the attacker quickly forwards the RREQ packet and receiver receives the rushed packet and discards the other RREQ packet. To identify the rushing attack by fixed the threshold value and minimize the chances of rushing attack using collect and store the RREQ and forwards randomly. When source node S want to send packets to destination node D. S will check route is available or not in route cache. If route is not available, it broadcast a RREQ packet include header. The header contains source address and request id. On receiving the RREQ packet each node checks the sources address and request id. If node received a RREQ packet from the same source discard the packet, otherwise node send the RREP packet to the source. Source node calculates the threshold value and threshold value is fixed value for all node. Packet should be reached before the fix interval of time; it means attacker is present in the network. The neighbour node will inform about the attacker and discard the packet. After the threshold time check out the paths.

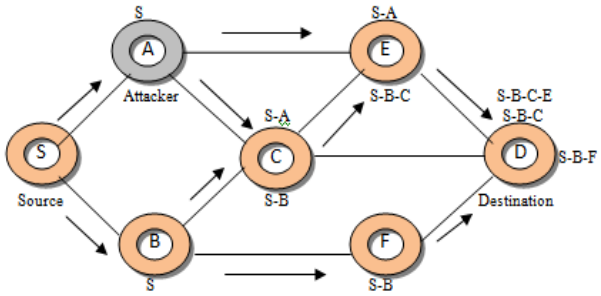

Fig.5 Working Principle

In On-Demand routing protocol, first received RREQ forwarded by all nodes and RREQ received after first are discarded. Fig. 5 there is many paths to reach the destination D. Every node does not forward the request comes first, it waits for some time , collect and store the number of request comes from different nodes and select a request from them to forward. Set a timer, for collecting the request and if time is over then discards the packet. If packet arrives before the timer collects and stores the packet and selects randomly to forward the packet by this method almost prevent the network from rushing attack.
Some steps on the working principle are:

1) Create the network of N mobile node in the MANET.
2) Create a connection between nodes.
3) Set the threshold time on the node.
4) Attacker takes the RREQ packet and quickly forwarded to the upcoming node.
5) Check the time of the packet if packet arrives before the threshold time it means malicious node in the network.
6) Neighbour nodes inform about the attacker and discard the packet.
7) After that collect and store method is applied.
8) Every node collects and stores the RREQ packet.
9) Randomly selects a request to forward, minimize the chances of attacker.

6. Performance Evaluation

The performance of the two routing protocols (AODV and DSR) is studied with implemented simulations.

6.1 Simulation Environment

The routing protocols have been implemented with Optimized Network Engineering Tool (OPNET). The reason of its popularity has attractive GUI (Graphical User Interface) and visual features.

Simulation Parameters shown in table:

Table 1: Simulationparameter

Parameters	*Values*
Simulation area	**50*50 km**
Simulation time	**10000 Second**
Numbers of Mobile Nodes	**17**
Routing Protocol	**AODV & DSR**
Data Packet Size	**1024 Bytes**
Data Rate	**15 Kbps**
Speed of Node	**10 Km/h**
Numbers of Malicious Nodes	**2**
Mobility	**Random Way point(0-30msec)**

The performance of the developed routing protocols has been measured in terms of following metrics:

6.2 Number of Hops per Route

Number of hops can be defined as number of intermediate nodes in the route (source to destination). Number of hops should be as low as possible which decrease the chances of link breakage.

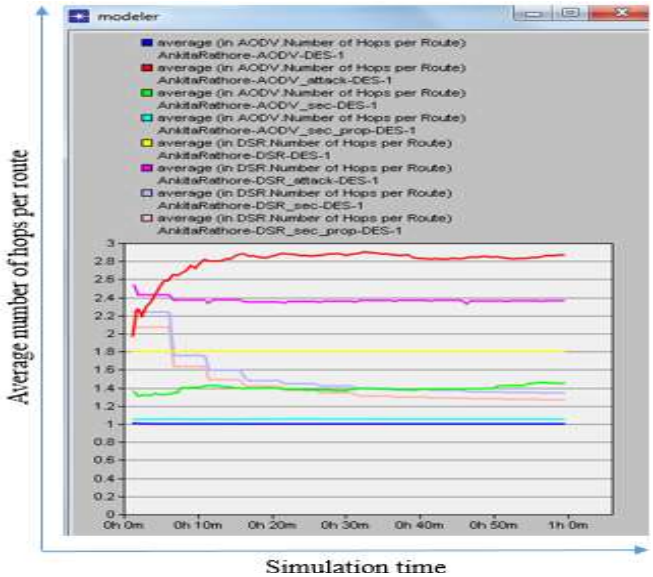

Fig. 6 Average number of hops per route

Based on Fig. 6, we are showing average number of hop per route is here when attack came in the network is shown

by blue color and pink color. When attack happen the graph goes up as compared to normal so number of hops per route near equal to normal condition after securing it.

6.3Route Discovery Time

Route Discovery Time is the time needed for the source node to discover a route to the destination.

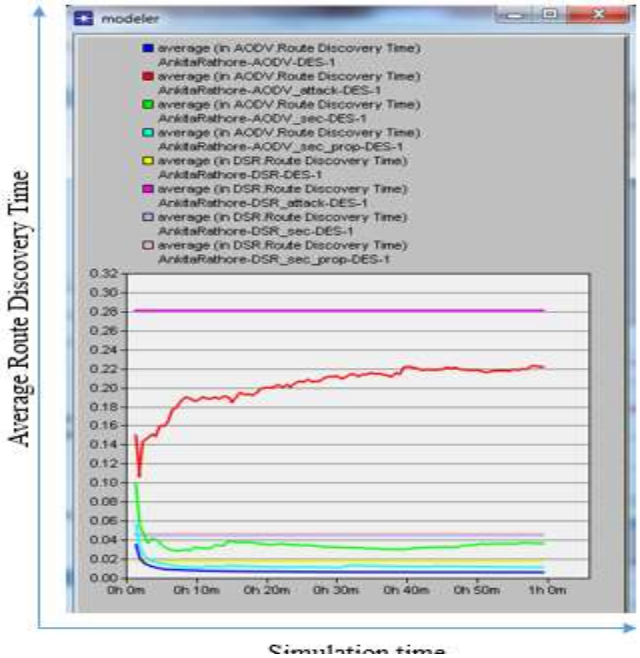

Fig.7 average route discovery time

Fig .7, graph showing a result in four condition of network one when there is not any attack in network another is when attack present in network, when a secure schema in the network and last when apply proposed schema between average route discovery time for AODV and DSR protocol. There is much better performance of network for the route discovery time

6.4Routing traffic received

Fig. 8, the graph plotted between x-axis simulation time in minute and on y-axis traffic received. No attack condition is depicted by violet and yellow color in AODV and DSR respectively. When rushing attack occurs performance of graph is high in compare to normal AODV and DSR. In this graphs shows better result as compared to attack condition after apply a secure proposed solution

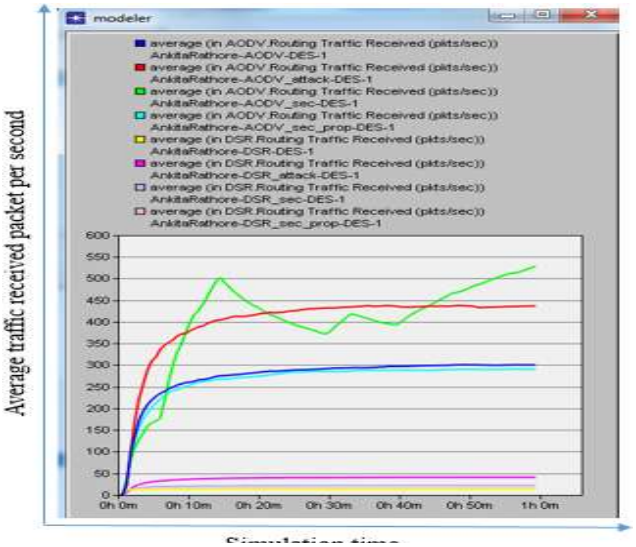

Fig. 8 average routing traffic received

6.5Routing Traffic Sent

Fig. 9, represent the average routing traffic sent for AODV and DSR, the graph plotted between x-axis simulation time in minute and on y-axis traffic sent. Normal condition is depicted by violet and yellow color where no attack happened. In DSR, when attack occur traffic sent packet very high as compared to normal. Hence in secure traffic sent packet is near equal to normal condition.

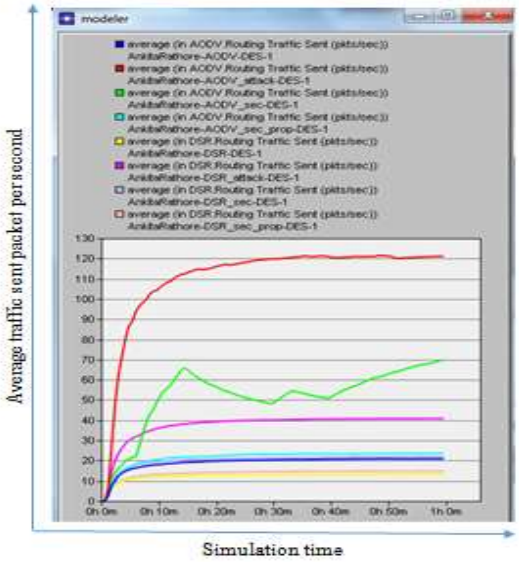

Fig.9average routing traffic sent

7. Conclusion

The overall idea of proposed method is to detect the rushing attack with the threshold value, threshold value is a fixed value for a transmission there packet should be reached at the fixed interval of time if packet reached before the time, attacker in the network. The proposed scheme prevent the network from the attacker by collect and store the packet for a particular time and choose one request to forward, the chance of attacker occurs in route is minimized so many paths to reach the destination in the particular network.The proposed schemeimproves the performance of network and provides the attacker free environment.

Acknowledgement

I will like to take the opportunity thank the supervisor of my project work "*Dr. Rajiv Srivastava*" for giving me valuable guidance and continuous support to complete this work. I would like to thank all the people who have helpedme directly and indirectly with the project, including my class fellows, reference library members and family members.

References

[1] AL Shahrani and Abdullah Saad, "Rushing Attack in Mobile Ad Hoc Networks," in IEEE Third International Conference on Intelligent Networking and Collaborative Systems*(INCoS)*, 2011, pp. 752–758.
[2] Yih-Chun Hu, AdrainPerrig and David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," in proceedings ACM on Wireless Security (WiSe), San Diego, California, USA, September 19 2003, pp. 30–40.
[3] L. TamilSelvan and V. Sankaranarayanan, "Solution to Prevent Rushing Attack in Wireless Mobile Ad Hoc Networks," in IEEE Ad Hoc ubiquitous Computing, (ISAUHC), 2006, pp. 42-47.
[4] A. Rawat, P. D. Vyavahare, "Evaluation of Rushing Attack on Secure Message Transmission (SMT/SRP) protocol for Mobile Ad Hoc Networks," in IEEE International Conference on Personal Wireless Communication (ICPWC), 2005, pp. 62-66.
[5] Sushant Kumar and BibhudattaSahoo, "Effect of Rushing on DSR in Wireless Ad Hoc Networks," ACM 978-1-4503-0729-9/2011.
[6] David B. Johnson, David A. Maltz and Josh Broch, "DSR: The Dynamic Source Routing For Multi-Hop Wireless Ad Hoc Networks", in Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, Addison Wesley, 2001, pp. 139-172.
[7] C. E. Perkins and E. M. Royers, "Ad Hoc On-Demand Distance Vector Routing", in Second IEEE Mobile Computing Systems and Applications, Proceedings WMCSA, , 1999, pp. 90-100.
[8] RushaNandy, Debdutta Barman Roy, "Study of Various Attacks in MANET and Elaborative Discussion of Rushing Attack on DSR with Clustering Scheme". Int. J. Advanced Networking and Applications, Vol. 03, 2011, Pages: 1035-1043.
[9] Mike Burmester and Breno de Mereiros, "On the Security of Route Discovery in MANETs", TRANSACTION ON MOBILE COMPUTING, Vol. 8, No. 9, September 2009, pp. 1180-1188.
[10] Eman S. Alwadiyeh and Ala F A Aburumman, "Interference-Aware Multipath routing protocols for Mobile Ad Hoc Networks," 13th Annual Workshop on Wireless Local Networks, IEEE, 2013, pp. 980-986.
[11] C. K. Toh, "Ad Hoc Mobile Wireless Networks", Pearson Education, 2002.
[12] Ranjankaparti, Dan Likarish, "OPNET IT GURU: A Tool for Networking", MSCIT Practicum Paper, REGIS University, 2008.
[13] V. Palanisamy, P.Annadurai, "Impact of Rushing Attack on Multicast in Mobile Ad Hoc Network", International Journal of Computer Science and Information Security (IJCSIS), Volume: 04, No. 1 and 2, 2009.