ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse71842019.pdf
https://doi.org/10.30534/ijatcse/2019/71842019

An Innovative Approach to Prevent Rushing Attack in Manet

Avinash Raipuria[1], Sellappan Palaniappan[2]
[1]Department of Information Technology, Malaysia University of Science and Technology, Malaysia
avinash.raipuria@phd.must.edu.my
[2]Department of Information Technology, Malaysia University of Science and Technology, Malaysia
sell@must.edu.my

ABSTRACT

An adhoc network can be a group of multiple mobile nodes. This group can be made a network without any central infrastructure. Through this we can network anywhere and anytime. There may also be a problem connecting this network: the network may not understand one node another node, whether this node belongs to our network or another. Sometimes an external attack can also occur on the network, hence the proper node to handle. We have used a digital signature and also used random forwarding technology. This tells that the node belongs to our network, and we can communicate this node with another. The practicality of our network will additionally increase, and therefore nodes are also protected. During this paper, we have once worked to secure an attacker network on a mobile node.

Key words: Rushing attack, DSR Protocol, RMF Technique, Digital Signature.

1. INTRODUCTION

A mobile ad-hoc network (MANET) (figure 1) can offer mobile nodes within the area routed through mobile nodes from the mobile nodes packet area unit instead of any fastening base station. To make a very network, mobile nodes run for the time when you have to interchange the data. When exchanging data, the node network may occur at any time. Within the applications we are interested in, networking infrastructure such as repeaters or base stations can either be undesirable or may eventually be approached, so nodes must be prepared to find the network and themselves out of volume. Support should be established without contact with each other. MANET is also called mesh network. With adhoc network again we can create network and exchange data with node. With this, we can also use it in flying object, Military battle Field and Natural Disaster management. [1]

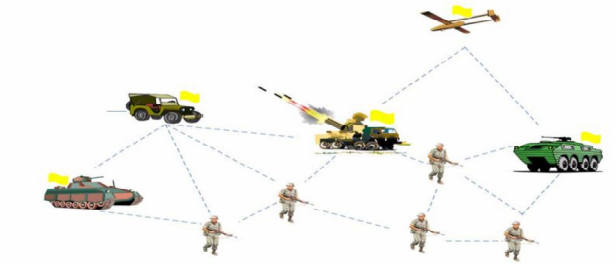

Figure 1: Mobile Adhoc Network

1.1 Routing Protocols

MANETs present many challenges to routing protocols compared to wired networks. Protocols were designed and developed to use information from a source to a destination from one source to another under the limitations of these networks. Whenever data is required to reach the crown from one place to another, it needs a source and destination. Simultaneous routing protocols (figure 2) are designed based on the absence of a centralized unit, so that loop-free routes can be created to minimize as communication changes. [1]

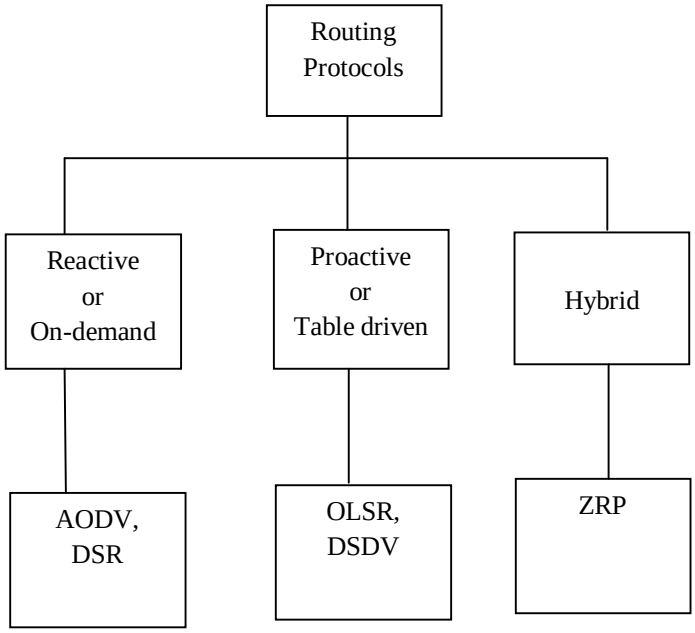

Figure 2: Classification of Routing Protocols

1.2 On Demand Routing Protocols

The reactive routing protocol field unit on-demand protocol started by a single source [3].Whenever the source node decides to send information to the destination node, the route is resorted to. The source node initiates a route discovery process by sending route requests to the network and waits until a reply is received from the destination node or an intermediate node to have a replacement route for this destination. As long as an established route is maintained through the specified route maintenance process.The overheads put forward by these protocols include significant delays before packets are transmitted and a large amount of control traffic once information is not properly exchanged.

This, reactive MANET protocol suits networks that have high node mobility1]

1.3 Dynamic Source Routing Protocol (DSR)

Dynamic Source Routing is a simple reactive protocol that is based on two main mechanisms route discovery and route maintenance. Both mechanisms are implemented in an adhoc network and in the absence of any time control messages.[2]

The route discovery and route maintenance steps involve three types of Messages.[4]

Route Request (RREQ): Whenever a source node wants to discover route to a destination, it will broadcast RREQ message. This message is then broadcasted by the next nodes until the destination receives this RREQ packet.

Route Reply (RREP): As presently as the destination receives a route request to itself, it originates a route reply (RREP) message and forwards it to the source through the path found within the RREQ packet.

Route Error (RERR): During the packet delivery, if the original path has modified, then the node, that is unable to send the packet, will send a Route Error (RERR) packet to the source (origin) of the packet.

Packet Formats: Packets in the DSR like RREQ, RREP, and RRER etc. contains fields which are separated by colon (:). Path if it contains multiple nodes then it will be separated by the comma. Different packet formats are as follows.

1. **RREQ Packet** RREQ packet is initiated by the node which wants to send the data to destination node whose address it does not have in its routing table RREQ packet.

RREQ	Source IP	UID	Destination IP	Path

RREQ: Packet type.
Source IP: contains IP address of the source node.
UID: Unique packet ID at source node.
Destination IP: Contains IP address of the destination node.
Path: List of IP addresses separated by the comma in the order from source to destination.

2. **RREP Packet** RREP packet is sent by the destination node or an neighbour node with the path information for the original source node through which it can send data.

RREP	Source IP	UID	Destination IP	Path

RREP: Packet type.
Source IP: contains IP address of the source node.
UID: Unique packet ID at source node.
Destination IP: Contains IP address of the destination node.
Path: List of IP addresses separated by the comma in the order from source to destination.

3. **Data Packet** This packet is generated by the node its has got the path from RREP packet or it had path originally in its routing table.This packet contains the message which is intended for the destination.

DATA	Source IP	UID	Destination IP	Message

DATA: Packet type.
Source IP: contains IP address of the source node.
UID: Unique packet ID at source node.
Destination IP: Contains IP address of the destination node.
Message: Message to be sent as a string.

4. **RERR Packet** This packet is initiated by the node when its timer goes explodes for receiving MACK acknowledgement from the node where it foreword data packet. This can happen if either link is broken or a node has unsuccessful. It contains information concerning path along which the data has traveled. This is often initiated to delete stale entries from the routing table and to find a new path to destination.

RERR	Source IP	UID	Destination IP	Path

RERR: Packet type.
Source IP: contains IP address of the source node.
UID: Unique packet ID at source node.
Destination IP: Contains IP address of the destination node.
Path: List of IP addresses separated by the comma in the order from source to destination.

5. **UACK Packet** Acknowledgement given by the destination node to the original sender node, to indicate the successful delivery of the data packet.

UACK	Original Source IP	Original UID	Source IP

UACK: Packet type.
Original Source IP: contains IP address of the original source IP.
Original UID: Unique packet ID at node sending the data packet.
Source IP: Contains IP address of the node which initiated the UACK packet i.e. destination where the data has reached.

6. **MACK Acknowledgement** given by the adjacent node to sign successful packet delivery. In short, this is easy hop to hop acknowledgement.

MACK	Original Source IP	Original UID

MACK: Packet type.
Original Source IP: contains IP address of the original source IP.
Original UID: Unique packet ID at node sending the data packet.

1.4 Rushing Attack

A fast attacker maintains the same pattern and moves the packet by searching for faster routes request and acquires access to that group. [1]

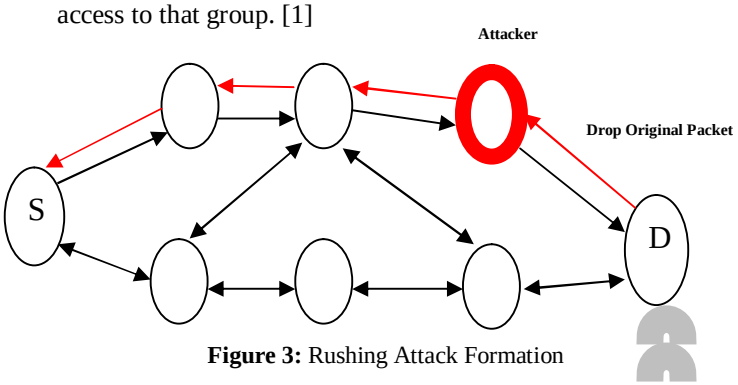

Figure 3: Rushing Attack Formation

When a node send route request packet (RREQ packet) to a further node in the wireless network, if there an attacker present then they will agree to the RREQ packet and convey to his neighbour with the high broadcast speed as compared to other nodes. Because of the high transmission speed, the packet forwarded by the attacker will achieve first to destination node. Destination node will allow this RREQ packet and speedily reply this request and reject other RREQ.

2. LITERATURE REVIEW

The offered that Mobile Adhoc network contains an self-sufficient collection of mobile nodes that can be moved openly and speak with each other without a stay Infrastructure. These nodes task as a Router or Host. In a mobile ad hoc network, no Central administration Authority, and therefore, the topology is not fixed. So this network is weaker when contrasted with Cable and Wireless Network. Various protocols in MANET work in the manner, as on-demand of AODV. The speeding assaulter (Rushing Attacks) takes advantage of the AODV Duplicate Suppression Mechanism, to hold away the attack. The researchers have reviewed the Rushing Attack and its Prevention Technique. By shifting some AODV the property, the Attack can be prevented or the consequences of the Attack can be decreased. The outcomes of Prevention were shown, and the impact of the Prevention in the different size of the network with different numbers of Attackers.[5]

The uniform on-demand routing protocols in mobile ad hoc networks were not primarily proposed to agreement with safety issues. A mobile Ad hoc network is a cluster of dissimilar type of nodes, which are associated to each other with the help of a wireless link. The cluster communications are a additional complicated safety measures in Manet because of the contribution of multiple senders and recipients. In this work, they proposed a rushing attack for aodv with a malicious node that increases the rapidity of the routing process. In this work of the paper, the aodv routing protocol is utilized for the knowledge of rushing attack.They furthermore estimated the better routing theme to security unarranged networks as unreceptive speeding attacks discrimination threshold value and also the calculation of the typical path value.[7]

The new technique built on the Rushing attack, a malicious node or an attacker increases the speed of the routing process. The scientist aim was to list the procedure that was used to overcome the rushing attack and furthermore to focus on their functioning performance; the scientist has given a method of threshold value which is able to be thought-about during the network for routing method to give permission it stop the rushing attack within the network. [6]

In their work on “Rushing The attack in Mobile Adhoc Networks” addressed the problem of safety in mobile ad hoc network by investigative various routes protocols such as AODV, DSDV and DSR. Different types of attacks which intimidate Manet were overviewed calculated in feature one of the solutions for preventing rushing attack in mobile ad hoc networks, SDSR and attempted to get better safety in this network with two important goals in mind: to lower overhead and to make sure there are protected neighbors in the network. This paper proposed two solutions: firstly, to decrease overhead by using the previous algorithm and secondly, the message that sent to the node itself to establish the safest and fastest route. All the earlier work recommended rushing attack and their countermeasures on how to prevent or eliminate rushing attack but nobody of them has worked with the facilitate of digital signature to prevent the rushing attacks in which malicious nodes are produced to infect the network or takes benefit of the duplicate suppression mechanism. Hence, this research work is based upon the prevention of novel Approach of Rushing Attack in Manet Using RMF Technique with digital signature. [1]

3. METHODLOGY AND EXPERIMENTS

When the source (S) wants to send a packet to the destination (D), there are many paths to reach D, as shown in Figure 4. Some nodes, (shown as dark nodes in Figure 4) are required to make a random choice in relation to which packet to forward, whereas the other nodes are required to do this. For example, in the following path from S to D:- S >> 2 >> 6>> 8 >> A >> D, the nodes 2 and 8 will forward the packet immediately whereas nodes 6 and A will hold the packets. S >> 2 >> 6>> 8>> 10 >> D, the nodes 2 and 8 will forward the packet immediately whereas nodes 6 and 10 will hold the packets and then make a random choice as to which one to send and take all route request of route discovery time. To reduce the problem of rushing attack, also use the concept of threshold value. In rushing attack, the attacker quickly forward the RR

packet or increase the transmission speed of packet. The receiver receives this faster packet and drops another valid RR packet; use a threshold value to correct this problem.

The limit value is a fixed value for transmission. There is a directive for all nodes that the packet must be delivered to the neighboring node at a fixed time interval. If there is an early attacker, it will forward the packet quickly and the packet will arrive ahead of time.The neighbor node will notify the attacker and can identify the attacker.In figure node S sends the packet to node D. For this it decides the threshold value. Now assume, threshold value for this network is 5 second, means a packet will take 5second in travelling to complete a hope. Node S sends a packet to A, B and C.The packet will reach in 5 second then node A sends a packet to 1 and 2, node 3 sends a packet to 4, 5 and 6, node 1 sends a packet to 4 and 5, node 6 sends a packet to 8 and 9, node 5 sends a packet to 7,8 and 9, node 4 sends a packet to 7 and 8, node 8 sends a packet to 10,11 and A, node 7 sends a packet to 10 and 11,node 9 sends a packet to 11 and A, it will reach in 5second and 9 sends a packet to A, A is an rushing attacker so it will quickly send the packet to D and this packet reach in 3.5 second to node D. Node D knows that the threshold value is 5 second and packet comes in 3.5 second, means there is an attacker so it inform to other node about the attacker and discard this packet. So that receiver node D will accept the packets which come from 10 and 11.This technique resolves all the problem of given scenarios.

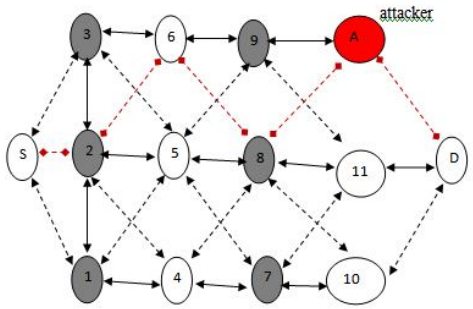

Figure 4: Randomized Message forwarding Technique with Threshold Value

In this section, a newly method is proposed for preventing the network from rushing attack, which exploits the replica suppression method. The proposed method uses the DSR protocol to forward the packet. These are reactive routing protocol, so safety concern is extremely high.

The proposed method is based on the following model, which consist of several steps.

Step 1: Source node to send the data to the destination, then it start RREQ packet and forward to its neighbors.

Step 2: Select the randomly route preference RREQ packet.

Step 3: Check the digital signature RREQ packet to the source.

Step 4: If node is standard RREQ packet forward to the next node otherwise attacker is here (present).

Step 5: Source node check the situation of threshold value is equivalent to or greater than the path (route) value.

Step 6: If the condition is fulfilled attacker is not present otherwise attacker is here (present).

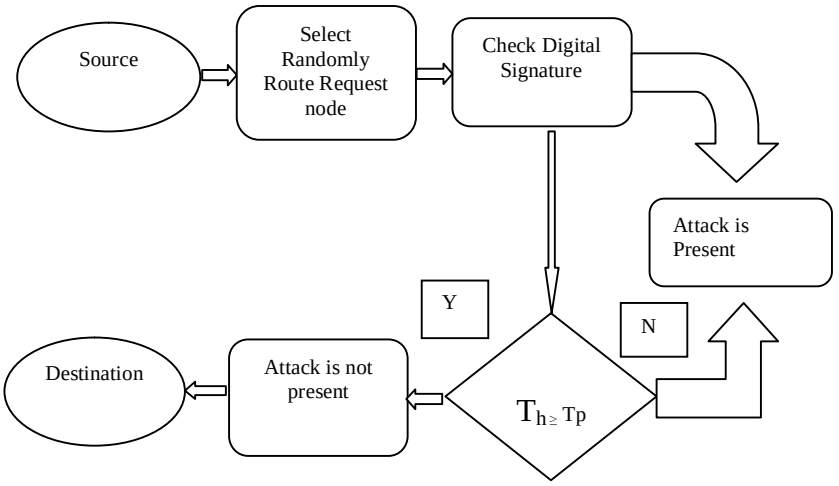

Figure 5: Adhoc Network Proposed Model

4. RESULTS AND SIMULATION

In this section, we estimate the performance of our proposed explanation by OPNET modeler 14.0.In our experiments, the ad-hoc network includes 15 mobile nodes placed randomly in square field site of 100 square kilometer area. For dissimilar scenarios of model (simulation); regular situation mobility and unsystematic (random) walk 2D mobility model are used. We have a variety of simulation parameters along with their values are scheduled (listed) in the table 1.

Table 1: Simulation Parameters

Parameters	**Values**
Routing protocol	DSR
Simulation time	100sec
Simulation area	10*10 kilometer
Numbers of mobile nodes	15
Data packet size	1024Bytes
Data rate	11Kbps
Speed of node	1Km/h
Antenna Type	Omni directional
Transmission range	200m
MAC protocol	802.11
Number of malicious nodes	1
Mobility	Random way point(0-25 msec)

We evaluate the performance of DSR along the following metrics:

1. $Hop\ per\ route\ H(i,k) = hop(k) + h(i,d)$

Current node i, destination node d, hope count message k.

2. $AverageEnd\ to\ EndDelay$

$$= \frac{\sum e\ (ReceivedTime - SentTime)}{\sum Number\ of packet\ received\ at\ destination}$$

$$e = Number\ of packet\ received\ at\ destination$$

3. $Average\ route\ discovery\ time$

$$= \frac{\sum e\ (sent\ Time\ +\ Received\ Time)}{\sum Number\ of packet\ received\ at\ source}$$

$$e = Number\ of\ packet\ received\ at\ source$$

The Average delay per hop of a packet is defined as the time a packet takes to travel from the source to the destination.Avearge delay its depend upon the graph sent packet at the source and received packet at the destination. The average delay takes over all the received packets.The dropping rate of packet is higher when attacker is attack on network. After applying the prevention technique,we can show that the dropping rate is decreased.

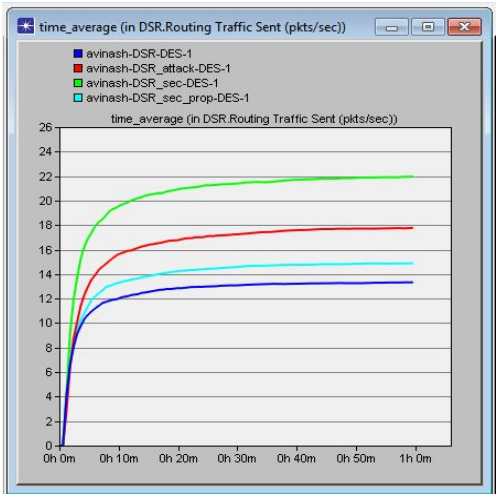

Figure 6: Average Sent Packet at the Source

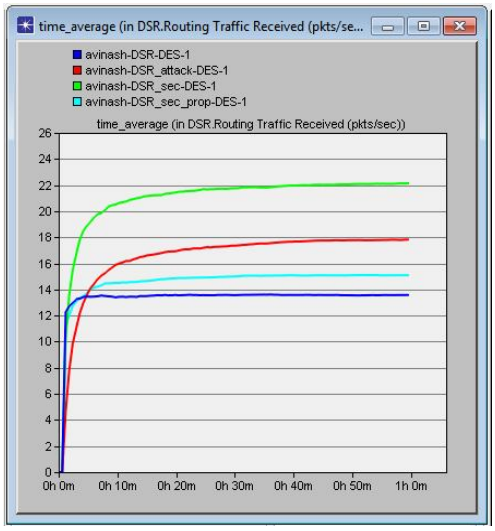

Figure 7: Average Received Packet at the destination

In the on top of result graph showing lead to the condition of the network once, there's not an attack in network another is once attack present in the network, when a secure schema in the network and last when applying projected schema figure is graph between average route discovery time for DSR protocol. We are able to see there's for a better performance of the network for the route discovery time.

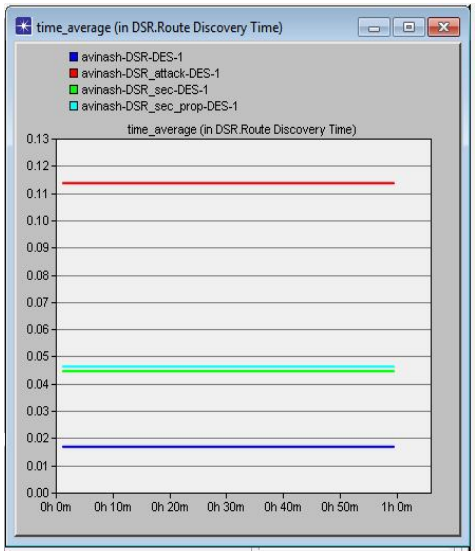

Figure 8: Average Route Discovery Time

Once the result is shown in the state of the network at the top of the result graph, an attack does not occur in the network once an attack exists in the network, when a secure schema and last schematic schema figure is applied to the network Average number of hop per route for the dsr protocol. We are able to see there for better network performance for hop count.

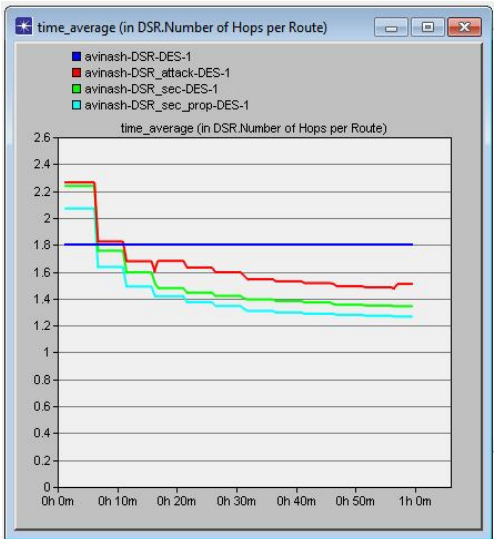

Figure 9: Average Number of Hop per Route

5. CONCLUSION

In this paper to prevent the attack using random message forwarding technique with digital signature. The proposed work to prevention the attack of network, and also overcome

the impact of rushing attack. Its define the Average route discovery time, hop, delay, which measures our network and also as well as secure the neighbours.

ABBREVIATIONS

DSR	Dynamic Source Routing
TORA	Temporally ordered routing algorithm
DSDV	Destination sequenced distance vector
AODV	Adhoc on demand distance vector
OLSR	Optimized link state routing
ZRP	Zone routing protocol
RMF	Randomized message forwarding
DS	Digital Signature

ACKNOWLEDGEMENT

I am thankful to Malaysia University of Science and Technology for providing facilities and resources for this paper.

REFERENCES

1. A.S. A.Shahrani. **Rushing attack in mobile Adhoc Networks,** *in Proc. 3rd Inter Conf. Intelligent Networking and Collaborative Systems*, IEEE Explore Japan,19 January 2012. https://doi.org/10.1109/INCoS.2011.145
2. D. B. Johnson. **The Dynamic Source Routing Protocol for Mobile AdHoc Networks (DSR),10th ed.** Rice University**,** *IETF, 19 July 2004*.
3. S. Taneja, A. Kush. A **Survey of Routing Protocols in Mobile AdHoc networks,** *IJIMT*, Vol.1, No.3.pp.279-285, August 2010.
4. P. kumar, Suresh P, T. Gupta; **Implementation of dynamic source Routing**, Mtech. Thesis, Dept CSE., IIT, Delhi, India, 2015**.**
5. C. Suthar, B. Panchal, **Rushing Attack Prevention with modified AODV in Mobile Ad hoc Network,** *IJBER*, volume2, India, 2014, page 3489-3493.
6. A. Raipuria.,S. rathi. **Prevention of Rushing attack in adhoc network using Randomized Message Forwarding Technique for dsr routing Protocol**, *IJBER,* Vol. 9,India, 2015, *p32-38.7p.*
7. V.S. Murugan, K.Selvakumar,**An Improved method of routing process and reducing Rushing attack for ad-hoc on-demand distance vector in Manet**,*JEAS,* volume11,India,2016.
8. A. Raipuria, S. Palaniappan. **A Skilled Hybrid Method to Protect Against Rushing Attack for the DSR Routing,** *European Journal of Scientific Research*, Vol.152, Jan 2019,Seychelles,pp. 290-297.
9. L.Tamilselvan, S. narayanan. **Solution to Prevent Rushing Attack in Wireless Mobile Adhoc Networks,** *in Proc,International Symposium on Ad Hoc and Ubiquitous Computing*,Surathkal,India,2006. https://doi.org/10.1109/ISAHUC.2006.4290645
10. K. M. A. Alheeti, A. Gruebler, Maier.**On the detection of grey hole and rushing attacks in self-driving vehicular networks**, *in proc.7th Inter Conf, Computer Science and Electronic Engineering Conference*, Colchester, UK,2015. https://doi.org/10.1109/CEEC.2015.7332730