VOL. 11, NO. 21, NOVEMBER 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

AN IMPROVED METHOD OF ROUTING PROCESS AND REDUCING RUSHING ATTACK FOR AD-HOC ON-DEMAND DISTANCE VECTOR IN MANET

V. Senthil Murugan and K. Selvakumar
Department of Computer Science Engineering, Annamalai University, Chidambaram, Tamilnadu, India
E-Mail: senthilkmvs@gmail.com

ABSTRACT

Standard on-demand routing protocols in mobile ad hoc networks were not originally designed to deal with security issues. Mobile Ad-hoc Network is a collection of different type of nodes, which are connected to each other via wireless link. The security issue of MANETs in group communications is even more challenging because of involvement of multiple senders and multiple receivers. In this work we propose rushing attack for AODV. In Rushing attack, a malicious node rising the speed of routing process. In this proposed work AODV protocol is used for study of rushing attack. We also propose the improved routing scheme to defend ad hoc networks against rushing attacks using threshold and average path value calculation.

Keywords: MANET, AODV, threshold value, average path value, rushing attack.

1. INTRODUCTION

A mobile ad-hoc network is an autonomous system of mobile nodes which communicates to each other via wireless links. MANET is an infrastructure less network. Network topology is dynamic which changes with time. Mobile nodes can be in the bus, train, building, military vehicle etc. There is no centralized controlling authority in the network. Mobile node works as routers to transmit the network information and also works as a host. As there is no centralized controlling authority, the network is more vulnerable. Attacker can easily participate in communication in the network and may affect the network. Mobile ad hoc network works mainly on two types of protocols: Reactive and Proactive. Reactive protocol is a table driven and Proactive is an on demand protocol. In an on demand protocol, performs path discovery when it wants to perform transmission. In this, sender sends request packet for path discovery and receives response from destination on successful completion.

MANET is wireless and dynamic topology network. So there are vulnerabilities like limited band width, lack of centralized authority, resource constraint, limited power supply, etc. So MANET is more vulnerable than the wired and wireless network. There are many security issues due to its characteristics in MANET. In MANET attacker can get easily participate as a router or a host in the transmission. There are different routing protocols in MANET. Routing protocols in MANET are mainly two: Proactive, which stores and updates the information of network in router tables. Examples are OLSR, DSDV, etc. Second is Reactive or on demand, which performs route discovery on request of sender for transmission. Examples are AODV, DSR, SAODV, etc. the dictionary meaning of 'RUSHING ATTACK' is "a sudden attack", or "to perform, accomplish, or complete with speed, eagerness, or violence". "RUSHING ATTACK" is also called as "novel attack" or "denial of service" attack in networking In this paper, we elaborates the detection & prevention Techniques for, rushing attack in Ad-hoc Network, which results in denial-of-service when used against all previously published on demand ad hoc network routing protocols.

2. RELATED WORK

Udhayakumar *et al.* [3] in their approach security mechanisms are introduced in order to prevent such network. Hence this paper described the different network layer attacks and detection mechanism of attacks in MANET. However, history shows that attackers regularly find new ways to attack and cause damage to computer systems and networks. So, it is treated that enabling a protection mechanism to learn from experience and to use the existing knowledge of attacks to detect new nosy activities in MANET is most important criteria in network security.

Aakanksha Jain *et al*. [4] in their process basic information about the features and applications of ad hoc networks and rushing attack was given. The issue of security, confidentiality and data integrity in mobile ad hoc networks was addressed by examining various previous important routing protocols such as AODV, DSDV, and DSR. Previous work in the area of rushing attack was explained and described, along with the solutions that can assist in preventing rushing attack.

Satyam Shrivastava *et al*. [5] has proposed on Rushing attack exploits this duplicate suppression mechanism by quickly forwarding route discovery packet in order to gain access to the forwarding group and focused on various techniques, which are used to overcome the rushing attack and also focus on how they work.

Swarnali Hazra *et al.* [7] describes the process of Rushing attack against on-demand ad-hoc routing protocol. It bring a denial-of-service against the ad-hoc routing have been described thoroughly and rushing attack against on demand ad-hoc routing protocol. The attacker floods the network with bogus request and increase the

traffic and thus the response time of nodes increases thus by using duplicate suppression mechanism gain access to information.

Parthiban *et al.* [10] has proposed a Neighbor attack, and novel and powerful attack against on-demand ad-hoc network routing protocols. This attack allows attacker to disturb multicast routes against previously proposed on-demand ad hoc network routing protocols. They have also presented Secure Neighbor Detection Mechanism (SNDM), a new mechanism that prevents the neighbor attack.

RushaNandy *et al.* [11] 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.

3. RUSHING ATTACK

In MANET there are different types of proto cols like routing protocols or table driven protocols and on demand protocols. In On demand protocols sender floods REQUEST packets to all the neighbors. In AODV protocol, to avoid the duplication of REQUEST packet, only first REQUEST is forwarded and other are discarded. When sender wants to communicate with other node, it performs route discovery. In that, it floods RREQ packets to neighbors, neighbors floods to their neighbors and so on until destination gets the request. If attacker is able to forward the REQUEST packet to neighbor of the destination first compared to other legitimate nodes, then the route which includes the attacker will be discovered. As the REQUEST from other legitimate node arrive later, they are discarded as duplicates. So the legitimate nodes will not be able to communicate with destination. So, rushing attack leads to Denial of Service attack.

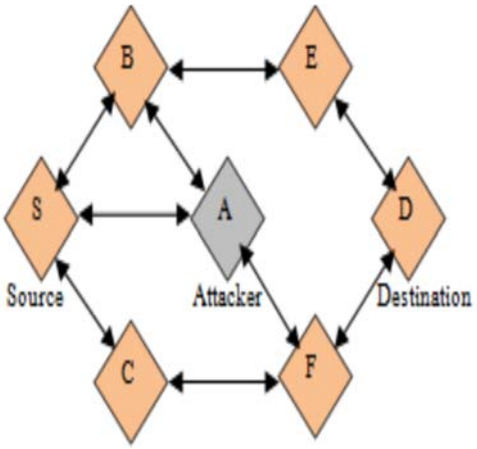

Figure-1. Rushing attack formation.

Figure-1 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 neighbour 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.

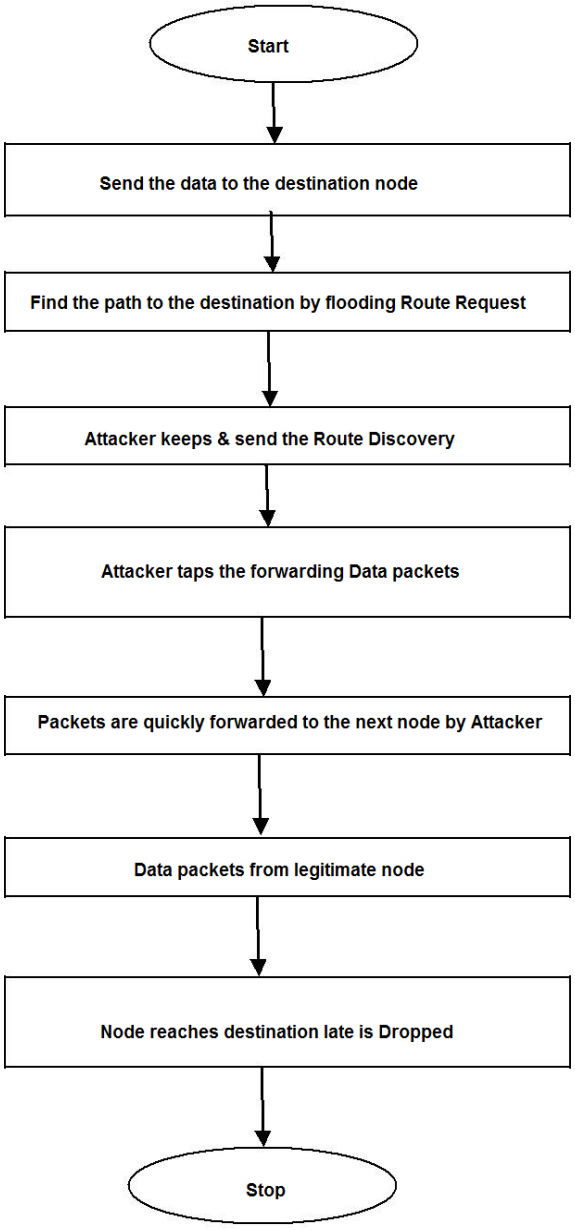

Figure-2. Rushing attack formation algorithm.

A rushing attacker uses the duplicate suppression mechanism thus the response timing of the malicious nodes is extremely fast and can send a route discovery to the sender, and gain access on the forwarding data. In this way the nonlegitimate node keep sending the requests and

hence accessing the networks queue. Because of this, attack requests sent by legitimate node will be considered as delayed request and hence discarded. The overall rushing attacks formation Algorithm given in Figure-2 flow chart.

4. PROPOSED METHOD

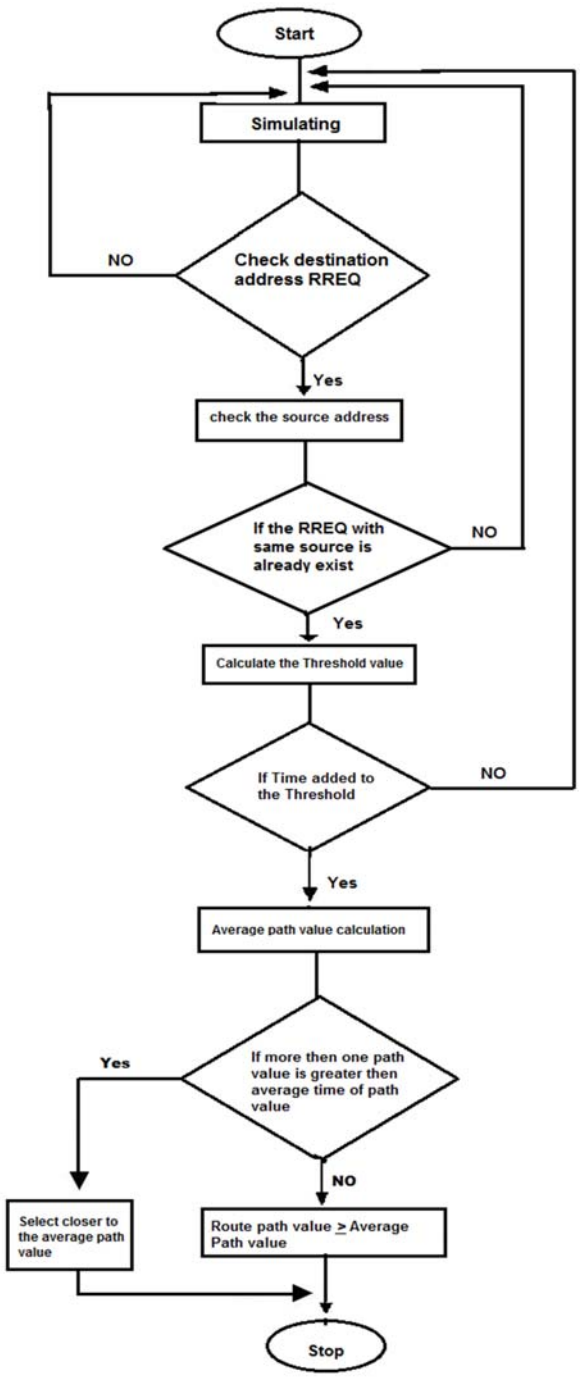

Figure-3. Flow diagram of proposed work.

An algorithm of proposed model as follows:

- Create the network of N mobile node in the MANET.
- Create connection between nodes.
- Check the source address and destination address with RREQ.
- Calculate the Threshold value.
- Check the time added to the Threshold value then calculate the Average path value.
- Check the path value with the Average path value time.
- Select closer Average path value which minimizes chances of Attacker.

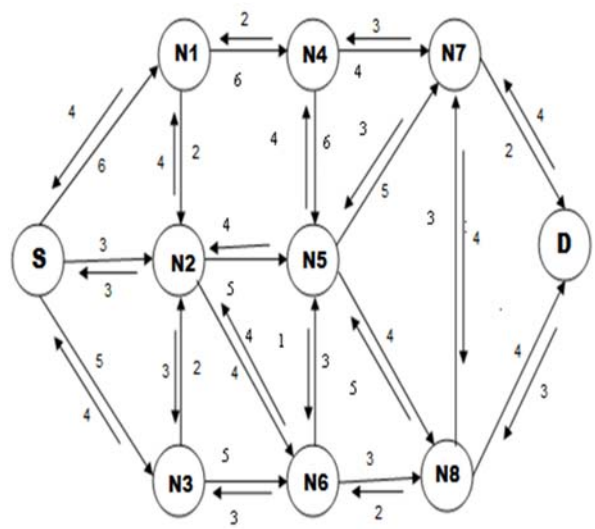

Figure-4. Mobile ad-hoc network.

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

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

Step 2: Intermediate nodes check the source address of the RREQ packet.

Step 3: If RREQ packet from the same source already exist, then intermediate node discard the packet, otherwise intermediate node send the RREP packet to the source.

Step 4: Source node calculates the average of the all acknowledgement packet. We called this average time of acknowledgement packet is threshold value.

Step 5: Source node adds this threshold value with individual RREQ packet sending time to its neighbours. We called path value to the addition

VOL. 11, NO. 21, NOVEMBER 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

of threshold value and RREQ packet sending time.

Step 6: Source node calculates the average time of path value.

Step 7: If there is more than one path value is greater than average time of path value, then source select the path value which is closer to the average path value.

Step 8: Otherwise Source node selects the route whose path value is greater than or equal to the average time of path value.

At node S, there are three links to node N1, N2 and N3. Source node S send the RREQ packet to the N1, N2 and N3. The transmission time from S to N1 is 6, S to N2 is 3 and S to N3 is 5. Source node will wait for the acknowledgement from N1, N2 and N3. The acknowledge time from N1 is 4, from N2 is 3 and from N3 is 4.

The average of all the acknowledgement to S is = (4+3+4) /3= 3.6.

We called this 3.6 as threshold value time.

Now this average acknowledgement is added to the sending time of the S to different nodes.

For node N1 = 6 + 3.6 = 9.6
For node N2 = 3 + 3.6 = 6.6
For node N3 = 5 + 3.6 = 8.6

We called these values are path values.

Now find the average of path values = (9.6 + 6.6 + 8.6) / 3 = 8.2

Now node S selects the path whose path value is greater than average of path value. The value which is closer to the average path value is selected and the path of this value is chosen for sending RREQ packet. With the help of this algorithm a path S-N3-N6-N8-D is chosen for sending the RREQ packet from S to D. This path is free from rushing attack and the communication will take place through this path. There are 10 nodes in the network. Node N2, N5 and N7 are the malicious nodes.

5. SIMULATED RESULTS

The figure below shows the Rushing Attacks detected in a 50, 100, 150, 200, 250,300 nodes keeping speed constant to 2 m/s. The metrics chosen are Packet Delivery ratio, Energy with 5 Attackers.

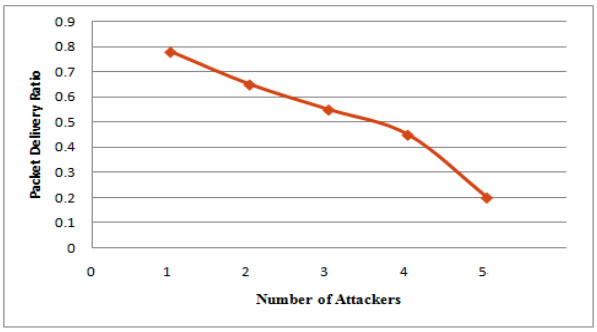

Figure-5. Packet delivery ratio vs number of attackers.

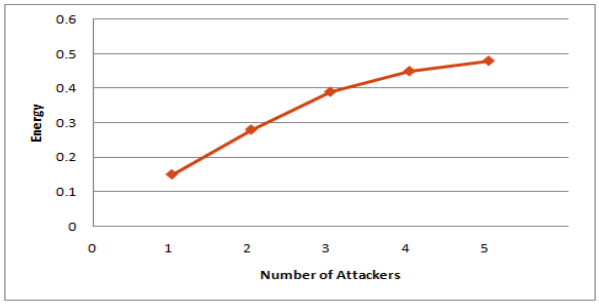

Figure-6. Energy vs number of attackers.

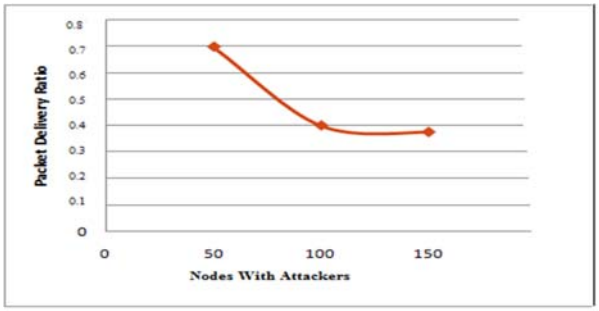

Figure-7. Packet Delivery ratio vs 150 nodes with 5 attackers.

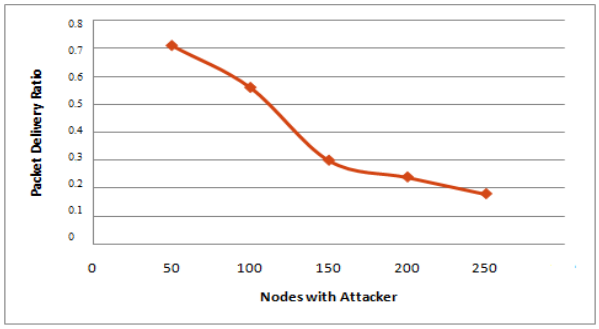

Figure-8. Packet delivery ratio vs 250 nodes with 5 attackers.

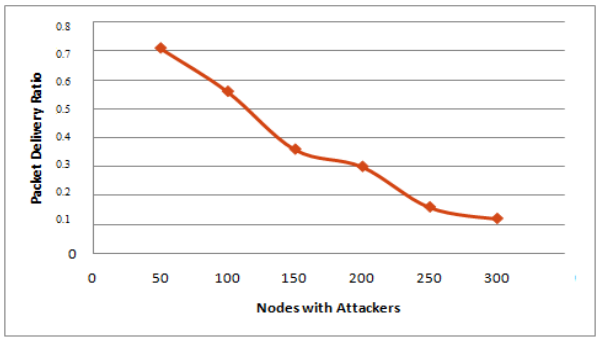

Figure-9. Packet delivery ratio vs 300 nodes with 5 attackers.

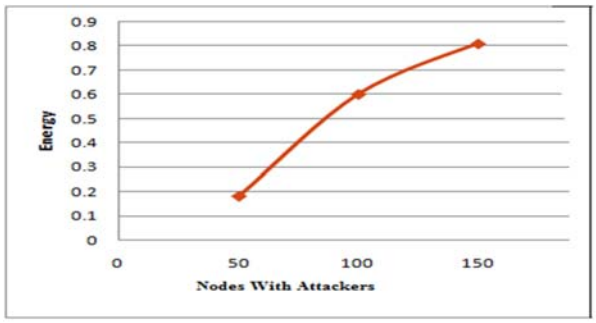

Figure-10. Energy vs 150 nodes with 5 attackers.

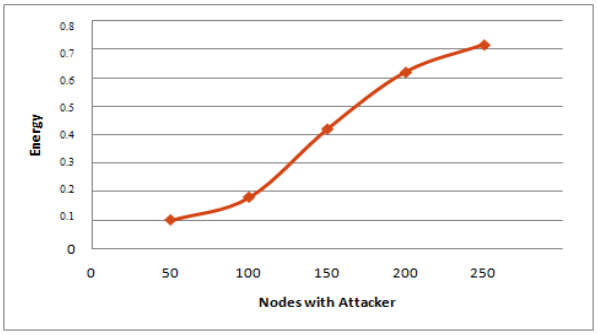

Figure-11. Energy vs 250 nodes with 5 attackers.

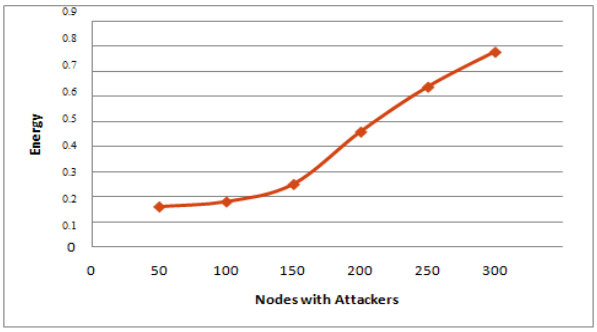

Figure-12. Energy vs 300 nodes with 5 attackers.

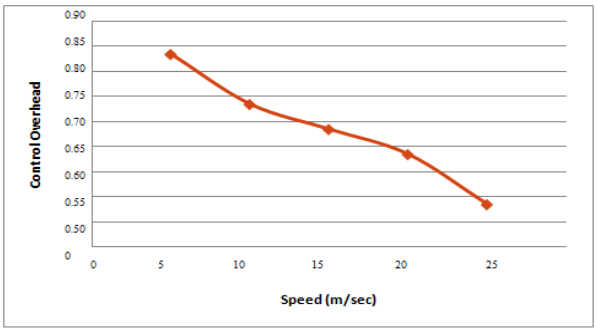

Figure-13. Control overhead vs speed

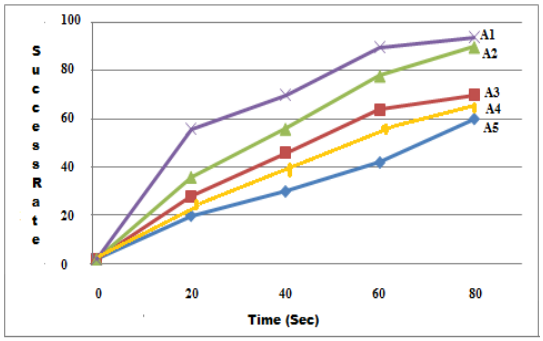

Figure-14. Security rate vs time.

6. CONCLUSIONS

This paper gives a study of rushing attack and its effect in MANET. It also describes how rushing attack formation can be done. In this context the effect of rushing attacks over AODV, which is defined as reactive distance vector protocol is presented in this work. This paper proposes Rushing attack prevention can be done by calculating threshold and average path value calculation. Simulation results shows that packet delivery ratio decreases in rushing attack also control overhead is decreases. In future, this can be compared with DSR protocol.

REFERENCES

[1] Chinkit Suthar and Bakul Panchal. 2014. A Survey on Rushing Attack and Its Prevention in Mobile Ad-hoc Network. International Journal of Advanced Research in Computer Science and Software Engineering. 4(3).

[2] Shikha Jain. 2014. Security Threats in MANETS: A Review. International Journal on Information Theory (IJIT). 3(2).

[3] K. Udhayakumar, T. Prasanna Venkatesan and R. Ramkumar. 2014. Security Attacks and Detection Techniques for MANET. Discovery Journal. 15(42).

[4] Aakanksha Jain, Dr. Samidha Dwivedi Sharma. 2014. Rushing Attack Prevention Algorithm for MANET using Random Route Selection to make DSR and AODV more Efficient. International Journal of Engineering and Computer Science. 3(6).

[5] Satyam Shrivastava. 2013. Rushing Attack and its Prevention Techniques. International Journal of Application or Innovation in Engineering and Management (IJAIEM). 2(4).

[6] Sivakumar and Selvaraj. 2013. Overview of Various Attacks in MANET and Countermeasures for Attacks.

International Journal of Computer Science and Management Research. 2(1).

[7] Swarnali Hazra and S.K. Setua. 2012. Rushing Attack Defending Context Aware Trusted AODV in Ad-Hoc Network. International Journal of Security, Privacy and Trust Management (IJSPTM). 1(3/4).

[8] Gagandeep Aashima and P. Kumar. 2012. Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review. International Journal of Engineering and Advanced Technology.

[9] Parthiban, Amuthan, Shanmugam, and Suresh Joseph. 2012. Neighbor Attack and Detection Mechanism in Mobile Ad-Hoc. Advanced Computing: An International Journal (ACIJ). 3(2).

[10] S.J. Lee, W. Su, and M. Gerla. 2002. On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks. Mobile Networks and Applications. Vol. 7.

[11] RushaNandy, Debdutta Barman Roy. 2011. 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.