ISSN:0975-9646

A New Technique to Prevent MANET against Rushing Attack

Satyam Shrivastava , Dharmendra Mangal

Computer Science & Engineering,
Medi-Caps Institute of Technology & Management,
Indore (MP), India

Abstract- **Mobile ad hoc network is a collection of mobile nodes communicating through wireless channels without any existing network infrastructure or centralized authority. Due to the limited transmission range of wireless network, multiple "hops" are needed to exchange data throughout the network. Routing in mobile ad hoc networks is a challenging task because nodes are free to move randomly. Routing protocols in Ad hoc networks have become an interesting issue due to the fact that the existing routing protocols supports only the fixed infrastructure and are not suitable for MANET. The routing protocols are necessary to maintain the network. Ad-hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) protocol are the reactive or on-demand routing protocol in MANET. Due to the nature of ad-hoc network, it is vulnerable from much kind of security attacks. In MANET, number of sender and receiver is varying time by time. A sender may have multiple links to the other node. This is the nature of the MANET stations that they reply to only the first receive route request. This is the reason of vulnerable of a network to the rushing attack. The security issue is the main problem of MANET, because many nodes perform many kind of misbehavior. The rushing attack, which result in denial of services when used against all previously published on-demand ad-hoc network routing protocol. Rushing attack exploits this duplicate suppression mechanism by quickly forwarding route discovery packet in order to gain access to the forwarding group.**

Keywords- MANET, Security attacks, AODV, Routing, and Rushing attack.

I. Introduction

In the past few years, the popularity of mobile computers has tremendous increase. It began in the year 1893 with Nikola Tesla. This was the year when first successful wireless information transmission was made. As a result the advantage of wireless communication which include no infrastructure requirement and encouraging mobile network. So researches' were interested to search for a new network which uses a cellular system without relying on fixed infrastructure and the network is called the mobile Ad-hoc network.

Mobile Ad-hoc Network is a collection of two or more nodes which are connect in wireless communication medium. These nodes are mobile nodes so they move from one place to another place in the network. This is the reason that MANET has no fixed infrastructure [1, 2]. Nodes in the MANET are capable to communicate with other without the requirement of centralized administrator or centralized authority; also the wireless node can dynamically form a network to exchange information without any existing fixed network infrastructure [3]. A mobile ad-hoc network is a self-organizing system in which nodes act as host and also act as router to forward packet to each other in the multi-hop fashion [4]. In MANET the connectivity between nodes may vary with time due to some of the node may leave the network and new node may arrive in the network [5]. This feature of MANET brings several challenges about the security. Multicasting in MANET is more appreciated then multiple unicast transmission for the better use of bandwidth. This is advantage to send single message to multiple receivers simultaneously. This way network bandwidth and resource may be same. There are two category of multicast routing in MANET, Tree based and Mesh based. Tree based routing offer a single path between source and destination, while mesh based routing offer multiple path between source and destination [6, 7]. So mesh based routing is more suitable than tree based routing for the system with frequently changes in topology [4].

II. Problem Statement

MANET is a type of multi-hop network, infrastructure less and the most important it is a self organizing structure [8]. Due to these reason there is a great challenge for security designers. In the last few years security problems in MANETs have attached much attention; most of the research efforts focusing on specific security areas, like securing routing protocols or establishing trust infrastructure or intrusion detection and response [9].

The security is the major problem of MANET, because many nodes perform many kind of misbehavior. Misbehavior may be defined as selfishness. Selfishness of a node state that, a mobile node uses the recourse of other node and preserve the resource of own. This malicious node creates the problem in MANET [10].

The rushing attack, which result in denial of services and it is very harmful attack when used against all previously published on-demand ad-hoc network routing protocol [11]. Rushing attack exploits this duplicate suppression mechanism by quickly forwarding route discovery packet in order to gain access to the forwarding group [12, 13].

This is the challenge for all the researchers to prevent the network from the attack. Mobile Ad-hoc network is open to all. Anyone can join or leave the network at any time, so we cannot prevent the network but we can create a secure path for data transmission to end users.

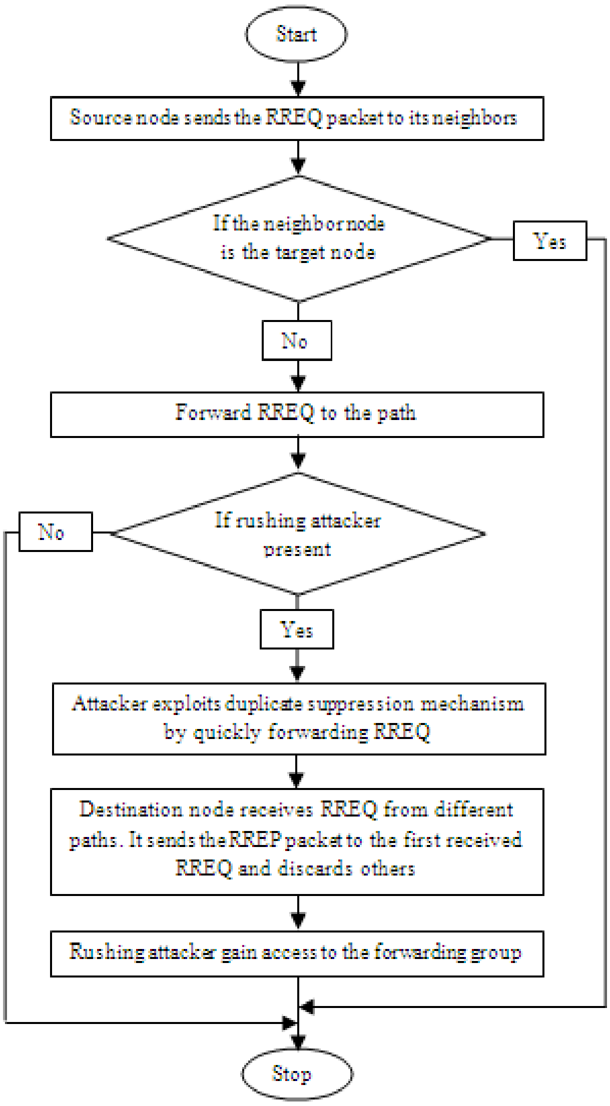
Start
Source node sends the RREQ packet to its neighbors
If the neighbor node is the target node
Yes
No
Forward RREQ to the path
If rushing attacker present
No
Yes
Attacker exploits duplicate suppression mechanism by quickly forwarding RREQ
Destination node receives RREQ from different paths. It sends the RREP packet to the first received RREQ and discards others
Rushing attacker gain access to the forwarding group
Stop

Fig 1 Dataflow diagram of Rushing Attack

III. Proposed Work

In this section, a new method is proposed for preventing the network from rushing attack, which exploits the duplicate suppression mechanism. The proposed method uses the AODV and DSR protocol to forward the packet. These are reactive protocol, so security requirement is high. We cannot restrict the attacker to come in the network but we can select a path from source to destination which is attacker free.

The proposed method is based on the following model, which consist of nine steps. An algorithm of proposed model is:

i) Source node want to send the data to the destination, then it initiate RREQ packet and forward it to its neighbors.

ii) Intermediate nodes check the source address of the RREQ packet.

iii) 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.

iv) Source node calculates the average of the all acknowledgement packet. We called this average time of acknowledgement packet is threshold value.

v) Source node adds this threshold value with individual RREQ packet sending time to its neighbors. We called path value to the addition of threshold value and RREQ packet sending time.

vi) Source node calculates the average time of path value.

vii) Source node selects the route whose path value is greater than the average time of path value.

viii) If there is more than one path value is greater than average time of path value, so source select the path value which is closer to the average path value.

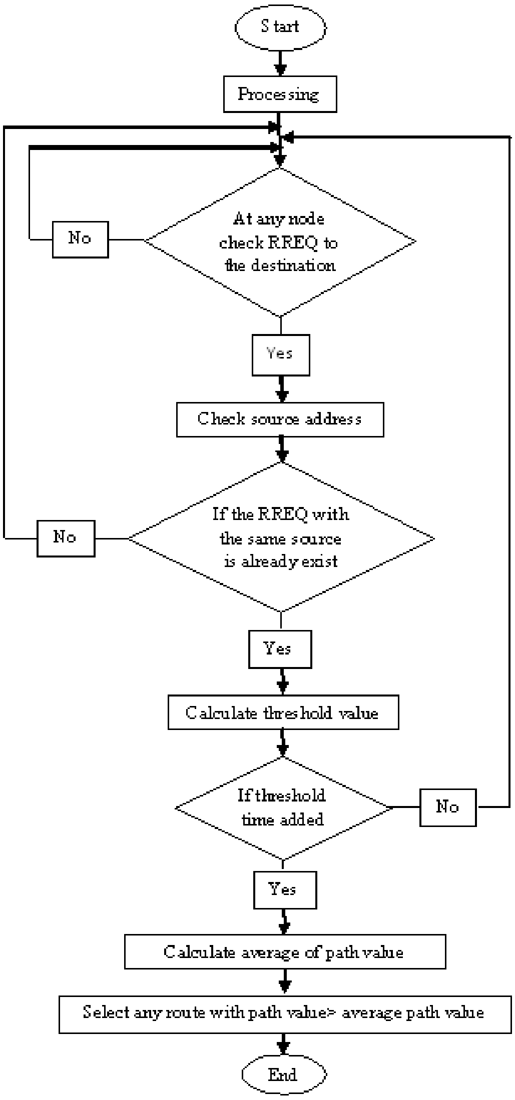
S tart
Processing
At any node check RREQ to the destination
No
Yes
Check source address
If the RREQ with the same source is already exist
No
Yes
Calculate threshold value
If threshold time added
No
Yes
Calculate average of path value
Select any route with path value> average path value
End

Fig 2 Dataflow diagram of Proposed Method

Here we take a network and try to find the suitable path with the help of proposed algorithm which is free from malicious node. There are 10 nodes in the network. Node C, F and H are the malicious nodes.

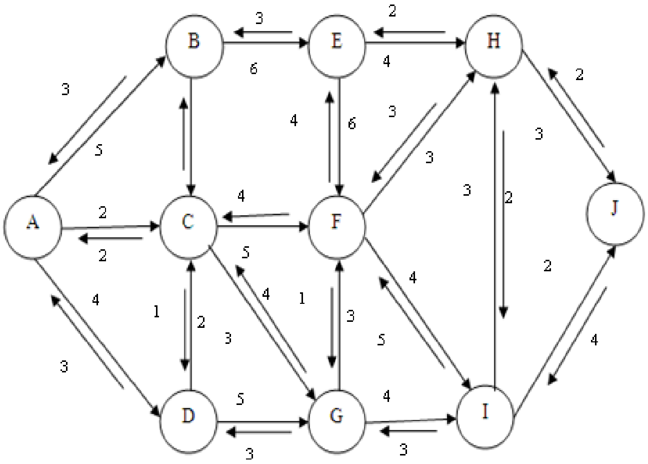

Fig 3 Mobile Ad-hoc Network

At node A, there are three links to node B, C and D.

Source node A send the RREQ packet to the B, C and D. The transmission time from A to B is 5, A to C is 2 and A to D is 3. Source node will wait for the acknowledgement from B, C and D. The acknowledge time from B is 3, from C is 2 and from D is 3.

The average of all the acknowledgement to A is = $(3 + 2 + 3)/3$ = 2.6

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

For node B = 5 + 2.6 = 7.6

For node C = 2 + 2.6 = 4.6

For node D = 4 + 2.6 = 6.6

We called these values path value.

Now find the average of path values = (7.6 + 4.6 + 6.6) / 3 = 6.2

Now node A selects the path whose path value is greater than average of path value. But in this case there are two paths value is greater than average path value. So 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 A-D-G-I-J is chosen for sending the RREQ packet from A to J. This path is free from rushing attack and the communication will take place through this path.

IV. Result And Discussion

The proposed method provides algorithm that can be used to improve the performance of the network.

This Optimized Network Engineering Tools (OPNET) is a very powerful network simulator. Main purposes of OPNET are to optimize the cost, improve the performance and availability. To build a network model the workflow starts with the Project Editor. This is used to create network models, collect statistics directly from each network object or from the Network as hole, execute a simulation and view results [8]. The simulation parameters are shown in the below table.

TABLE I
SIMULATION PARAMETERS

Parameters	**Value**
Simulation time	1 hour
Number of nodes	17
Environment size	10km X 10km
Seed	128
Value per statistic	100
Update interval	500000 events
Simulation kernel	Based on kernel type preference
Area of movement	Within network
Speed	287,170 events/sec
Total event	23,718,553

These graphs gives the comparison between the AODV routing, AODV routing after the attack and AODV routing with the proposed method on the basis of different scenarios. Blue line, red line and green line represent the AODV process, attack and proposed method respectively. It is clear from all the graphs that, attack disturb the routing process but after applying proposed method, the graph is more similar to routing process. Graphs are given below-

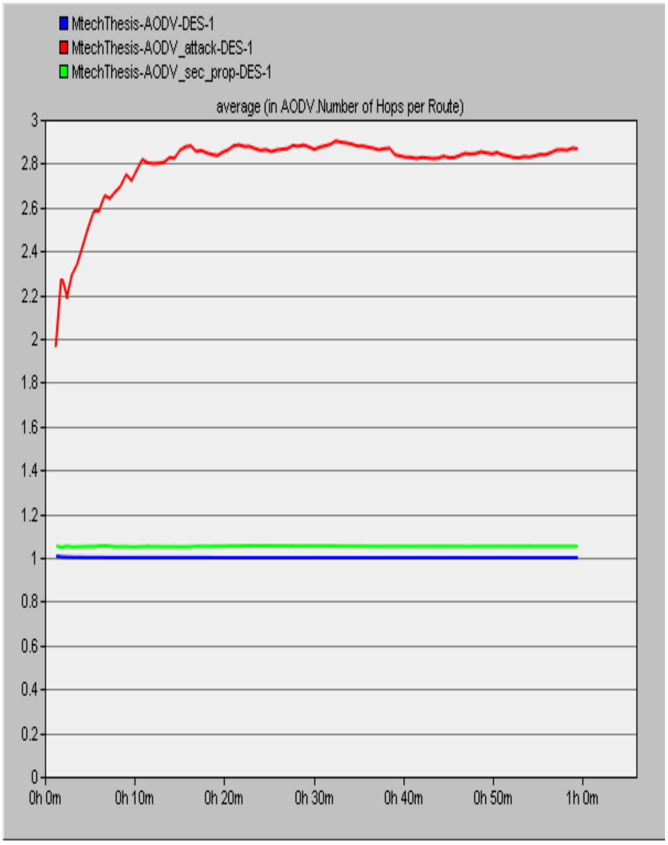

Fig 4: Number of hops per route

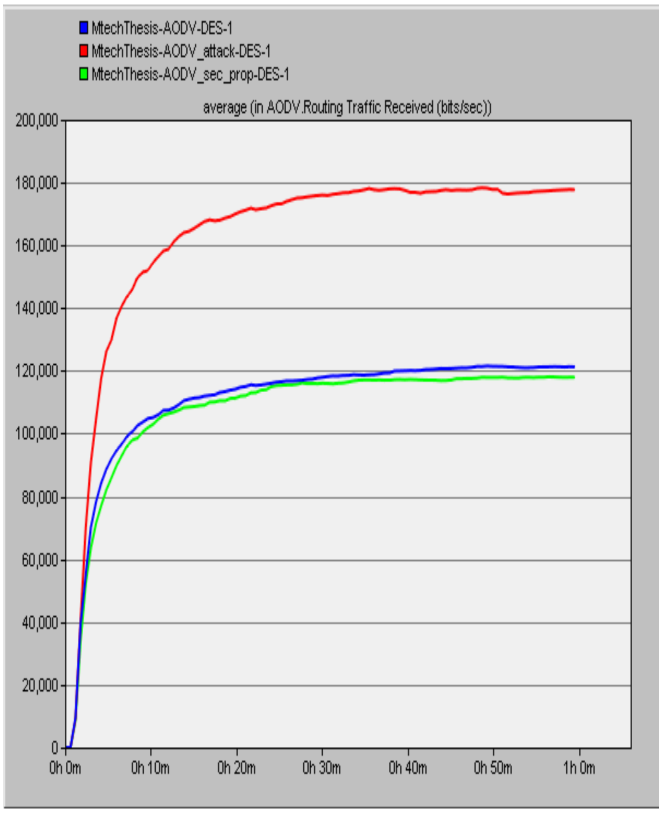

Fig 5 Routing traffic received (bits/sec)

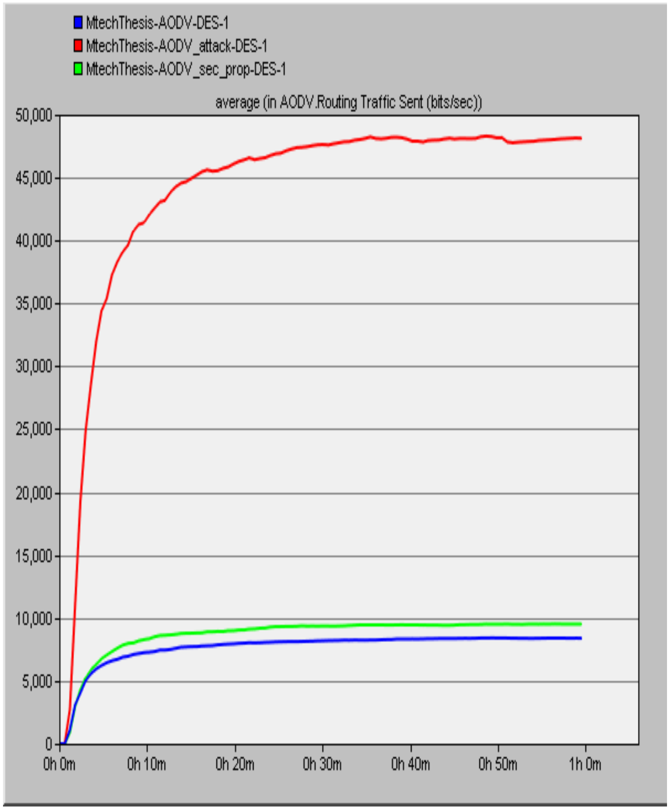

Fig 7 Routing traffic sent (bits/sec)

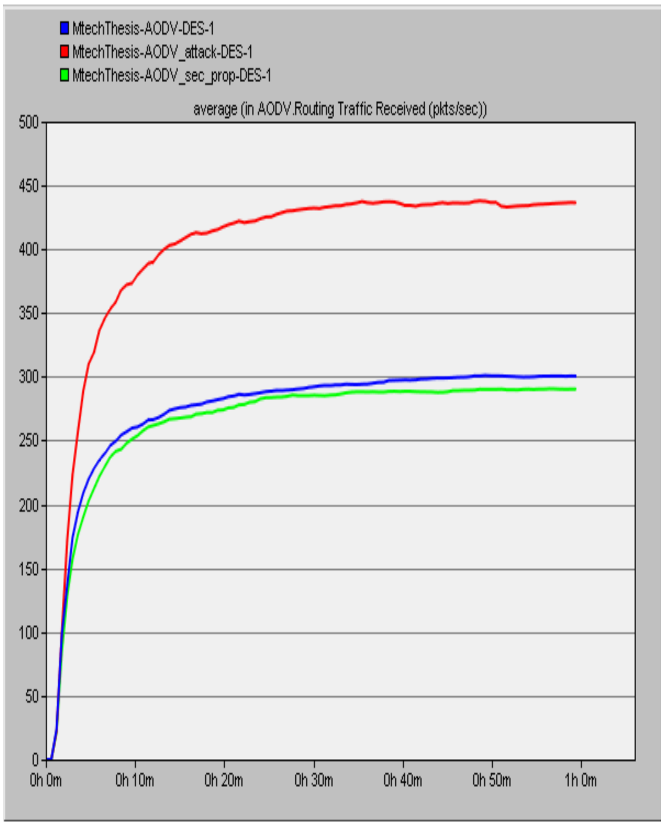

Fig 6 Routing traffic received (packets/sec)

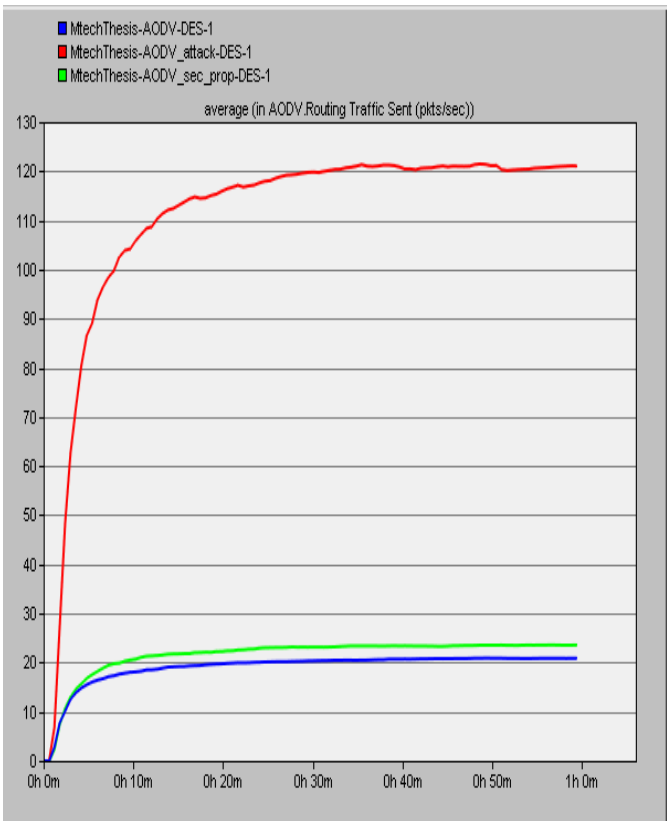

Fig 8 Routing traffic sent (packets/sec)

V. CONCLUSION AND FUTURE WORK

In MANET, number of sender and receiver is varying time by time. A sender may have multiple links to the other node. This is the nature of the MANET stations that they reply to only the first receive route request. This is the reason of vulnerable of a network to the rushing attack

The security issue is the main problem of MANET, because many nodes perform many kind of misbehavior. The rushing attack, which result in denial of services when used against all previously published on-demand ad-hoc network routing protocol. Many researchers proposed method against rushing attack but some method were applicable for AODV and some were for DSR. This proposed method is working for both AODV and give the more accurate result than the previously proposed methods.

If we compare proactive and reactive protocols, the proactive protocols incur shorter delay in sending out packets and they also maintain the entire network topology information. In future we will try to minimize the delay and also will apply this proposed method for TORA.

REFERENCES

[1] K. Sharma, N. Khandelwal, M. Prabhakar, “An Overview Of security Problems in MANET”.

[2] S. Shrivastava , S. Jain, “A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network”, *International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345,* Vol. 4, No. 03, March 2013.

[3] A. Ghaffari, “Vulnerability and Security of Mobile Ad hoc Networks”, *Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization,* Lisbon, Portugal, September 22-24, 2006.

[4] Gagandeep, Aashima, Pawan Kumar, “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review”, *International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958,* vol-1, Issue-5, June 2012.

[5] M. A. Al-Shabi, “Attack and Defence in Mobile Ahoc Networks”, *International Journal of Reviews in Computing ISSN: 2076-3328,* vol. 12, December 31, 2012.

[6] P. Goyal, S. Batra, A. Singh, “A Literature Review of Security Attack in Mobile Ad-hoc Networks”, *International Journal of Computer Applications (0975 – 8887),* vol. 9, no.12, November 2010.

[7] Nikhil Pateria, PERFORMANCE ANALYSIS OF DYNAMIC ROUTING PROTOCOL IN MOBILE AD HOC NETWORK, Journal of Global Research in Computer Science, Volume 2, No. 10, October 2011.

[8] S. Albert Rabara1 and S.Vijayalakshmi2, “Rushing Attack Mitigation In Multicast MANET (RAM3)”, *International Journal of Research and Reviews in Computer Science (IJRRCS),* vol. 1, no. 4, December 2010.

[9] S. Arya And C. Arya2, “Malicious Nodes Detection In Mobile AHoc Networks”, *Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762,* vol. 3, issue 1, pp-210-212, 2012.

[10] K. Vats, M. Dalal, D. Rohila, V. Loura, “Opnet based simulation and performance analysis of GRP routing protocol”, *International journal of advanced research in computer science and software engineering ISSN: 2277128X,* vol. 2, issue 3, March 2012.

[11] Abdullah Saad Al Shahrani. "Rushing Attack in Mobile Ad Hoc Networks", 2011 Third International Conference on Intelligent Networking and Collaborative Systems, 11/2011

[12] V. Palanisamy, P.Annadurai, “Impact of Rushing attack on Multicast inMobile Ad Hoc Network”, *International Journal of Computer Science and Information Security,* Vol. 4, No. 1 & 2, 2009.

[13] T. G. Lupu, “Main Type of Attacks in Wireless Sensor Network”, *Recent Advances in Signals and Syatems, ISSN: 1790-5109*.

[14] R. Agrawal, R. Tripathi, S. Tiwari, “Performance Evaluation and Comparison of AODV and DSR Under Adversarial Environment”, *IEEE International Conference on Computational Intelligence and Communication Systems,* 978-0-7695-4587-5/11, 2011.

[15] S. Basagni, I. Chalamtse, V. R. Syrotiuk, “Dynamic Source Routing for Ad Hoc Networks Using the Global Positioning System”, *IEEE,* 0-7803-5668-3 99, 1999.

[16] A. Rawat, P. D. Vyavahare, A. K Ramani, “Evaluation of Rushing Attack on Secured Message Transmission (SMT/SRP) protocol for Mobile Ad-Hoc Networks”, *IEEE,* 0-7803-8964-6/05/$20, 2005.

[17] H. L. Nguyen and U. T. Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks”, *IEEE Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL’06)* 0-7695-2552-0/06 $20.00, 2006.

[18] L. Tamilselvan and Dr. V. Sankaranarayanan2, “Solution to Prevent Rushing Attack in Wireless Mobile Ad hoc Networks”, *IEEE,* 1-4244-0731 -11/061$20.00, 2006.

[19] A. L. Shahrani, A. Saad, “Rushing Attack in Mobile Ad Hoc Networks”, *IEEE Third International Conference on Intelligent Networking and Collaborative System,* 978-0-7695-4579-0, 2011.