PREVENTION OF MULTIPLE RUSHING ATTACKS IN MOBILE AD HOC NETWORK USING AODV ROUTING PROTOCOL

***Junaid, W; Iqbal, A.**
The University of Agriculture, Peshawar. Pakistan.
*Corresponding author**: Waqas Junaid**
Tel: + 923159471064
E-mail: waqasjunaid1@gmail.com, arshadiqbal84@hotmail.com

ABSTRACT: *Mobile Ad Hoc Network (MANET) is a collection of multi-hop wireless mobile nodes. The communication of MANET is on mutual trust. The topology is changing rapidly and unproductively, there is no central control for routing of packets. Due to its dynamic topology, open medium and scalable characteristics, these networks are more vulnerable to security attacks. Securing MANETs from various attacks becomes a challenging task. One such attack is a rushing attack in Mobile Ad hoc Network. In rushing attack, the attacker quickly forwards the packet in order to get easy access to the route discovery path. Once the route established between the attacker and the destination, then all the information obtained from the source which is false or hardened" [Mention here what is done with the information once it is obtained.]. In this research, we will evaluate the multiple rushing attacks (two, three, and four rushed nodes) and their prevention by setting a time threshold value (0.02) using AODV routing protocol. We will then analyze the previous work with our proposed scheme. The results show that it successfully prevents the multiple rushing attacks by using a time threshold value in mobile ad hoc network and it shows a better performance as compared to previous works by using time threshold value.*

Keywords: *Mobile Ad hoc Network, Ad hoc On demand Distance Vector routing protocol, AODV.*

INTRODUCTION

Wireless ad hoc network are known as On Demand since they forward the data based on the nodes connectivity. The wireless ad hoc network is suitable for the emergency-like situation because it can be deployed in no time since it requires the very least configuration [9]. There are three generations of wireless ad-hoc network. In 1972 the first generation was called packet radio network (also known as PRNET). In the 1980s the second generation came into the market with survivable adaptive radio network (SURAN). In the 1990s the concept of commercial ad hoc networks came into the field with notebook computers as well as with the idea of mobile nodes. In today's world, they are called the third generation of ad hoc network with near-term digital radio (NTDR) and global mobile information system (GloMo) [1]. The application of wireless ad hoc network is mobile ad hoc network (MANET), vehicular ad hoc network (VANET), and wireless mesh network (WMN). Mobile ad hoc network (MANET) can either be infrastructure or non-infrastructure network. In the infrastructure network, there is a base station where all the communication is taken place. In the non-infrastructure network, the communication is purely based on the connected nodes within the transmission range. The MANET is clearly an example of the non-infrastructure network [8]. The MANET is a collection of wireless nodes that work as a peer to peer network [3]. Since the MANET's topology changes from time to time it leads to different security issues and makes it vulnerable to different types of attacks. One of the attacks on the MANET is the rushing attack. In the rushing attack, the adversary quickly forwards the RREQ packet in-order to be a part of the communication [4].

The Rushing attack is one of the security concerns in Mobile Ad hoc Network (MANET). In the presence of a rushing attack, the attacker exploits the duplicate suppression mechanism by rapidly sending route discovery packets so as to access the forwarding group. As the rushed nodes forward the packets faster than the normal nodes, the destination nodes reject the packets from the normal nodes because it is considered as a duplicate packet. So we would need to find the solution to the problem of preventing the multiple rushing attacks using AODV routing protocol and also to investigate the impact of multiple rushing attacks on Average Throughput and Average End to End Delay.

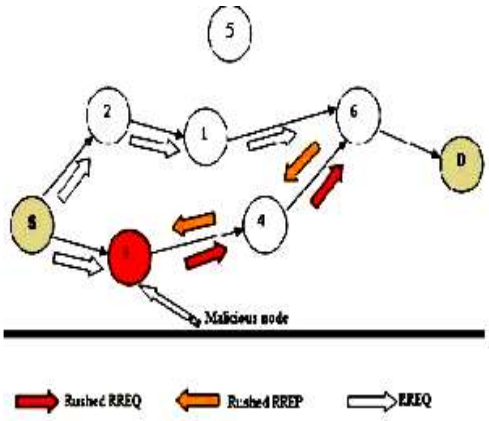

Figure 1: rushing attack [2]

Some of the previous work studied under rushing attack will be discussed in this section.

In a work by Shrivastava [6], the new technique built on the Rushing attack, a malicious node or an attacker increases the speed of routing process. The researcher aim was to list the techniques, which was utilized to defeat the rushing attack and also to concentrate on their working behavior, the researcher presented a technique of threshold value which will be considered throughout the network for routing process to let it prevent the rushing attack in the network.

Suthar and Panchal [7] presented that Mobile Ad-hoc Network contains an autonomous arrangement of mobile nodes that can move openly and speak with each other without a settled Infrastructure. These nodes function as a Router or Host. In MANET there is no Central Control Authority and the topology isn't static. 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 Rushing Attacker takes advantage of the AODV Duplicate Suppression Mechanism, to carry out the Attack. The researchers have reviewed the Rushing

Attack and its Prevention Technique. By altering some AODV Property, the Attack can be prevented or the consequences of the Attack can be decreased. The outcomes of Prevention was shown and the impact of the Prevention in the dissimilar size of the network with dissimilar numbers of Attackers.

Murugan and Selvakumar's [5] standardized on-demand routing protocols in mobile ad-hoc networks were not initially proposed to deal with security issues. Mobile ad-hoc network is a group of different type of nodes, which are linked to each other with the help of wireless link. The group communications is a more difficult security concern in MANET because of participation of multiple senders and recipients. In this work, they proposed rushing attack for AODV with a malicious node that increases the speed of the routing process. In this work of dissertation, AODV routing protocol is utilized for the learning of rushing attack. They also proposed the improved routing scheme to protect ad-hoc networks opposed to rushing attacks using threshold value and the calculation of the average path value.

Valiveti et al [10] Ad hoc network provide decentralized infrastructure-less environment, where nodes cooperate with each other for the purpose of communication, thus susceptible to compromise. This characteristic of ad hoc network leads to security threats. The networks are particularly vulnerable to a denial of service (DoS) attacks that are launched through colluding nodes. This paper's focus is on the Byzantine Flood Rushing attack that threatens the security of the system, and studying its effect on ad-hoc network. The objective of work is to implement Flood Rushing attack in AODV enabled ad-hoc network. Paper presents an approach to implement and analyze the effect of Byzantine Flood Rushing attack and implementation results are plotted.

All of the previous work suggested rushing attack and their countermeasures on how to prevent or eliminate rushing attack but none of them has worked on multiple rushing attacks in which more than one rushed nodes or malicious nodes are created to infect the network or takes the advantage of the duplicate suppression mechanism. Hence, this research or work is based upon the prevention of multiple rushing attacks and the techniques used to prevent the multiple rushing attacks are the time threshold value.

PROPOSED SYSTEM

The prevention of multiple rushing attacks (PMRA) is shown in figure 2. But before the PMRA starts working, a route request is requested towards the destination.

At first the time threshold value is fetched for prevention. It then checks for the packet arrival time for further process since the rushed node or malicious node takes the advantage of the duplicate suppression mechanism which means that it sends the packets faster than the normal nodes or shows itself as the shortest route towards the destination than a condition is put to prevent the rushing attacks as the packet arrival time is greater than the time threshold value or the time threshold is smaller than the packet arrival time then it discards the route request packet (RREQ) and if the time threshold value is greater or equal than the packet arrival time than it accepts the RREQ packet and the same route is used for communication if either the topology changes or doesn't change the same process is repeated for accepting the route request (RREQ) as shown in PMRA figure 2.

The PMRA is based on the performance of the below table 1. The network simulator used is ns-2.35 with a simulation time of 150 seconds. The number of nodes is 25 and AODV is the routing protocol. The size of the packet is 500 bytes; the number of malicious nodes is 2, 3 and 4. The transmission range of the nodes is 250 m. The random mobility model is used as a mobility model. The complete list of simulation parameters is shown in Table 1.

Table 1: Simulation Parameter

PARAMETER	VALUE
Simulator Version	NS 2.35
Area	500m x 400m
Performance Parameters	Throughput, Packet Delivery Ratio, and End to End Delay
Channel type	Wireless
Number of nodes	25
Simulation time	150sec
Routing Protocol	AODV
Packet Size	500 bytes
Rushed nodes	2, 3, 4
Transmission Range	250 m
Transport protocol	TCP
Maximum Mobility	10 m/s
Mobility Model	Random Mobility Model

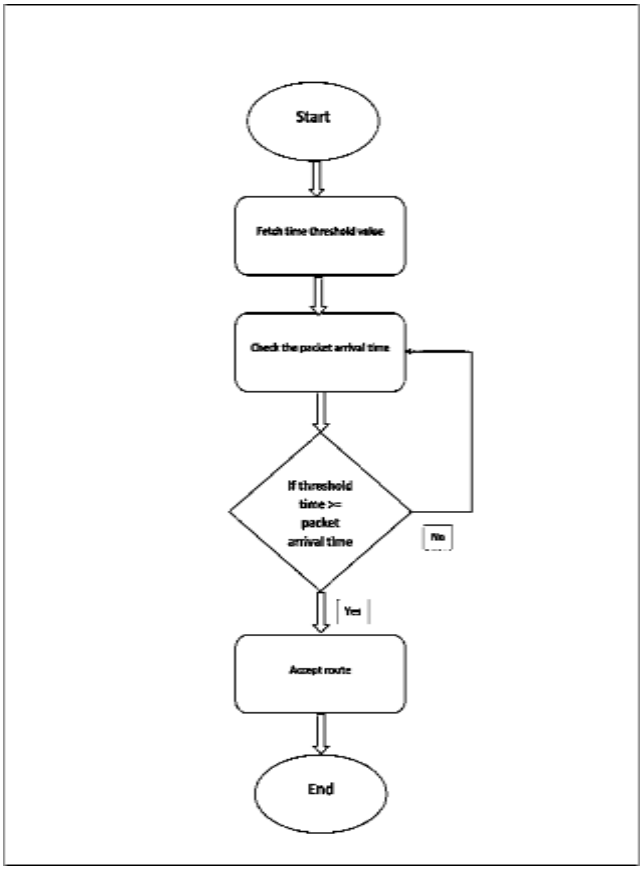

Figure 2: prevention of multiple rushing attacks (PMRA)

RESULTS AND DISCUSSIONS

The number of simulations is drawn on the simulator and results are carried out. At first, the 25 normal nodes with source and the destination node are labeled as shown in figure 3.

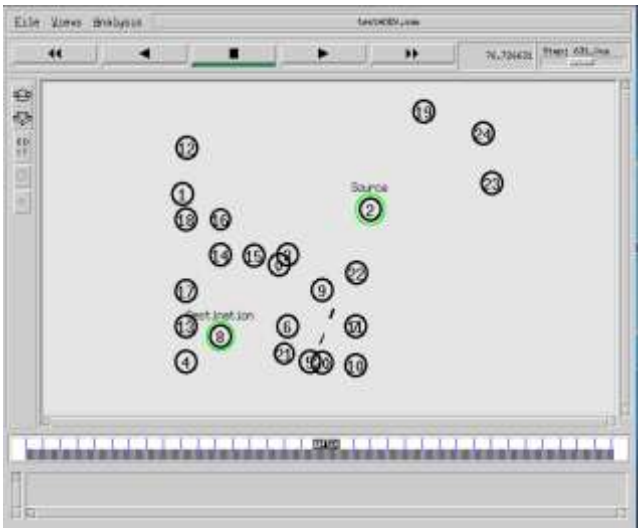

Figure 3: Simple MANET

In figure 3, the source Node is 2 while the destination Node is 8. Clearly, it is seen from the figure that the communication is from the intermediate Node 5.

Since the communication is from Node 0 and 2 then these two nodes are configured and drawn as rushed nodes as shown in figure 4.

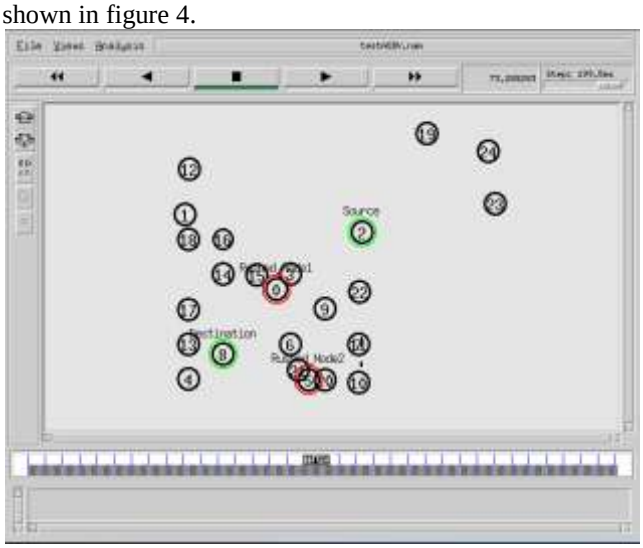

Figure 4: **prevention of 2 rushed nodes**

In figure 4 the two rushed nodes named as Node 0 and Node 5 are prevented using the threshold value as the process described in figure 2 by having a communication through intermediate Node 10 between source Node 2 and destination Node 8.

Then, after this, the three rushed nodes are configured by adding another rushed node as shown in below figure 6.

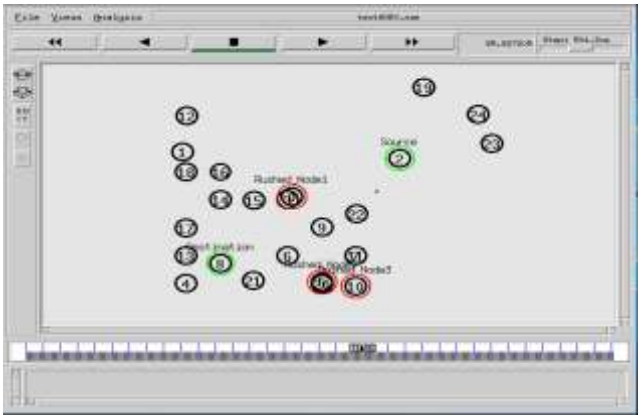

Figure 5: prevention of 3 rushed nodes

The 3 rushed nodes 5, 0, and 10 are prevented using the time threshold value by communicated source Node 2 and destination 8 through intermediate Node 22.

Since the intermediate node was 22, it is taken as the rushed node number 4th as shown in Figure 6.

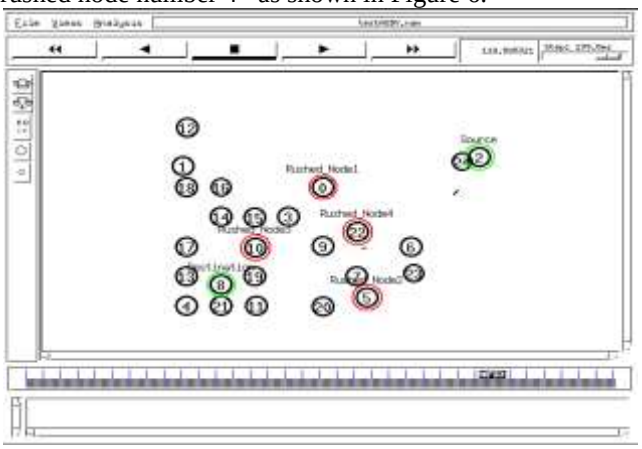

Figure 6: prevention of 4 rushed nodes

In Figure 6 the node number 22 was added as a malicious node so the total number of the rushed nodes becomes 4. These rushed nodes are prevented using the time threshold value. The communication between source and destination is held by the intermediate nodes 6 and 9.

The results generated is the percentage of throughput with two, three, and four rushed nodes of the previous work and after PMRA of two, three, and four rushed nodes as shown in figure 7.

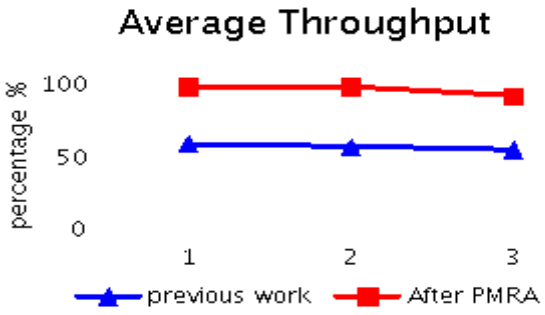

Figure 7: Throughput

The results showing in Figure 7 is shown in percentage. These results are compared with [10] previous work and thus showing better performance with our PMRA as compared to the previous work. The triangle line showing the performance of previous while the square line showed the performance of PMRA.

The results of Packet Delivery Ratio (PDR) of two, three, and four rushed nodes of previous work and after PMRA of two, three, and four rushed nodes is given in Figure 8:

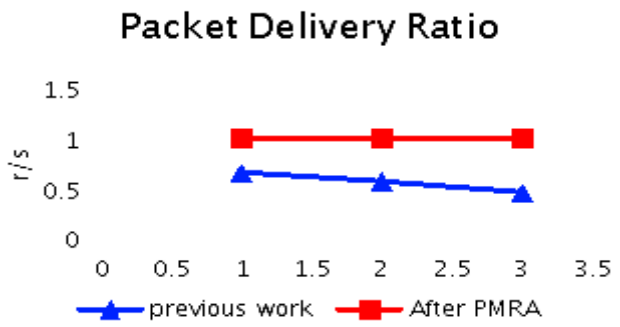

Figure 8: packet delivery ratio

The Figure 8 of packet delivery ratio shows better performance with PMRA and shows low performance when it tern with the previous work [5] as seen by the triangle and rectangle line of the figure.

The End to End Delay is shown in Figure 9 with previous work and after PMRA of two, three, and four rushed nodes.

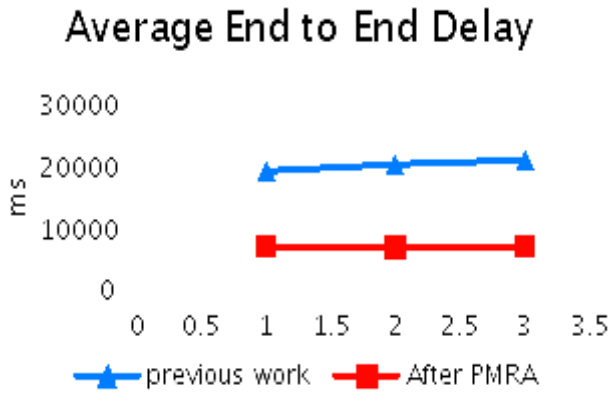

Figure 9: end to end delay

Table 2: Impact of multiple rushing attacks on throughput, PDR and end to end delay

Performance parameters	With previous work of two rushed nodes	With previous work of three rushed nodes	With previous work of four rushed nodes	After PMRA of two rushed nodes	After PMRA of three rushed nodes	After PMRA of four rushed nodes
Throughput	57.37 %	55.41 %	53.18 %	96.7 %	96.37 %	90.1 %
End to End Delay	18858 ms	19864 ms	20664 ms	6701 ms	6614 ms	6721 ms
PDR	0.65 r/s	0.56 r/s	0.45 r/s	0.9961 r/s	0.9977 r/s	0.9962 r/s

The end to end delay is compared with [10], the PMRA showing better results as compared with previous work as it is assumed that the network with less delay is better than with higher delay.

The impact of multiple rushing on throughput, end to end delay is shown in table 2 where all the data generated using the AWK from ns-2.35.

CONCLUSION AND FUTURE WORK

The purpose of this research was to prevent the multiple rushing attacks in mobile ad hoc network, which it has adequately and effectively accomplished. Also, in this research, a suggested model has been used in which a time threshold mechanism for the prevention of multiple rushing attacks has been proposed. By using of this proposed model, multiple rushing attacks were prevented. After preventing the multiple rushing attacks (PMRA), the valid route was used with genuine delay time, and also the network integrity, authentication, and performance were increased. With the ability that MANETs have now permanent wired-network infrastructure, even in the difficult environment, one can effortlessly configure networks. This simulation uses network simulator (ns-2.35), demonstrating the execution of system with and without rushing attack. During the rushing attacks, all the data was rushed by rushed nodes and prevent the rushed nodes and valid communication start without rushing attacks, there was no secure communication between the source and the destination nodes in the network.

In future work, it is assumed to have only one source and one destination node in the network with multiple rushed nodes for future it can be stretched out by including more source and destination nodes in the network with multiple malicious nodes between the networks.

REFERENCES

1. Bakht, H., "The history of mobile ad-hoc networks," *ComputingUnplugged*, 2005.
2. Bharti, M. Goyal., Goyal, R., "Detection of rushing attack by comparing energy, throughput and delay with AODV," *IPASJ International Journal of Computer Science (IIJCS)*, **2**(11): 2014.
3. Khan, F., Sonar, M., Vyas, M. T., "A Survey Paper on Detection of Sybil Attack in MANET," *IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC)*, **6**(1): 2016.
4. Kumar, C. N., Satyanarayana, N., "Detection of Sybil attack using position Verification method in MANETS," *International Journal of Modern Trends in Engineering and Research*, **01**(06): 2014.

5. Murugan, V. S., Selvakumar, K., "An Improved method of routing process and reducing Rushing attack for ad-hoc on-demand distance vector in MANET," *Journal of Engineering and Applied Sciences*, **11**(21): 2016.
6. Shrivastava, S., "Rushing Attack and its Prevention Techniques," *International journal of Application or Innovation in Engineering & Management (IJAIEM)*, **2**(4): 2013.
7. Suthar, C., Panchal, B., "Rushing Attack Prevention with modified AODV in Mobile Ad hoc Network," *International Journal of Engineering Development and Research*, **2**(4): 2014.
8. Taneja, S., Kush, A., "A Survey of Routing Protocols in Mobile Ad Hoc Networks," *International Journal of Innovation, Management and Technology*, **1**(3): 2010.
9. Tonguz, O. K., Ferrari, G., "Ad hoc Wireless Networks: A Communication-Theoretic Perspective. Wiley," 2006.
10. Valiveti, S., Sharma, S. R., Kotecha. K., "Performance Evaluation of Byzantine Flood rushing attack in ad-hoc network" I*nternational Journal of Electronics and Communication Engineering & Technology (IJE D COMMUNICATION ENGINEERING & TECHNOLOGY (IJECET)*, 5(2): 2014.