# Effect of Rushing Attack in AODV and its Prevention Technique

Gajendra Singh Chandel
HOD, CSE
SSSITS, Sehore
Madhya Pradesh, India

Rajul Chowksi
Student, (M.Tech.)
SSSITS, Sehore
Madhya Pradesh, India

## ABSTRACT

The MANET incorporates mobile nodes that forward information or packets from node to node without a wired connection. The topology changes rapidly and unproductively, there is no central control for routing of packets hence the communication is on mutual trust. There are many proposed routing protocol in which on-demand routing is most preferable among all as its overhead is very low. Thus attention has been paid on developing a secure reactive protocol against various attacks. In this proposed work effect of rushing attack is presented over AODV. This attack results in denial-of-services and is effectively damaging as it can also be performed by weak attacker. Thus we develop a Rushing attack prevention (RAP) is a generic rushing attack prevention mechanism for the reactive protocols. In this proposed work AODV protocol is used for study of rushing attack and implemented the proposed techniques over it then compared the results of AODV with attack and with prevention technique.

## General Terms

Mobile Ad-hoc networks (MANET).

## Keywords

MANET, rushing attack, RAP, Reactive Protocol, AODV

## 1. INTRODUCTION

Ad-hoc network is collection of autonomous nodes where all the nodes are dynamically configured without any centralized management thus form of network without any pre-existing infrastructure. Such networks is applicable in many fields like military & police exercises,, disaster relief, operations, robot data accumulation, mine site operations etc. MANET [1, 3, 4,] is prone to various types of attacks as compared to wired networks, but is used largely due to the reason that the network can be setup at any place & anytime without any pre-existing infrastructure.

Attacks in MANET:

A. Passive attack: It does not disrupt the operation of data or data is not altered.
B. Active attack: It alters the data or destroys the data that is being transmitted.

Some common types of attacks in MANET:-

i. **Wormhole attack**: In this attack two malicious node tunnels between and traffic and transfers packet.
ii. **Blackhole attack**: The attacker reply for the route request with the short path and thus get access to the data.
iii. **Byzantine attack**: In this attack the intermediate node perform collision of data, forming loops dropping of packets thus degrading the routing services.
iv. **Rushing attack**: This attack provides a denial-of-service, which uses duplicate suppression mechanism & quickly forward route discovery and gain access on data.

## 2. RELATED WORK

AODV is the type of reactive protocol which is on demand protocol. As its name implies it works only when user demand for communication related to the transmission and receiving the data packets. The AODV routing protocol is the up gradation of the destination sequenced distance vector routing. The main advantage of the AODV is that, it provides the better communication in the network without any congestion. The noteworthy contribution related is as follows:

Yin-Chun Hu et al [2] presented in year 2003 a new type of attack " Rushing attack", this attack results in denial of services (DoS) when used against on-demand routing protocol. All on demand protocols are unable to detect this attack. This attack can also be performed by weak attacker. Thus a generic rushing attack prevention (RAP) have been developed it exploits no cost unless the underlying protocol fails to find a working route .This method provide provable prevention even for strong attackers.

S. Albert Rabara, and S. Vijayalakshmi [3] proposed how rushing attacker works in multicasting network. Rushing attack is the processes of disturbing routing mechanism by pumping a high speed malign MRREQ (Multicasting Route Request) to reach the last node, thus increasing the network traffic . The solution suggested is threshold technique ($D^3UT^3$) *in which a alarm is triggered when the number of requests is greater than the defined threshold value.*

Rusha Nandy, and Debdutta Barman Roy [4] 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 a 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 than the node is malicious and hence removed from the cluster.

Desilva et al [7] proposed rushing attack prevention technique aka RAP. This paer have proposed an adaptive method of threshold value calculation where value is not fixed and predefined . Threshold value can also be statically calculated..

V. Palanisamy and P.Annadurai [10] presented the rushing attack, in this attack the malicious node exploits duplicate suppression mechanism and quickly forwarding route discovery packets to gain access on the forwarding data .Thus attacker provide route discovery first and hence the possibility of false route selection increases .This paper compare the performance of attacker and its success rate in three scenario: near sender ,near receiver ,anywhere in network.

Hyojin Kim et al. [11] proposed here a novel, robust routing scheme to defend ad hoc networks against rushing attacks. This scheme utilizes the "neighbor map mechanism". This methodology focuses on route maintenance rather than using route discovery. By using this methodology path recovery delay is reduced and thus provide energy efficient solutions.

Swarnali Hazra and S.K.Setua [14] extended the AODV protocol witch is based on trust model and provide secure network. This model is based on threshold value of trust ,the network consist of trust evaluating node which takes the decision to include or not to include the trustee node in routing path depending on the final trust value computed by the trust model . AODV is enhanced with different functional modules: Node Manager, Trust Module and Decision Manager. Trust based AODV secures the routing path by isolating the rushing attacker, based on their trust value.

## 3. RUSHING ATTACK

A rushing attack uses duplicate suppression mechanism by which it quickly forward the route discovery reply to the routing request broadcasted in order to gain access to the forwarding data; the rushing attacker gain access in forwarding group and thus can tap data. The Rushing attacker can forward route discovery or route request more quickly than the authentic node thus the chances of selection of path that includes attacker increases. The attacker can gain high speed in access of request by slowing down the response time of other nodes. The attacker can increase the traffic in network by keeping the network transmission queues full of the nearby nodes. Hence nodes will respond to the request late due to heavy traffic. The authentic nodes will be busy authenticating request containing bogus authentications thus slowing down their response ability.

## 4. RUSHING ATTACK PREVENTION TECHNIQUE

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 non-legitimate node keep sending the requests and hence accessing the networks queue. By this attack requests sent by legitimate node will be considered as delayed request and hence discarded. The overall rushing attacks formation Algorithm given in flow chart.

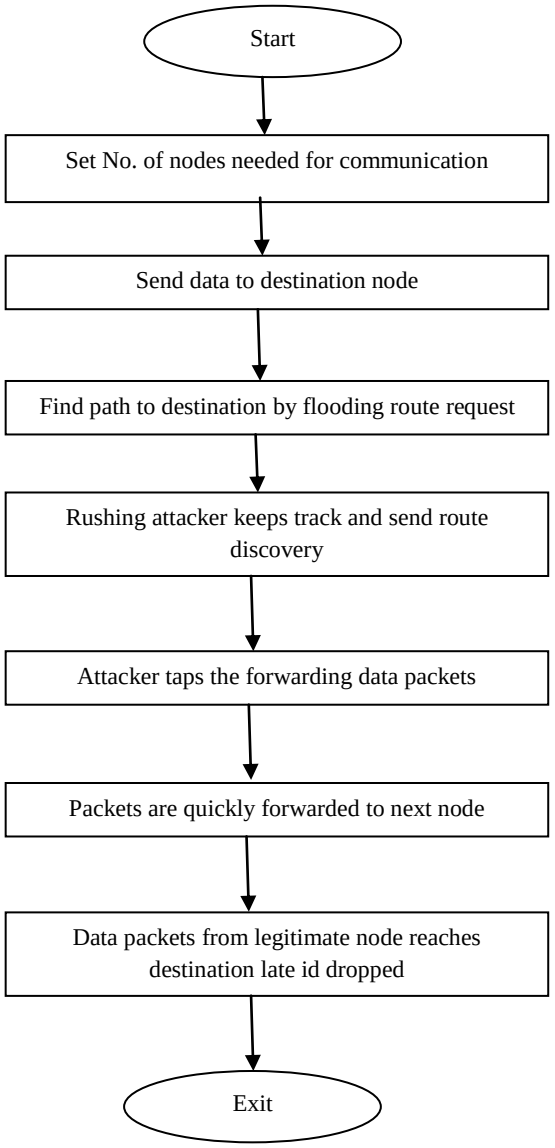


**Fig. 2 Rushing attack formation Algorithm [15]**

This flooding attacker that increases network traffic by bogus request can be detected by individual node analysis. In this case each node can use a check measure on its neighbors. We can define a threshold value, and the nodes should always check request RREQ of neighbors. If the request rate exceed the threshold value than the node should put the neighbor in its BLACK LIST (malicious node list) this approach can be fruitful in detecting the rushing attacker but the point of concern is that predefined threshold value should be set proper so that it can detect the attacker. And hence consequences; if the threshold value is not set properly than the genuine node can also be black listed. We proposed an addition of them average time calculation, if the Request time is greater than average time then it has to pass the simulation process again.

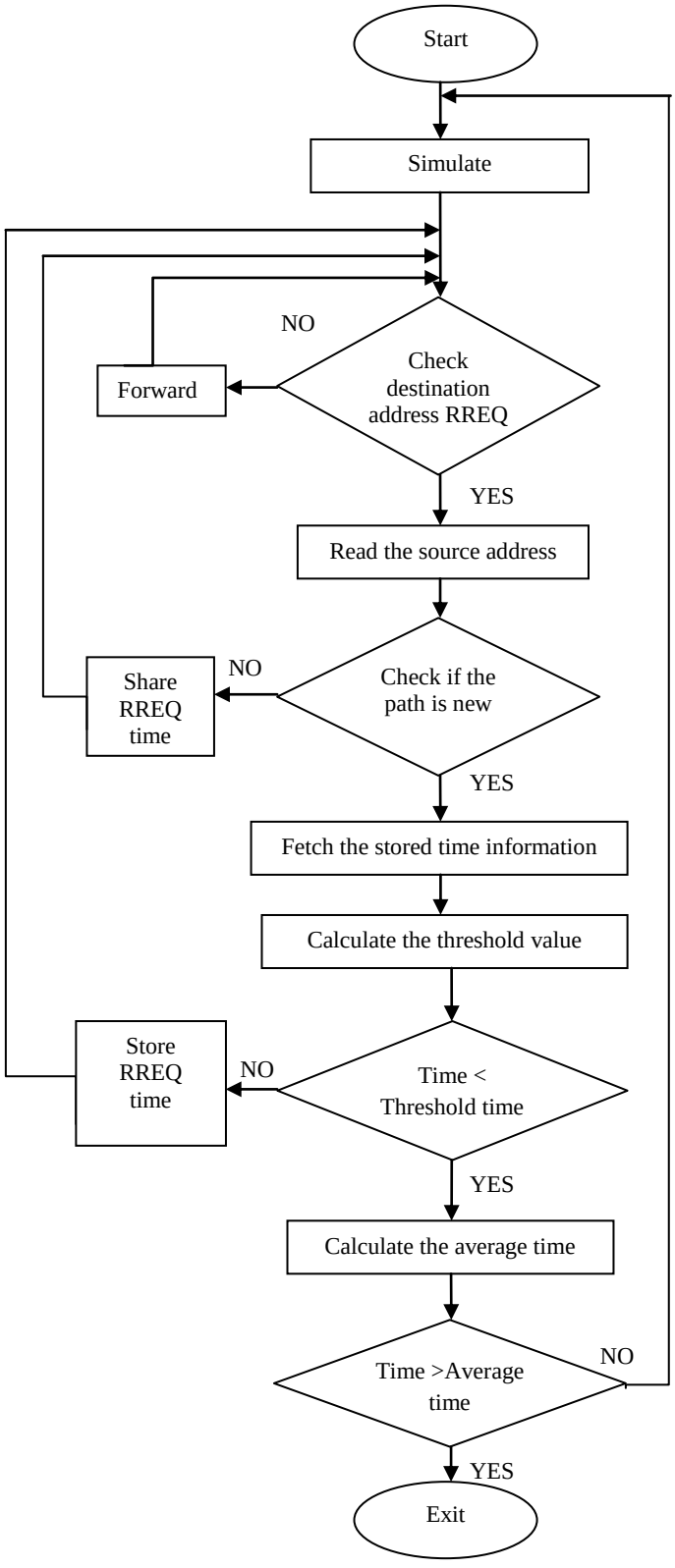


**Fig. 3 Proposed Rushing attack Prevention technique**

## 5. SIMULATION PARAMETER & RESULTS

Simulation parameter details are required the parameters are as follows And generated results using OPNET 14.0A Modeler.

### 5.1 Simulation Parameter

The simulation parameters can be as follows:-

i. Number of nodes
ii. Network size (m2)
iii. Simulation duration (Sec.)
iv. Packet Inter- arrival time ( Sec)
v. Packet Size (bits)
vi. PDR (Packet delivery ratio) in presence of malicious nodes

For the simulation OPNET 14.0A Modeler is used as a simulator. The performance comparison of AODV can be done under:

- **Without attacks:** As a Normal AODV.
- **With attacks:** Where the Rushing attacks with one attacker, two attackers and three attackers.
- **Proposed Method:** Result drawn by RAP method implemented in AODV.

### 5.2 Simulation Scheme

- Campus with 10km X 10 km
- 17 Nodes
- MANET
- Reactive Protocol: AODV
- Attack: Rushing Attack

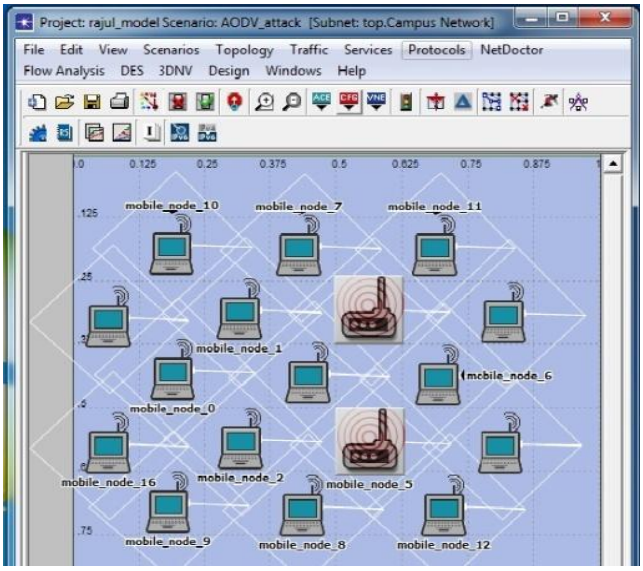


**Fig.4 Proposed MANET Scheme**

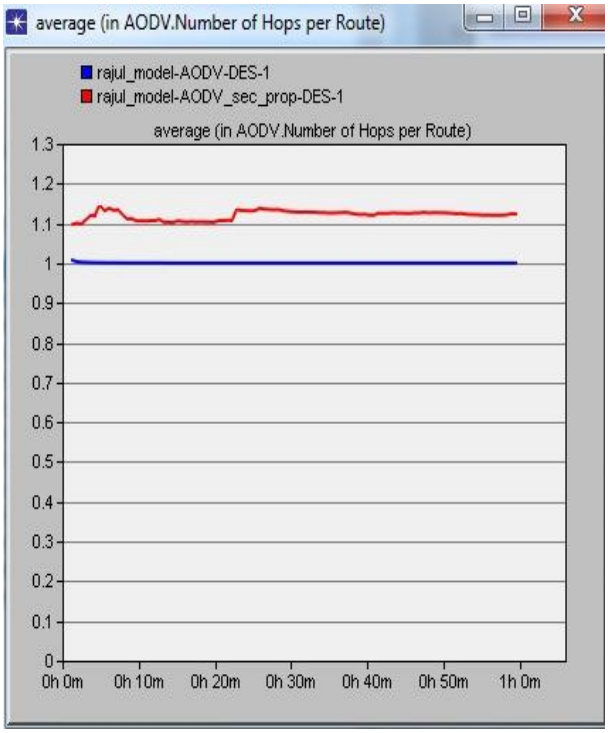


**Fig. 5 AODV no. of Hopes per Route (Average)**

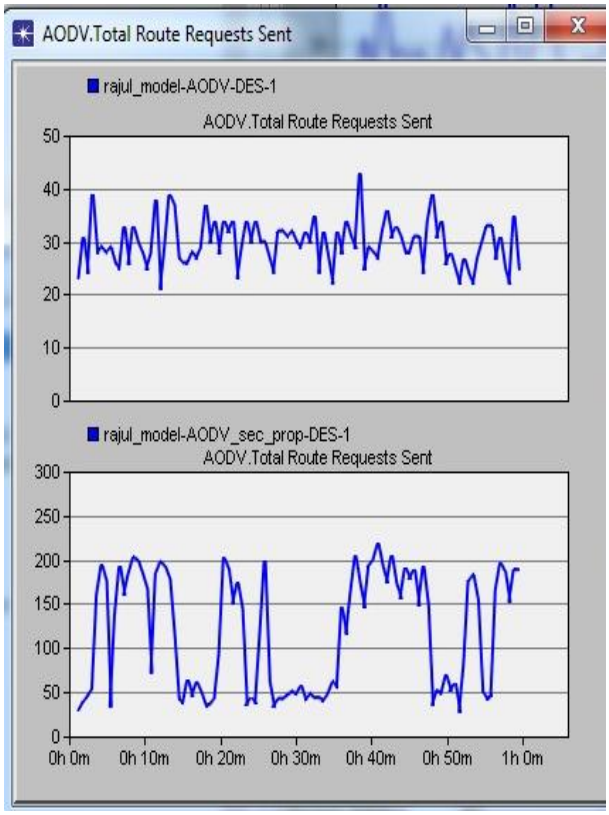


**Fig.6 AODV Total Route request sent (Average)**

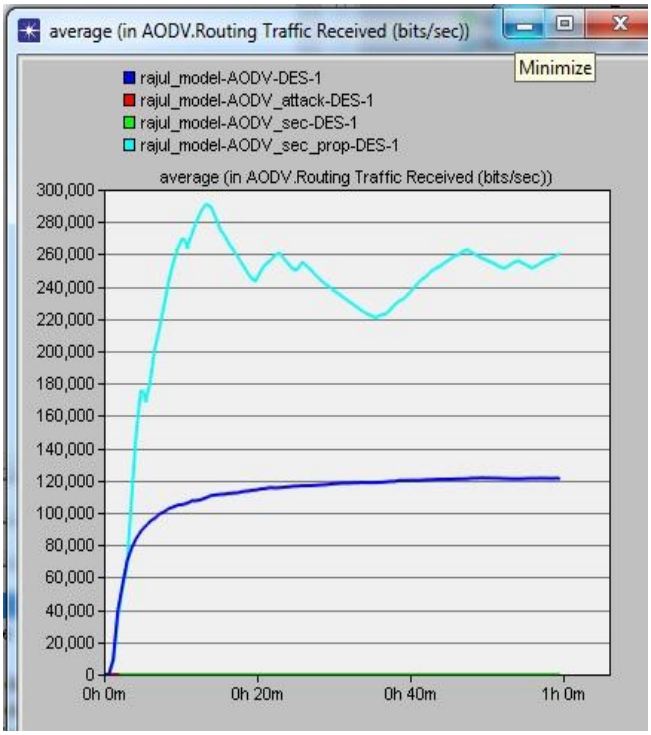


**Fig. 7 AODV Routing Traffic received (Average)**

## 6. CONCLUSION

In this paper MANET and its security attacks taxonomy is described in conjunction with various attacks. 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 time and average time and comparing it with request time. The result depicts the proposed method working with a small network cluster i.e. around 20 nodes. This work can be extending to multiple attackers and large network nodes (50-70 nodes). And the same scheme can be tried to DSR protocol and comparison can be made with AODV and DSR protocol.

## 7. REFERENCES

[1] Bing Wu, Jianmin Chen and Jie Wu, Mihaela Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer© 2006, pp. 1-38.

[2] Yin-Chun Hu, Adrian Perrig and David B. Johnson, "Rushing attack and Defense in Wireless Ad Hoc Network Routing Protocols", Wise 2003, San Diego, California, USA.

[3] S. Albert Rabara, and S. Vijayalakshmi, "Rushing attack Mitigation in Multicast MANET (RAM3), IJRRCS,Vol.1, No.4, December 2010, pp. 131-138.

[4] Rusha Nandy, and Debdutta Barman Roy, "Study of Various Attacks in MANET and Elaborative Discussion of Rushing Attack on DSR with clustering scheme", International Journal of Advanced Networking and Application, Vol. 3, Issue 01, 2011, pp. 1035-1043.

[5] Supriya and Manju Khari, "MANET Security Breaches: Threat to a Secure Communication Platform", IJANS, Vol.2, No.2, April 2012, pp. 45-51.

[6] Shobha Arya and Chandrakal Arya, "Malicious Nodes Detection in Mobile Ad Hoc Networks", Journal of Information and Operations Management, Vol.3, No.1, 2012, pp. 210-212.

[7] S.Desilva, and R.V.Boppana, "Mitigating Malicious Control PacketFloods In Ad Hoc Networks,"Proceedings of IEEE Wireless Communications and Networking Conference 2005, , vol. -4, pp. 2112-2117, March 2005.

[8] Y.Guo, S.Gordon, S.Perreau, "A Flow Based Detection Mechanism against Flooding Attacks in Mobile Ad Hoc Networks," Wireless Communications and Networking Conference, IEEE (WCNC 2007), pp.3105-3110, March 2007.

[9] Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks," Journal Of Computing, Volume 3, Issue 1, January 2011.

[10] V. Palanisamy and P.Annadurai, " Impact of Rushing attack on Multicast in Mobile Ad Hoc Network," International Journal of Computer Science and Information Security (IJCSIS), Vol. 4, No. 1 & 2, 2009.

[11] Hyojin Kim , Ruy de Oliveira, Bharat Bhargava and JooSeok Song, "A Novel Robust Routing Scheme against Rushing Attacks in Wireless Ad Hoc Networks." Published online: 12 July 2012© Springer Science+Business Media, LLC. 2012.

[12] Satyam Shrivastava and Sonali Jain, "A brief introduction of different types of security attacks in found in Mobile Ad-hoc Networks," International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4, No. 3, March 2013.

[13] Satyam Shrivastava," Rushing Attack and its Prevention Techniques, "International Journal of Application or

[14] Innovation in Engineering and Management (IJAIM), Vol. 2, No. 4, April 2013, ISSN 2319 – 4847.

[15] Swarnali Hazra1 and S.K.Setua, "Rushing Attack Defending Context Aware Trusted Aodv In Ad-Hoc Network," International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 3/4, August 2012.

[16] Gajendra Singh Chandel and Rajul Chowksi, "Study of Rushing attack in MANET," International journal of ucterion (IJCA), Vol. 79, No. 10, Oct. 2013.