Study of Rushing Attack in MANET

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

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

ABSTRACT
A mobile ad-hoc network or MANET incorporates mobile nodes that forward information or packets from node to node without a wired connection. This is the topology changes rapidly and unproductively, there is no central control for routing of packets. The communication is on mutual trust. There are many proposed routing protocol, on-demand routing is most preferable among all as its overhead is very low. This significantly attention has been paid on developing a secure reactive protocol against various attacks. In this paper a survey and study about rushing attack is provided. This attack results in denial-of-services and is effectively damaging as it can also be performed by weak attacker. Thus a Rushing attack prevention (RAP); generic rushing attack prevention mechanism introduced for the reactive protocols.

General Terms
Mobile Ad-hoc networks(MANET).

Keywords
MANET, rushing attack, RAP, Reactive Protocol.

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 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:-

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

Table 1: Security Attacks Classification [1]

Attacks	Example
Passive Attack	Eavesdroping, traffic analysis and monitoring.
Active Attack	Jamming, Spoofing, modification, replaying and DoS.

Table 2: Security Attacks on each layer of the Internet Model [1]

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11),WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

2. 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.

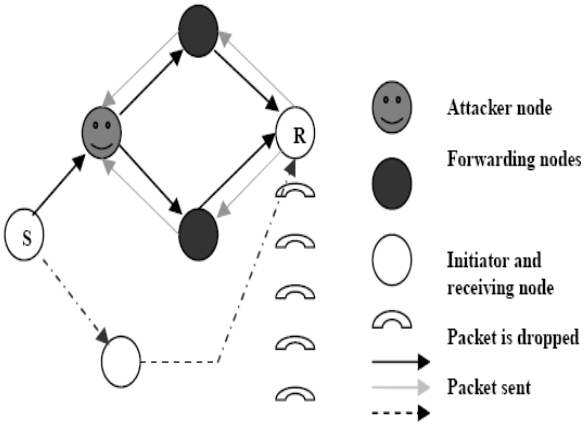

Fig.1 Rushing attack formation [4]

3. RUSHING ATTACK PREVENTION (RAP):

A rushing attacker use 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.

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.

Desilva et al [7] have proposed an adaptive technique in which the parameter is not predefined the threshold value can be detected by using statically.

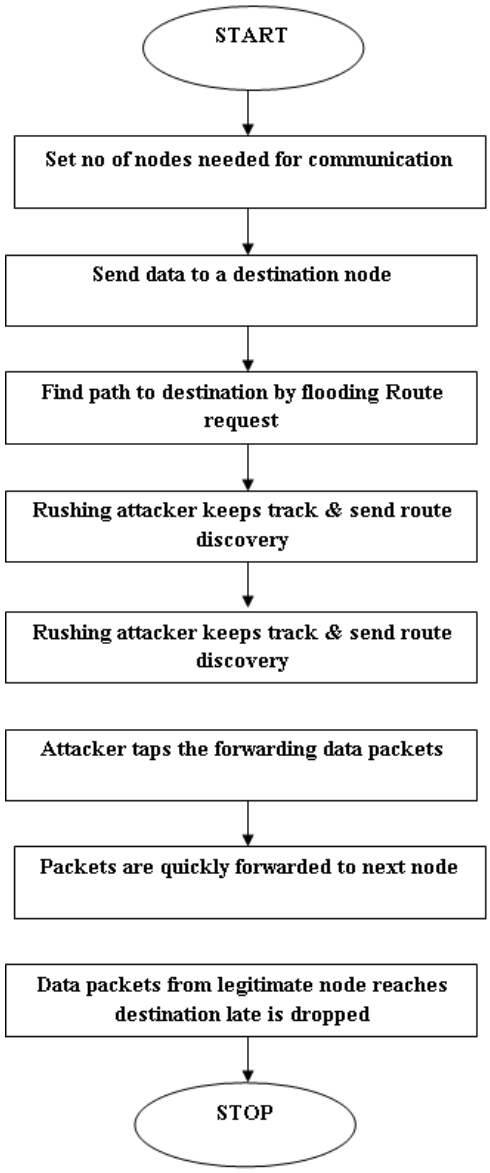

Fig. 2 Rushing attack formation Algorithm

4. CONCLUSION

In this paper it is described various types of attacks, rushing attack have been described thoroughly. Rushing attack against on-demand ad-hoc routing protocol. It provides a denial-of-service against the ad-hoc routing have been described thoroughly and rushing attack against on-demand ad-hoc routing protocol. It provides a denial-of-service against the ad-hoc routing protocol.

The attacker floods the network with bogus request and increase the traffic & thus the response time of nodes increases thus by using duplicate suppression mechanism gain access to information.

In this paper a technique proposed of RAP (Rushing attack prevention) in which a threshold value set to a level for the response time. This technique further can be modified with threshold value and average time calculation to identify the source of bogus requests.

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