International Journal of Advanced Technology in Engineering and Science
Vol. No. 09, Issue No. 06, June 2021
www.ijates.com
ijates
ISSN 2348 - 7550

Rushing Attack in MANET: A Review

M.krishnamoorthy , Srinivasan.J

[1,2] *Assistant professor, Department of Computer Science & Application, SCSVMV University.*

ABSTRACT

Ad hoc networks are the special networks formed for specific applications. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in a peer-to-peer fashion without involving central access points. Many routing protocols like AODV, DSR etc have been proposed for these networks to find an end to end path between the nodes. These routing protocols are prone to Rushing attack due to malicious nodes. There is a need to detect and prevent these Rushing attack in a timely manner before destruction of network services.

KEYWORDS: ***Network Protocols, Wireless Network, Mobile Network, Ad-hoc Networks, Routing Protocols, Security, and Attackers.***

1. INTRODUCTION

Ad hoc Networks are the networks formed for a particular purpose. These networks assume that an end to end path between the nodes exists. They find their use in special applications like military, disaster relief etc that are in a need of forming a new infrastructure less network with all pre-existing infrastructure being destroyed. Characteristics of Ad hoc networks include:

1) Lack of fixed infrastructure: An ad-hoc network is a collection of nodes that do not rely on pre-existing infrastructure for their connectivity. So these types of networks are flexible and easily reconfigurable.
2) Limited resources: Due to lack of fixed infrastructures, these networks have limited resources for their use. Resources like battery power, bandwidth, computation power, memory etc have to be used judiciously for the survival and proper functioning of the network.
3) Dynamic Topology: Nodes in the ad hoc networks are often mobile wireless devices like laptops, PDAs, smart-phones etc resulting in frequent change of their location, resulting in a dynamic topology.

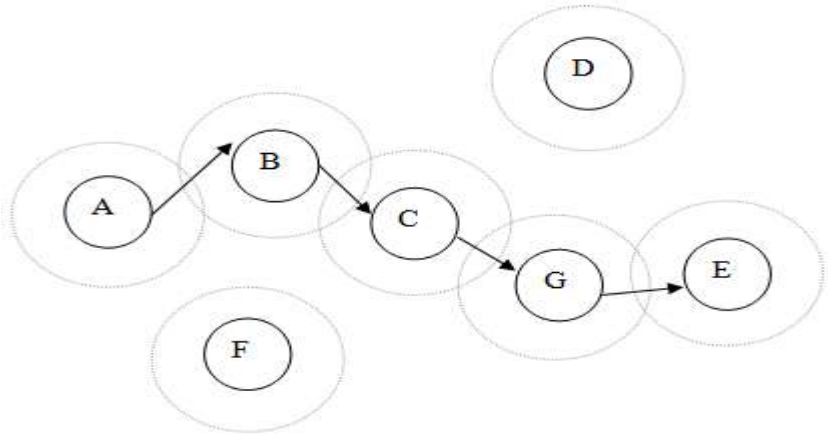

Figure 1 : An Example of Ad Hoc Networks

An example of ad hoc networks is shown in Figure.1. Here ad hoc network is being established by communication between wireless mobile nodes A, B, C, D, E, F and G. Node A wants to send a message to another node E in the network. Routing in the network for such a scenario takes place through multiple intermediate relay hops present in between A and E, assuming that all nodes in the network are trustworthy. Since A and B are in the wireless range of each other, A sends the message to B, B and C are in range of each other so message will get passed to C and so on till the message finally reaches E via the path A, B, C, G and E.

The organization of this paper is as follows. Section II explores the various routing protocols in ad-hoc networks. Section III highlights the various security attacks involved. Conclusion and future work is categorized in Section IV.

2. ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS (MANETS)

The main goal of routing protocols in ad hoc networks is to find out the optimal path with minimum overhead, minimum bandwidth consumption and minimum delay between the source and the destination node. As most of the nodes in ad hoc networks are wireless mobile nodes, the topology of such type of a network does not remain fixed. As a result, it becomes the node's responsibility to regularly discover the network topology in order to route the messages properly.

Therefore, there is a need for various routing protocols to discover an optimal path from the source to the destination. A single routing protocol cannot work optimally in different network scenarios. A need is therefore felt for an appropriate protocol selection taking in consideration different network parameters such as density, size and the mobility of the nodes.

On the basis of the network topology, the routing protocols in MANETS are broadly categorized as Proactive Routing Protocols, Reactive Routing Protocols and Hybrid Routing Protocols which are discussed as follows:

1. **Proactive Routing Protocols** - In the proactive routing protocols, routing is done using the information present in routing tables maintained at each node i.e. table driven routing. These tables are exchanged on a periodic basis between the nodes. Each entry in the table contains the information of the next hop for reaching to a node or subnet and the cost of this route. Since information of the neighboring nodes is maintained at each node, the time for route selection becomes minimal.

Following are the problems from which pro-active routing algorithms suffer:

a) Dynamic topology of the network results in some frequent changes in the routing table resulting in invalid routes as the new routes cannot be updated very frequently. As a result, there is a slow reaction on restructuring and hence, the failures of links.

b) Increase in network size results in increase in size of routing table which in turn increases the network load while updating or exchanging tables.

Scenarios for which these types of protocols are best suited are:

i) Lesser node mobility

ii) Lesser density or fewer nodes

iii) Small sized networks.

Various pro-active routing algorithms are Optimized Link State Routing (OLSR) [10], Landmark Routing Protocol (LANMAR) , Topology Broadcast based on Reverse Path Forwarding (TBRPF) etc.

2. Reactive Routing Protocols - In case of Reactive Routing protocols, the routing is done by the nodes only on demand i.e. only when the node needs to send a message. The sender floods its neighbors with Route Request (RREQ) packets to find route in the network. Any destination/intermediate node in the network having path to the destination will reply back with Route Reply (RREP) to the sender and the routing is accomplished.

These suffer from following disadvantages:

a) There is a time delay in finding the routes since a large number of control packets have to be exchanged before the exchange of actual data.

b) Network congestion may result due to excessive flooding of packets. Reactive Routing find their applications in the following network scenarios:

i) High mobility networks.

ii) Medium size networks.Various Reactive routing algorithms are Ad Hoc On-Demand Distance-Vector (AODV)[10], Dynamic MANET On Demand (DYMO), Admission Control enabled On demand Routing (ACOR).

3. Hybrid Routing Protocols - Hybrid Routing Protocols takes the advantage of both reactive and pro-active routing algorithms. In the initial stages, the nodes identify the routes using some pro-active algorithms and later on uses reactive algorithms for on demand routing. Both pro-active and reactive nature of the protocol can be used interchangeably depending on the different network scenarios. Since neither pure proactive nor the reactive approach can alone handle all the network requirements, so the hybrid approach may be in general the optimal choice.

The main disadvantages of such algorithms are:

i) Number of activated nodes determines the advantage that can be taken
ii) Reaction to the traffic demand depends on the gradient of traffic volume. Various Hybrid routing algorithms are Zone Routing Protocol (ZRP) , Zone-Based Hierarchical Link State (ZHLS) etc.

3. ROUTING ATTACKS

3.1. Flooding Attack

It is the basic form of Denial of Service (DoS) Attack. The aim of this attack is to paralyze the whole network by exhausting network resources like bandwidth of the network, battery of nodes etc.

1. Attackers may initiate massive bogus route request (RREQ) packets that will definitely be rebroadcast on and on by other nodes. Bogus may be in the sense that the destination address does not exist in the network. As there will not be any reply for these RREQs, network will be flooded leading to the consumption of battery power and bandwidth of all nodes. For example, consider a simple network scenario shown in Figure 2. Here node D generates RREQ packets destined to the node address H, which is actually not present in the network and broadcast it to all neighboring nodes(C, G and E) in the network. Since no neighbor node will be able to find H, they will again rebroadcast it assuming that some other nodes may be able to find the path to H. In this way battery power and bandwidth are being wasted without doing any useful work with RREQ flooding.

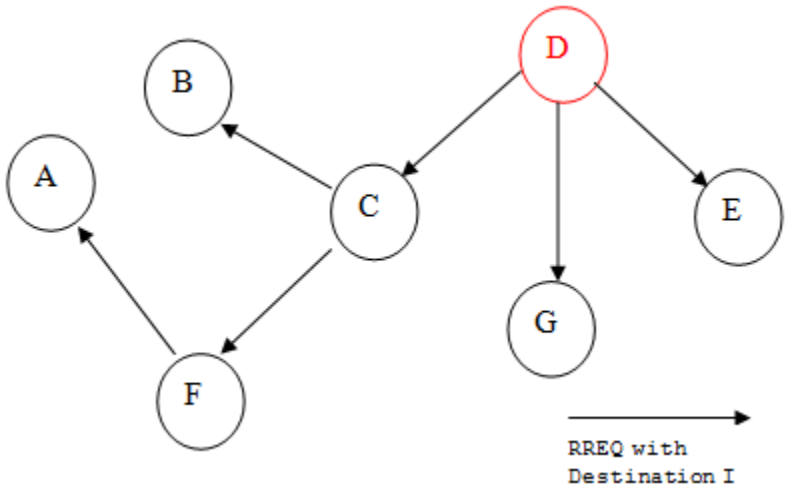

Figure 2 : Example of Flooding Attack

2. Analogous to RREQ flooding, a malicious node can do data flooding also. In this technique after setting path to all the nodes, attacker node sends useless data packets to them.

Detection of flooding attack can be done in following ways:

☐ The detection of any attack can be performed with the cooperation of genuine nodes in the network. For detecting the presence of a malicious node responsible for RREQ flooding in the network, rate of packet (or RREQ) generation of any node should be checked by the neighboring nodes. If the rate exceeds some threshold value (set either statically or dynamically by the algorithm) that node should be put into the blacklist and this information should be broadcasted in the network as proposed in [2, 3, 4, and 5].

☐ Similarly for the prevention of data flooding, a threshold for data rate generation by any node in the network is to be set and should be checked periodically for all the neighboring nodes in the network as proposed in [6].

Some of the approaches that solve this attack are presented as follows:

In [6], authors have proposed solutions for both the types of flooding (RREQ flooding and data flooding). They categorized all system nodes as strangers, acquaintances and friends depending on the trust level which is calculated using various parameters like association length, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, etc. The trust relation

between the above categorized nodes is as follows: Trust threshold (friend) > Trust threshold (acquaintance) > Trust threshold (Stranger).

For the prevention of RREQ and data flooding, different thresholds are being set for different node categories like if Xrs, Xra, Xrf denotes RREQ flooding threshold for a stranger, acquaintance and friend node respectively, then their values satisfy the given mathematical relation Xrf > Xra > Xrs.

3.2. Rushing Attack

The term "rushing" suggests that the attacker will speed up to become a hop of the path to a targeted node. This is done by forwarding RREQ quickly than the authorized nodes to increase the probability that routes discovered will be the ones including attacker. It can thus tamper the message traffic passing through it. This type of attack can be caused in the following way:

An attacker can enhance its forwarding speed by flooding the neighboring nodes with bogus RREQ packets in order to slow their processing speed.

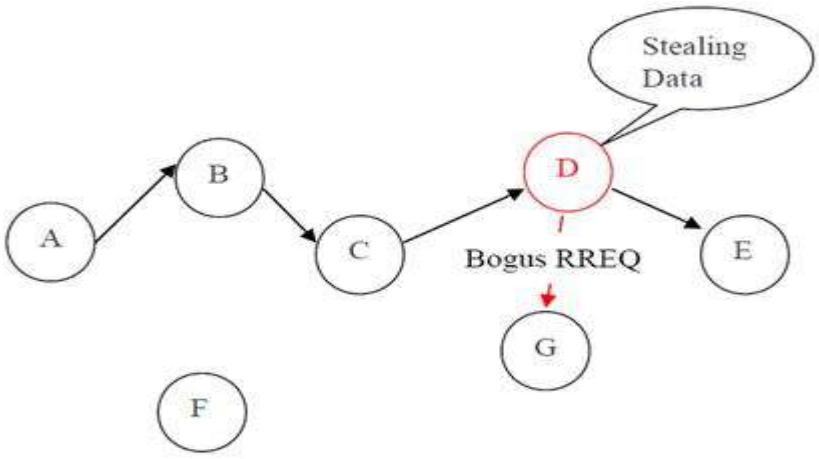

Figure 3: An example of Rushing Attack

Consider a scenario in Figure 3 where node A requests for the route to node E by sending RREQ packets. Now D which is a rushing node, after getting the RREQ request engages other nearby node G by sending bogus RREQ packets which in turn slows down the processing speed of G. Taking advantage of that, D becomes the part of the route from A to E.

Attacker can also speed up its RREQ packets transmission by transmitting them at higher transmission power, thus decreasing the number of hops required to reach the destination. [9] described a set of generic mechanisms that together defend against the rushing attack which are *secure Neighbor Detection*, *secure Route delegation* and *randomized* ROUTE REQUEST *forwarding*.

4. CONCLUSION AND FUTURE WORK

This paper presented a popular attack like rushing attack in MANETs. Various issues that need to be addressed keeping in view the security of MANETS have also been highlighted. The need of the hour is to detect and prevent these Rushing attack in a timely fashion in time. In the future work, the author would like to propose an integrated security system which will analyze the network for detecting the presence of these Rushing attack. After detection of a Rushing attack author will try to pinpoint the attacker nodes and then mitigate their affect by excluding those nodes from the system.

REFERENCES

[1] S. Agrawal, S. Jain, and S. Sharma, "A survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks," Journal of Computing, Volume 3, Issue 1, January 2011, ISSN 2151-9617.

[2] V. Balakrishnan, V. Varadharajan, U.K. Tupakula, "Fellowship: Defense Against Flooding and Packet Drop Attacks In MANET," Network Operations and Management Symposium, NOMS 2006, pp. 1- 4, 2006.

[3] 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.

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

[5] Y. Sasson, D. Cavin, A. Schiper, "Probabilistic Broadcast for Flooding in Wireless Mobile Ad hoc Networks," 2003 IEEE Wireless Communications and Networking, (WCNC 2003), New Orleans, LA, USA, vol.2, March 202003, pp.1124-1130.

[6] Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao, "Performance Analysis of Flooding Attack Prevention Algorithm in MANETs," World Academy of Science, Engineering and Technology 2009.

[7] M.A. Shurman, S.M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conference, pp. 96-97, 2004.

[8] J. CAI, P. YI, J. CHEN, Z. WANG, N. LIU, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network," 2010 24th IEEE International Conference on Advanced

Information Networking and Applications (AINA),Perth, Australia, April 20-23, 2010, pp.775- 780,.

[9] Y.C. Hu, A. Perrig and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," September 2003.

[10] T.H. Clausen, G. Hansen, L. Christensen, and G. Behrmann, "The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation," Proceedings of IEEE Symposium on Wireless Personal Mobile Communications 2001, September 2001.