BLACK HOLE ATTACK IN MANETS: A REVIEW

Srinivasan.J,
Assistant professor, Department of Computer Science and Applications, SCSVMV University, TamilNadu.

ABSTRACT-Ad hoc networks are the special networks formed for specific applications. Operating in ad-hoc mode allows all Mobile 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, SAODV, SBR, ARSA etc have been proposed for these networks to find an end to end path between the nodes. These routing protocols are prone to attacks like Black-hole attack by the malicious nodes. There is a need to detect and prevent this Black-hole 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 are often created on-the-fly and for one-time or temporary use. 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) 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.

2) 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.

3) Autonomous Networks i.e. stand-alone self-organized system: Due to their decentralized nature, these networks eliminate the complexities of infrastructure setup, enabling devices to create and join networks "on the fly" anywhere, anytime, for any application. A node in the ad hoc networks can communicate with all other nodes which are in its transmission range.

Nodes in the network are self-sufficient for the purposes like routing application messages, assuring security of the network and so on.

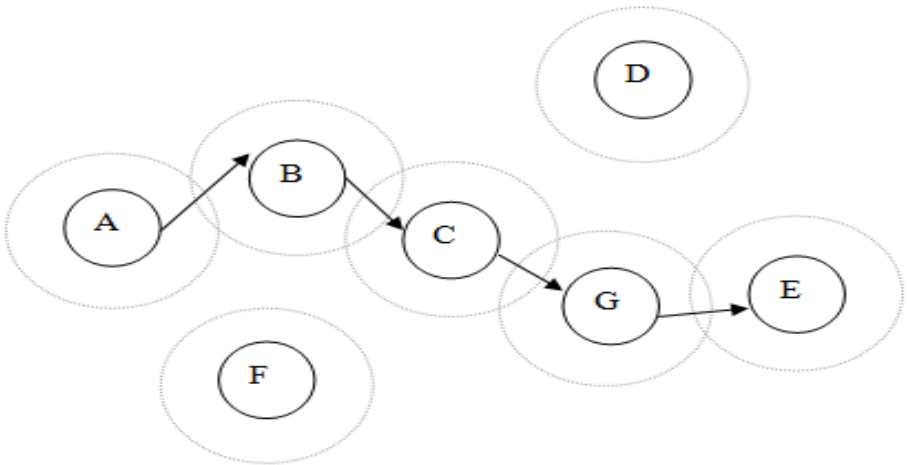

Figure 1 : An Example of Ad Hoc Networks

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 presents the various routing attacks. Section IV concludes the paper.

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.

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.

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.

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.

3. ROUTING ATTACKS

3.1. Black hole Attack

The term “black hole” suggests a node which absorbs all information passing through it by not forwarding it to the destination node. As a result of the dropped packets, the amount of retransmission needed increases leading to congestion. A black hole attacker misuses the routing protocol to tamper the normal working of the network in the following ways [7, 8]:

[1] A black hole node after receiving the RREQ packets for a particular destination sends the route reply (RREP) packet, with modified higher sequence number to the source claiming that it is the destination. Source after getting this pseudo RREP sends all the data to this attacker node.

[2] It can also send false RREP packet to the source to advertise that it has the shortest path to destination. A black hole can easily intercept the packets for a particular destination. As an example, consider Figure. 4 as a network scenario with F as a black hole attacker intercepting packets of node E. When it receives a RREQ packet for E say from A, then it replies back to A with a RREP packet informing that it is having shortest path to E. Now as per working of AODV routing protocol A assumes that shortest path to E is from F and sends all the data destined for E to F which in turn will drop those packets.

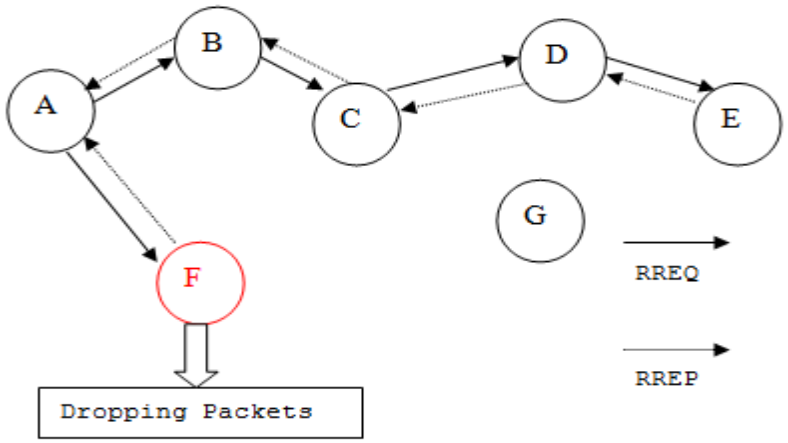

Figure 4: An Example of Black Hole Attack

Detection of black hole attack can be done in various ways. First is by overhearing the actions of all neighbor nodes as in [8]. Authors in [10] suggest two solutions for prevention of the network from black hole attacks which are presented as follows:

a) First algorithm finds more than one route (at least three) to the destination node. Sender sends RREQ packets to its neighbors. All the intermediate nodes (including malicious node as well as destination node) will reply to this pinged packet. Source then waits for receiving a number of paths having some common intermediate nodes in between it and destination. Using

these shared nodes, it can confirm a safe route to the destination and transfer the buffered data packets. If it does not get any shared nodes in between, it will wait for more route replies RREP packets from the neighbors hoping it will get one with shared nodes soon. This approached suffers from drawbacks like time delay in finding more routes and selecting the safest one.

4. CONCLUSION AND FUTURE WORK

This paper presented a popular attack like black hole 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 the black hole attack in a timely fashion. In the future work, we would like to propose an integrated security system which will analyze the network for detecting the presence of these black hole attacks. After detection of this Black hole attack we 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.