A SURVEY ON BEHAVIOUR OF BLACKHOLE IN MANETS

Pinki Tanwar*

Shweta**

ABSTRACT

A mobile adhoc network is a collection of mobile nodes which form a network which is not fixed. The nodes in the network dynamically add and join the network. This nature of nodes makes them susceptible to malicious attacks. Ad hoc On-demand Distance Vector routing (AODV) is a widely adopted network routing protocol for Mobile Ad hoc Network (MANET). But the routing protocol should be safe enough to avoid such types of attacks.. This paper discusses the AODV protocol suffering from black hole attack. An analysis has been given which shows the amount of packet loss in the presence and absence of black hole in the network.

Keywords – Attacks, black hole attack, Packet loss, MANET.

* Assistant Professor, JMIT, Radaur,

** Assistant Professor, JMIT, Radaur

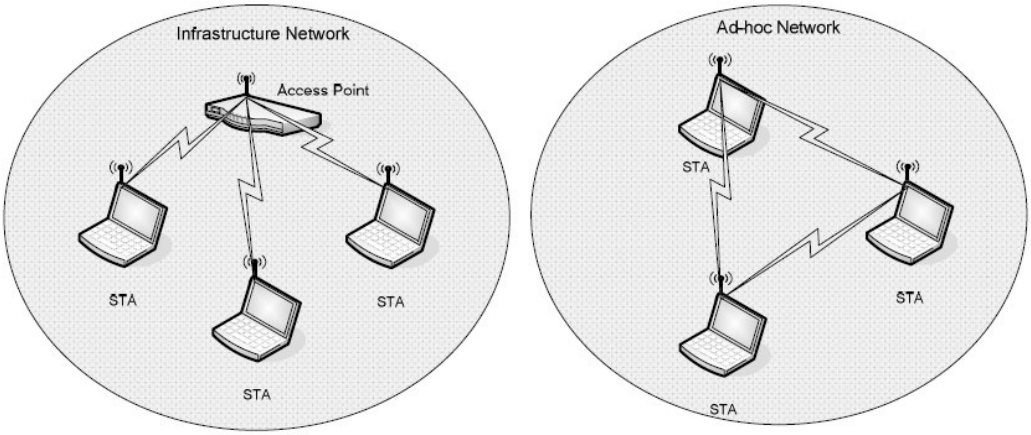
INTRODUCTION

Wireless communication is used to transfer data among users without a wired infrastructure. Using electromagnetic waves, mobile users transmit and receive data over the air. Wireless communication spreads from home RF to satellites, from cellular phones to walkie-talkies. Its mobility, simplicity and cost saving installation advantages make the wireless communication more popular, especially in recent decades Increasing user mobility needs and developments in the use of laptop computers and PDA's is one of the main reasons of the popularity of wireless networks.

A mobile ad hoc network (MANET) [4] is a collection of wireless mobile nodes [2] which have the ability to communicate with each other without having fixed network infrastructure or any central base station. The major disadvantage is their limited bandwidth, memory, processing capabilities and open medium and these are more prone to malicious attacks. Two basic system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET).

As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV.

Figure 1: Infrastructure and Adhoc Network



One such routing protocol which is prone to attacks is AODV which consists of two phases: *route discovery* and *route maintenance.* This paper discusses AODV and how black hole in a network following AODV affects the performance of the network.

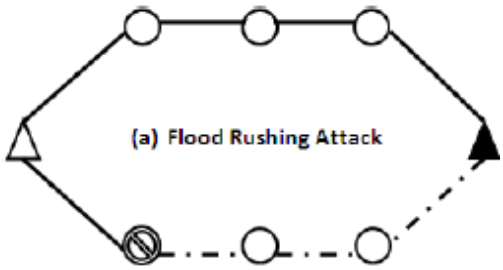
TYPES OF ATTACKS

Our paper discusses following four kinds of attacks which make devastating effects if initiated together in certain combination:

Flood rushing attack*:* This attack exploits the weaknesses during the propagation of legitimate flood of route discovery process in reactive routing protocols. Being the route discovery as its target, the initiating (adversary) node attempts to include itself in the selected route. As discussed above, the first route request is been accepted and following route discovery requests are discarded (flood suppression) in route discovery by reactive routing protocols. So, the adversaries do its best to make themselves a part of first request to reach the destination. Unlike a valid node, an adversary node cheats the route discovery process by

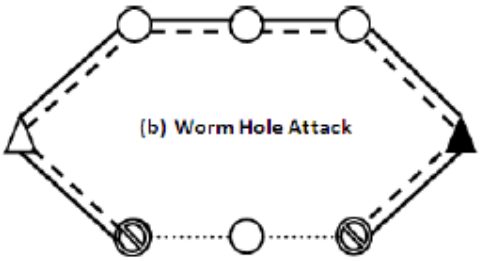
forwarding the route request without specified delay. Such delays are specified by routing protocols to avoid collision of route request packets

Figure 2: Flood Rushing Attack



Wormhole attack: Consider the attack which involves the cooperation of two or more adversarial nodes. As we know that in AODV route discovery mechanism, every intermediate node have to increment the hop count field of the packet which is passing through it and the route with minimum hop count is selected for data packets. Being the route discovery as its target, the objective of this attack is to minimize this increment and thus increase the probability that a route with adversaries is selected due to least hop.

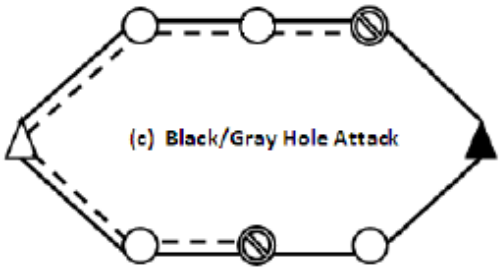
Figure 3: Worm Hole Attack



Gray Hole Attack: The gray hole attack is variation of black hole attack as it do selective forwarding with certain probability. Initially the malicious node behaves well and built a good reputation around its vicinity. It turns into misbehaving node in certain time [5]. Node

initiating this attack does not need extra effort to be part of a route because of its initial behaviour as a legitimate node. This attack exists in two versions: stand alone or cooperative.

Figure 4: Black/Gray Hole Attack



Black Hole Attack

This attack effects on data packet forwarding and not on route maintenance. Black hole attack is a denial of service [1] attack in which a malicious node can attract all the packets claiming a *fresh enough* route to the destination and dropping all the packets reaching at that node.

Behaviour of blackhole node: A blackhole has two properties stated as follows.

1. The node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination, even though the route is spurious, with the intention of intercepting packets.
2. The node consumes the intercepted packets. In an ad hoc network that uses the AODV protocol, a blackhole node absorbs the network traffic and drops all packets

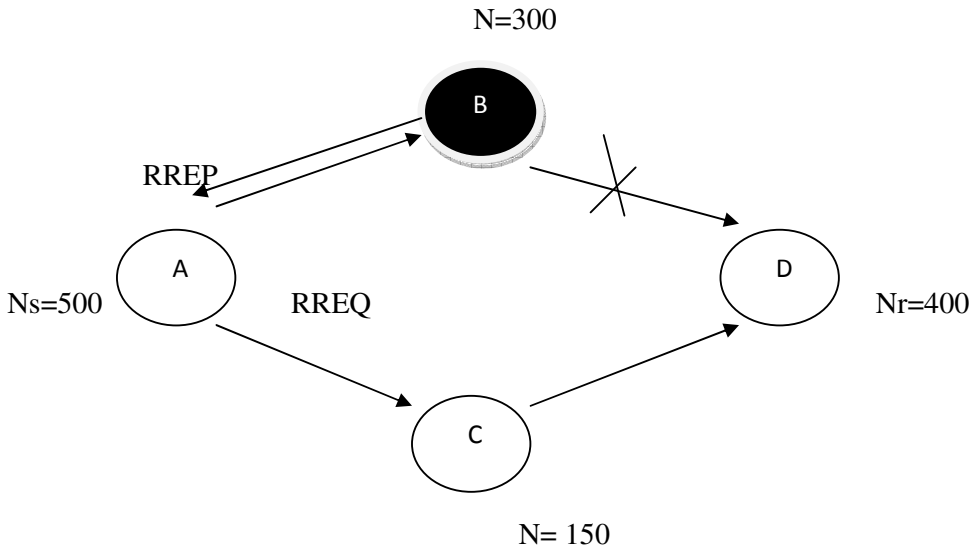
The Problem

When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighbouring nodes. The malicious nodes being part of the network, also receive the RREQ [6]. Since the Black hole nodes have the characteristic of responding first

to any RREQ, it immediately sends out the RREP. The RREP [6] from the Black hole reaches the source node, well ahead of the other RREPs.

On getting the reply, the source node assumes that the process of route discovery is complete and it ignores further coming replies from other nodes. It selects the reply from the malicious node as the best route to send the messages [10] using data packets. The reply sent from the malicious node has the highest sequence number which signifies the route to be the "fresh enough" and the source node relies on that reply. The attacker now drops all the packets coming to it.

Figure 5: Problem Description



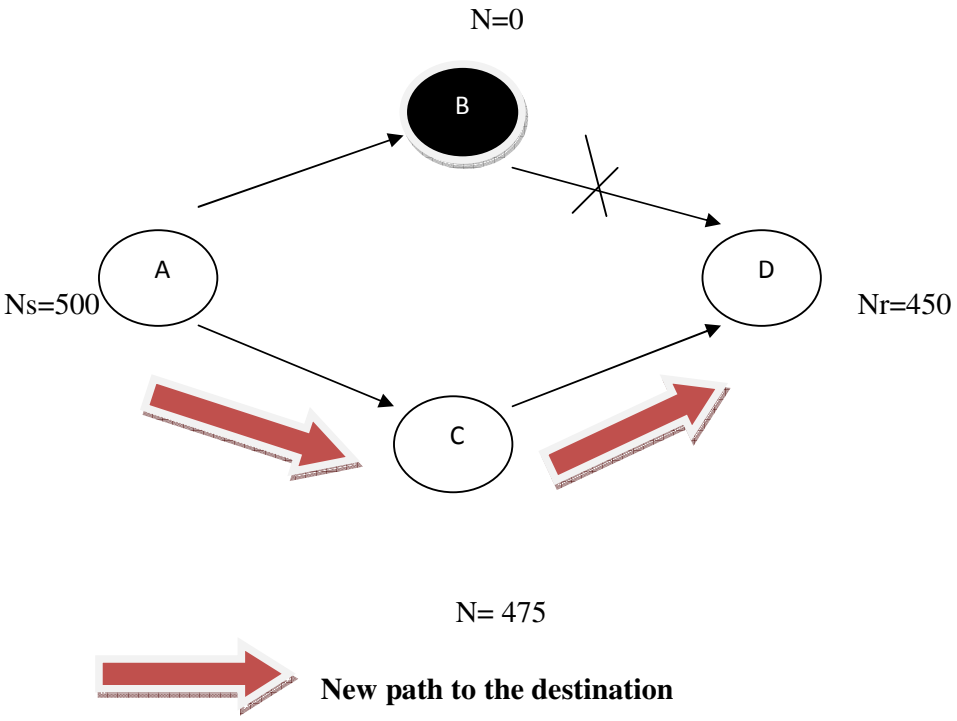
Here, node A is sending packets to node D. Node B does not contain any route to node D but it responds to A as if it has fresh enough route to node D. This node B is known as black hole node. All the packets sent by A destined for D are dropped by B. This is the problem in the network and in this paper proposes a solution to this problem.

The Solution

One of the problems is to detect in the network, the blackholes by examining the no of sent packets at that node which will always be equal to zero for most of the cases.

After the malicious black nodes have been detected we can adopt the following method to avoid the receptance of incoming packets at these blackholes. The packets coming at the intermediate nodes between the paths to blacknodes are propagated back to the sender and the sender follows an alternative safer route to the destination.

Figure 6: Solution to black hole attack



Result

To calculate the amount of packet loss due to the presence of blackhole [5] in the network can be analysed as follows:

A. Presence of black hole in the network

$$L = ((500-400)/500) * 100 \quad (1)$$

$$\mathbf{L = 20\ \%} \quad (2)$$

B. When the solution is adopted

$$L = ((500-450))/500)* 100 \quad (3)$$

$$\mathbf{L = 10\ \%}$$

The above calculation shows that the presence of black hole effectively increases the amount of packet loss and by adopting the above solution; the packet loss can be decreased.
Further, the performance can be studied using the network simulator ns-2 [7] [8] [9].

CONCLUSION AND FUTURE WORK

In this paper we have presented a survey of the state of the art on securing MANETs against packet dropping attack. But the analysis being done considers the network to be at an instance of time which may be considered as a static state. The solution is based on certain assumptions which are not always valid in the nature of mobile adhoc networks. The future work includes the mobility of nodes and considers the system to be dynamic in nature. The performance analysis shows that the amount of packet loss in case of presence of black hole is much more than that in the absence of such a node.

REFERENCES

[1] T. R. Andel and A. Yasinsac, Surveying Security Analysis Techniques in MANET Routing Protocols, *IEEE Commun. Surveys & Tutorials*, 9(4): 70-84, Fourth Quarter 2007.

[2] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine, October 2002..

[3] C. Perkins. "(RFC) request for Comments-3561", Category: Experimental, Network, Working Group, July 2003.

[4] V. Karpijoki, "Security in Ad Hoc Networks", Seminar on Net Work Security, HUT TML 2000.

[5] B. Sun, Y. Guan, J. Chen and U. W.Pooch, "Detecting black-hole attack in mobile ad hoc networks", *Proc. 5th European Personal Mobile Communications Conference*, Apr 2003, pp. 490-495.

[6] I. Stamouli, "Real-time intrusion detection for ad hoc networks", Master's thesis, University of Dublin, September 2003.

[7] I. Stamouli, P. G. Argyroudis and H. Tewari, "Real-time intrusion detection for ad hoc Networks", *Sixth IEEE Intl Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05)*, 2005, pp. 374-380.

[8] Y. Huang, W. Fan, W. Lee and P. Yu, "Cross-Feature analysis for detecting ad-hoc routing anomalies", *Proc. of the 23rd IEEE Intl Conference on Distributed Computing Systems (ICDCS'03)*, May 2003.

[9] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile ad hoc networks by Dynamic Learning Method", Intl Journal of Network Security, vol 5, no. 3, Nov. 2007, pp. 338-346.

[10] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile ad hoc networks by Dynamic Learning Method", Intl Journal of Network Security, vol 5, no. 3, Nov. 2007, pp. 338-346.