Global Journal of researches in engineering
Electrical and electronics engineering
Volume 12 Issue 3 Version 1.0 March 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Comparison of Packet Delivery for Black Hole Attack in ad hoc Network

By Yatin Chauhan, Prof Jaikaran Singh & Prof Mukesh Tiwari
Sri Satya Sai Institute of Science and Technology, Sehore M.P. India

Abstract - Black hole attack is a serious threat in a mobile ad hoc network (MANET). In this attack, a malicious node injects a faked Route Reply message to deceive the source node so that the source node establishes a route to the malicious node and sends all the data packets to the malicious node. The black hole attack can degreed the performance of different routing protocols. During this attack, a malicious node captures packets and not forwards them in the network. This paper illustrates how black hole attack can affect the performance of Mobile Ad hoc networks by using NS-2.34 simulator.

Keywords : *MANET; Black hole attack.*

GJRE-F Classification : *FOR Code: 291704*

Strictly as per the compliance and regulations of:

Comparison of Packet Delivery for Black Hole Attack in ad hoc Network

Yatin Chauhan [α], Prof Jaikaran Singh [α] & Prof Mukesh Tiwari [α]

Abstract - Black hole attack is a serious threat in a mobile ad hoc network (MANET). In this attack, a malicious node injects a faked Route Reply message to deceive the source node so that the source node establishes a route to the malicious node and sends all the data packets to the malicious node. The black hole attack can degreed the performance of different routing protocols. During this attack, a malicious node captures packets and not forwards them in the network. This paper illustrates how black hole attack can affect the performance of Mobile Ad hoc networks by using NS-2.34 simulator.

Keywords : *MANET; Black hole attack;*

I. Introduction

Mobile ad hoc network (MANET) is one of the recent active fields and has received spectacular consideration because of their self-configuration and self-maintenance. Early research assumed a friendly and cooperative environment of wireless network. As a result they focused on problems such as wireless channel access and multihop routing. But security has become a primary concern to provide protected communication between mobile nodes in a hostile environment. Although mobile ad hoc networks have several advantages over wired networks, on the other side they pose a number of non-trivial challenges to the security design as they are more vulnerable than wired networks [1]. These challenges include open network architecture, shared wireless medium, demanding resource constraints, and, highly dynamic network topology. In this paper, we have considered a fundamental security problem in MANET to protect its basic functionality to deliver data bits from one node to another. Nodes help each other in conveying information to and fro and thereby creating a virtual set of connections between each other. Routing protocols play an imperative role in the creation and maintenance of these connections[4,5]. In contrast to wired networks, each node in an ad-hoc networks acts like a router and forwards packets to other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is a blurry boundary separating the inside network from the outside world.

Author α : Department of Electronics and Communication, Sri Satya Sai Institute of Science and Technology,Sehore M.P. India.
E-mails : yatin.dd@gmail.com, jksingh81@yahoo.co.in

Many different types of routing protocols have been developed for ad hoc networks and have been classified into two main categories by Royer and Toh (1999) as *Proactive* (periodic) protocols and *Reactive* (on-demand) protocols. In a proactive routing protocol, nodes periodically exchange routing information with other nodes in an attempt to have each node always know a current route to all destinations [2]. In a reactive protocol, on the other hand, nodes exchange routing information only when needed, with a node attempting to discover a route to some destination only when it has a packet to send to that destination [3]. In addition, some ad hoc network routing protocols are hybrids of periodic and on-demand mechanisms.

Wireless ad hoc networks are vulnerable to various attacks. These include passive eavesdropping, active interfering, impersonation, and denial-of-service. A single solution cannot resolve all the different types of attacks in ad hoc networks. In this paper, we have evaluated MANET with and without black hole attack. In Section II of this paper, we summarize the basic operation of AODV (Ad hoc On-Demand distance Vector Routing) protocol on which we base our work. In Section III, we describe the effect of blackhole attack in AODV. Section IV presents the performance evaluation based of MANET with and without black hole attack on simulation experiments. Section V presents conclusion and future work.

II. AODV

One of the typical routing protocols for MANET is called Ad hoc On-Demand Distance Vector (AODV) [4]. In this protocol, if a source node wants to send data packets to a certain destination node, the source node broadcasts a Route Request (RREQ) packet. Every node that receives the RREQ packet checks whether the node is the destination for that packet and if it is the case, the node sends back a Route Reply (RREP) packet. If it is not the case, then the node checks with its routing table to determine if it has a route to the Destination. If it does not have such a route, it relays the RREQ packet by broadcasting the packet to its neighbours. If it has a route to the destination, then the node compares the destination sequence number in its routing table with that in the RREQ packet. The number in the RREQ packet was obtained by the source node from the packet transmitted by the destination to the source node. If the number in the routing table is larger

than that In the RREQ packet, the route is fresher and the data packets can be sent through this route. Then this node becomes an intermediate node and sends back a RREP packet to the source node along the route through which it received the RREQ packet. The source node then updates its routing table and starts to send its data packets through this route. However, this protocol is highly susceptible to routing attacks especially the black hole attack [6] because of the dynamic topology and lack of any infrastructure in the network.

III. Black Hole Attack

An ad-hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile adhoc network. Being one of the category of ad-hoc routing protocols, on-demand protocols such as AODV (Ad-hoc On demand Distance Vector) and DSR (Dynamic Source Routing) establish routes between nodes only when they are required to route data packets. AODV is one of the most common adhoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network.

In an ad-hoc network that uses AODV as a routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired destination node. This process is called route discovery. Every neighbouring node that receives RREQ broadcast first saves the path the RREQ was transmitted along to its It subsequently checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQ message. The freshness of a route is indicated by a destination sequence number that is attached to it. If a node finds a fresh enough route, it unicasts an RREP (Route Reply) message back along the saved path to the source node or it re-broadcasts the RREQ message otherwise. The same process continues until an RREP message from the destination node or an intermediate node that has fresh route to the destination node is received by the source node. Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, which an adversary can exploit to perform a black hole attack on mobile ad-hoc networks. A malicious node in the network receiving an RREQ message replies to source nodes by sending a fake RREP message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising (by sending a fake RREP to confirm it has a path to a destination node) to source nodes that it will forward data, a malicious node starts to drop all the network traffic. An ad hoc network is the assortment of cooperative wireless nodes without existence of any access point or infrastructure. However, none of them deal with the issues of security. The presence of malicious nodes in an ad hoc network deteriorates the network performance.

IV. Performance Evaluation

Some assumptions, which are considered realistic, are presented. First of all, the MANET is based on IEEE 802.11 standards. We consider a rather large scale MANET which is deployed in a hostile environment. Nodes are limited in their storage and computational and communication resources. Every node has the same transmission range and non-directional antenna. The nodes are battery-powered, and hence it is crucial to conserve energy to prolong the lifetime of the network. Due to the wireless communication, each node can overhear the message broadcasted by other nodes in the transmission range. Every node locates randomly and moves randomly, which means the immediate neighboring nodes of any nodes are not known by each other without exchanging any messages. The network is rather dense so that a message in general could be overheard by multiple nodes. We assume that neither source node nor destination node is malicious and the adversary who plays black hole attack is an intermediate node. In addition, we assume there are one or more nodes that perform the black hole attack in the MANET. Moreover, a malicious node has knowledge of other malicious nodes' ID and is able to cooperate with these other malicious nodes. Table summarizes the simulation parameters for our simulation. One of the basic assumptions for the design of routing protocols in MANETs is that every node is honest and cooperative. That means, if a node claims it can reach another node by a certain path or distance, the claim is trusted/true; similarly, if a node reports a link break, the link will no longer be used.

Table - Simulation Parameters

Parameter	Value
Simulator	NS-2.34
MAC Layer Protocol	IEEE 802.11
Mobility Model	Random Way Point
Node Placement	Random Uniform
Terrain Range	1200 × 1200 m^2
Examined Protocol	AODV
Number of Mobile Nodes	25
Simulation Time	500 s
Channel Bandwidth	2 Mbps
Maximum Speed	10 – 500 m/s
Application Traffic	CBR
Packet Size	400 & 512 Bytes
Maximum Connection	29

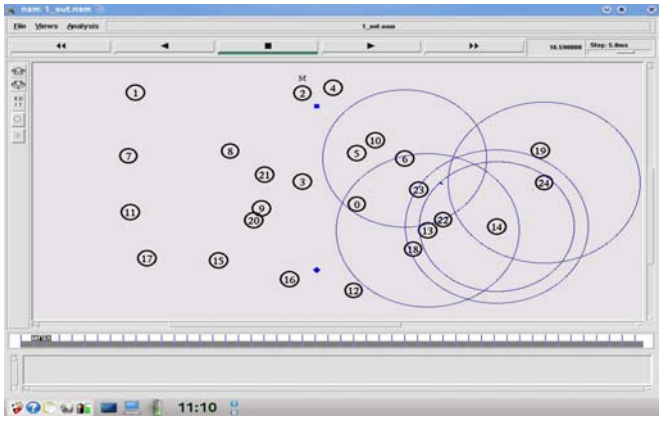

Fig. 1

While this assumption can fundamentally facilitate the design and implementation of routing protocols, it meanwhile introduces a vulnerability to several types of denial of service (DoS) attacks [4], particularly packet dropping attack. To launch such attack, a malicious node can stealthily drop some or all data or routing packets passing through it. Due to the lack of physical protection and reliable medium access mechanism, packet dropping attack represents a serious threat to the routing function in MANETs. A foe can easily join the network and compromise a legitimate node then subsequently start dropping packets that are

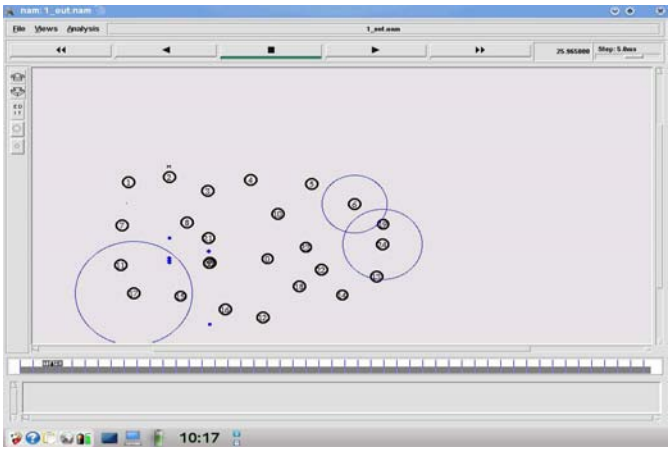

Fig. 2

Expected to be relayed in order to disrupt the regular communications consequently, all the routes passing through this Node fails to establish a correct routing path between the source and destination nodes. Figure 1 and 2 shows the results (snapshots) of our simulation which is performed with NS-2.34[7]. Different nodes are numbered which are written in circles. Blue circles show the coverage area of nodes. Blue Colored Square is packet drop from node. Node 2 is implemented as malicious node. So more packets are dropped by it. Figure 3 shows the packet drop by node when there is black hole attack in Mobile Adhoc Network. As packets are sent constantly, they will reach after some time delay to destination and some number of packets is drop between nodes. As mobility of node increase the packet dropping is also increase. In figure the packet received and drop for nodes for different mobility of node is shown.

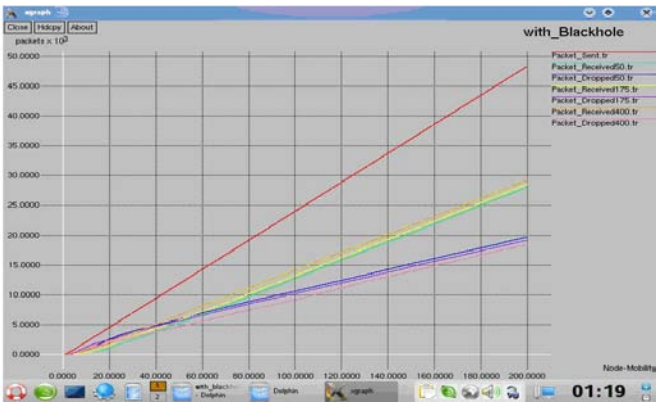

Fig. 3 : With Black hole

In the case when there is no black hole attack in Mobile Adhoc network, the performance is improved as shown in fig. 4. The packet dropping is very less as shown in figure.

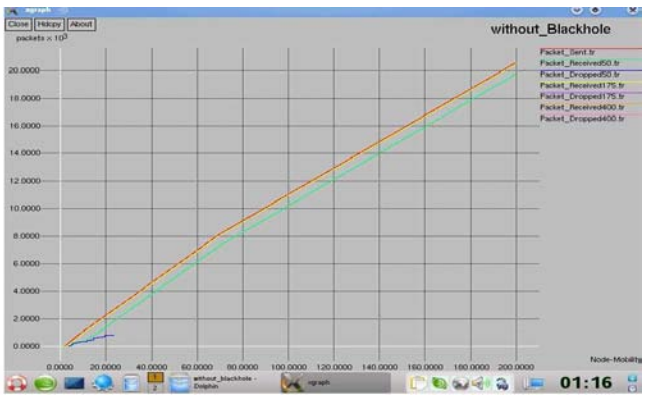

Fig. 4 : Without Black hole

V. Conclusion

In this paper we have presented of the state of the art on securing MANETs. The attack in Without Black hole and With Black hole attack schemes, as well as detection have been explored. A comparative study between them was then conducted to highlight their respective effectiveness and limitations. We concluded that the packet drop is more in MANET with black hole attack than without black hole attack. We believe it is an interesting and significant topic for further exploration with more evaluation of performance of MANET. As well as detection and prevention of black hole attack is also an area of future research.

References Références Referencias

1. Elizabeth M, Royer, and Chai-Keong Toh: "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, (April 1999)
2. C.E. Perkins, S,R, Das, and E. Royer: "Ad-I-Ioe on Demand Distance Vector(AODV)", RFC 3561
3. H. Lan Nguyen and U, Trang Nguyen: "A study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Network,Vol.6,No. I, (2007)
4. L. Zhou and Z. 1. Haas: "Securing Ad Hoc Networks", IEEE Network Magazine, Vol.13, No.6, (November/ Deeember 1999)
5. H. Deng, W. Li, and D. P. Agrawal: "Routing security in wireless ad hoc network". IEEE Communications Magazine, pages 70- 75, (2002)
6. Mohanmmad Al-Shurrnan et al: "Black Hole Attack in Mobile Ad Hoc Network", ACMSE' 04, (April 2004) [S] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto: "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Network by Dynamic Learning Method", International Journal of Network Security, Vo1.5, PP.33S-346, (November, 2007)
7. The Network Simulator—ns-2. [Online]. Available: http://www.isi.edu/nsnam/ns/