Global Journals Inc.

Global Journal of researches in engineering
Electrical and electronics engineering
Volume 12 Issue 2 Version 1.0 February 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Performance Evaluation of AODV based on black hole attack in ad hoc network

By Yatin Chauhan, Prof Jaikaran Singh, Prof Mukesh Tiwari, Dr Anubhuti Khare

Sri Satya Sai Institute of Science and Technology, Sehore M.P. India

Abstract - A Mobile Ad hoc Network (MANET) is a new networking paradigm. In the development of Mobile Ad hoc networks routing is the main issue. There are different security flaws and attacks on routing protocols in MANETs. These attacks can affect the performance of different routing protocols. Blackhole is one of these attacks. The blackhole attack can affect 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 blackhole attack can affect the performance of routing protocol, AODV, in Mobile Ad hoc networks by using NS-2.34 simulator.

Keywords : MANET, AODV, Black Hole attack;.

GJRE-F Classification: FOR Code: 099999

Performance Evaluation of AODV based on black hole attack in ad hoc network

Yatin Chauhan[α], Prof Jaikaran Singh[α], Prof Mukesh Tiwari[α], Dr Anubhuti Khare[σ]

Abstract - A Mobile Ad hoc Network (MANET) is a new networking paradigm. In the development of Mobile Ad hoc networks routing is the main issue. There are different security flaws and attacks on routing protocols in MANETs. These attacks can affect the performance of different routing protocols. Blackhole is one of these attacks. The blackhole attack can affect 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 blackhole attack can affect the performance of routing protocol, AODV, in Mobile Ad hoc networks by using NS-2.34 simulator.

Keywords : MANET, AODV, Black Hole attack;

I. Introduction

Mobile ad hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. Since mobile nodes are not controlled by any other controlling entity, and network management are done, they have unrestricted mobility and connectivity to others. Nodes routes cooperatively by each other nodes. Due to limited transmission power, multi hop architecture is needed for one node to communicate with another through network. In this multi hop architecture, each node works as a host and as well as a router that forwards packets for other nodes that may not be within a direct communication range. Each node participates in an ad hoc route discovery protocol which finds out multi hop routes through the mobile network between any two nodes. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to form own wireless network on the fly. Thus, mobile ad hoc networks provide an extremely flexible communication method for any place where geographical or terrestrial constraints are present and any fixed architecture, such as battlefields, and some disaster management situations. Recent research on MANET shows that the MANET has larger security issues than conventional networks [1, 2].

In our study, we simulated the blackhole attack on AODV routing protocol. Extensive simulations have been carried out using NS-2.34 simulator. We have analyzed the network performance with and without blackhole attack. This paper is organized as follows; section II describes the background or related work and section III explains about the AODV. Section IV describes blackhole attack. In section V simulation results shows the impact of blackhole attack on the performance of routing protocols which is followed by conclusion in section VI.

II. Background

The problem of security has received considerable attention by researchers in the ad hoc network community. In this section, some of these contributions are presented. The problem of securing the routing layer using cryptographically secure messages is addressed by Hu et al. [4], Papadimitratos and Haas [5], and Sanzgiri et al. [6]. Schemes to handle authentication in ad hoc networks assuming trusted certificate authorities have been proposed by Kong et al. [7]. Hubaux et al. [8] have employed a self-organized PGPbased scheme to authenticate nodes using chains of certificates and transitivity of trust. Stajano and Anderson [9] authenticate users by imprinting in analogy toducklings acknowledging the first moving subject they see as their mother.

In contrast to securing the routing layer of ad hoc networks, some researchers have also focused on simply detecting and reporting misleading routing misbehavior. *Watchdog* and *Pathrater* [10] use observation-based techniques to detect misbehaving nodes, and report observed misbehavior back to the source of the traffic. Pathrater manages trust and route selection based on these reports. This allows nodes to choose better paths along which to route their traffic by routing around the misbehaving nodes. However, the scheme does not punish malicious nodes; instead, they are relieved of their packet forwarding burden.

CONFIDANT [11] detects misbehaving nodes by means of observation and more aggressively informs other nodes of this misbehavior through reports sent around the network. Each node in the network hosts a *monitor* for observations, *reputation records* for firsthand and trusted second-hand reports, *trust records* to control the trust assigned to the received warnings, and a *path manager* used by nodes to adapt their behavior according to reputation information. Subsequent research has found that reputation schemes can be beneficial for fast misbehavior detection, but only when one can deal with false accusations [12].

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

Researchers have also investigated means of discouraging selfish routing behavior in ad hoc networks, generally through payment schemes [13]. These approaches either require the use of tamperproof hardware or central bankers to do the accounting securely, both of which may not be appropriate in some truly ad hoc network scenarios. In the per-hop payment scheme proposed by Buttyan and Hubaux [15], the payment units are called *nuglets* and reside in a secure tamper-proof module in each node. They have observed that given such a module, increased cooperation is beneficial not only for the entire network but also for individual nodes. The scheme can result in unfairness to some hosts, but its simplicity and performance may be appropriate in some cases.

Bansal and Baker [14] have proposed a scheme that relies on first-hand observations. Directly observed positive behavior increases the rating of a node, while directly observed negative behavior decreases it by an amount larger than that is used for positive increments. If the rating of a node dips below the faulty threshold, the node is added to a faulty list. The faulty list is appended to the route request by each node broadcasting it to be used as a list of nodes to be avoided. A route is rated good or bad depending on whether the next hop is on the faulty list. If the next hop of a route is in the faulty list, the route is rated as bad. As a response to misbehavior of a node, all traffic from that node is rejected. A second chance mechanism for redemption employs a timeout after an idle period. After a timeout, the node is removed from the faulty list with its rating remaining unchanged.

Sen et al. have presented a scheme for detection of malicious packet dropping nodes in a MANET [15]. The mechanism is based on local misbehavior detection and flooding of the detection information in a controlled manner in the network so that the malicious node is detected even if moves out a local neighborhood.

Deng, Li and Agarwal [3] have suggested a mechanism of defense against black hole attack in adhoc networks. In their proposed scheme, as soon as the *RouteReply* packet is received from one of the intermediate nodes, another *RouteRequest* is sent from the source node to a neighbor node of the intermediate node in the path. This is to ensure that such a path exists from the intermediate node to the destination node. For example, let the source node *S* send *RouteRequest* packets and receive *RouteReply* through the intermediate malicious node *M*. The *RouteReply* packet of *M* contains information regarding its nexthop neighbor node. Let it contain information about the neighbor *E*. Then, the source node *S* sends *FurtherRouteRequest* packets to this neighbor node *E*. Node *E* responds by sending a *FurtherRouteReply* packet to source node *S*. Since node *M* is a malicious node, and thus not present in the routing list of node *E*, the *FurtherRouteReply* packet sent by node *E* will not contain a route to the malicious node *M*. But if it contains a route to the destination node *D*, then the new route to the destination through node *E* is selected, and the earlier selected route through node *M* is rejected. While this scheme completely eliminates the black hole attack by a single attacker, it fails completely in identifying a cooperative black hole attack involving multiple malicious nodes.

III. AODV

In this section, a brief overview of the AODV routing protocol is presented and the security threat that are associated with this routing protocol are briefly discussed.

AODV is a reactive routing protocol that does not require maintenance of routes to destination nodes that are not in active communication. Instead, it allows mobile nodes to quickly obtain routes to new destination nodes. Every mobile node maintains a routing table that stores the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If such a route is not available in its cache, the node initiates a route discovery process by broadcasting a *RouteRequest* (RREQ) message to its neighbors. On receiving a RREQ message, the intermediate nodes update their routing tables for a reverse route to the source node. All the receiving nodes that do not have a route to the destination node broadcast the RREQ packet to their neighbors. Intermediate nodes increment the hop count before forwarding the RREQ. A *RouteReply* (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other intermediate node that has a current route to the destination. As the RREP propagates to the source node, the forward route to the destination is updated by the intermediate nodes receiving a RREP. The RREP message is a unicast message to the source node.

AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes. In case of multiple routes, a nodeselects the route with the highest sequence number. If multiple routes have the same sequence number, then the node chooses the route with the shortest hop count. Timers are used to keep the route entries fresh.

When a link break occurs, *RouteError* (RERR) packets are propagated along the reverse path to the source invalidating all broken entries in the routing table of the intermediate nodes. AODV also uses periodic *hello* messages to maintain the connectivity of neighboring nodes.

Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out many attacks against AODV. This paper provides routing security to the AODV routing protocol by eliminating the threat of 'Black Hole' attacks.

IV. Black Hole Attack

In black hole attack [17], all network traffics are redirected to a specific node, which does not exist at all. Because traffics disappear into the special node as the matter disappears into Black hole in universe. So the specific node is named as Black hole. A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. Black hole attacks in AODV protocol routing level can be classified into two categories -- RREQ Blackhole attack and RREP Blackhole attack.

a) Black hole attack caused by RREQ

An attacker can send fake RREQ messages to form black hole attack [17]. In RREQ Blackhole attack, the attacker pretends to rebroadcast a RREQ message with a non-existent nodes will update their route to pass by the non destination node.

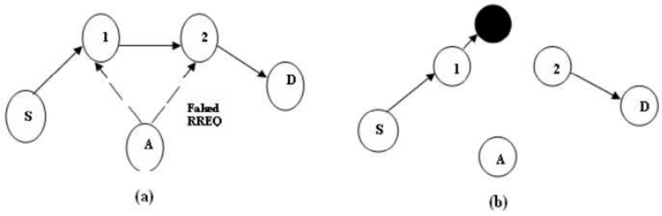

Fig.1 : Black hole is formed by Faked RREQ

As a result, the normal route will be broken down. The attacker forms a Black hole attack between the source node and the destination node by faked RREQ message. It is shown in figure 1.

b) Black hole attack caused by RREP

The attacker unicasts the faked RREP message to the originating node. When originating node receives the faked RREP message, it will update its route to destination node through the non existent node. Then RREP Black hole is formed. It is shown as figure 2.

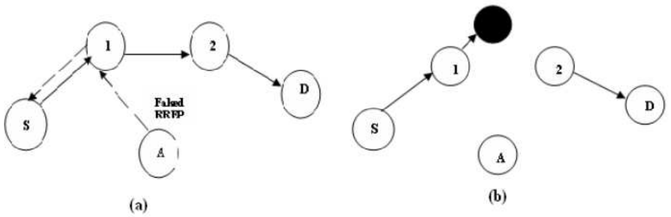

Fig.2 : Black hole is formed by Faked RREP

V. Simulation Environment

We have implemented blackhole attack in simulator. For our simulation, we use CBR (constant bit rate) application, IEEE 802.11 MAC, and a physical channel based on two ray propagation model. The simulated Mobile Ad hoc network consists of 25 nodes in 1200*1200 m2. The node transmission range is 250 meters. Random waypoint model is used for scenarios with node mobility. The size of data payload is 512 bytes. The simulation is done to analyze the performance of the network by varying node speed under blackhole attack. The following performance met used in the above mentioned scenario.

Throughput: It indicates the fraction of channel capacity used for successful data transmission.

Average End-to-End Delay: End-to-End Delay can be defined as the time a packet takes to travel from source to destination. Average End-to-End Delay is the average of the end-to-end delays taken over all received packets.

Node Mobility: Node mobility indicates the mobility speed of nodes.

a) Simulation Results

The Fig.3 shows the effect to measured for the AODV protocol when the node increased. The result shows both the cases, with the blackhole and without the blackhole attack. It is measured that the packet delivery ratio is dramatically decreases nodes in the network. For example, the packet when there is no effect of Blackhole attack and moving at the speed 50 m/s. but due to effect of the Blackhole the packet delivery ratio decreases to 47 packets are dropped by the blackhole node.

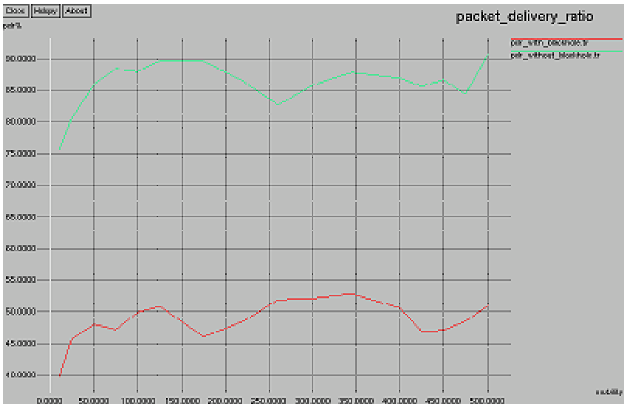

Fig.3 : Impact of Blackhole attack on packet delivery ratio

Figure 4 shows the effect of throughput for AODV protocol when node mobility is increased. The result shows the cases, with blackhole and without blackhole attack on AODV. It has been measured that throughput decreases with blackhole nodes in the Ad hoc network on AODV routing protocol as compared to without blackhole nodes.

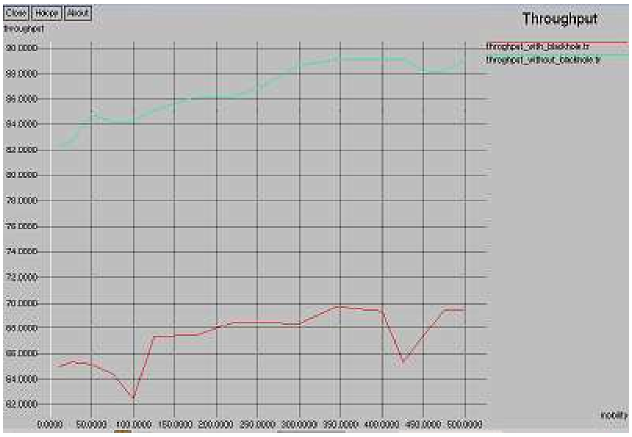

Fig.4 : Impact of Blackhole attack on the Network Throughput.

From the figure 5 it can be observed that, there is slight increase in the average end-to-end delay without the effect of blackhole, as compared to the effect of blackhole attack, This is due to the immediate reply from the malicious node i.e. the nature of malicious node here is it would not check its routing table.

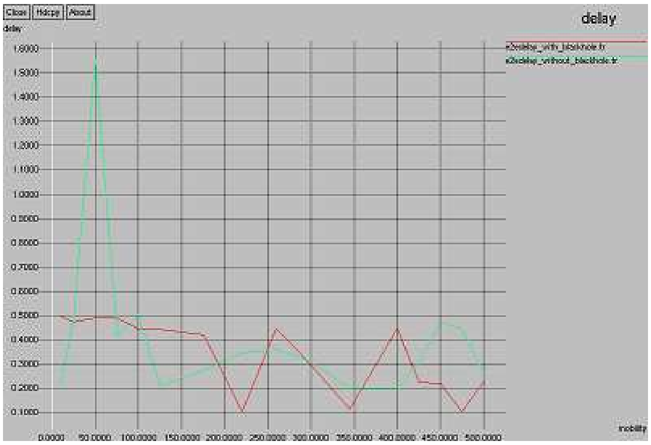

Fig.5 : Impact of Blackhole attack on the Avg. E -E delay.

It is observed from the figure 6 that, avg. jitter between the nodes is more without the blackhole attack, as compared to the Avg jitter between the nodes with the effect of blackhole attack. This is due to the malicious nodes provides the path with fewer number of nodes, or smaller path. Thus average jitter between the nodes is reduces.

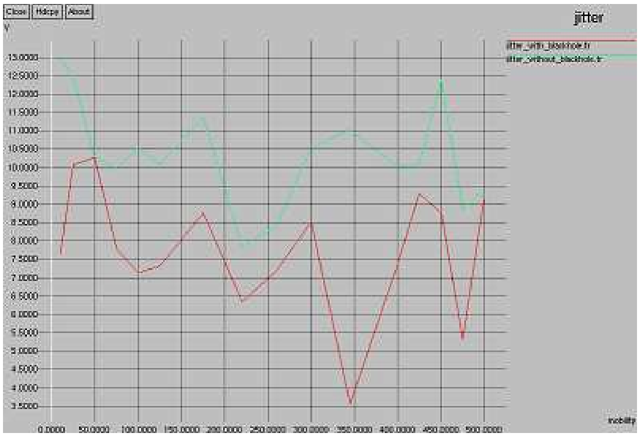

Fig.6 : Impact of Blackhole attack on the Avg. Jitter

VI. Conclusion

With development in computing environments, the services Based on Ad Hoc Networks have been increased. Wireless Ad Hoc Networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. In this paper the effect of packet delivery ratio, Throughput, End -to-End Delay and Jitter has been detected with respect to the variable node mobility. There is reduction in Packet Delivery Ratio, Throughput, E-E Delay, and Jitter as shown in fig. 3-6. In Black hole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and nodes as shown in the result of the simulation. The detection of Cooperative Black holes in ad hoc networks is still considered to be a challenging task.

References Références Referencias

1. D. M. Chess. Security issues in mobile code systems. In Proc. Conf. on Mobile Agent Security, LNCS 1419, pages 1-14, 1998.
2. C. Cooper, R. Klasing, and T. Radzik. Searching for blackhole faults in a network using multiple agents. In Proc. 10th Int. Conf. on Principles of Distributed Systems (OPODIS 2006), pages 320-332, 2006.
3. H. Deng, H. Li, and D. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, Vol. 40, No. 10, Oct 2002.
4. Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on –demand routing protocol for ad hoc networks, In Proceedings of the 8th International Conference on Mobile Computing and Networking (Mobicm 2002), pp. 12-23, ACM, Atlanta, GA, Sept 2002.
5. P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks", In SCS Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002) , San Antonio, TX, Jan 2002.
6. K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E . Belding-Royer, "A secure routing protocol for ad

hoc networks", In International Conference on Network Protocols (ICNP) , Paris, France, Nov 2002.

7. J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for m obile ad hoc networks", Innternational Conference on Network Protocols (ICNP) , pp. 251-260,2001.
8. J.Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks", In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC) , 2001.
9. F. Stajano and R. Anderson, "The resurrecting duckling", Lecture Notes in Computer Science, Springer-Verlag, 1999.
10. S. Marti, T. Giuli, K.Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of MOBICOM 2000, pp. 255-265, 2000.
11. S. Buchegger and J. Boudec, "Performance analysis of the ONFIDANT protocol: Cooperation Of Nodes - Fairness In Dynamic Ad hoc NeTworks", In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC) , Lausanne, CH, Jun 2002.
12. S. Buchegger and J. Boudec, "The effect of rumor spreading in reputation systems for mobile ad hoc networks", In WiOpt '03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks , Mar 2003.
13. M. Jakobsson, J. Hubaux, and L. Buttyan, "A micropayment scheme encouraging collaboration in multihop cellular networks", in Proceedings of Financial Crypto 2003.
14. S. Bansal and M. Baker, "OCEAN: Observationbased cooperation enforcement in ad hoc networks", Technical Report, Stanford University, 2003.
15. S. Ki, P. Naldurg and R. Kravets, "Security aware ad hoc routing for wireless networks", in Proceedings of the 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing , Poster Session, pp 299- 302, Long Beach, California, October 2001.
16. Chen Hongsong, Ji Zhenzhou, Hu Mingzeng, "A novel security agent scheme for AODV routing protocol based on thread state transition". Department of Computer Science and Technology Harbin Institute of Technology, 150001.