World Research Journal of Computer Architecture
ISSN: 2278-8514 & E-ISSN: 2278-8522, Volume 1, Issue 1, 2012, pp.-19-23.
Available online at http://www.bioinfo.in/contents.php?id=97

SECURING BLACK HOLE ATTACK IN ROUTING PROTOCOL AODV IN MANET WITH WATCHDOG MECHANISMS

SURANA K.A.*, RATHI S.B., THOSAR T.P. AND SNEHAL MEHATRE

Department of Computer Science and Engineering, JDIET, Yavatmal-445001, MS, India.
*Corresponding Author- Email- kirtisurana08@gmail.com

Received– March 09, 2012; Accepted- May 18, 2012

Abstract- An ad hoc network is a collection of mobile nodes that dynamically form a temporary network. It operates without the use of existing infrastructure. One of the principal routing protocols used in Ad-Hoc networks is AODV (Ad-Hoc On demand Distance Vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called ‘Black Hole’ attack. This paper analyze the black hole attack which is occurs in ad hoc network. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. By doing this, the malicious node can deprive the traffic from the source node In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. In this paper we have propose a watchdog mechanism which first detect the black hole attack and then give new route to this node.

Keywords- AODV, Black Hole, MANET, RREP, RREQ.

Citation- Surana K.A., et al. (2012) Securing Black Hole Attack in Routing Protocol Aodv in Manet with Watchdog Mechanisms. World Research Journal of Computer Architecture, ISSN: 2278-8514 & E-ISSN: 2278-8522, Volume 1, Issue 1, pp.-19-23.

Introduction

An ad hoc network is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. Such a network may work in a standalone way, or may be connected to the larger Internet. A mobile ad hoc network [2] is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes [3]. A MANET is particularly vulnerable due to its fundamental characteristics [4], [5], such as open medium, dynamic topology, distributed cooperation, and constrained capability.

Security Challenges in MANET

Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature. As a result, there exist a slew of attacks that can be performed on an Ad hoc network. [3,6].
Challenges to MANET are discussed as follows-

Confidentiality- It ensures that classified information in the network is never disclosed to unauthorized entities. In MANETs, this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed. Sensitive information, such as strategic military decisions or location information requires confidentiality. Leakage of such information to enemies could have devastating consequences.

Availability- Availability is the most basic requirement of any network. It assures that the services of the system are available at all times and are not denied to authorized users.

Integrity- It guarantees that a message being transferred between nodes is never altered or corrupted and the message must be genuine. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network.

Authenticity- Enables a node to safeguard the characteristics of the peer node it is communicating, without which an attacker would duplicate a node, thus attaining unauthorized admission to resource and sensitive information and snooping with operation of other nodes.

Non-repudiation- It ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

Access Control- To prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems.

Routing Approaches in MANET

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 ad-hoc network. Following are the categories of routing protocols in MANET.

Table-driven or Proactive Protocols- Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network. As the resulting information is usually maintained in tables, the protocols are sometimes referred to as table-driven protocols. Representative proactive protocols include- Destination-Sequenced Distance- Vector (DSDV) routing, Optimized Link State Routing Protocol (OLSR).

On-demand or Reactive Protocols- A different approach from table-driven routing is reactive or on-demand routing. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Once a route has been established, it is maintained by the node until either the destination becomes inaccessible or until the route is no longer used or has expired. Reactive routing protocols include- Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) routing protocol.

Hybrid Routing Protocols- Purely proactive or purely reactive protocols perform well in a limited region of network setting. However, the diverse applications of ad hoc networks across a wide range of operational conditions and network configuration pose a challenge for a single protocol to operate efficiently.

AODV Routing Protocol

Ad hoc On-Demand Distance Vector (AODV) [7] is a reactive routing protocol which creates a path to destination when needed and is an adaptation of the DSDV protocol for dynamic link conditions [8,9]. AODV is capable of both unicast and multicast routing. AODV's basic working principle contains three main procedures [9], i.e. path discovery, establishment and maintenance of the routing paths.

In AODV, route is created only on demand. When network node needs a connection then it broadcasts a request for connection. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, the request will be forwarded to other neighbor nodes. Before forwarding the packet, each node will store the broadcast identifier and the previous node number from which the request came. Timer will be used by the intermediate nodes to delete the entry when no reply is received for the request. If there is a reply, intermediate nodes will keep the broadcast identifier and the previous nodes from which the reply came from. The broadcast identifier and the source ID are used to detect whether the node has received the route request message previously. It prevents redundant request receive in same nodes. The source node might get more than one reply, in which case it will determine later which message will be selected based on the hop counts. When a link breaks down, for example due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable due to the loss of the link. It then creates a route error (RERR) message which lists all of these lost destinations. The node sends the RERR upstream towards the source node. Once the source receives the RERR, it reinitiates route discovery if it still requires the route.

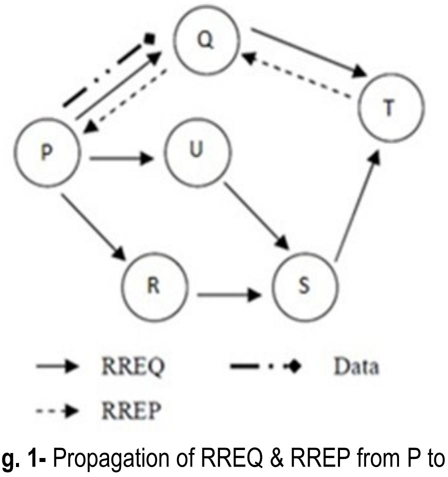

Fig. 1- Propagation of RREQ & RREP from P to T

Black Hole Attack

A Black Hole attack [3,10] is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. A black hole attack is referred to as a node dropping all packets and sending forged routing packets to route packets over itself. In this type of attack, a malicious node spuriously announces a short route to the sink node (the destination) to attract additional traffic to the malicious node and then drops them. A source node wants to send data packets to destination node, and initiates the routing discovery process. In the following illustrated figure 2, imagine a malicious node ‘M’. When node ‘P’ broadcasts a RREQ packet, nodes ‘Q’, ‘R’ and ‘M’ receive it. Node ‘M’, being a malicious node, does not check up with its routing table for the requested route to node ‘T’

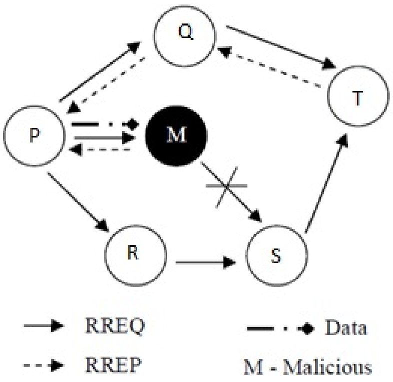

Fig. 2- Blackhole Attack in AODV

Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node ‘P’ receives the RREP from ‘M’ ahead of the RREP from ‘Q’ and ‘R’. Node ‘P’ assumes that the route through ‘M’ is the shortest route and sends any packet to the destination through it. When the node ‘P’ sends data to ‘M’, it attracts and absorbs all the data without forwarding to destination and thus acts like a ‘Black hole’ [5]. In this way an attacker node M can completely modify the packet and generate fake information, this cause the network traffic diverted or dropped.

Proposed Worked

To find the effect of black hole we activate the wireless ad-hoc network with and without the black hole node present in the network. To overcome this effect, we present new protocol, which we called “Modified AODV”. Watchdog mechanism is an approach for detecting and securing black hole attack. In Watchdog mechanism, every node keeps two extra tables, one is called pending packet table and another one is called node rating table. In pending packet table, each node keeps track of the packets which they sent. There are four fields, Packet ID, Next Hop, Expiry Time and Packet Destination in pending packet table.

- Packet ID- ID of packet sent.
- Next Hop- Address of next hop node
- Expiry Time- Time-to-live of packet
- Packet Destination- Address of destination node.

Similarly, there are four fields in node rating table which are Node Address, Packet drops, Packet forwards and Misbehave. This table is updated corresponding to pending packet table.

- Node Address- Address of next hop node.
- Packet Drops- Counter for counting the packets dropped.
- Packet Forwards- Counter for counting the forwarded packet.
- Misbehave- It has two values 0 and 1, 0 for well behaving node, 1 for misbehaving node

Watchdog Mechanism

In pending packet table, each node maintains path of the packets which it sent. It contains a unique packet id, address of the next node to which the packet was forwarded, address of the destination node and an expiry time after which a still-existing packet in the buffer is considered not forwarded next node.

In node rating table, each node maintains rating of adjacent node. The last field of the node rating table is calculated by the ratio of dropped packets and successfully forwarded packets, if this ratio is greater than a given threshold value then this node misbehave value will be 1(means it is considered as a misbehaving node), otherwise it is considered as a genuine node. An expired packet in the pending packet table causes the packet drops counter to increment for the next hop associated with the pending packet table entry. For deciding whether a node is misbehaving or act as a legitimate one, depend on the selection of threshold value. For example if we take a threshold value of 0.5. This means that as long as a misbehaving node is forwarding twice packets as it drops it will not be detected. If we take a lower value of threshold then it will increase the percentages of false positives [8].

After detecting a misbehaving node, a node will try to do local repair [8] for all routes passing through this misbehaving node. If local repair process fails, then it will not send any RERR packet upstream in the network. This process tries to prevent a misbehaving node from dropping packets, and also prevent blackmailing of genuine nodes. To avoid constructing routes, which traverse misbehaving nodes, nodes drop all RREP messages coming from nodes currently marked as misbehaving. For stopping the misbehaving node to act actively in a network, the entire packet originating from this node has been dropped as a form of penalty[1].

The algorithm for the proposed work [1] is as follows-

```
1. Data packet forwarded or sent.
2. Copy and keep the data packet in pending packet table until it is expired or forwarded
3. If (data packet forwarded)
        {
        Increment the corresponding *forwarded packet* in the node rating table and remove the data packet
        from pending packet table
        }
       4. If (data packet expires in the pending packet table)
        {
        Increments the corresponding dropped packet in the node rating table and remove the data packet
        from pending packet table
        If (dropped packet >threshold (th1)) then
        {
        If (dropped packet /forwarded packet)>threshold(th2))
        {
        Node is misbehaving
        Promiscuous node locally tells all the node of its wireless range that particular node is
        misbehaving node.
        Discard RREP message coming from the misbehaving node
 }
 }
 }
```

Simulation Result

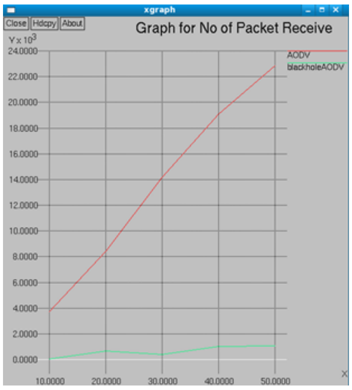

Fig. 3- No. packet received in AODV and black hole AODV

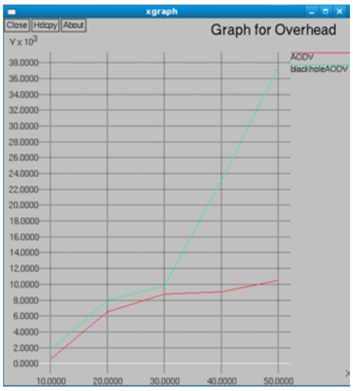

Fig. 4- Comparison of overhead in AODV and black hole AODV

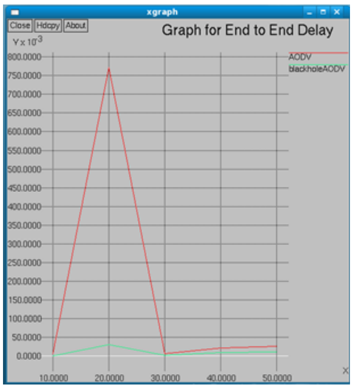

Fig. 5- Comparison of end to end delay in AODV and black hole AODV

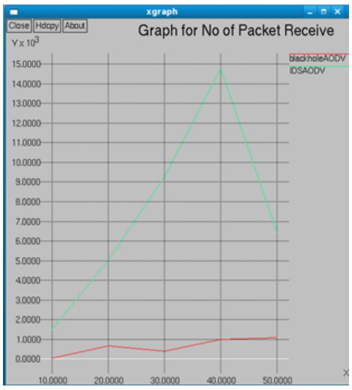

Fig. 6- No. packet received in AODV and black hole AODV in presence of black hole node

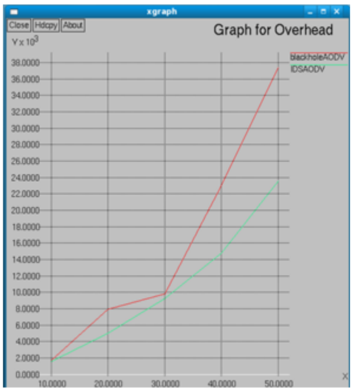

Fig. 7- Snapshot for comparison of overhead in AODV and black hole AODV in presence of black hole node

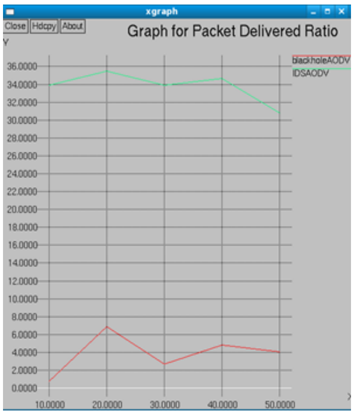

Fig. 8- Snapshot for comparison of PDF in AODV and black hole AODV in presence of black hole node

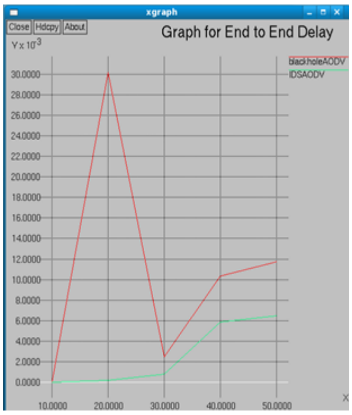

Fig. 8- Snapshot for comparison of end to end delay in AODV and black hole AODV in presence of black hole node

To evaluate the packet delivery ratio, End-to-End delay and overhead, simulation is done in which we varies number of nodes from 10 to 50 and time for simulation kept constant. For that we also plot graph which are shown above. In first scenario i.e. in comparison of aodv and black hole aodv overhead, packet delivery ratio and end to end delay is more in presence of black hole in aodv and as more number of packet is dropped no of packet received get decreased.

In second case we simulate black hole aodv with secure black hole AODV protocol. In this it seems that number of packet received by black hole AODV is more in presence of black hole.

Also overhead and end to end delay in network gets reduced. The experimental results show that when the black hole nodes is increased up to 6% of total network nodes then in the presence of watchdog active throughput increases up to 3% to 8% for different scenarios. When the black hole nodes is increased up to 10% of total network nodes then in the presence of watchdog active throughput increases up to 10% to 18% for different scenarios.

Conclusion

Existing ad hoc routing protocols are subject to a variety of attacks that can allow attackers to influence a victim's selection of routes. There are number such attacks occurring in network and they are easily exploited. In particular, we introduced the notion black hole attack, in which the attacker consumes the intercepted packets without any forwarding. Secondly, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets.

In this paper, we analyzed effect of the Black Hole in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. Moreover, we also implemented a solution that attempted to reduce the Black Hole effects in NS-2 is black hole AODV protocol. Watchdog mechanism AODV tries to eliminate the Black Hole effect at the route determination mechanism of the AODV protocol that is carried out before the nodes start communication of data packets.

Finally we have compared the two protocol for various design metrics and comes to conclusion that black hole AODV proves to better than AODV in presence of black hole node.

References

[1] Kanika Lakhani, Himani bathla, Rajesh and Yadav (2010) *International Journal of Computer Science and Network Security* (*IJCSNS*), 10(5).

[2] Hu Y.C., Johnson D.B. and Perrig A. (2002) *Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications. Washington*, DC, USA, *IEEE Computer Society*, 3-13.

[3] Hongmei Deng, Wei Li, and Agarwal D.P. (2002) *IEEE Communications magazine*.

[4] Kurosawa S., Nakayama H. and Kato N. (2007) *International Journal of Network Security*, 338-346.

[5] Latha Tamilselvan and Sankaranarayanan V. (2007) *2nd International Conference on Wireless Broadband and Ultra Wideband Communications* (Aus. Wireless).

[6] Lidong zhou and Zygmunt J. Haas (1999) *IEEE network*, special issue.

[7] Harris Simaremare and Riri Fitri Sari (2011) *International Journal of Computer Science and Network Security*, 11, 6.

[8] Perkins C.E., Das S.R. and Royer E. (2000) *Ad-Hoc on Demand Distance Vector* (*AODV*), *http-//www.ietf.org/internet-drafts/draft-ietf-manet-aodv- 05.txt*.

[9] Charles E. Perkins, Elizabeth M. Belding-Royer and Das S.R. (2003) *Mobile Ad Hoc Networking Working Group*, Internet Draft.

[10] Yi-Chun Hu and Adrian Perrig (2004) *IEEE Security and Privacy*.