BLACKHOLE ATTACK IMPLEMENTATION IN AODV ROUTING PROTOCOL

MONIKA ROOPAK
Assistant Professor
Ansal University,Guraon,
monikaroopak@gmail.com

Prof. BVR Reddy
Professor, USIT,GGSIPU
Delhi

Abstract-Mobile Ad-hoc networks are a collection of mobile hosts that communicate with each other without any infrastructure. Because of security vulnerabilities of the routing protocols, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. One of the attacks is the Black Hole Attack against network integrity in this all data packets are absorbed by malicious nodes. Since the data packets do not reach the destination node on account of this attack, data loss will occur. In this paper we see how to implement black hole attack in Ad hoc On demand Distance Vector protocol using network simulator 2.34

Keywords- Ad hoc network, black hole , AODV, MANET, RREQ, RREP

INTRODUCTION

Wireless network is the network of mobile computer nodes or stations that are not physically wired. The main advantage of this is communicating is keep in contact with rest of the world while being mobile. The disadvantages are their limited bandwidth, memory, processing capabilities and open medium[1]. Two basic system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET). An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. 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 [2].In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. We will implement Black Hole attack in AODV protocol.

AODV routing protocol

AODV (Ad hoc On-Demand Distance Vector) [3] is a reactive routing protocol composed of two modules:

- Route discovery module: To send data to a given destination D, the source node S consults its routing table. If it finds a valid entry (a route) towards this destination D, it uses it immediately, else it launches a route discovery procedure (see Figure 1.), witch consists in broadcasting, by the source node S, a route request (RREQ) message towards neighbors. When RREQ is received by an intermediate node, this last consults it routing table to find a fresh route (the route is fresh If the sequence number of this route is larger than that of RREQ) towards the requested destination in RREQ. If such a route is found, a route reply (RREP) message is sent through the preestablished reverse route (established when RREQ pass through intermediate nodes) towards the source S . If the intermediate node does not find a fresh route, it updated its routing table and sends RREQ to these neighbors. This process is reiterated until RREQ reaches the destination node D. The destination node D sends RREP to S by using the pre-established reverse route. It should be noted that the source S can receive several RREP, it will choose that whose destination's sequence number is larger, if destination's sequence numbers of several RREP are equal, that of which the smallest hope counter will be selected.

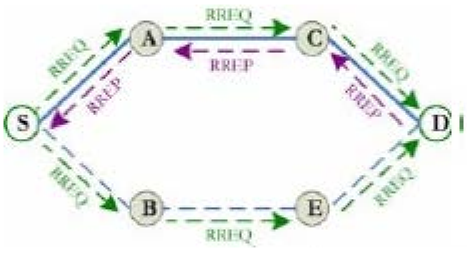

Figure 1.Route discovery process of AODV

- Route maintenance module: AODV uses Hello messages to maintain the connectivity between nodes. Each node periodically sends a Hello message to these neighbors and awaits Hello messages on behalf of these neighbors. If Hello messages are exchanged in the two directions, a symmetrical link between nodes is always maintained if no link interrupt occurs. The broken link can be repaired locally by the node upstream, else a route error (RERR) message is sent to the source S (see Figure 3.). This last can launch again,if necessary, the route discovery procedure. It should be noted that the link interrupt is the consequence of the mobility or the breakdown of nodes.

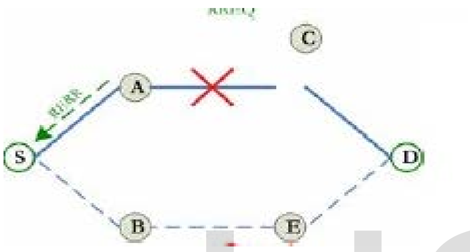

Figure 2.Route maintenance process of AODV

BLACK HOLE ATTACK SPECIFICATION

In a black hole attack[4], the malicious node refuses to forward data packets to the following node in the route connecting a given source and destination. To conduct its attack, the malicious node must initially belong to the data route, then it pass to the action which is the data dropping .According to the specification of the target routing protocol ,the manner with which the malicious node fits in the data route differs. Since our case of study is the AODV protocol, we will see how a malicious node can make a success of its attack in AODV.
Two kinds of black hole attack can be distinguished:

- Internal black hole attack: The malicious node is an internal node which does not seek to fit in an active route between a given source and destination, and if the chance would have it, this malicious becomes element of an active data route, it will be able to conduct its attack as the transmission of the data starts..
- External black hole attack: The malicious node is an external node which seeks to fit in an active route. For that, it violates the routing protocol specification and executes the process schematized in Figure 2. and summarized in the following points:

- The malicious node detects the existence of an active route and takes note of the destination address.

-The malicious node prepares a route replay packet(RREP) in which: the destination address field is set to the spoofed destination address, the sequence number is set to a greatest value and the counter hope is set to a smallest value.

-The malicious node sends this route reply RREP to the nearest intermediate node belonging to the real active route (not necessarily to the data source node himself).

-The route reply RREP received by the intermediate node will be relayed through the preestablished inverse route towards the data source node.

-The source node updates its routing table by the new information received in the route reply.

-The source uses the new route to sending data.

-The malicious node starts to drop the data in the route to which it belongs.

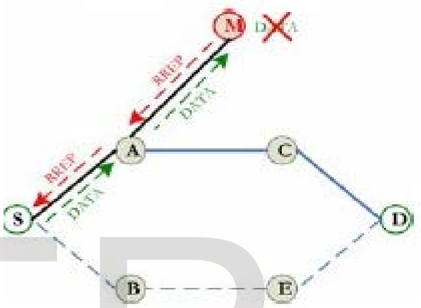

Figure 3. Black hole attack specification

IMPLEMENTATION

NS Network Simulator

NS is an event driven network simulator program, developed at the University of California Berkley, which includes many network objects such as protocols applications and traffic source behavior.

Implementing new protocol

In [6] Implementation of a New Manet Unicast Routing Protocol in NS-2 is described. To implement our contribution we have used the details explained in this paper. In our work, we have used the nodes that exhibit black hole behavior in wireless ad-hoc network that use AODV protocol. Since the nodes behave as a Black Hole they have to use a new routing protocol that can participate in the AODV messaging.

All routing protocols in NS are installed in the directory of "ns-2.34".We start with duplicating aodv folder in the folder ns-allinone-2.34/ns-2.34. Then we rename all the files in the folder as baodv instead of aodv eg aodv.cc as baodv.cc., aodv.h as baodv.h and so on. Then we change all classes, functions, structs, variables and constants from aodv to baodv names in all the files in the directory.

Changes made in baodv.cc

First modify recv fucntion bAODV::recv(Packet *p, Handler*) in near line number 559 as

```
bAODV::recv(Packet *p, Handler*) {

struct hdr_cmn *ch = HDR_CMN(p);

struct hdr_ip *ih = HDR_IP(p);

baodv_rt_entry *rt;

 assert(initialized());

  if(ch->ptype() == PT_AODV) {

   ih->ttl_ -= 1;

   recvbAODV(p);

   return;

 }
if((ih->saddr() == index) && (ch->num_forwards() ==
0))

{

   forward((baodv_rt_entry*) 0, p, NO_DELAY);

}
else
drop(p, DROP_RTR_ROUTE_LOOP);
}
```

Second we change recvRequest fucntion (bAODV::recvRequest(Packet *p)) near line number 671 by doing modification at the end of this funciton change paramameter seqno in funciton sendReply to some very large number as given below

```
sendReply(rq->rq_src,
          1,
          index,
          4294967295,
          MY_ROUTE_TIMEOUT,
          rq->rq_timestamp);
      Packet::free(p);
```

Changes need to be done in ns2

We made changes at 3 places .

1. First, we will add baodv in ns-allinone-2.34/ns-2.34/tcl/lib/ns-packet.tcl file as

near line number 165 write baodv as

```
 foreach prot {
baodv
AODV
ARP
NV
}
```

2. We will make changes to the ns-2.34/Makefile by adding following code near line number 275

```
            baodv/baodv_logs.o baodv/baodv.o \
            baodv/baodv_rtable.o    baodv/baodv_rqueue.o
\
```

(note: the \ at the end of line turn purple in colour other wise it will give you error)

3. At last we will make changes to ns-

2.34/tcl/lib/ns-lib.tcl by adding following code (near line number 630)

```
bAODV {
set ragent [$self create-baodv-agent $node]
    }
```

(near line 848)

```
Simulator instproc create-baodv-agent { node } {
    set ragent [new Agent/bAODV [$node node-addr]]
    $self at 0.0 "$ragent start"
    $node set ragent_ $ragent
    return $ragent
}
```

Then to recompile ns2 open terminal go to ns-2.34 folder and type following commands and press enter

```
make clean
make
```

We have now installed a new protocol in ns2.

Changes in Tcl script

Output with our original script.is shown in fig-4

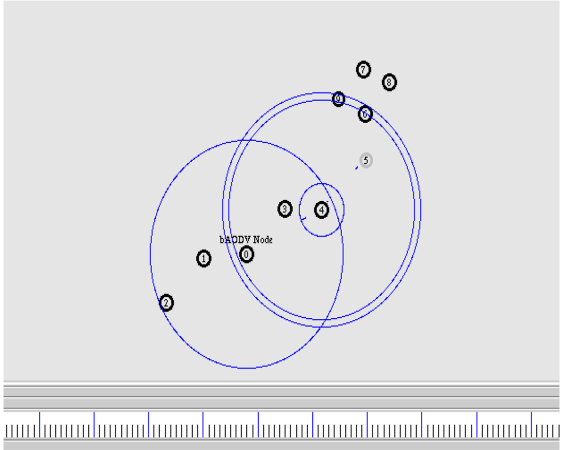

Figure 4-Tcl script showing packet transmission from node 1 to node 5

Following modification are to be done in our original Tcl script for installing black hole attack.

Our script we have created 10 nodes

Suppose you want to make node 0 be the malicious node then type following code

$ns node-config -adhocRouting bAODV

set n(0) [$ns node]

$ns at 0.0 "$n(0) label \"black hole Node\""(to lable the malicious node)

$n(0) color "red"

$n(0) shape "circle"

$ns node-config -adhocRouting AODV

here define all other nodes from 1 to 9

set n(1) [$ns node]

$n(1) color "red"

$n(1) shape "circle" similary for other nodes

or you can put a for loop here for node 1 to 9

Above first bold statement, "$ns node-config -adhocRouting blackholeAODV" is to add the BlackHole bAODV behavior to the nodes created from this point on. But we only define Node 0 as a Black Hole AODV and we have to change to AODV protocol after Node 0 again with the third statement. The second statement just puts a notification to Node 0 defining it as a Black Hole Node. Node 0 being a Black Hole AODV Node absorbs the packets.

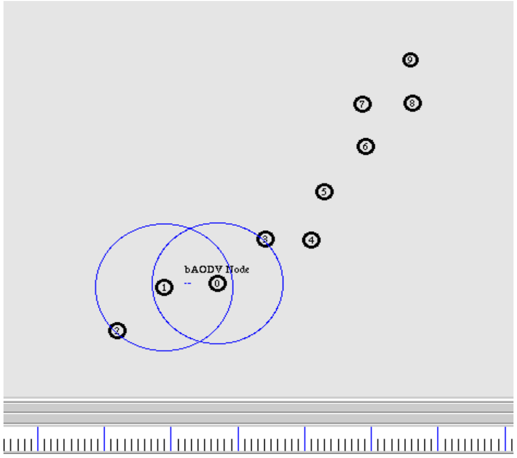

Figure-5 node 0 behaving as black hole node

Now we have successfully injected blackhole attack in AODV.

Figure 6 shows the Packet Delivery Ratio with and without blackhole attack.

It is clear from the graph that packet delivery has drastically reduced because of the attack.

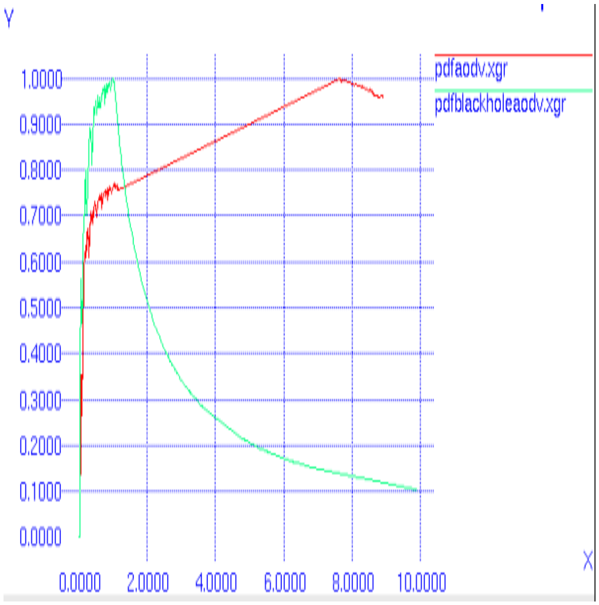

Figure -6 X-axis : Time Y-axis: PDF with Blackhole With no attack

REFERENCES

1. Virendra Singh Kushwah "Implementation of New Routing Protocol for NodeSecurity in a Mobile Ad Hoc Network" (IJCSIS) International Journal of Computer Science and Information Security,Vol. 8, No. 9, December 2010
2. Tamilselvan, L.; and Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. AusWireless, 21-21.
3. C. Perkins, E. B. Royer, and S. Das, "Ad hoc on-demand distance vector(aodv) routing," RFC: 3561, Nokia Research Center, 2003
4. Abderrahmane Baadache, Ali Belmehdi "Avoiding-Black-Hole-and-Cooperative-Black-Hole-Attacks-in-Wireless-Ad-hoc-Networks "IJCSIS) International Journal of Computer Science and Information Security,Vol. 7, No. 1, 2010
5. Virtual InterNetwork Testbed, http://www.isi.edu/nsnam/vint, 14 May 2006
6. F. J. Ros and P. M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2", December, 2004, http://masimum.dif.um.es/nsrt-howto/pdf/nsrthowto.pdf, 25 July 2005.