Effective Measure to Prevent Cooperative Black Hole Attack in Mobile Ad-hoc Wireless Networks

Mrs.M.Jhansi, Assoc.Professor,
Computer science and engineering,
Samskruti college of engineering and technology,R,R Dist.A.P,India

Ms. K.RoopaDevi,(M.Tech)
Computer science and engineering
Tirumala engineering college,Bogaram,A.P,India

Mr.B.Mukesh Chandra,Asst. Professor
Computer science and engineering
Vignan inst. Of Technology and science,A.P,India.

Abstract— **A mobile ad hoc network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. 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 [1]. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. In this paper, we address the problem of coordinated attack by multiple black holes acting in group. And we propose a complete protocol to detect a chain of cooperating malicious nodes in an ad hoc network that disrupts transmission of data by feeding wrong routing information. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack.**

Keywords - Ad hoc networks, Black hole, security, routing protocols, AODV.

I INTRODUCTION

Ad hoc network [1] is a wireless network without having any fixed infrastructure. Each mobile node in an ad hoc network moves arbitrarily and acts as both a router and a host. A wireless ad-hoc network consists of a Collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. Black hole attack [2] is one of many possible attacks in MANET. Black hole attack can occur when the malicious node on the path directly attacks the data traffic and intentionally drops, delay or alter the data traffic passing through it. This attack can be easily lessen by setting the promiscuous mode of each node and to see if the next node on the path forward the data traffic as expected. Another type of black hole attack is to attack routing control traffic. Fig. 1: shows the black hole attack, where M is the malicious node, S is the source node, D is the destination node and A, B and C are the intermediate nodes.

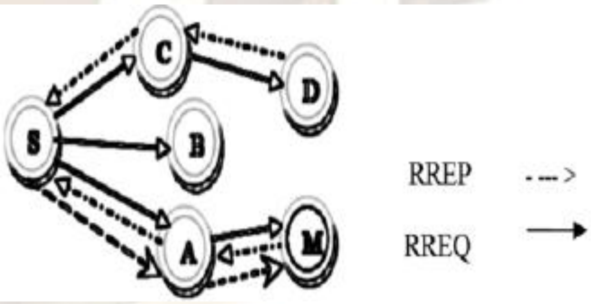


Fig. 1: Black Hole attack

II ROUTING PROTOCOLS

There are currently three main routing protocols for ad hoc networks [1], Destination- Sequenced Distance Vector routing (DSDV) [12], Dynamic Source Routing (DSR) [9], and AODV [2]. DSDV is a table driven routing protocol. In DSDV, each mobile node in the network maintains a routing table with entries for every possible destination node, and the number of hops to reach them. The routing table is periodically updated for every change in the network to maintain consistency. This involves frequent route update broadcasts. DSDV is inefficient because as the network grows the overhead grows as O(n2) [1]. DSR is an on-demand routing protocol and it maintains a route cache, which leads to memory overhead. DSR has a higher overhead as each packet carries the complete route, and does not support multicast. AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains 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 not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further 2 propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself. Each intermediate node receiving the RREQ, makes an entry in its routing table for the node that forwarded the RREQ message, and the source node.

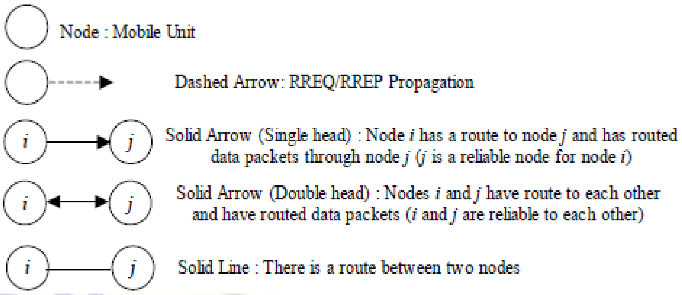
The destination node or the intermediate node with a fresh enough route to the destination node, uncast the Route Response (RREP) message to the neighboring node from which it received the RREQ. An intermediate node makes an entry for the neighboring node from which it received the RREP, then forwards the RREP in the reverse direction. Upon receiving the RREP, the source node updates its routing table with an entry for the destination node, and the node from which it received the RREP. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP.

However, the proposed method cannot be applied to identifying a cooperative black hole attack involving multiple nodes. In this paper, we develop a methodology to identify multiple black hole nodes cooperating as a group. The technique works with slightly modified AODV protocol and makes use of the Data Routing Information (DRI) table in addition to the cached and current routing tables. The rest of the paper is organized as follows. In Section 3, we introduce the cooperative black hole attack. Next, in Section 4, we present a new methodology to prevent a cooperative black hole attack. Finally, in Section 5, we conclude and discuss future work.

III COOPERATIVE BLACK HOLE ATTACK PROBLEM

3.1 Black Hole

A Black Hole attack is a kind of denial of service 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. Co operative Black hole means the malicious nodes act in a group. 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. We define the following conventions for protocol representation.


Node : Mobile Unit
Dashed Arrow: RREQ/RREP Propagation
i
j
Solid Arrow (Single head) : Node i has a route to node j and has routed data packets through node j (j is a reliable node for node i)
i
j
Solid Arrow (Double head) : Nodes i and j have route to each other and have routed data packets (i and j are reliable to each other)
i
j
Solid Line : There is a route between two nodes

3.2 Cooperative Black Hole Attack

According to the original AODV protocol, when source node S wants to communicate with the destination node D, the source node S broadcasts the route request (RREQ) packet. The neighboring active nodes update their routing table with an entry for the source node S, and check if it is the destination node or has a fresh enough route to the destination node. If not, the intermediate node updates the RREQ (increasing the hop count) and floods the network with the RREQ to the destination node D until it reaches node D or any other intermediate node which has a fresh enough route to D, as depicted by example in Figure 2.

The destination node D or the intermediate node with a fresh enough route to D, initiates a route response (RREP) in the reverse direction, as depicted in Figure 3. Node S starts sending data packets to the neighboring node which responded first, and discards the other responses. This works fine when the network has no malicious nodes.

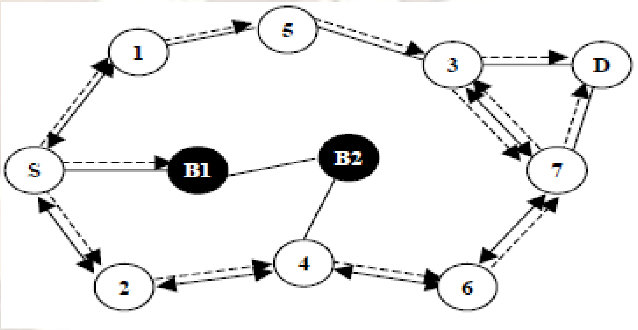


Figure 2: Network flooding of RREQ

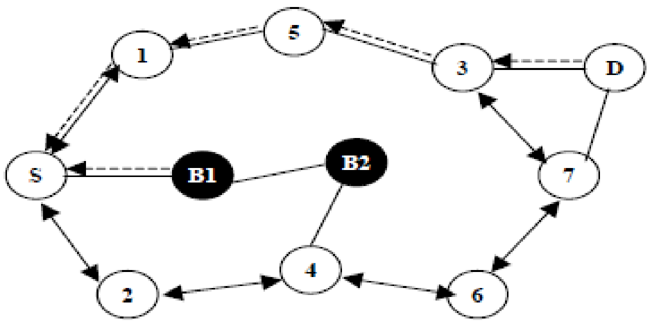


Figure 3: Propagation of RREP messages

Researchers have proposed solutions to identify and eliminate a single black hole node [3]. However, the case of multiple black hole nodes acting in coordination has not been addressed. For example, when multiple black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its teammates B2 as the next hop, as depicted in Figure 3. According to [3], the source node S sends a "Further Request (FRq)" to B2 through a different route (S-2-4-B2) other than via B1. Node S asks B2 if it has a route to node B1 and a route to destination node D. Because B2 is cooperating with B1, its "Further Reply (FRp)" will be "yes" to both the questions. Now per the solution proposed in [3], node S starts passing the data packets assuming that the route S-B1-B2 is secure. However, in reality, the packets are consumed by node B1 and the security of the network is compromised.

IV SOLUTION

In this section, we propose a methodology for identifying multiple black hole nodes cooperating as a group with slightly modified AODV protocol by introducing Data Routing Information (DRI) Table and Cross Checking.

4.1 Data Routing Information Table

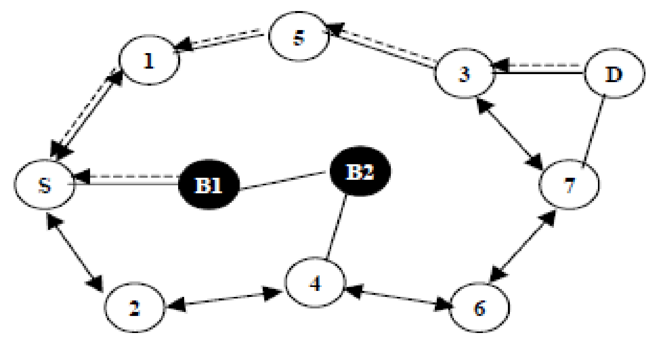


Figure 4: Solution to avoid cooperative black hole attack

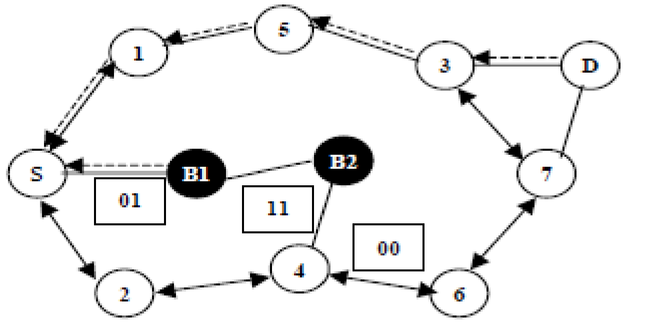
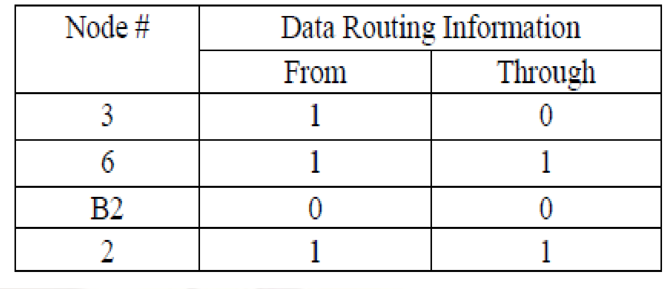


Figure 5: Solution to identify multiple black hole nodes in one-time check

The solution to identify multiple black hole nodes acting in cooperation involves two bits of additional information from the nodes responding to the RREQ of source node S. Each node maintains an additional Data Routing Information (DRI) table. In the DRI table, 1 stands for 'true' and 0 for 'false'. The first bit "From" stands for information on routing data packet *from* the node (in the Node field) while the second bit "Through" stands for information on routing data packet *through* the node (in the Node field). In reference to the example of Figure 4, a sample of the database maintained by node 4 is shown in Table 1. The entry 1 0 for node 3 implies that node 4 has routed data packets from 3, but has not routed any data packets through 3 (before node 3 moved away from 4). The entry 1 1 for node 6 implies that, node 4 has successfully routed data packets from and through node 6. The entry 0 0 for node B2 implies that, node 4 has NOT routed any data packets from or through B2.



Node #	Data Routing Information	
	From	Through
3	1	0
6	1	1
B2	0	0
2	1	1

Table 1. Additional table of data routed from, and routed to nodes maintained by node 4.

4.2 Cross Checking

In our techniques we rely on reliable nodes (nodes through which the source node has routed data) to transfer data packets. The modified AODV protocol, and the algorithm for our proposed methodology are illustrated in Figure 6.

In the protocol, the source node (SN) broadcasts a RREQ message to discover a secure route to the destination node. The Intermediate Node (IN) generating the RREP has to provide its Next Hop Node (NHN), and its DRI entry for the NHN. Upon receiving RREP message from IN, the source node will check its own DRI table to see whether IN is a reliable node.

If source node has used IN before to route data, then IN is a reliable node and source node starts routing data through IN. Otherwise, IN is unreliable and the source node sends FRq message to NHN to check the identity of the IN, and asks NHN:

1) if IN has routed data packets through NHN
2) who is the current NHN's next hop to destination, and
3) has the current NHN routed data through its own next hop.

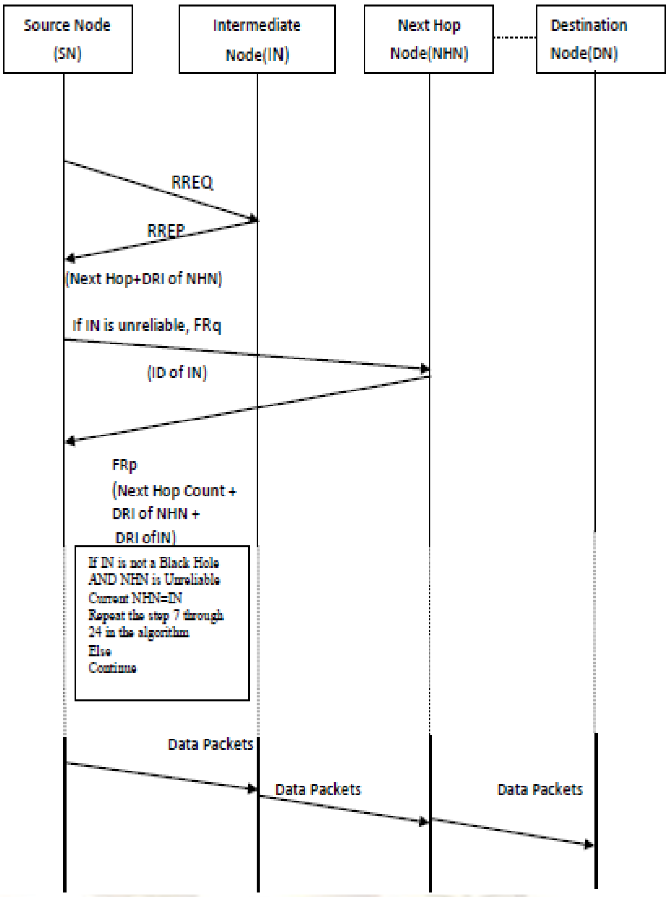
The NHN in turn responds with FRp message including

1) DRI entry for IN
2) the next hop node of current NHN, and
3) the DRI entry for the current NHN's next hop.

Based on the FRp message from NHN, source node checks whether NHN is a reliable node or not. If source node has routed data through NHN before, NHN is reliable; otherwise, unreliable. If NHN is reliable, source node will check whether IN is a black hole or not. If the second bit (ie. IN has routed data *through* NHN) of the DRI entry from the IN is equal to 1, and the first bit (ie. NHN has routed data *from* IN) of the DRI entry from the NHN is equal to 0, IN is a black hole.

If IN is not a black-hole and NHN is a reliable node, the route is secure, and source node will update its DRI entry for IN with 01, and starts routing data via IN.

If IN is a black-hole, the source node identifies all the nodes along the reverse path from IN to the node that generated the RREP as black hole nodes. Source node ignores any other RREP from the black holes and broadcasts the list of cooperative black holes.



If NHN is an unreliable node, source node treats current NHN as IN and sends FRq to the updated IN's next hop node and goes on in a loop from steps 7 through 24 in the algorithm.

As an example, let's consider the network in Figure 5. When node B1 responds to source node S with RREP message, it provides its next hop node B2 and DRI for the next hop (i.e. if B1 has routed data packets through B2). Here the black hole node lies about using the path by replying with the DRI value equal to 0 1. Upon receiving RREP message from B1, the source node S will check its own DRI table to see whether B1 is a reliable node.

Since S has never sent any data through B1 before, B1 is not a reliable node to S. Then S sends FRq to B2 via alternative path S-2-4-B2 and asks if B2 has routed any data from B1, who is B2's next hop, and if B2 has routed data packets through B2's next hop. Since B2 is collaborating with B1, it replies positively to all the three requests and gives node 6 (randomly) as its next hop. When the source node contacts node 6 via alternative path S-2-4-6 to cross check the claims of node B2, node 6 responds negatively. Since node 6 has neither a route to node B2 nor has received data packets from node B2, the DRI value corresponding to B2 is equal to 0 0 as shown in Figure 4.

Based on this information, node S can infer that B2 is a black hole node. If node B1 was supposed to have routed data packets through node B2, it should have validated the node before sending it. Now, since node B2 is invalidated through node 6, node B1 must cooperate with node B2. Hence both nodes B1 and B2 are marked as black hole nodes and this information is propagated through the network leading to their listing as black holes, and revocation of their certificates. Further, S discards any further responses from B1 or B2 and looks for a valid alternative route to D.

Algorithm to prevent cooperative black hole attack in MANETs

Notations :

SN: Source Node IN: Intermediate Node
DN: Destination Node NHN: Next Hop Node
FRq: Further Request FRp: Further Reply
Reliable Node: The node through which the SN has routed data
DRI: Data Routing Information
ID: Identity of the node

```
SN broadcasts RREQ
SN receivesRREP
IF (RREP is from DN or a reliable node) {
    Route data packets (Secure Route)
}
ELSE {
    Do {
        Send FRq and ID of IN to NHN
        Receive FRp, NHN of current NHN, DRI entry for
        NHN's next hop, DRI entry for current IN
        IF (NHN is a reliable node) {
            Check IN for black hole using DRI entry
            IF (IN is not a black hole)
                Route data packets (Secure Route)
            ELSE {
                Insecure Route
                IN is a black hole
                All the nodes along the reverse path from IN to the node
                that generated RREP are black holes
            }
        }
        ELSE
            Current IN = NHN
    } While (IN is NOT a reliable node)
}
```

Figure 6: Modified AODV protocol and algorithm to prevent cooperative black hole attack

The process of cross checking the intermediate nodes is a onetime procedure which we believe is affordable to secure a network from multiple black hole nodes.

The cost of cross checking the nodes can be minimized by letting nodes sharing their trusted nodes list (DPI table) with each other.

V CONCLUSION AND FUTURE WORK

In this paper we have studied the routing security issues of MANETs, described the cooperative black hole attack that can be mounted against a MANET and proposed a feasible solution for it in the AODV protocol. The proposed solution can be applied to

1.) Identify multiple black hole nodes cooperating with each other in a MANET; and

2.) Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation.

As future work, we intend to develop simulations to analyze the performance of the proposed solution. We also plan to study the impact of GRAY hole nodes (nodes which switch from good nodes to black hole nodes) and techniques for their identification.

References

[1] Hongmei Deng, Wei Li, and Dharma P. Agarwal, “Routing Security in Wireless Ad Hoc Networks”, University of Cincinnati, IEEE Communications magazine,Vol.40, no.10, October 2002.

[2] Bo Sun,Yong Guan,Jian Chen,Udo , “Detecting Black-hole Attack in Mobile Ad Hoc Network” , The institute of Electrical Engineers, Printed and published by IEEE, 2003.

[3] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, “Detecting Black holeAttack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Vol.5, issue 3, Nov 2007, pp 338–346.

[4] 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.

[5] Charles E. Perkins, and Elizabeth M. Royer, “Ad-hoc On-Demand Distance Vector (AODV) Routing,” Internet Draft, November 2002.

[6] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Network,” IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[7] S. Marti et al., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” 6th Int’l. Conference Mobile Comp. Net., pp. 255-265, August 2000.

[8] Vesa Kärpijoki, “Security in Ad hoc Networks,” http://www.tcm.hut.fi/Opinnot/Tik110.501/2000/papers/karpijoki.pdf.

[9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Volume 5, Number 3, 2007, pp 338–346

[10] Lidong Zhou, and Zygmunt J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6, November/December 1999.

[11] Janne Lundberg, "Routing Security in Ad Hoc Networks," routing-security-in-ad.pdf

[12] Bo Sun Yong, Guan Jian Chen and Udo W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks",The Institution of Electrical Engineers (IEE) ,Volume 5, Number 6, 2003, pp 490-495

[13] Y. Zhang, W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," 6th Int'l. Conference Mobile Comp. Net., Mobicom 2000, pp. 275-283, August 2000.

[14] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu and Lixia Zhang, "Self-securing Ad Hoc Wireless Networks,"http://www.cs.ucla.edu/~jkong/publications/ISCC02.pdf.

[15] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Computer Communications Review, pp. 234-244, October 1994.

M..Jhansi, working as Assoc.prof. in Samskruti College of Engineering and Technology, R.R.Dist. MTech from Nishitha College of Engineering and Technology.JNTUH. B.Tech from University College of Engineering,KU. Her research interests are in Computer Networks, wireless communication networks and network security.

K.RoopaDevi, Pursuing M.Tech from Tirumala Engineering College, R.R.Dist. MCA from Vaagdevi P.G.College,KU. Her research interests are in Computer networks and network security.

B.Mukesh Chandra, working as Asst.prof. in Vignan Institute of Technology and Science, Nalgonda Dist. MTech from Sreedatha Engineering College,JNTUH. M.Sc, physics from Osmania University,His research interests are Computer networks and network security.