MITIGATING CO-ATACKING MULTIPLE BLACK HOLE ATTACK USING DRI AND RELIABILITY TABLE IN WIRELESS AD HOC NETWORKS

Vinit, Research Scholar, Manav Bharti University Solan (H.P).

ABSTRACT

Mobile ad hoc networks (MANETs) are extensively used in military and civilian applications. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. This generic characteristic of MANET has rendered it vulnerable to security attacks. In this paper, we address the problem of coordinated attack by multiple black holes acting in-group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative multiple black hole attack.

***Keywords**: Ad hoc networks, Black hole, Security, Routing, Reliability Measurement Ttable, AODV*

INTRODUCTION

Ad hoc networks have a large number of potential applications. Military uses such as Connecting soldiers or other military units to each other on the battlefield or creating sensory arrays with thousands of sensors are two typical examples. Ad hoc networks provide a possibility of creating a network in situations where creating the infrastructure would be impossible or prohibitively expensive. Unlike a network with fixed infrastructure, mobile nodes in ad hoc networks do not communicate via access points (fixed structures). Each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network. 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 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, unicasts 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. Some researchers discuss the vulnerabilities in Ad hoc routing protocols and the attacks that can be mounted. The AODV protocol is vulnerable to the well-known black holeattack.

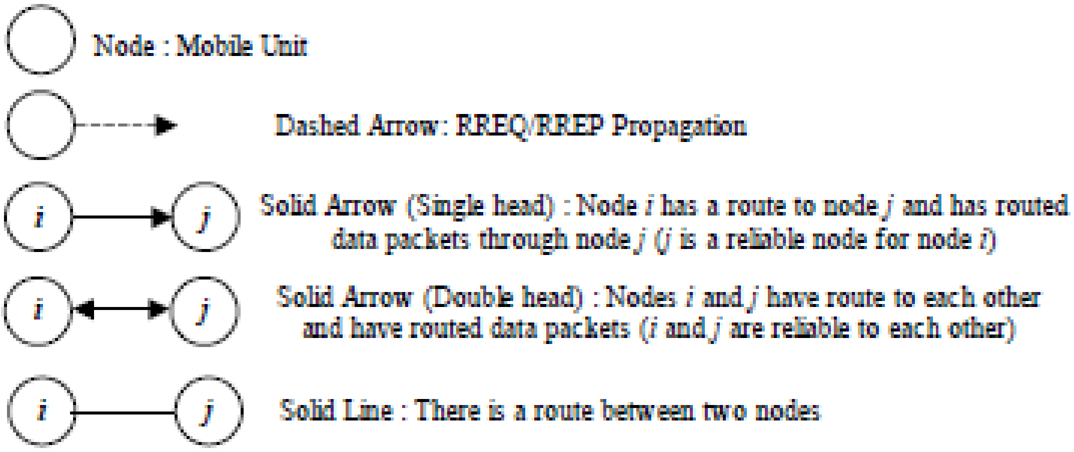
A black hole is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. Since a black hole does not have to check its routing table, it is the first to respond to the RREQ in most cases. When the data packets routed by the source node reach the black hole node, it drops the packets rather than forwarding them to the destination node. Deng, Li, and Agrawal [3] assume the black hole nodes do not work as a group and propose a solution to identify a single black hole. 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 withslightly modified AODV protocol and makes use of the Data Routing Information (DRI) table in addition to the cached and current routingtables.

The rest of the paper is organized as follows. In Section 2, we introduce the cooperative Black hole attack. Next, in Section 3, we present a new methodology to prevent a cooperative black hole attack with the reliability measurement. Finally, in Section 4, we conclude and discuss future work.

MULTIPLE BLACK HOLE ATTACK PROBLEM

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. 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

MULTIPLE 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 1. 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 maliciousnodes.

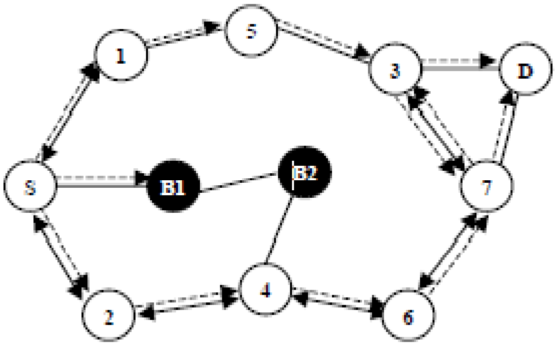


Figure 1: Network floodingofRREQ

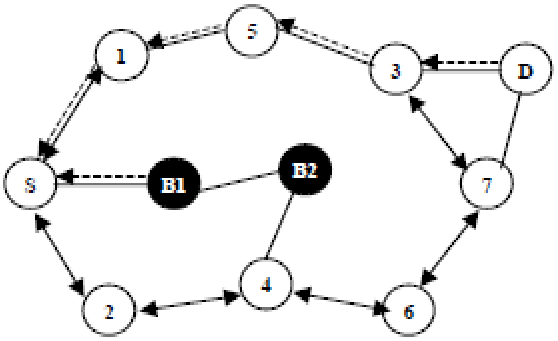


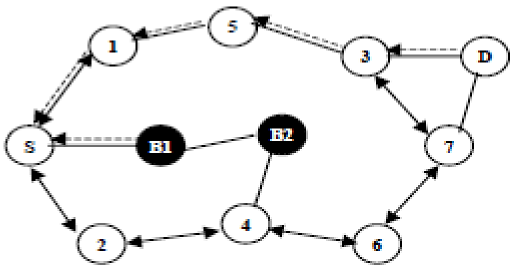
Figure 2: Propagation of RREPmessages

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 2. 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 perthe 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.

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.

3.1 Data Routing Information Table



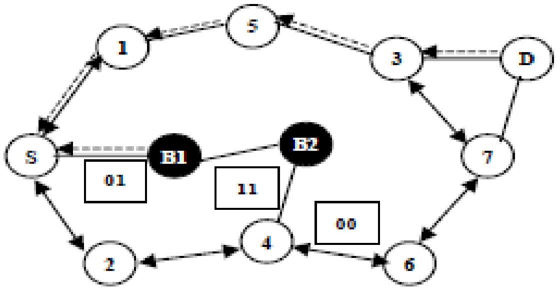


Figure 3: Solution to avoid multipleblackhole Attack.

Figure 4: Solution to identify multiple blackhole nodes in one-timecheck

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.

Node Address	Packet drops	Packet forwards	Misbehave

Table1.1. Node reliability table.

Node Address: Address of next hop node.

Packet Drops: Counter for counting the dropped packet.

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.

CROSS CHECKING

Figure 3: Solution to avoid cooperative black hole attack Figure 4: Solution to identify multiple black hole nodes in one-time check 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 5. 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 grater then the thrshould1 and thrshould2 according to reliability algorithm 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)oftheDRIentryfromtheNHNisequalto0,INisablackhole.IfINisnotablack-holeandNHNisareliable 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. Here we cannot measure the reliability at different threshold so that after this we measure the reliability with the help of reliability table at each node.

Pseudo code of prevent multiple black hole attack in MANETs

Notations :

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

```
1 SN broadcasts RREQ
2 SN receives RREP
3 IF (RREP is from DN or a reliable node>th1or th2) {
4     Route data packets (Secure Route)
5 }
6 ELSE{
7     Do{
8         Send FRq and ID of IN toNHN
9         Receive FRp, NHN of current NHN, DRI entryfor
10        NHN's next hop, DRI entry for currentIN
11        IF (NHN is a reliable node>th1or th2) {
12            Check IN for black hole using DRI entry
13            IF (IN is not a black hole)
14                Route data packets (SecureRoute)
ELSE{
Insecure Route
IN is a blackhole
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)
}
```

Pseudo code of reliability table mechanism

```
1.Data packet forwarded orsent.
2.Copy and keep the data packet in DRI table until it is expired or forwarded
3.If (data packetforwarded)
   {Increment the corresponding forwarded packetin the node-reliability table and remove the data packet from DRI table}
4.If (data packet expires in the DRI table)
   {Increment the corresponding  dropped packet  in the  node-reliabilitytableand      remove the data packet from DRI 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
```

```
        }
    }
}
```

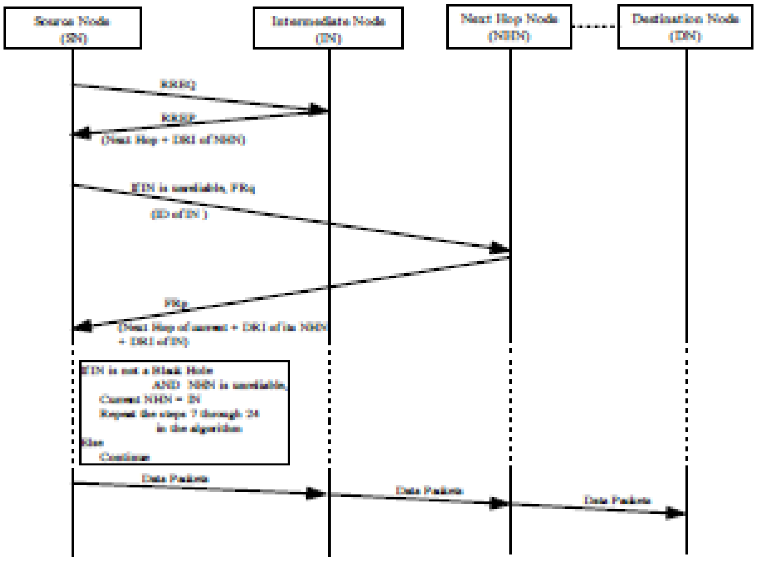


Figure 5: Modified AODV protocol and algorithm to prevent cooperative black hole attack

As an example, let's consider the network in Figure 4. 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 nexthop.

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. The process of cross checking the intermediate nodes is a one time 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 eachother.

Simulation approach:-

Average received Throughput: - It is the total number of received packet per unit time. In another term, throughput is the packet size (in term of bits) that is going to be transmitted divided by the time that is used to transmit thesebits.

Average sending Throughput: - It is the total number of sending packet per unit time. In another term, throughput is the packet size (in term of bits) that is going to be transmitted divided by the time that is used to transmit thesebits.

Total throughput = (Average received throughput / Average sending throughput)*100%

End-to-end delay: - This is defined as the delay between the time at which the data packet was originated at the source and the time it reaches thedestination.

Delay = Receiving time - Sending time

Paket loss percentage: - The ratio between the number of packets originated by the CBR sources and the number of packets received by the CBR sink at the final destination.

Packet loss =((Total No. of packet sent -Total No. of packet received) / (Total No.of packet sent))*100%

1) First, results are calculated for throughput vs. number of black holenode,

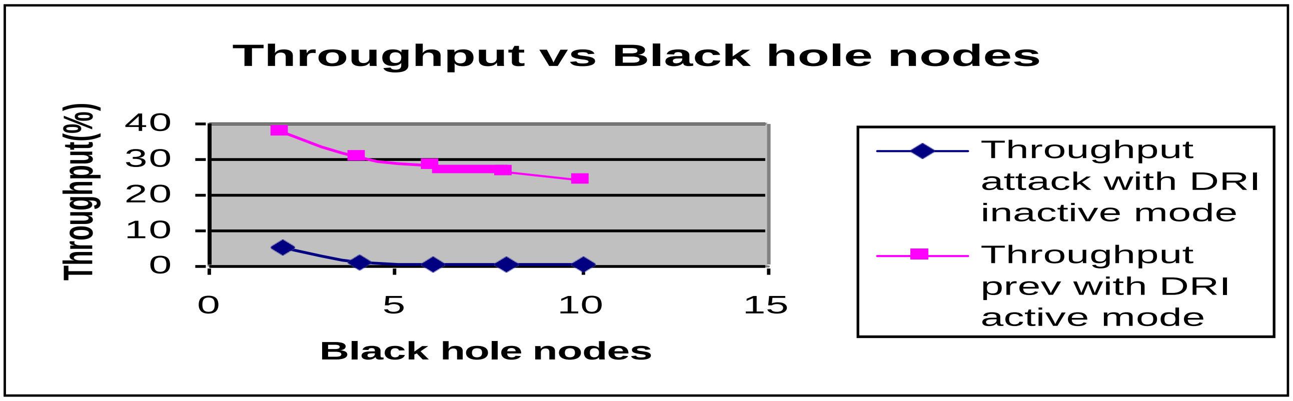


Figure 6: Throughput vs. Black hole nodes for 50 nodes

The results are shown in table 9 increases in the value of throughput when the modified AODV based on DRI mechanism is active in the presence of 2,4,6,8,10 black hole nodes.

Table 5.2: Percentage increase in Throughput in the presence of 2,4,6,8,10 Black hole nodes

Blackhole .nodes	Throughput attack	Throughput prev
2	5.41	37.44
4	1.411	30.37
6	0.611	28.5
8	0.505	26.6
10	0.411	24.047

2) Second, results are calculated for packet loss vs. number of black hole node, these line charts are shownbelow:-

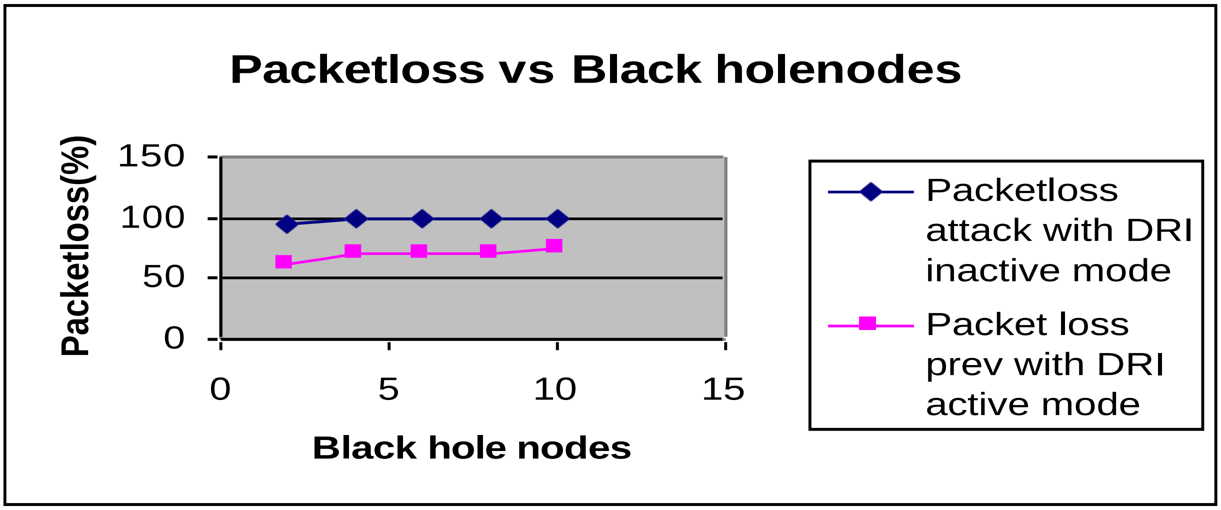


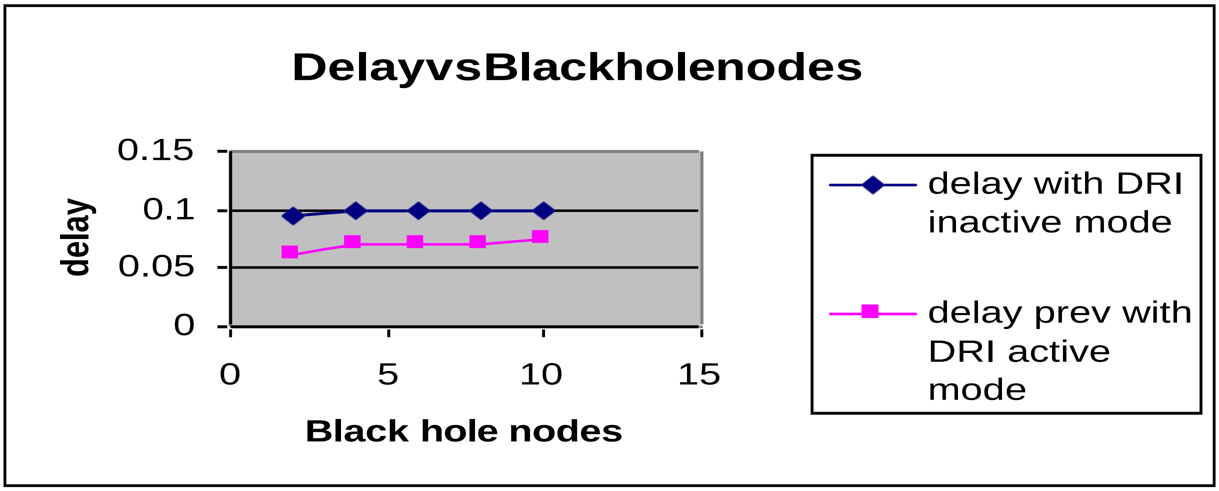
Figure 7: packet loss vs. Black hole nodes for 50 nodes

The results are shown in table 10 decrease the value of packet loss when the modified AODV based on DRI mechanism is active in the presence of 2,4,6,8,10 black holenodes.

Table 5.3: Percentage decrease the packet loss in the presence of 2,4,6,8,10 Black hole nodes

Blackhole node	Pktloss attack	Pktloss prev
2	95.59	62.55
4	98.58	69.62
6	99.38	71.49
8	99.45	70.41
10	99.55	75.96

3) Results are calculated for delay vs. number of black hole node, these line charts are shownbelow:-



The results are shown in table 11 decrease the value of dealy when the modified AODV based on DRI mechanism is active in the presence of 2,4,6,8,10 black hole nodes.

Table 5.4: Percentage decrease the dealy in the presence of 2,4,6,8,10 Black hole nodes

Blackhole node	Delay attack	Delay prev
2	0.0956	0.0626
4	0.0986	0.0696
6	0.0994	0.0715
8	0.0995	0.0704
10	0.0996	0.076

Analysis:- The experimental results show that when we using same simulation parameter with reliability measurement and modified AODV were tested on above-mentioned networks having the black hole nodes are increased such as 2,4,6,8,10 in the network then in the presence of DRI active mode throughput increases up to 24% to 32% and packet loss decrease 40% to 30% and delay decrease 0.04 ms to 0.03 ms, compare with the DRI inactive mode.

CONCLUSIONS 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 and its implementation. As future work, we intend to study the impact of GRAY hole nodes (nodes which switch from good nodes to black hole nodes) and techniques for theiridentification.

REFERENCES

[1] Elizabeth M. Royer, and Chai-Keong Toh, "A Review of Current Routing Protocols for AdHoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, April1999.

[2] CharlesE.Perkins,andElizabethM.Royer,"Ad-hocOn-DemandDistanceVector(AODV)Routing,"Internet Draft, November2002.

[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October2002.

[4] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," 6th Int'l.Conference Mobile Comp. Net., pp. 255-265, August2000.

[5] Lidong Zhou, Zygmunt J.Hass, ``Securing Ad Hoc Networks", IEEE Special Issue on Network Security, vol-13, pp 24-30 Nov-Dec1999

[6] Srdjan Capkuny, Levente Butty´an, and Jean-Pierre Hubaux, "Self-Organized Public-Key Management forMobile Ad Hoc Networks," Technical Report at EPFL, http://ic2.epfl.ch/publications/documents/IC_TECH_REPORT_200234.pdf.

[7] Lidong Zhou, and Zygmunt J. Haas, “Securing Ad Hoc Networks,” IEEE Network Magazine,vol. 13, no.6, November/December1999.

[8] Janne Lundberg, “Routing Security in Ad Hoc Networks,”netsec-lundberg.pdf/routing-security-in-ad.pdf

[9] David B. Johnson, and David A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” *Mobile Computing*, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[10] Y. Zhang, W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks,” 6th Int’l. Conference Mobile Comp. Net., Mobicom 2000, pp. 275-283, August2000.

[11] 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.

[12] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV)for Mobile Computers,” Computer Communications Review, pp. 234-244, October1994.

[13] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, ``Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada,USA.

[14] L.Venkatraman and D.P. Agrawal, ``Strategies for Enhancing Routing Security in Protocols for Mobile Ad Hoc Networks", IEEE Network Magazine, vol. 13, no-6, Nov1999

[15] The Network Simulator - ns-2 http://www/isi.edu/nsnam/ns.

[16] Kevin Fall and Kannan Varahan, editors. "NS Notes and Documentation", the VINT Project, UC Berkeley, LBL, USC/ISI, and Xerox PARC, November1997.

[17] K.Gorantala, ``Routing Protocol in Mobile Ad-hoc Networks," Technical report Department of ComputerScience from UMEA University,June-2006.

[18] X. Hong, Kaixin Xu, and Mario Gerla, ``Scalable routing protocols for mobile ad hoc networks", IEEE Network Magazine, pp11-21,July-Aug2002

[19] V.D.Park and M.S.Corson, ``A Highly Adaptive Distributed Routing Algorithm for Mobile WirelessNetworks," Proc. INFOCOM,Apr-1997.

[20] L.Buttyan and J.P.Hubaux, ``Enforcing service availability in mobile ad hoc networks", in Proceedings of MobiHOC, USA, Aug2000.

[21] S.Buchegger and J.Y.L.Boudec, ``Performance analysis of CONFIDANT protocol: Cooperation ofnodes", In Proceedings of IEEE Workshop on Mobie adhoc network, Lausanne, June2002

[22] P.MichiardiandR.Molva,``Core:Acollaborativereputationmechanismtoenforcenodecooperation inmobilead hoc networks", in Proceedings of Sixth Conference on CMS 2002. Portoroz, Slovenia,2002

[23] B.Awebuch, D.Holmer and H.Rubens, ``An on-demand secure routing protocol resilient to Byzantine failure",in Procedding of Security Workshop on MobiCom,2002

[24] R. Ramanujan, S.Kudige, T.Nguyen and F. Adlestein, ``Intrusion-resistant ad hoc wireless networks",in Proceedings of MilCom, October 2002

[25] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , ``Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" in florida atlantic university, pp 1-38, jan2006

Author would like to extend his heartfelt thanks to the academic and infrastructural support received from his respective Dept./University.