COOPERATIVE BLACK HOLE NODE DETECTION BY MODIFYING AODV

Kundan Munjal*

Shilpa Verma*

Aditya Bakshi**

Abstract-

The black hole attack is a well known severely occurring security threat in wireless mobile ad hoc networks. A black hole is a malicious node that spuriously replies for any route request without having any active route to the specified destination. It then absorbs all the data packets and drops them fully or sometimes partially so that the destination node will not be able to get the data packets results in affecting the PDR (packet delivering ratio) to a great extent. Sometimes the Black Hole Nodes cooperate with each other with the same aim of dropping packets these are known as cooperating Black Hole nodes and the attack is known as *Cooperative Black Hole attack*. In this paper our goal will be on proposing an algorithm for detecting these cooperative black hole nodes in the network and propagating this information throughout the network. Our focus specifically, is on ensuring the security against the Black hole attacks.

Keyword- *Mobile ad hoc network (MANET); black hole; AODV.*

* Dept. of Computer Science and Applications, Kurukshetra University, Kurukshetra, India-132119.

** Dept. of Computer Engineering, YMCA University, Faridabad, India-121001.

1 INRTODUCTION

A Mobile Ad hoc network (MANET) is a self-configuring network that does not require any pre-existent (fixed) Infrastructure, which minimizes their deployment time as well as cost. As each node in this network is free to move which makes the network to change its topology continuously. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to form own wireless network on the fly. Because of the dynamic nature, these networks are more vulnerable to attacks so security is an important as well as serious issue in mobile ad hoc networks. The nature of these[1] networks makes them extremely vulnerable to various malicious attacks the Black Hole attack is one of them. This paper is organized as follows In the remaining part Section 1 related work for detecting Black Hole attack has been discussed Section 2 provides an overview of AODV protocol with the description of black hole attack characteristics Section 3 describes the proposed solution for detecting cooperative Black hole attacks in mobile ad hoc networks. In Section 4 we will show the working of the algorithm with the help of an example. We conclude plan for future work in section 5.

1.1 RELATED WORK

Payal N. Raj, Prashant B. Swades [19] proposed DPRAODV (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The

RREP is accepted if its sequence number is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than the threshold value than it is considered as the malicious node.

Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park [21] proposed two different approaches to solve the black hole attack. The first solution the sender node needs to verify the authenticity of the nodes that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination. The SN unicast the ping packet using different routes. The IN or destination node or malicious node will

ping requests. The SN checks the acknowledgement and processes them to check which one is safe or having malicious node. In the meantime the SN buffered until it found the safe route.

Chang Wu Yu, Tung-Kuang, Wu, ReiHeng, Cheng, and Shun Chao Chang [22] proposed a distributed and cooperative procedure to detect black hole node. In this each node detect local anomalies. It collects information to construct an estimation table which is maintained by each node containing information regarding nodes within power range. This scheme is initiated by the initial detection node which first broadcast and then it notifies all one-hop neighbors of the possible suspicious node. They cooperatively decide that the node is suspicious node.

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamlipour, and Yoshiaki Nemoto [23] uses an anomaly detection scheme. It uses dynamic training method in which the training data is updated at regular time intervals. Multidimensional feature vector is identified to express state of the network at each node. Each dimension is counted on every time slot. It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They calculate mean vector by calculating some mathematical calculation. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack.

Latha Tamilselvan, DR. V Sankaranarayanan [25] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is give to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide to that node. Any node having '0' value is considered as malicious node and is eliminated.

Hesiri Weerasinghe [26] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is slightly modified version of

AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (RREP).

2. AODV AND BLACK HOLE ATTACK

A. OVERVIEW OF AODV

AODV is a reactive [2] routing protocol that does not require maintenance of routes to destination nodes. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is demand from mobile node. In ad hoc network first route discovery takes place, which means if a mobile node that wishes to communicate with other node first broadcast a RREQ (Route Request) message to find a fresh route to a desired destination node. Every neighbor node that receives RREQ broadcast first saves the path the RREQ was transmitted along its routing table. It then checks its routing table to see if it has a fresh enough route to the destination node provided in RREQ message. Destination sequence number attached to it indicates the freshness. If a node finds a fresh enough route it unicasts a RREP (route reply) message back along the saved path to the source node or it rebroadcast the RREQ message otherwise. The same process continues until an RREP message from the destination node or an intermediate node that has a fresh route to the destination node received by the source node.

B. BLACK HOLE ATTACKS

A black hole attack is a kind of Denial of service attack in mobile ad hoc networks. In this attack, a malicious node sends [4] a fake RREP packet to the source node that has initiated a route discovery, in order to show itself as a destination node or an intermediate node to the actual destination node. In such a case the source node would send all of its data packets to the malicious node the malicious node then absorbs all the packets and drops them fully or sometimes partially. As a result source and destination node will not be able to communicate with each other..

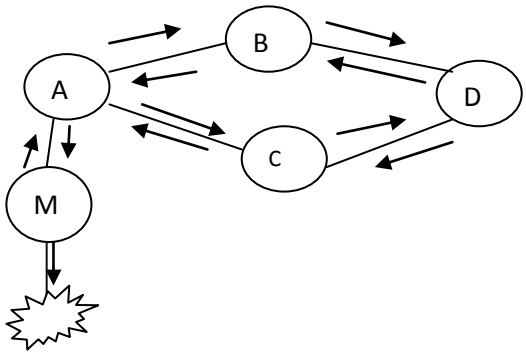

Fig.1 Route discovery and Black Hole attack by malicious node M.

Consider the case in fig. 1 where A is the source node D is the destination node and M is the malicious node here node A starts with the route discovery process then the node M advertises itself as having a valid shortest route to the destination, even though the route is fake with the purpose of intercepting packets. Moreover a malicious node does not need to check its routing table when sending a spurious message; its response is more likely to reach the source node first. This makes the source node think that the route discovery process is complete, ignore all other reply messages and begin to send data packets. As a result, all the packets through the malicious node are simply absorbed discarded and then lost. The malicious node could be said to form a black hole in the network. Sometimes these malicious nodes cooperate with each other with the same aim of dropping packets these are known as cooperative Black Hole nodes and the attack is known as ***Cooperative Black Hole attack.*** In this way it causes an attack to the network with very little efforts to its part.

3. PROPOSED SOLUTION AGAINST COOPERATIVE BLACK HOLE ATTACK

In the proposed scheme, a mechanism for detecting as well as defending against a cooperative black hole attack is identified and presented by an algorithm. In this proposed scheme the modification of Ad Hoc on Demand Distance Vector Routing Protocol takes with the introduction of two types of concepts

1. Maintenance of Routing Information Table (RIT).

2. Reliability checking of a node.

3.1 MAINTENANCE OF ROUTING INFORMATION TABLE

In the proposed scheme, each and every node maintains three bit information from which two bits of the information are sent by the nodes that respond with the RREP message to the source node during route discovery phase and third bit information is broadcasted by any node in the network. In the routing information table (RIT) the bit 1 stands for 'true' and the bit 0 stands for 'false'. The three types of information stored are:

1. from Node
2. through Node
3. through any Trustful Node

3.1.1 From Node: It stands for the information on routing data packet from the node in question.

3.1.2 Through Node: It stands for the information on routing data packet through the node in question.

3.1.3 Through any trustful node: This bit is set if any trustful node has routed data packet through the node in question.

Consider the table 3.1 in which the routing information for node 8 is maintained. The entry 1 1 0 for node 4 shows that node 8 has routed data from node 4 before, node 8 has also successfully routed data through node 4 before, but any other trustful node hasn't routed data through node 4.

NODE ID	FROM NODE	THROUGH NODE	THROUGH ANY TRUSTFUL NODE
4	1	1	0
5	1	0	1
6	0	0	1
7	1	1	1
9	0	0	0

Table 3.1 RIT entry for Node 8.

Similarly, node 5 entry is 1 0 1 which shows that node 8 has successfully routed data from node 5 but not through node 5 but the third entry shows that any other node (trustful node) has successfully routed data through node 5. The entry for node 6 is 0 0 1 which shows that node 8 has never routed data from or through node 6 but any other trustful node had successfully routed through it in the past. The route entry for node 9 is 0 0 0 which shows that no node in the network had routed data from or through node 9.

WHICH NODE IS TRUSTFUL?

Nodes through which source node or any trustful node has routed data previously then that nodes are considered as **reliable or trustful nodes**. Consider the table 3.1 in which:

1. Node 4 is trustful as node 8 had routed data through it previously.

2. Node 5 is trustful as any other trustful node had routed data through it previously.

3. Node 9 is not trustful as no node in the network had routed data through it.

3.2 RELIABILITY CHECKING OF A NODE

In the modification the source node (SN) broadcasts a RREQ message to discover a reliable route to the destination. The intermediate node that generates the RREP has to provide the information

about the Next Hoping Node (NHN) and the table entry (RIT entry) for the NHN. Upon receiving the RREP message from the intermediate node the source will check its own routing information table to see whether IN is a trustful node or not. If SN has routed data through IN before then IN is trustful and it starts routing data through IN but if it hasn't routed before then IN is unreliable and SN sends Additional Request (ARq) message to next hop node about following information:

1. If IN has routed data through NHN

2. Who is the current NHN's next hop towards the destination?

3. The RIT entry for NHN's next hop.

Based on the Additional reply message (ARp) from NHN, SN checks whether NHN is reliable or not. If SN has routed data through NHN before then NHN is reliable. Otherwise NHN is unreliable for SN. If NHN is unreliable then SN will check whether IN is Black Hole or not. If the second bit entry for the IN is 1 then it shows that IN has routed data through NHN before but if the first bit entry of the NHN is 0 then it shows that NHN hasn't routed data from IN before so this contradiction shows that IN is a Black Hole node. And, if IN is not a Black Hole and NHN is reliable node then the route is reliable and SN will update its RIT entry with 0 1 0 and also broadcasts a B_REPLY message with the identity of the IN to show that this node is reliable.

On the other hand the node receiving the B_REPLY message first checks whether the B_REPLY message is from the node through which it had routed data before or any trustful node had routed data before (i.e. trustful node). This checking is made as cooperative Black Hole nodes can also broadcast a B_REPLY message for e.g. Consider two Cooperative Black Hole nodes B1 and B2. B1 can also broadcast a B_REPLY message with the ID of B2 to show that B2 is trustful. And, if the broadcasted B_REPLY message is from the trustful node then the node receiving the B_REPLY message will set the third bit in the RIT to 'true' for the respective IN.

4. EXAMPLE TO SHOW THE WORKING OF ALGORITHM IN DIFFERENT CASES

Case No 1: When there are no black hole nodes in the network and the reply is from reliable node.

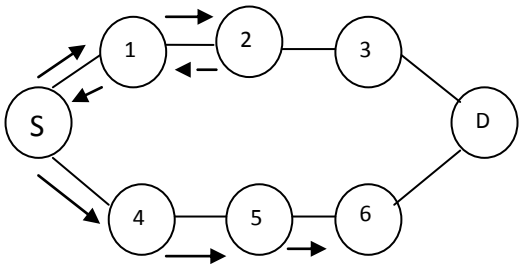

Fig 4.1 Reply from Reliable node 2.

Consider the case in the figure 4.1 in which the source node S broadcasts a route request packet (RREQ) packet to the destination node D**,** node 2 replies with a RREP packet, node S check its RIT entry for node 2 i.e. 1 1 1 which means that (Table 4.1) it has routed data through this node previously and also some other trustful node had also routed data successfully through this node as second and third bit entry are set to true (1). Therefore, node 2 is reliable and the route is secure.

```
NOTATIONS
SN    : Source node
IN    : Intermediate node
DN    : Destination node
NHN   : Next Hop node
ARq   : Additional Request
ARp   : Additonal Reply
RIT   : Routing Information Table
ID    : Identity of node

 1. SN starts route discovery by Broadcasting RREQ
 2. SN receives RREP
 3. If( RREP is from DN or Trustful node){
 4.       Route  data packets as the route is secure
 5. }
 6. Else{
 7.       Do{
 8.          Send ARq and ID of IN to NHN
 9.          Receive ARp, NHN of Current NHN, RIT entry
10.          for Current NHN's Next Hop, RIT entry for
11.          Current IN.
12.          If ( NHN is a reliable node){
13.               Check IN for Black Hole node using RIT entry
14               If ( IN is not a Black Hole){
15.                  Route data packets as the route is secure
16.                  Broadcast a B_REPLY message in the network
17.               }
18.               Else{
19.                  Unreliable Route
20.                  IN is a Black Hole node
21.                  All the nodes on the reverse path from
22.                  IN to the node that generated RREP are
23.                  Black Hole nodes.
24.               }
25.          }
26.          Else
27.               IN=NHN
28.       }While (IN is not a trustful node)
29. }
```

Fig 4.2 Algorithm to check reliability of node

```
1. If (B_REPLY is from trustful node){
2.    Set third bit to 'true'in the RIT entry
3.    for the node ID which is in B_REPLY
4.    message
5. }
6. Else{
7.     Discard the message
8. }
```

Fig 4.3 Algorithm to check B_REPLY message for the third bit entry

Case No.2 When there are Cooperative Black Hole Nodes in the network and the route reply is from one of the black hole node.

NODE ID	FROM NODE	THROUGH NODE	THROUGH ANY TRUSTFUL NODE
1	1	1	1
2	1	1	1
3	0	0	1
4	1	0	1
5	0	0	0
6	0	0	0

Table 4.1 RIT entry for node S

Consider the case in the figure 4.4 with two Black Hole nodes in the network cooperating with each other. Here, node S request for a route to the destination D by broadcasting a RREQ packet.

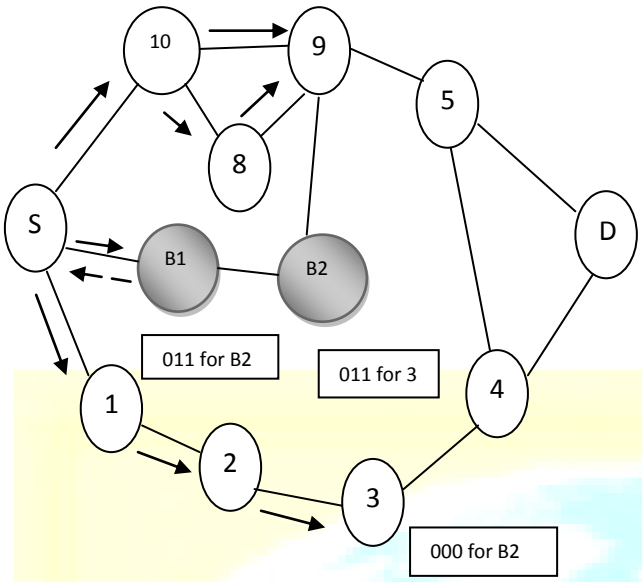

Fig 4.4 Cooperative Black Hole Attack Detection

The node B1 immediately replies spuriously with RREP packet showing that it is having the shortest as well as fresh enough route to the destination. The SN according to the algorithm first checks whether the RREP is from the destination node or from the trustful node i.e. it checks the RIT entry for that node but it finds the node B1 unreliable and then it checks it for reliability. It asks B1 for its next hop and also the RIT entry for the next hop. It provides its next hop B2 and it lies with the RIT entry with value 0 1 1. Since no node in the network has sent data through B1 before, B1 is not a trustful node to S. Therefore S sends additional request (ARq) to B2 via alternative path S-10-9-B2 and ask B2 about three things:

1. Whether B2 had routed any data from B1.

2. Who is B2's next hop to the destination?

3. Whether B2 had routed data packets through B2's next hop.

Since B2 is maliciously collaborating with B1 it replies positively to all the three queries and gives node 3 with its next hop. Since node 3 has neither a route to node B2 nor it has received data packets from B2 the RIT entry value with respect to B2 as in routing information table of

node 3 is 0 0 0. Based on this information node S infers that B2 is a black hole and source node S also infers that node B1 is maliciously cooperating with node B2. Hence both nodes B1 and B2 are marked as Black Hole nodes and this information is propagated throughout the network.

Case No. 3 when a node broadcasts a B-REPLY message

Consider the case in the fig4.5; here node 3 starts a route discovery process by broadcasting a route request (RREQ) packet for node 7. Node 6 replies with a route reply (RREP) packet, now node 3 checks its routing information table (RIT) to see whether node 6 is reliable or not. It found node 6 unreliable and then checks it for reliability. Suppose node 6 found to be reliable at the end then node 3 will broadcast this message as B_REPLY message in the whole network with the id of node 6 to show that this node is trustful.

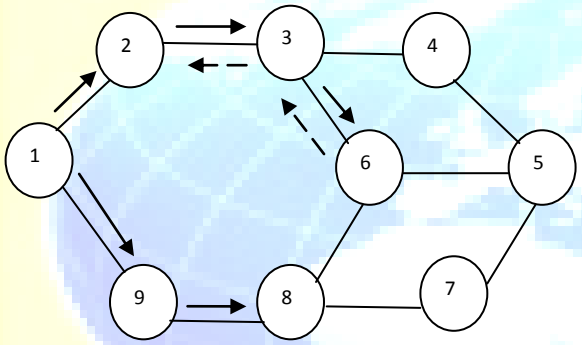

Fig 4.5 Node 3 broadcasting a B_REPLY message with id of node 6

This broadcast message is known as B_REPLY message. Now consider the case when this B_REPLY message reaches node 1 then node 1 first checks that which node had broadcasted it whether it is trustful or not through its RIT table after checking the table (Table 4.2) node 2 found to be reliable and then it will set the third bit entry for node 6 to be true. Now consider the case in fig 4.6 when node 1 starts a route discovery process by broadcasting a route request packet for node 5 and node 6 replies with a route reply packet. As the third bit entry for node 6 is true in the routing information table for node 1 there is no need for reliability check i.e. node 6 is a trustful node.

Fig 4.6 node 1 broadcasting RREQ packet for node 5 and node 6 replying with RREP packet.

NODE ID	FROM NODE	THROUGH NODE	THROUGH ANY TRUSTFUL NODE
2	1	1	1
3	1		0
8	0	0	0
6	0	0	
.	.	.	.
.	.	.	.

Table 4.2 Routing information table for node setting the 3rd bit entry true for node 6 by checking the reliability of node 3

5. Conclusion and Future Work

5.1 Conclusion

Mobile Ad hoc networks have the ability to set up network without any infrastructure. They need wireless links to communicate. So from the previous discussion it can be concluded that security is the main concern for providing secure communication between the nodes participating in MANET. One of the security threats can be caused by a malicious node which is part of MANET. The communication should be secure from such malicious nodes so that the cooperation of the network should not be compromised. Malicious nodes in the routing degrade the performance and effect the data routing of the packets. One of the malicious nodes can be a Black Hole node. Black hole node can absorb the packets passing through itself in such way that sending node will assume that packets have reached the destination.

In this paper, an Algorithm to detect cooperative Black Hole Attack has been proposed and examination has been done by considering three different cases. In the first case there were no malicious node present in the network and the reply for route request was from the reliable node so based on this previous information of reliability of node the route is confirmed to be secured. In the second case there were two black hole nodes in the network mutually cooperating with each other as there was no previous information for these two nodes so they are checked for reliability and found malicious at the end and this information of malicious behavior was propagated throughout the network. In the third case a node is found to be reliable and this information is broadcasted throughout the network and 3rd bit w.r.t that node is set to true which shows that the node in question is trustful node.

Finally it has been concluded that this algorithm works well in all the three cases with the aim of detecting Cooperating Black Hole Attack and ensuring a secure as well as reliable route from source to destination.

5.2 Future Scope

The proposed algorithm is efficient in detection of cooperative black hole attacks in the network but improvement can be done mainly in two directions as follows:

End-to-End Delay: Due to processing involved in the proposed algorithm, end to end delay got increased. Further improvement can be done to decrease the end to end delay along with the successful removal of Black Hole nodes.

Routing Overhead: In the proposed algorithm, control packets like alarm packets, 3 bit information storage as well as broadcasting of B_REPLY message results in increase of routing overhead. Improvement can be done to reduce the transfer of packets involved and hence to decrease the routing overhead involved.

REFERENCES

[1] Y.F.Alem and Z.C.Xuan, "Preventing black hole attacks in mobile ad-hoc networks using Anomaly detection", Second International Conference on Future Computer and Communication, Vol.3, (21-24 may 2010)

[2] J.Sen ,S.Koilakonda and A.Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks", second international conference on intelligent system, modeling and simulation ,innovation lab, Tata consultancy services ltd. , Kolkata, 25-27 jan 2011.

[3] S.Marti, T.J.Giuli, K.lai and M.bakery " Mitigating routing misbehaviour in mobile ad hoc networks", 6th MobiCom, Boston, Massachusetts, August 2000.

[4] N.Mistry,D.C.Jinwala and M.Zaveri, "Improving AODV protocol against black hole attacks", international multiconference of engineers and computer scientists 2010, vol 2, IMECS 2010, march 17-19 2010, Hong Kong.

[5] A.patcha andA.Mishra " Collaborative security architecture for black hole attack prevention in mobile ad hoc networks", Radio and Wireless conference, 2003.RAWCON'03, 13-13 aug 2003.

[6] B.Sun, Y.Guan, J.Chen, U.W.Pooch "Detecting black hole attacks in mobile ad hoc networks", Proc.5th European personal mobile communications conference, Apr 2003 , pp.490-495.

[7] R.Ranjan, N.Trivedi, A.Srivastava "Mitigating of black hole attacks in manets", VSRD International Journal of Computer science & Information Technology, Vol 1(2),2011,pp. 53-57.

[8]Poongothai T. and Jayarajan K., "A non cooperative game approach for intrusion detection in Mobile Adhoc networks", Internatonal conference of computing, communication and networking (ICCC), 18-20 Dec 2008, St. Thomas, VI, pp 1-4.

[9] DjamelDjenouri and LyesKhelladi, "A survey of security issues in mobile ad hoc and sensor network", IEEE communications Surveys and Tutorials journal,Volume 7, Number 4, 2005, pp 2-29.

[10] Michele Nogueria Lima, AldriLuiz dos Santos and Guy pujolle, "A Survey of Survivability in Mobile Ad Hoc Networks", IEEE Communications Surveys and Tutorials COMSUR), Volume 11, Number 1, 2009, pp 1-3.

[11] NishuGarg and R.P Mahapatra, "MANET Security Issues", International journal of Computer Science and Network Security (IJCSNS), Volume 9, Number 8, 2009, pp. 241-246.

[12] Wenjia Li and Anupamjoshi, "Security Issues in Mobile Ad hoc Networks – A Survey". Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore Country, 2006.

[13] Bing Wu, Jianmin Chen, Jie Wu and MihaelaCardei, " A Survey on Attacks and countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network security, ch-12,2006.

[14] Hao yang, Haiyunlyo, Fan Ye,Songwu Lu and Lixia Zhang, "Security in Mobile Ad-hoc Networks: Challenges and Solutions", IEEE Wireless communications, Volume 11,Number 1, 2004, pp 38-47.

[15] KamanshisBiswas and Md. Liakat Ali, "Security Threats in Mobile Ad Hoc Network", Master Thesis Computer Science, Thesis no: MCS-2007:07, 22nd March, 2007.

[16] Rashid HafeezKhokhar, MdAsriNagdi and Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, Volume 2, Number 3, 2008, pp 18-29.

[17] Sheenu Sharma and Roopam Gupta, " Simulation Study of Black Hole Attack in the Mobile Ad Hoc Networs", Journal of Engineering Science and Technology, Volume 4, Number 2, 2009, pp-243-250

[18] Hao Yang, HaiyunLuo, Fan Ye, Songwu Lu and Lixia Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications Journal, Volume 11, Number 1, 2004, pp 38-47.

[19] Payal N. Raj and PrashantB.Swadas, "DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[20] S. Ramaswamy, H.Fu, M.Sreekantaradhya, J. Dixon, and K.Nygard, "Prevention of Cooperative black hole attack in wireless ad hoc networks," International conference (ICWN'03), Las Vegas, Nevada, USA,2003, pp 570-575.

[21] Mohammad Al-shurman, Seong-Moo Yoon and Seungjin park, "Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, Proceedings of the 42nd annual southeast regional conference , 2004, pp 96-97.

[22] Chang Wu Yu, Tung-Kuang, Wu, ReiHeng, Cheng and Shun Chao Chang, "A distributed and Cooperative Black Hole Node Detection and Elimination mechanism for Ad Hoc Networks", PAKDD 2007 International Workshop, May 2007, Nanjing, China, pp 538-549

[23] 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.

[24] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.

[25] LathaTamilselvan and V Sankarnarayana, " Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp 13-20.

[26] HesiriWeerasinghe "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, Volume 2, 2007, pp 362-367.

[27] Mehdi Medadian, M.H. Yektaie and A.M.Rahmani, " Combat with Black Hole Attack in AODV routing protocol in MANET", First Asian Himalayas International Conference on Internet (AH-IC12009), 3-5th Nov, 2009.

[28] Bo sung Yong, Guan Jianchen 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.

[29] ElmarGerhards- Padilla, Nils Aschenbruck, Peter Martini Marko Jahnke and Jens Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", 32nd IEEE Conference on Local Computer Networks, 15-18th Oct 2007, Dublin, pp 1043-1050.

[30] GaoXiaopeng and Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", IFIP International Conference on Network and Parallel Computing – Workshops, 18-21 Sep 2007, Dalian, China, pp 449-460, 2009.

[31] Ming Yu, Mengchu Zhou and Wei Su, " A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Volume 58, Number 1, pp 449-460, 2009

[32] K. Lakshmi et al. "Modified AODV Protocol AgainstBlackhole Attacks in MANET" International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449.

[33] Mohammad Al-Shurman and Seong-Moo Yoo" Blackhole Attack in mobile ad-hoc networks" Electrical and Computer Engineering Department The University of Alabama in Huntsville, Alabama 35899.