Detecting Malicious Nodes in MANET based on a Cooperative Approach

Reena Sahoo
Dept. Of Information Technology
Sambalpur University
Sambalpur, Odisha, India

Dr. P. M. Khilar
Dept. of CSE
NIT, Rourkela, Odisha, India

ABSTRACT
Mobile Ad hoc Network (MANET) is a self configuring network of mobile nodes connected by wireless links and considered as network without infrastructure. Securing MANETs is an important part of deploying and utilizing them, since they are often used in critical applications where data and communications integrity is important. Existing solutions for wireless networks can be used to obtain a certain level of such security. These solutions may not always be sufficient, as ad-hoc networks have their own vulnerabilities that cannot be addressed by these solutions. In the network, some malicious nodes pretend to be intermediate nodes of a route to some given destinations, drop any packet that subsequently goes through it, is one of the major types of attack. We propose a cooperative method to detect malicious nodes in MANETs. The mechanism is cooperative because nodes in the protocol work cooperatively together so that they can analyze, detect malicious nodes in a reliable manner. We verify our method by running simulations with mobile nodes using Ad-hoc on-demand Distance Vector (AODV) routing. It is observed that the malicious node detection rate is very good; the overhead detection rate is low, packet delivery ratio is little bit high and also the response time is observed when there is a change of mobility speed.

General Terms
Malicious, MANET, Cooperative Approach

Keywords
MANET, Malicious, Overhead, Packet delivery ratio, Black hole, AODV

1. INTRODUCTION

An Ad-hoc network is an autonomous, self configuring network made up of mobile nodes connected via wireless links [5]. The mobile nodes are free to move at any rate/direction. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. They are characterized by a dynamic topology and the lack of any fixed infrastructure [1][5][11]. The communication medium is broadcast. The nodes are wireless mobile hosts with limited power, range and bandwidth [1][11].

The decentralized nature, scalable setup and dynamically changing topology makes ad hoc networks ideal for a variety of applications ranging from front-line zones(military, industrial and natural) to data collection(machinery analysis, biosensing) [3] [10] [11]. But due to the inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks [1] [5]. A node is malicious if it is an attacker that can't authenticate itself as a legitimate node due to the lack of valid cryptographic information [1]. Our work specifically deals with a special type of attack known as black hole attack which causes data packet dropping by malicious nodes. Due to the presence of malicious nodes in the MANET, source and destination nodes became unable to communicate with each other. A number of protocols were proposed to solve the black hole problem.

In scheme [3], each node transmits data to a next node, stores a copy of the data in its buffer and overhears whether the next node transmits the data. If the node overhears data transmission of the next node within a predetermined length of time, the node considers that the data was properly transmitted and deletes the copy of the data from the buffer. If not so, the node increases a failure tally for the next node. If the failure tally is greater than a threshold, the node determines that the next node intentionally dropped the data and reports this fact to all nodes over the network. Each of the nodes receiving the report determines whether a reporter and a suspect node listed in the report are recorded in its report table. When the number of times that a node reports to the source node S is greater than k equivalent to the number of malicious nodes over the network, the node is determined as a malicious node and excluded from the network.

The dynamic method [4] is proposed a distributed and cooperative procedure to detect black hole node. Each node after finding the local anomalies, the sender node calls for a cooperative detective by sending a message to the neighbor of the infected node. In local data collection, each node collects information through overhearing packets to evaluate if there is any suspicious node in its neighborhood. If finding one, the detecting node would initiate the local detection procedure to analyze whether the suspicious one is a malicious black hole node. The cooperative detection procedure is initiated by the initial detection node, which proceeds by first broadcasting and notifying all the one-hop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one. As soon as a confirmed black hole node is identified, the notification message is sent to the whole network. If all the nodes vote for the infected node, then the node is declared as black hole node.
The TCLS protocol [5] is proposed a Trust based packet forwarding scheme in MANETs without using any centralized

infrastructure. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. Each intermediate node marks the packets by adding its hash value and forwards the packet towards the destination node. The destination node verifies the hash value and check the trust counter value. If the hash value is verified, the trust counter is incremented, otherwise it is decremented. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. This paper concentrates on to find those malicious nodes. In this paper a node is suspected as malicious first then it is confirmed as a black hole node by further detection. Hence it tries to secure the MANET by identifying and isolating the black hole nodes from the network.

Section 2 describes security issues in MANET. Section 3 proves the good performance of the proposed scheme through a simulation and section 4 provides the conclusion of this paper.

2. SECURITY ISSUES IN MANET

The threats on a MANET can be from the unauthorized nodes those are outside the network or from the nodes inside the network. Threats from the nodes outside of the network are likely to be more easily detected than the internal nodes of the network. The threats from the internal nodes are difficult to detect as they are from trusted sources. Threats on the MANET can be broadly divided into 2 categories such as (i) external threats and (ii) internal threats [14]. In the presence of an authentication protocol to protect the upper layers, external threats are detected at the physical and data link layers. The threats posed by internal nodes are very serious; as internal nodes have the necessary information to participate in distributed operations. Malicious nodes exploit the routing protocol to their own advantage, e.g. to enhance performance or save resources. The main attack by malicious nodes is the packet dropping where most routing protocols have no mechanism to detect whether data packets have been forwarded.

2.1 Types of Attacks

The attacks can be divided into 2 categories [1].
Active attacks are lunched intended to disrupt the service of a network. Such attacks produce threats to confidentiality, integrity and availability of data and services in MANET. Here the term active attack has been used to mean that if any of the node's intention in the network to disrupt any of the security goals intended, such types of attack can be termed as active attack. In contrast the passive attack is an attack which is performed by the nodes to benefice itself only. The node has no other intention to disrupt the service of the network [10].

Passive attacks are done by some of the malicious nodes selfishly to conserve power by not forwarding the packets to the destination. One type of such attacks is known as the black hole attack or the wormhole attack which causes data packet dropping. These nodes are very difficult to detect.

2.2 Black hole Attack

A node which is a black hole has two properties – it participates in the route discovery process and the second property is that, it sometimes does not forward the data packet towards the destination. These nodes create problems in data transmission if they come in the route to destination. The nodes in the MANET are resource constrained; resource may be bandwidth, energy etc. Most of the nodes in MANET rely on batteries as their source of power; so, some of the nodes behave maliciously to conserve their limited battery power [16]. So, when the data packets are forwarded to the destination these selfish nodes simply do not forward the data packets towards the destination [15][18]. So all the packets move up to that node and disappear. Hence, these nodes act as a black hole which causes data packet dropping.

2.3 Proposed Solution

To detect the malicious node we have proposed one method which uses a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV)[12] routing for analysis of the effect of the black hole attack when the destination sequence number is changed via simulation. The proposed algorithm first detects those nodes, which may be malicious. Then the neighbor of the malicious node initiates a cooperative detection mechanism to detect the actual black hole node. In AODV routing, messages contain only the source and the destination addresses. It uses destination sequence numbers to specify the valid route. At first the sender broadcast the Route Request (RREQ) message to its neighbors. Each node that receives the broadcast, checks the destination to see if it is the intended recipient. If yes it sends a Route Reply (RREP) message back to the originator. RREP message contains the current sequence number of the destination node. The same process continues till the packets reach to destination or reach to an intermediate node, which has a fresh, enough routes to destination. Every node keeps track of its neighbor by maintaining two small size tables. One is sequence table (SnT) to keep the neighbor node's id and neighbor node's sequence number and other is the status table (ST) to keep track of the node's status whether it is a safe node or a malicious one. Every node also maintains a neighbor list (N_List) and this list is updated periodically. When an intermediate node receives a RREP checks if the difference between the Dst_Seq present in the RREP message and the sequence no present in its table is greater than some predefined threshold value? if so then the intermediate node stops forwarding the message and mark the node as 'M' or malicious in the status table(ST) and send a notification message(NM) to source node along with the malicious node's id and neighbor list of the malicious node. The threshold value is the average difference of Dst_Seq in each time slot between the sequence number of RREP message and the one held in the table.

The source node has an additional table called Flag Table (FT). M1HN's after receiving the Further Detection message, broadcast a RREQ message by setting destination address to source node's address. If it receives a RREP message from the malicious node, it sends a Test packet (TP) to the source node via malicious node, and at the same time it sends a Acknowledgment Packet (AP) to source node(SN) though some other route. Then the source node waits for '*wt*' time until it receives the entire test and acknowledgement packet. If, SN receives a TP, it updates the Flag Table (FT) by adding the source node id to the table and set the flag of the node as 'Y' and if an AP is received set the flag as 'N' and update the count field. If all the entries for the malicious node are 'N' then source

node updates the status table (ST) by adding the MN's id to the ST and making the status as 'B' i.e. Black hole.

Algorithm

1. SN broadcast RREQ along with the Dst_Seq
2. For each IN receives the RREQ check
If DN=IN and Dst_Seq in RREQ <= Dst_Seq in SnT?
Send RREP with the Dst_Seq in SnT and N_List.
Else
Broadcast the updated RREQ message.
3. For each node IN receives RREP Check
If (Dst_Seq in RREP -Dst_Seq in SnT) >Thr
Add the Node's id to the ST and make the status as 'M', stops forwarding RREP and send a notification message (NM) to SN contains node's id and N_List
Else
add the Node's id to the ST and make the status as 'S' and forward RREP.
4. After receiving the NM, SN broadcast a Further Detection message to all M1HNs
5. For each M1HN receive further detection message
Broadcast RREQ (with DN being set to SN)
If MN sends a RREP to M1HN
M1HN send a Test packet to SN via this route
Else
M1HN send an acknowledgement packet (AP) to SN by using some other path.
6. SN waits for 'wt' time
If a Test Packet is received
Add the source node id to FT and set flag as 'Y'.
Else
If an acknowledgement packet is received then add the source node id to FT and Set flag as 'N'.
7. If all the flags are 'N',
SN updates its status table (ST) by adding MN's id and setting Status as 'B'.
Else
Set the status as 'S'.
8. End

2.4 Illustration

As in Fig 1, source is node 1 and the destination is node 10.

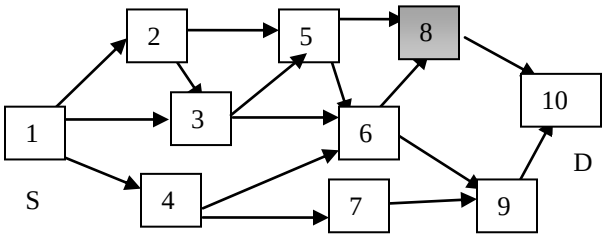

Fig 1: A MANET of 10 nodes

If we consider node 6, first it will find out the nodes which are within its radio range and store in its N-List. According to Fig.1 neighbor list of node 6 are 3, 4, 5, 8 and9.Then node 6 sends the RREQ to all its neighbor nodes shown in Table 1.

Table 1. Neighbor List (N_List)

Node ID	Neighbors
6	3,4,5,8,9

Each neighbor node that receives the broadcast checks the destination to see if it is the intended recipient. If yes it sends a RREP message back to the node 6. RREP message contains the current sequence number of the destination node. At the same time node 3, 4, 5, 8, 9 maintain the sequence number in the SnT and sequence numbers are generated randomly in simulation shown in Table 2.

Table 2. Sequence Table(SnT)

Node ID	Dst_Seq
3	10
4	7
5	8
8	6
9	5

When an intermediate node receives a RREP checks if the difference between the Dst_Seq present in the RREP message and the sequence no present in its table is greater than some predefined threshold value? if so then the intermediate node stops forwarding the message and mark the node as 'M' or malicious in the status table(ST) and send a notification message(NM) to source node along with the malicious node's id and neighbor list of the malicious node. Node 6 keeps track of the status of each neighbor node in the ST whether it is a safe node or a malicious one. Suppose we consider node 8 as malicious. The ST is shown in Table 3.

Table 3. Status Table (ST)

Node ID	Status
3	S
4	S
5	S
8	M
9	S

The neighbor nodes of node 8 are 5, 6, 10.Then these nodes after receiving the Further Detection message, broadcast a RREQ message by setting destination address to source node's address.

If it receives a RREP message from the malicious node, it sends a Test packet (TP) to the source node via malicious node, and at the same time it sends a Acknowledgment Packet (AP) to source node(SN) though some other route. Then the source node waits for '*wt*' time until it receives the entire test and acknowledgement packet. If, SN receives a TP, it updates the Flag Table (FT) by adding the source node id to the table and set the flag of the node as 'Y' and if an AP is received set the flag as 'N' and update the count field. Table 4 shows the Flag Table maintained by node 1 is as follows:

Table 4. Flag Table (FT)

Node ID	Flag
5	N
6	N
10	N

If all the entries for the malicious node are 'N' then source node updates the status table (ST) by adding the MN's id to the ST and making the status as 'B' i.e. Black hole. After confirmation of the Black hole node the ST of source node 1 is given in Table 5.

Table 5. Status Table (ST) for node 1

Node ID	Status
8	B

3.RESULTS AND DISCUSSION

We conducted our experiments using NS-2 version 2.34, a scalable simulation environment for network systems. The routing protocol we use is AODV. Our simulated network consists of 100 mobile nodes placed randomly within a 1000 m x 1000 m area. All nodes have the same transmission range of 250 meters. The channel capacity is 2 Mbps. The random waypoint model was used in the simulation runs. In this model, a node selects a destination randomly within the roaming area and moves towards that destination at a predefined speed 10, 20, 30, 40 and 50m/s. Once the node arrives at the destination, it pauses at the current position for 10 seconds. The node then selects another destination randomly and moves towards it, pausing there for 10seconds, and so on. Each simulation executed for 70 seconds of simulation time. The traffic used is UDP/CBR traffic between random node pairs. The size of data payload is 512 bytes. Multiple runs with different seed numbers were conducted for each scenario and measurements were averaged over those runs.

In our experiment we have assumed 5 percent of the number of nodes as malicious i.e. 3 nodes are malicious for 50 nodes, 5 nodes are malicious for 100 nodes and 7 nodes are malicious for 150 nodes. We study the detecting technique of the packet delivery ratio, overhead and response time for 50 node network, 100 node network and 150 node network. We run the simulation 5 times and all the data are plotted using MATLAB, averaged from the 5 runs.

The Fig 2 shows the packet delivery ratio for the network having 50 nodes, network having 100 nodes, network having 150 nodes respectively.

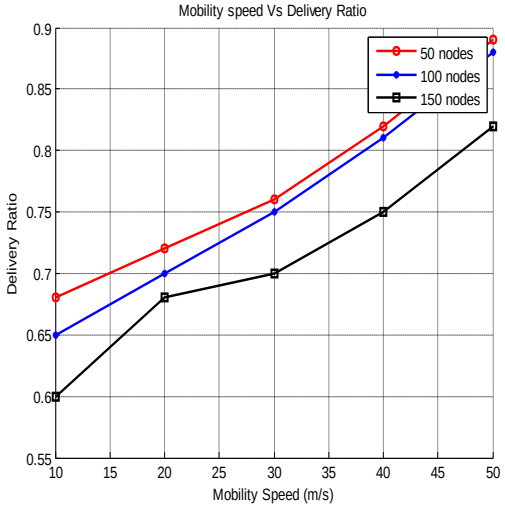

Fig 2: Comparison of Packet delivery ratio

The packet delivery ratio is shown as a function of mobility speed. As the number of nodes increases and malicious node increases, the packet delivery ratio decreases with the varying of mobility speed.

The Fig 3 shows the overhead for the network having 50 nodes, network having 100 nodes, network having 150 nodes respectively.

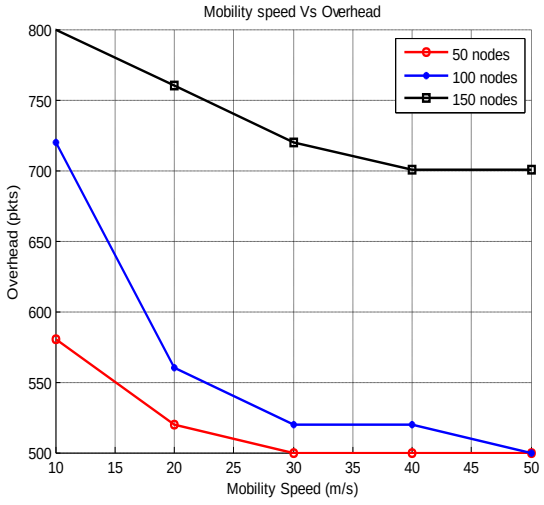

Fig 3: Comparison of Overhead

The overhead is shown as a function of mobility speed. As the number of nodes increases and malicious node increases, the overhead increases with the varying of mobility speed.

The Fig 4 shows the response time for the network having 50 nodes, network having 100 nodes, network having 150 nodes respectively.

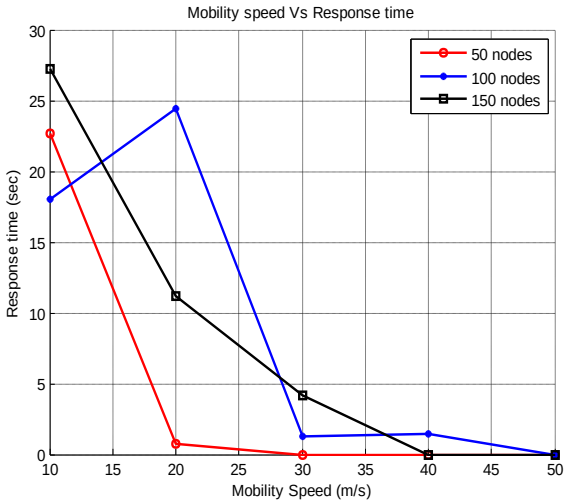

Fig 4: Comparison of Response time

The response time is shown as a function of mobility speed. In our experiment we have taken the random way point model which changes the position of the node arbitrarily. So the response time changes arbitrarily when the number of nodes increases and malicious node increases.

Fig 5 shows the packet delivery ratio in two different scenarios i.e. for proposed model and the existing model TCLS.

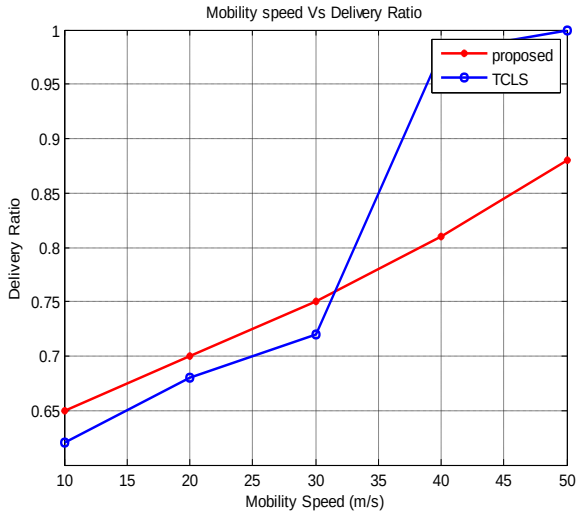

Fig 5: Comparison of Packet delivery ratio for proposed model and TCLS

As the mobility speed increases, the packet delivery ratio increases in both the cases. But from the graph it is cleared that the packet delivery ratio for the mobility speed 10, 20, 30 m/s of the proposed model is improved as compared to TCLS whereas for the mobility speed 40 and 50 m/s, it is decreasing as compared to the existing one.

Fig 6 shows the overhead in two different scenarios i.e. for proposed model and the existing model TCLS.

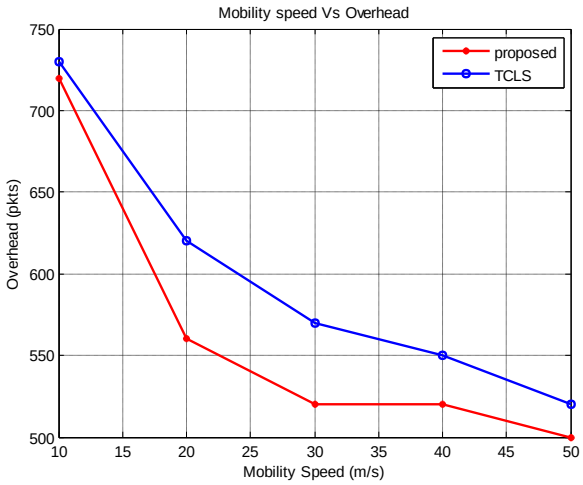

Fig 6: Comparison of Overhead for proposed model and TCLS

As the mobility speed increases, the overhead decreases in both the cases. From the graph it is cleared that the overhead of the proposed model is improved as compared to TCLS.

4.CONCLUSION

Black hole attack is one of the most important security problems in MANET. The black hole attack causes dropping of data packets by malicious nodes in the path source to destination. In this paper, we have analyzed the black hole attack and detected the malicious nodes. This paper is proposed to minimize the number of data packet dropping. Also it reduces false detection rate. This is a reliable algorithm since all mobile nodes cooperate together to analyze and detect possible multiple black hole nodes. The proposed scheme in this thesis work has been implemented to minimize the number of data packet dropping in the network and improves the efficiency of the network.

5. REFERENCES

[1] Suman Deswal and Sukhbir Singh," Implementation of Routing Security Aspects in AODV", International Journal of Computer Theory and Engineering. Vol. 2, No. 1, February, 2010.

[2] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang,"Security in Mobile Ad hoc Networks: Challenges and Solutions", UCLA Computer Science Department.

[3] Jongoh Choi, Si-Ho Cha, GunWoo Park, and JooSeok Song."Malicious Nodes Detection in AODV-Based Mobile Ad Hoc Networks" GESTS Int'l Trans. Computer Science and Engr., Vol.18, No.1 49, Oct.2005.

[4] Satoshi Kurosawa , Hidehisa Nakayama, Nei Kato, Abbas Jamalipur, Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad hoc Networks by Dynamic

Larning Method", International Journal of Network Security, Vol.5, No. 3,pp.338-346, Nov. 2007.

[5] A Rajaram, Dr.S.Palaniswami." Detecting Malicious Node in MANET Using Trust Based Cross-Layer Security Protocol" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2), 2010.

[6] Aishwarya Sagar Anand Ukey, Meenu Chawla," Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No. 1, July 2010.

[7] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard." Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".

[8] Ganesh Reddy, P.M. Khilar."Routing Misbehavior Detection and Reaction in MANETs", Proceedings of International Conference on Industrial and Information System, 2010, Surathkell.

[9] Sunil kumar Senapati, Pabitra Mohan Khilar, "Securing FSR against data dropping by malicious nodes", International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS), ISSN: 0974-3596, April'09-September'09.

[10] Fanzhi Li and Sabah Jassim." Malicious nodes seriously affect the performance of mobile ad hoc networks".

[11] Dr. Nakkeeran, B.Partibane, S.Sakthivel Murugan, N.Prabagarane." Detecting the malicious faults in MANET".

[12] Charles E Perkins, Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing".

[13] Frank Kargl, Andreas Klenk, Stefan Schlott, Michael Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks", University of UIm, Dep. Of Multimedia Computing, UIm, Germany.

[14] Po-Wah Yau; Mitchell, C.J., "Reputation methods for routing security for mobile ad hoc networks", Mobile Future and Symposium on Trends in Communications, 2003.

[15] Payal N Raj, Prashant B. Swadas, "DPRAODV: A Dynamic Larning System Against Blackhole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[16] Akanksha Saini, Harish Kumar," Comparision between Various Blackhole Detection Techniques in MANET", NCCI 2010 -National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 19-20 March 2010.

[17] Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil," Black Hole Attack Injection in Ad hoc Networks".

[18] N Bhalaji, Sinchan banerjee, A.Shanmugam, "A Novel Routing Technique against Packet Dropping Attack in Adhoc Networks", Journal of Computer Science 4 (7): 538-544, 2008.

[19] Ganesh Reddy, P.M. Khilar."Secure Routing in MANET", International Journal of Data Warehousing, Vol.2 No.1, Jun-2010, pp.53-62.

[20] S Rangrajan, et. al., "A Distributed System level Diagnosis Algorithm for Arbitrary Network Topologies, IEEE Trans. on comp. Vol 44, No. 2, February 1995,pp.312-334.