Volume 2, Issue 8, August 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET

Ira Nath
JIS College of Engg.Kalyani, Nadia,INDIA

Dr. Rituparna Chaki
West Bengal University of Technology Calcutta 700064, INDIA

Abstract-Black hole attack is one kind of routing disturbing attacks and can bring great damage to all clusters of a MANET. Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, and infrastructure-less property. As a result, an efficient algorithm to detect black hole attack is important. This paper proposes and evaluates strategies to detecting black hole attacks and build reliable and secure inter cluster routing in wireless ad hoc networks. We choose AODV protocol to test our algorithm and ns-3 as our simulation tool.

Keywords- Black hole attack, MAMET, Cluster, Ad-hoc, security, malignant node.

I. INTRODUCTION

MANET plays a critical role in places where a wired (central) backbone is neither available nor economical to build, such as law enforcement operations, battle field communications, and disaster recovery situations, and so on. Such situations demand a network where all the nodes including the base stations are potentially mobile. In MANET, the flat routing schemes do not scale well in terms of performance. With an increase in the size of the networks, its performance rapidly decreases. Another disadvantage of flat routing scheme is that the routing tables and topology information in the mobile stations also get tremendously large. It may result in low bandwidth utilization in large networks with high load and longer source routes. To solve this problem some kind of organization is required in large MANET. This is possible by grouping a number of nodes into easily manageable set known as cluster. Certain nodes, known as cluster heads, would be responsible for the formation of clusters and maintenance of the topology of the networks. Clustering algorithms in MANETS should be able to maintain its cluster structure as stable as possible while the topology changes [1]. All nodes and cluster heads are movable and the topology of the network is changing dynamically in a clustered Ad Hoc Networks, which brings great challenges to the security of all clusters in an entire Ad Hoc Network. As a result, attackers can take advantage of flaws in routing protocols to carry out various attacks [1] [2]. If it is possible to secure all clusters of a MANET, then entire network must be secured. Black hole attack and gray-hole attacks [3] are two classical attacks under Ad Hoc networks, which could disturb routing protocol and bring about huge damage to the clusters as well as whole network's topology. This kind of attacks result in many detecting methods fail and causes more immense harm to all clusters in a MANET. It is impossible to secure all clusters in an entire MANET by using wired network security mechanism as it has wireless links, no fixed infrastructure and dynamic topology. A cluster head may act as a black hole. In this paper we propose a new approach for black hole detection and secure routing among different clusters of same MANET. It detects existence of malicious cluster heads as well as cluster members, finds out their exact position at any time instant t, selects route and also secures inter cluster routing. Finally, the detected malicious node is listed in the black hole list and notices all other nodes in the network to stop any communication with them. As a result our proposal can reduce packets loss that cause by the malicious nodes and have better packet delivery ratio within less time period. The rest of the paper is organized as follows. In section II, we introduce about Black Hole attack among different clusters in MANET. The review work is depicted in Section III. Next, in section IV we develop our proposed method. Analysis the simulation result is in section V. Finally, the conclusion is depicted in section VI.

II. BLACK HOLE ATTACK

In inter cluster routing, a malignant cluster head can attract all packets by falsely claiming a fresh route to the destination and then assimilate them without forwarding them to the destination. In the following illustrated Fig.1, imagine a malignant cluster head 'M'. When 'CH1' cluster head broadcasts a RREQ packet, cluster heads 'CH2', 'CH3' and 'CH4' (within the transmission range of 'CH1') receive it. Cluster head 'CH4', being malignant node, does not check up with its routing table for the requested route to the destination cluster head 'CH2'. So, it immediately sends back a RREP packet, claiming a route to the destination. Cluster head 'CH1' receives the RREP

from 'CH4' (M) in advance of the RREP from 'CH2' and 'CH3'. Source cluster head 'CH1' assumes that 'CH4' (M) is the nearest cluster head in its transmission range and sends the actual packet to 'CH4'. When 'CH4' (M) gets the packet from 'CH1', it assimilates the packet and thus behaves like a Black hole.

TABLE I
SYMBOLIC NOTATIONS USED IN FIG.1.

Cluster head	
Cluster member	
Gateway	

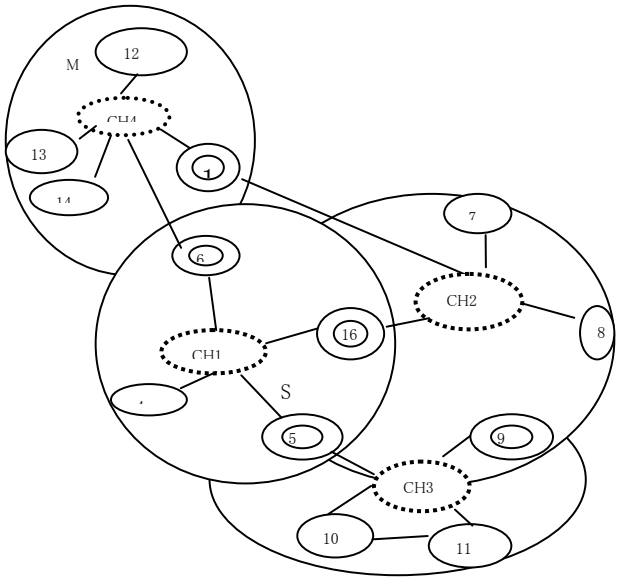

Fig.1. Black hole Attack in clustered MANET

III. REVIEW WORK

Black hole attack is one of the active DoS attacks possible in MANETs so has got lots of attention by the researchers. Research focus mainly given to securing existing routing protocols, developing new secure routing protocols, and intrusion detection techniques. There indeed have been numerous attempts published in the literature that aim at countering the Black attacks. We survey them in the following. In [3], the authors discuss a protocol to solve black holes and wormholes and present a watchdog mechanism and time of flight to detect respectively. This improves the data security in mobile ad-hoc network. Two different algorithms are used to solve black holes and worm holes in MANET. It is very difficult to choose algorithm according to the nature of attack. SAODV, a secured routing protocol based on AODV has been proposed in paper [4]. The SAODV algorithm claims to be able to avoid black hole attack. To reduce the attack this algorithm proposes to wait and check the replies from the entire neighbouring node. The source node will store the 'sequence number' and the time at which the packet arrive in a 'Collect Route Reply Table (CRRT)'. If more than one path exists in CRRT, then it randomly chooses a path from CRRT. This reduces the chances of black hole attack. Here, for each node maintaining a CRRT is an overhead. That may reduce the performance level of the network. In Reference [5], an approach called PCBHA has been proposed for preventing black hole attack when more than one node behaves maliciously. They have used a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'black hole' and it is eliminated. The source node transmits the RREQ to all its neighbours. Then the source waits for 'TIMER' seconds to collect the replies, RREP. A reply is chosen based on the following criteria, in each of the received RREP, the fidelity level of the responding node, and each of its next hop's level are checked. If two or more routes seem to have the same fidelity level, then select the one with the least hop count; else, select the one with the highest level. The fidelity levels of the participating nodes are updated based on their faithful participation in the network. On receiving the data packets, the destination node will send an acknowledgement to the source, whereby the intermediate node's level will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented. Here for each node maintaining the 'Fidelity Table' is an overhead. That may reduce the performance level

of the network. In [6], the authors discuss a protocol that requires the intermediate nodes to send RREP message along with the next hop information. When the source node gets this information, it sends a RREQ to the next hop to verify that the target node (i.e. the node that just sent back the RREP packet) indeed has a route to the intermediate node and to the destination. When the next hop receives a Further Request, it sends a Further Reply which includes the check result to the source node. Based on information in Further Reply, the source node judges the validity of the route. In this protocol, the RREP control packet is modified to contain the information about next hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP. Obviously, this increases the routing overhead and end-to- end delay. In addition, the intermediate node needs to send RREP message twice for a single route request. In [7], the authors describe a protocol in which the source node verifies the authenticity of a node that initiates RREP by finding more than one route to the destination. When source node receives RREPs, if routes to destination shared hops, source node can recognize a safe route to destination. Sanjay Ramaswamy, et al [8] proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets. In BHIDS [10], two-layered cluster formation algorithm is used. In this algorithm it is assumed that a cluster head should not be a malicious node. It is really a typical matter. Another assumption is the node with minimum node ID in a cluster becomes the cluster head for that cluster. In this process a worst quality node (low mobility, low transmission range, less battery power etc.) with minimum ID can become a cluster head. As a result, performance of the MANET must be decreased. If a stranger node with low ID demands itself as destination node. According to BHIDS cluster formation algorithm it may become a cluster head and if it is a malignant node, it can collapse the whole network. In BHIDS procedure the source node broadcasts RREQ. More than one node can send RREP along with source ID and dst_seq number. The source node selects the node with maximum dst_seq number as destination node. It also updates its own routing table according to the information of the node with max. dst_seq number and send the packet through that route. The destination node (or intermediate node) captures the packet. After capturing the packet False Packet Rate calculation is occurred. If the destination node itself (or any node in its route) is a malignant node, then the procedure BHIDS cannot work properly. In [12] all the RREQ Destination Sequence Number (DSN) and its Node Id are stored in RR-Table until the computed time exceeds. In MAPBAM it is assumed that the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then the first destination sequence number is compared with the source node sequence number, if there exists much more differences between them, certainly that node is the malignant node. Here this node is immediately removed from the RR-Table. It may happen that an actual destination node having greater destination sequence number replies first. Then this process of malignant node selection is totally failure. For malignant node selection no threshold value is considered here.

IV. PROPOSED METHOD

A. Identification of relationships between cluster head neighbours in ad hoc network

In an ad hoc network, the relationship of a cluster head node i to its neighbour node j can be any one of the following types

i) cluster head node i is a *stranger* to neighbour cluster head node j:

Cluster head node i has never sent/received messages/few messages to/from node j. Their trust levels between each other will be very low. Any new node entering an ad hoc network will be stranger to its entire neighbour. There are high changes of malicious behaviour from stranger nodes.

ii) Cluster head node i is a *friend* to neighbour node j:

Cluster head node i has sent/received plenty of messages to/from node j. Their trust levels between each other will be very high. There are less changes of malicious behaviour from friend nodes.

The above relationships are represented as a Friendship table1 for each cluster head node in an ad hoc network. A trust estimator is used in each cluster head to evaluate the trust level of its neighbouring nodes in every t_{stamp} time interval. The Friendship Table is updated according to the t^{th} time result of the trust estimator. The trust level is a function of two parameters like ratio of the number of packets forwarded successfully by the neighbour to the total number of packets sent to that neighbour and ratio of the number of packets received successfully from the neighbour to the total number of packets sent from that cluster head node.

TABLE II
FRIENDSHIP TABLE FOR CLUSTER HEAD 1(CH1)

Neighbours	Relationship
CH2	F
CH3	F
CH4	ST
4	F

5	F
6	F
16	F

B. Routing Mechanism

The source cluster head(S) floods RREQ packets across the network to find out a route to the destination cluster head D (i.e. either itself or its own cluster member is the destination). In the above fig.1, S (CH1) wants to broadcast to D. So, it first dispatches the RREQ to its own cluster members as well as all the neighbour cluster heads (CH2, CH3 and CH4) within its transmission range through gateway nodes 16, 5 and 6 respectively. Here CH2, CH3 and CH4 receive this request. The malignant node has no intention to transmit the DATA packets to the destination D but it wants to collect the DATA from the source node S. So it immediately replies to the request. Instead of transmitting actual DATA packets immediately through CH4 (CH4-6-CH1), S has to wait for the reply from the other cluster heads. After some time it will receive the reply (RREP) from CH3 (CH3-5-CH1) and CH2 (CH2-16-CH1). S collects these RREP packets into a buffer. More than one cluster heads (here CH2 and CH4) demand themselves as the destination cluster heads (D) and some cluster heads (here CH3) demand themselves as intermediate cluster heads (D'). S selects the shortest path and next shortest path according to hop count and checks its own friendship table to examine the status of one-hop neighbour node in its shortest path. The Friendship Table of Cluster Head 1(CH1) is depicted in TableII. If its one-hop neighbour node is a friend, then Data packet is transmitted through that node. If its one-hop neighbour node is a stranger, then Data packet is transmitted through that node according to the k value calculated by node S (invoking the trust estimator). In this way, an optimal path is chosen based on the degree of friendship existing between the neighbour nodes and k_{trust} values as shown in Table III.

1) Find out the Exact Location of Black Hole:

To calculate k_{trust} value of a stranger the trust estimator is invoked here. S first sends false packets to the stranger. The malicious node must show its behaviour according to its character. It may act as a black hole. In such cases the packets are dumped and not retransmitted. It may carry out a fabrication attack (if a self generated fallacious packet is transmitted).When the malicious cluster head gets the false packet then it works according to its nature. If the stranger is not the black hole then it returns back the false packet after getting the request of return the packet to the sender. Otherwise the stranger acts like a dump and cannot returns back the false packet to the sender. The trust level of the stranger is calculated using the following formula.

$$k_{trust} = \frac{PKTF(ST)}{PKTR(ST)} + \frac{PKTR(ST,S)}{PKTR(S,ST)} \quad \text{.....(1)}$$

where,
PKTF(ST)- Number of packets forwarded by the stranger
PKTR(ST)- Number of packets received by the stranger
PKTR(ST,S)- Number of packets received from the stranger
PKTR(S,ST)-Number of packets received from the cluster head

This can be represented by a set S_k which is a set of all values of k_{trust} over a span of time (t_1 to t_n).

$S_k=\{k_{trust1}, k_{trust2}, \ldots\ldots, k_{trusti}, \ldots\ldots, k_{trustn}\}$
where, $k \leq k_{trusti} \leq 1$

k_{trusti}-ratio defined at the i^{th} time interval.

k-threshold value for trust level.

When $k_{trust}=1$, the stranger node can be upgraded to friend .

In this figure1, the malignant cluster head M (CH4) is enthusiastic to seize the data from the source cluster head S (CH1). So, exact location of the Black hole is identified (here CH4) using the above mentioned method. S now discards this identified cluster head from the buffer and broadcasts a message to all other neighbour cluster

head sets to discard this black hole cluster head from their list.

TABLE III
PATH CHOSEN CRITERIA

Next hop neighbour in the best path P_1	Next hop neighbour in the next best path P_2	Action Taken
F	F	F is chosen in P_1
F	ST	F is chosen in P_2
ST	F	ST or F based on k_{trust} value.
ST	ST	ST is chosen in P_1 after invoking the trust estimator.

2) Algorithm:

Begin
Step1: Source cluster head(S) broadcasts RREQ.
Step2: S receives RREP.
Step3: S selects the shortest and next shortest path according to hop count.
Step4: S checks Friendship table for one-hop neighbour nodes.
Step5: If neighbour node is a friend then
Route data packet.
Else
Send false packets to the stranger.
Invoke the trust estimator.
Calculate k_{trust} for stranger applying Formula(1).
Add status of stranger to the friendship table of S
End if
Step6: If $k \leq k_{trusti} \leq 1$ then
Route data packet.
Else
Broadcasts stranger as black hole.
End if
Step7: Update the friendship table of S after each time interval $t_{stamp.}$
Step8: Repeat step 4 to 7 until the destination node gets the data packet.
End

3) flowchart:

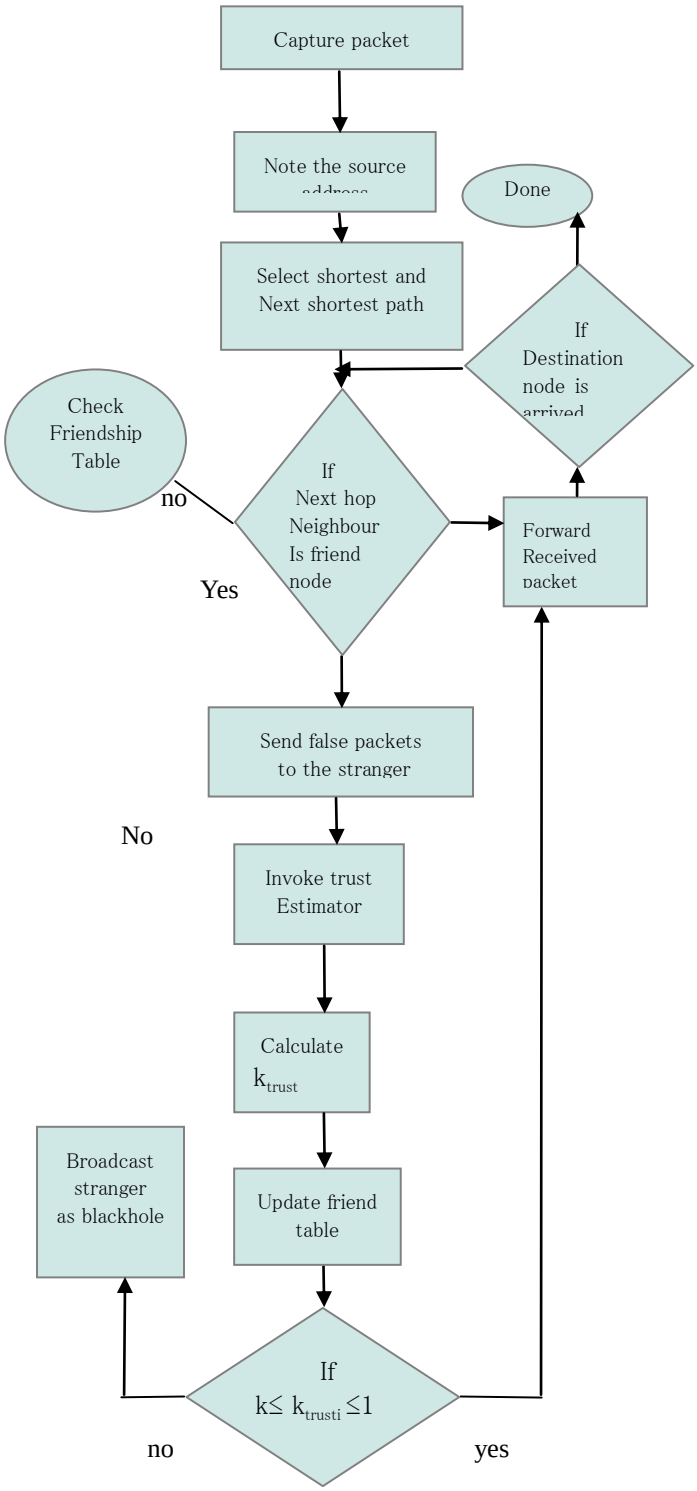

Fig.2 represents flowchart of our BHAPSC.

V. SIMULATION

A. simulation setup

In this section, we describe our simulation environment and report the simulation results.

The simulation is being implemented in the ns3 simulator [13] [14]. The simulation parameters are provided in Table IV. We set the traffic source to Continuous Bit Rate (CBR). The CBR traffic is generated with a rate of 4 packets per second. A clustered MANET network is constructed for simulation purpose and monitored for a number of parameters. The simulation models 30 mobile nodes, moving over a rectangular flat space. Simulation time is 1200 seconds. The random waypoint model is selected as a mobility model in a rectangular field (700m × 700m) with a node's speed uniformly between 0 and a maximum value of 90m/s. We add the function of our method to AODV to detect the black hole attacked nodes.

1) performance metrics:

We use the following metrics to evaluate our protocol:

Average Detection Time (ADT): ADT is the average time to detect that the network has black hole attacks. It is measured by the attack detection time minus the traffic start time.

Packet Delivery Ratio: The ratio between the number of packets originated by the application layer sources and the number of packets received by the sink at the final destination.

Routing Overhead: The overhead of routing control packets to detect the attacks.

We compare PCBHA with our BHAPSC.

TABLE IV
SIMULATION PARAMETERS

Parameter	Value
Application traffic	CBR
Transmission range	250m
Packet size	64 bytes
Transmission rate	4packets/s
Pause time	10s
Speed	0-90m/s
Simulation time	1200s
Number of nodes	30
Area	700m*700 m

B.results

1) Average Detection Time vs. Mobility changes: As we can see from the Fig.3 that ADT increases when mobility increases. For both the methods, MANET with low mobility values performs better in black hole detection time analysis. But in increased mobility the ADT changes rapidly for PCBHA. As a result, when mobility changes to 90m/s, the ADT of PCBHA and BHAPSC are 350sec and 99 sec respectively. We measure different ADT values from 0-90 m/s mobility with pause time 10s.

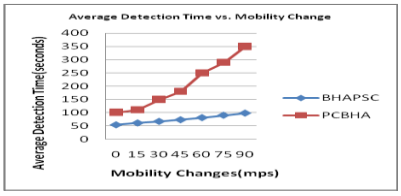

Fig3. Average Detection Time vs. Mobility changes

2) Comparison of Routing Overhead in increasing mobility: Figure 4 shows the comparison of Routing Overhead due to increasing mobility. In PCBHA each node maintains the 'Fidelity Table'. It is an overhead. That reduces the performance level of the network. However, in our method only each cluster head maintains 'Friendship Table'. This reduces the control packet overhead for our method. We use kByte unit to measure routing overhead of MANET. From the Figure4 it is clear that for increased mobility values the routing overhead can be severe for PCBHA. Here we allow 30 nodes for the MANET in any instant of time t_{stamp}.

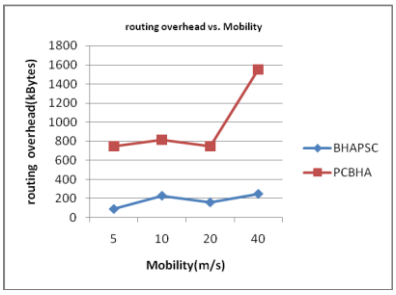

Fig4.Comparison of Routing Overhead in increasing mobility

3)Delivery Packet Ratio vs. Malignant nodes: When malignant node percentage in a MANET increases then it is obvious that packet delivery ratio will also be decreased. But in figure 5, at first for increasing malignant nodes the performances of both the methods decrease. But BHAPSC gives a constant packet delivery ratio after some increased percentage of malignant nodes. On the otherhand the packet delivery ratio rapidly decreases for higher malignant node percentage presence in MANET.

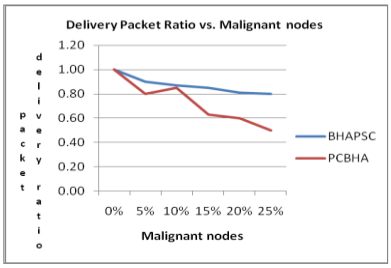

Fig.5. Comparison of packet delivery ratio between BHAPSC and PCBHA

VI.CONCLUSION

In this paper, we studied the problem of black hole attacks in inter cluster MANET routing. We proposed a feasible solution for it on the top of AODV protocol to avoid the black hole attack, and also prevent the network form further malicious behaviour. We simulated our proposed solution [4] using the NS-3 simulator and compared the performance with PCBHA in terms of throughput and packet delivery ratio. Simulation results show that (1) the PCBHA greatly suffers from black holes in terms of packet delivery ratio. (2) Our solution also presents good performance in terms of black hole node detection time requirements as well as routing overhead with increasing mobility in an already formed cluster.

ACKNOWLEDGMENT

I owe my sincere feelings of gratitude to Dr. Rituparna Chaki for her valuable guidance and suggestions which helped me a lot to write this paper.

REFERENCES

1. Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU,"An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",2010 24th IEEE International Conference on Advanced Information Networking and Applications.
2. Yibeltal Fantahun Alem Zhao Cheng Xuan,"Preventing Black Hole Attack in Mobile Ad-hoc Networks Using

Anomaly Detection",[Volume3], 2010 2nd International Conference on Future Computer and Communication,IEEE.

3. Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre,"Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012.
4. Zapata MG. Secure ad hoc on-demand distance vector(SAODV) routing. ACM SIGMOBILE Mobile Computing and Communications 2002; 6(3): 106—107.
5. Tamilselvan L, Sankaranarayanan V. Prevention of co-operative black hole attack in MANET. Journal of Networks 2008; 3(5):13—1320.
6. H. Deng, W. Li, and D. P. Agrawal. "Routing Security in Ado Networks." In: IEEE Communications Magazine, Vol. 40, No. 10,pp. 70-75, Oct. 2002.
7. M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks." In: Proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97, Apr. 2004.
8. 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.
9. Rituparna Chaki,Nabendu Chaki,"IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network", 6th International Conference on Computer Information Systems and Industrial Management Applications (CISIM'07), 2007, IEEE Computer Society.
10. Debdutta Barman Roy, Rituparna Chaki and Nabendu Chaki," BHIDS: a new, cluster based algorithm for black hole IDS", SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks. 2010; 3:278–288 Published online 21 September 2009 in Wiley InterScience (www.interscience.wiley.com) DOI: 10.1002/sec.144
11. Gaurav Sandhu, Moitreyee Dasgupta,"Impact of Blackhole Attack in MANET", International J. of Recent Trends in Engineering and Technology, Vol. 3, No. 2, May 2010.
12. K. Lakshmi, S.Manju Priya, A.Jeevarathinam, K.Rama, K. Thilagam,"Modified AODV Protocol against Blackhole Attacks in MANET" K. Lakshmi et al. / International Journal of Engineering and Technology Vol.2 (6), 2010, pp.444-449.ISSN : 0975-402.
13. K. Fall; K. Varadhan, NS notes and documentation, The VINT Project, UC Berkely, LBL, USC/ISI, and Xerox PARC, 1997.
14. ns-3 Tutorial, Release ns-3.11,ns-3 project, May 25, 2011.

