Efficient Approach to Detect Grayhole Nodes in MANET

[#1]Shirish Bhosale
Department of Computer Engineering
K. J. College of Engineering & Management Research
[1]shirish.a.bhosale@gmail.com

[#2]Prof Deepak Mehetre
Department of Computer Engineering
K. J. College of Engineering & Management Research
[2]dcmehetre@gmail.com

***Abstract*—Information Technology is one of the fast growing area. Users of Information Technology devices such as computer, handled devices are from students to Researchers. To fetch the information or to exchange the information from one another devices, this devices are interconnected to each other using some protocols. These devices may be connected with wired network or by wireless network. The medium of communication may be un secure and the transmitted data can be prone to malicious activity. Wireless networks are more prone to malicious activity than wired network. Ad hoc networks is special kind of interconnection of wireless network. They are created temporary as per requirement area or application. Devices itself acts as router in MANET. Any device can join or leave network at any instance hence, malicious devices can join the network any time without any detection. This malicious device can act as router; hence packets passing through malicious device can be captured. For routing packets in ad hoc networks various routing algorithms or protocols are implemented like AODV, DSR. It is possible and feasible to detect malicious activity at routing level i.e. at network layer. Ad hoc network are established where there is absence of interconnection backbone and mostly use in emergency needs. They are easily deployable and most users are migrating to mobile devices hence Most of the research is going in this field of area and one of them is security. There are various types of attacks such as eavesdropping, Wormhole attack, Misdirection, Flooding attack, Packet drop attack, black hole attack, gray hole attack. Among them most destructive is black hole attack whos intention is to degrade the overall performance of network. Gray hole is similar to black hole attack but it switches from black to normal and vice versa, Hence detection of gray hole attack is difficult.**

***Index Terms*—AODV, DOS, DSR, Intermediate Node, MANET, Malicious Node, Grayhole Node, Grayhole Attack, Network Simulator2, RREQ, RREP.**

I. INTRODUCTION

A. ADHOC Networks

Computer Network or internet is the interconnection between the computers or devices. Wired networks are the networks which have the network backbone or infrastructure using fixed wires (using optic fiber or cat5, cat 6 cables using RJ45) their distance among each node is fixed with respect to one another, nodes are not mobile hence static topology is maintained. While ad hoc networks are temporary in nature. They are established for specific time being, for specific use where the backbone for communication is absent. It is especially useful in any place where the deployment of base stations or access points is impossible or expensive such as disaster rescues, battlefields, dangerous environment, etc. MANET is the internet among the mobile computers or communication devices, mobile node can join or leave network anytime and the nodes at any instance may change their position with respect speed and mobility pause time, hence the network topology is dynamic and multi hop in nature. Each device/node acts as host as well as router, to route a packets from source to destination as per route request. Reliability, security and availability of ad hoc networks are less than wired networks because of the constraints like individual node's battery power, Range of communication, speed, pause time, adaptation in changing environment. Network can be,

- The devices in the network having different architecture, Operating System and characteristics. As mobiles with android OS and IOS, Mac-Book, Windows machine.
- Devices in the network having same hardware architecture, Operating System. As network of only android phones.

B. Challenges in Ad hoc Networks

- Due to mobility network topology is dynamic.
- Frequent network partitions and grouping of nodes.
- Every node can be mobile or static to some position for certain period of time.
- Limited power capacity(battery)
- Limited wireless bandwidth Presence of varying channel quality(some node configuration may be good some may not).
- Sensitive to malicious attacks.

C. Routing Challenges in Ad hoc Networks

- Routers are moving i.e. Intermediate node are mobile.
- Link changes as neighboring node are changing positions
- Packet losses due to transmission errors.
- Flooding of Control message increasing routing overhead.
- Routing loop may exist even using sequence numbers.

D. Issues in Ad hoc Networks

As nodes in ad hoc network are not static in terms of position and basically most of them are battery powered, this

creates the power issue. Characteristics of joining and leaving network creates a problem in routing, checking the link are broken or not is one of the overhead due to mobility. Flooding of control message creates the routing overhead.

1) Mobility: Mobility depends on speed, pause time. E.g. Ad hoc networks of racing cars, here speed of each node varies. If on the way a car fails, hence that node waits for maintenance for some pause time. Mobility patterns may be different Student sitting in canteen(speed of mobility is less, all are within range). Racing car network(speed is higher, quickly nodes go out of range). Military movements (variable speed ,variable range). Personal area network or WiFi ad hoc network of laptops (can be static for some time period).

2) Power: Devices in ad hoc network can be laptop, palmtop, generator powered. Most of them battery powered. Wireless transmission, reception, retransmission, consumes power. E.g. Consider a ad hoc network established in forest by military, here there is no resources charging their devices, after certain time period battery may drain.

E. AODV Protocol

AODV is reactive routing protocol routes are created only when they are needed hence AODV discovers the route from source to destination only on demand rather than table driven approach, hence partial network copy is not maintained. It does not make sense to maintain due to mobility. AODV protocol has different processes like route discovery, route table management, route maintenance and local connectivity management. In route discovery process source node communicate to the destination node through intermediate nodes (routing nodes) if there is no direct connection between source and destination.

If there is no routing information available in the routing table of source node, route discovery starts by broadcasting route request (RREQ) packet to all the neighboring nodes within range of source node/IN nodes, RREQ goes on propagating through Intermediate nodes until valid path is not found.

Sequence numbers ensure the freshness of routes and guarantee the loop-free routing. Sequence numbers are always incremented. They are incremented only when RREP packet are received and RREQ packet are sent.

The reverse path sets up automatically when RREP packet is sent. Replying node (IN) generates the route reply (RREP) to the source (requesting) node. Source may receive multiple RREP. But the valid and shortest is selected. Forward path is the reverse of reverse path setup.

In path maintenance, continuously hello messages are used to ensure that neighbours links are available. If link is failed, route discovery process restarts and finds the route. In local connectivity management, nodes broadcast the hello messages to its neighbors node for checking its availability. Hello message does not change sequence numbers.

F. Sequence Numbers

Sequence Numbers serve as time stamps and allow nodes to compare how fresh their information on the other node is so as to eliminate loop routing. However when a node sends any type of routing control message, RREQ, RREP, RERR etc, it increases its own sequence number. Sequence number are never decremented. Hello messages do not change sequence numbers. Higher sequence number is more accurate information and whichever node sends the highest sequence number, its information is considered (selected as next hop) and route is established over this node by the other nodes. The sequence number is a 32-bit unsigned integer value (i.e., 4294967295). This value is large enough so that maximum value will never reach. Continuous transmission up to 248 days at rate of 200 packets/sec would be needed to exhaust this series and reset it to zero. Ad hoc networks are temporary. It would not operate for long duration exhausting the series suddenly. If the sequence number of the node reaches the possible highest sequence number, 4294967295, then it will be reset to zero (0). If the results of subtraction of the currently stored sequence number in a node and the sequence number of incoming AODV route control message is less than zero, the stored sequence number is changed with the sequence number of the incoming control message. Sequence numbers are basically used for loop free routing. Concept of sequence number is taken from DSDV protocol. e.g Suppose Node 1 forwards the RREP message coming from Node 2, it compares its own previously stored sequence number with that of Node 2. If it notices that the sequence number is newer than its own, then it changes its route table entry as necessary.[2]

G. Black Hole Attack

Black hole attack is kind of DoS attack where black hole node attracts all packets by pretending shortest route to the destination to route requesting node. It drops all attracted packets of source or intermediate nodes. As almost all packets of nodes within its range are attracted and dropped hence it degrades the performance of the network. Black hole node pretends that it has valid and shortest path with less hop count towards destination. Requesting node accepts it as next hop assuming cost of transmission through that node is less. Black hole intentionally attracts all packets so as to degrade performance of network.

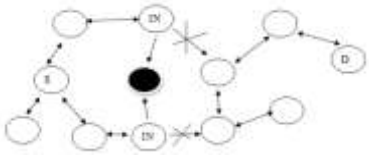

Fig. 1. Black hole pretending Intermediate nodes that it has valid and shortest path.

H. Gray Hole Attack

Gray hole attack is a specialized version of black hole attack, it has all characteristics of black hole attack. But gray hole switch its states from black hole to normal and vice versa any instance of time. Detection of gray hole attack is difficult

because it cannot predicted when a node will be switched to normal mode and when in malicious mode.

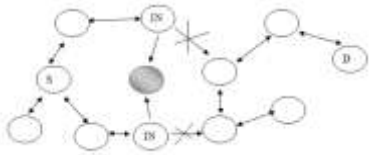

Fig. 2. Gray hole in malicious mode pretending Intermediate nodes that it has valid and shortest path.

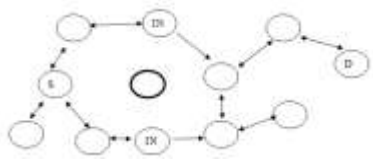

Fig. 3. Gray hole in normal mode, Intermediate nodes selects valid routes.

I. Packet Drop Attack

Packet Droppers are the malicious nodes which do not forward the packet(or route the packet through it) they just drop the packets routing through them. Packet drop attack is minor attack compared to black hole and gray hole attack Black hole intentionally attracts the packet towards them and drops them while packet dropping nodes drops only packets passing or trying to route through them. Packet drop attacks intention is not to degrade the overall performance of network but its purpose may be To save energy by not routing other nodes packets. To drop specific packets from specific nodes on specific routes.

II. Literature survey

a) : Shalini Jain[8] proposed the technique of detection using defragmenting data. Processes performed at Source node. Packets are divided into n number equal parts this parts sent to destination in the form of messages. When the destination receives count of number of messages, then sources starts sending actual data. A timer is set until all packets are not received by destination. If number of announced data packets from destination is less than a limit, initiates removing process of black/gray hole attack as it is assumed that some packets has been dropped. If after terminating of timer, did not get any message from destination, starts removing function of black hole attack. Detection process at destination node. After getting the total number of data packets timer is to zero and starts counting data packets. After a timeout, returns data packet numbers to source node. Detection neighbour nodes. By getting monitoring message from source node, each node starts a counter for counting number of data packets of its neighbors. Source node gets the information malicious node with the help of neighbour monitoring. And select the node as malicious which have been set malicious by neighbours (like a vote).If votes of neighbors about maliciousness exceeds from a limit, source enters that node in blacklist and finds (selects)a new route to destination.

b) : S.Marti [9] proposed a technique, in which watch-dog timer is used. Each node in the network monitors its next hop node in the route. If it finds any packet forwarding misbehaviour or any packet dropping in a predefined period of time for its next hop node, it will introduce the next node as a malicious node to the source. Source node should trust the other nodes information about one nodes misbehaviour. This technique is not so effective as it is not using proper required data for detection of next hop node.

c) : Abderrahmane Baadache[10] proposed technique in which he used Merkle tree concept. Merkle tree is a binary tree which each leaf contains a hash value and intermediate nodes use leaves hash values to create a new combined hash.For detecting black hole attack, each node contains a hash which is combination of nodes id and a secure value that only the node knows. Source node has concatenation of all hashes of one route to destination in its memory. Each node sends concatenation of its hash and previous nodes in route with RREP packet from destination to source. Source node compares this value with prior saved hash value of this route in its memory and if any differences found, it then informs other nodes about maliciousness of this route. Difference between saved value and new value shows that one node may drops RREQ packets and does not send packets to destination that does not have correct value. This technique may create calculation overhead.

d) : Ramaswamys[11] approach Data Routing Information (DRI) table is maintain at each node that has two fields named from bit and through bit. Consider a node. For a node. FROM means I have accepted or routed packet from so and so node. THROUGH means I have routed or forwarded my packets through so and so node. During route discovery source initiates by sending RREQ packets. If destination sends back RREP, source trusts to its answer as it may it next hop. If an intermediate node returns RREP, that node should also send its DRI table and ID of next neighbor in the route to source. If source previously sent a message to that node, it is a trustable node for source and starts sending data packets through that to destination. If source does not know that node, it sends a packet to next node of marked node and asks it for DRI table and also ID of its next node. In crosschecking the data provided by DRI table is checked whether its correct or not.

e) : Y.Hu[12] proposed a Secure Efficient Ad hoc Distance Vector routing protocol (SEAD) based on the structure of Destination Sequenced Distance Vector (DSDV). It uses the reply protection of routing update messages. It is uses the one way hash function. This protocol is examined against DSR protocol. This protocol can protect from external attack only. It will not protect from internal attack. Hence it is not possible to detect eavesdropping. Because of hashing technique there is calculation overhead.

f) : Payal Raj[13], DPRAODV technique uses packet sequence number(RREP) of replying node and threshold value. It uses the concept of dynamic learning method, in which

threshold value is dynamically updated through at instance of time when RREP packet is received. If RREP packet sequence number is higher than the threshold value, then the node is suspected to be malicious and it will add in blocked list. It sends ALARM packet to the neighbors informing about malicious node. This protocol takes higher routing overhead due to ALARM packets. This modified protocol does not detect gray hole attack[4].

g) : Kimaya[14],Proposed Authentication Routing for Ad-hoc Networks (ARAN) is a mechanism for detection using cryptographic techniques. It uses public key encryption system. This mechanism examines against AODV and DSR protocol. This protocol also protects from internal as well as external attacks. Overhead is high in this protocol because of cryptographic keys mathematical calculations.

h) : S. Kurosawa[17] proposed an algorithm for detection scheme using dynamic learning method. Which is similar to threshold value concept. The training data is updated regular time interval as in DPRAODV. Destination sequence number is considered to detect the black hole attack. It is rise when the number of connections increases. The average of the difference between the Destination sequence number in RREQ message and the number held in the list are calculated for each time slot. This method is not detecting the gray hole attack. As per the higher sequence number of the node entered in blocked list even the node is not malicious.

i) : S. Banerjee[18] proposed a solution for detection and removal of chain of cooperative black hole and gray hole attack. In this solution, all nodes monitor to each other. This mechanism examines AODV protocol. Due to monitoring network it has high overhead and also consumes more energy for monitoring. Detection process for malicious node is slow.

j) : Jhaveri R.H.[19] approach uses intermediate node dynamically calculating peak value after every time interval, technique uses three parameters for calculation. RREP sequence number, routing table sequence number and number of replies received. RREP received from malicious node is marked as DO NOT CONSIDER.

III. Motivation

1) : It is analyzed that ad hoc networks are more prone to malicious attacks as discussed. Major destructive attacks are black hole attack and gray hole attack where they pretend that they are having valid shortest path, intentionally attracting the packets and finally dropping them, it has proved by simulation in paper[7].

2) : Black hole drops more packets than gray hole attack but detection of black hole can be done easily than gray holes, as gray holes are switchable in nature.

3) : Objective of paper is to design a technique to detect the gray hole/malicious node in the aodv network and isolate them.

4) : Mobiles nodes have limited resources E.g battery power,etc. Hence a mechanism has to be designed keeping in mind this parameters. Hence objective is to design algorithm to detect gray hole attacks.

5) : It is proved in [4] that DPRAODV cannot detect gray hole attack.

6) : Below disadvantages are observed in DPRAODV, Kurosawas and Jhavaris approach.

It calculates peak/threshold value on the basis of 3 parameters.

- Routing table sequence number
- RREP packets sequence number
- No of replies to the node at current instance.

IV. System Architecture and Mechanism

Approach is extension to Raj P N, Swades P B, DPRAODV:A Dynamic Learning System Against Black hole Attack in AODV based MANET, DPRAODV[13]. Algorithm detects gray hole nodes and prevent the normal nodes with higher sequence number to enter in black list. Proposed approach dynamically calculates peak value as in DPRAODV, but it uses some more parameters than DPRAODV.

A. Input Parameters

The parameters used to calculate the peak value are

- Routing table sequence number.
- Reply packet sequence number.
- Elapsed time of ad hoc network, which is analogous to Current simulation time of simulator in simulation environment.
- Elapsed time of ad hoc network, which is analogous to Current simulation time of simulator in simulation environment.
- Total number of reply packets received by the intermediate/neighbor/replying node.
- Reply Forward Ratio (RFR) of replying node.

B. Scenario

When the node gets detected, it would not send any alarm packet. Hence it reduces routing overhead. Every node maintains a data structure in their local RAM which acts as a black list cum FALSE REPLY list of the nodes in the network. FALSE REPLY are the replies which are detected as a fake from malicious i.e. black/gray hole pretending shortest and valid path. Depending on the number of FALSE REPLY from the node it is decided that node is to be black listed or not. Using this approach, gray/malicious node are added to black list and eliminate normal nodes to enter in black list.

Gray hole is a node which switches from black to normal and vice versa. Whenever it switches to black, it will generate false reply which helps to detect it as a gray hole. Also it gives every node an attempt/chance before adding to black list, hence resources of gray hole for packet forwarding can be utilized to some extent, when they are in normal state.

1) : In this technique, detection of malicious nodes (m-node) is done during route discovery process. But the m-node is not black listed during first attempt of malicious activity. Whenever a malicious activity is detected by receiving node, it increases a false reply count for Whenever a malicious activity is detected by receiving node, it increases a false reply count for replying node in its local black list buffer.

2) : In this approach it is 6 attempts of false reply to add a m-node in the black list. Black list is local for each node. Each node maintains its own black list buffer. Information of the list is never broadcasted to any nodes. The black list is private to each node individually.

3) : Each and every node use detection and black listing locally. Hence any m-node will not broadcast false alarm packet pretending that particular node is malicious node (even it is normal) to other nodes in the network.

4) : M-node is detected and black listed when receiving /source node detects malicious activity from replying nodes. When any node in network detects as a m-node it will not propagate alarm to its neighbors. Hence, scanning and detection is locally done and alarm is not broadcasted reducing routing overhead.

5) : Gray holes are switching nodes from good to bad and vice versa. To detect them track has been kept on their switching activity. It has uses number of false reply concept.

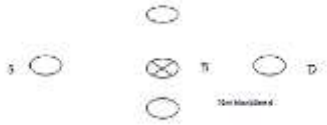

Fig. 4. Node receiving false reply from node B.

C. Modified flow in AODV Architecture

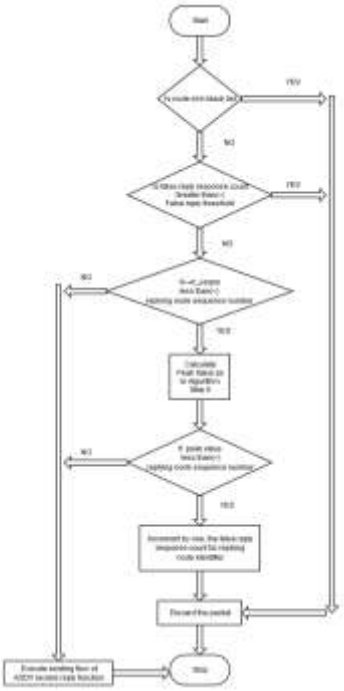

Fig. 5. Modified flow diagram

D. Algorithm for Gray Hole Attack Detection

1) : Start (for each node which receives RREP).

2) : Check if a replying node has generated False Reply Count greater than False Reply Threshold if yes goto step 3, no goto step 4

3) : Black list the node, dont accept any RREP packet (discard) from this node further.

4) : Check if routing table sequence number is less than reply packet sequence number. if yes goto step6 no goto step5

5) : Skip detection engine and goto step10.

6) : Calculate

D = Difference between routing table sequence number and route reply sequence.

RFR = Reply Forward Ratio.

No RR = No. of replies received by replying node.

ST = Simulation Time.

$$Peak = ([((D) * RFR) + NoRR + ST])/3 \quad (1)$$

7) : Check if peak ¡ route reply sequence number If yes goto step8 No goto 10

8) : Add/Increment the false reply count to corresponding replying node.

9) : Free the packet (RREP)

10) : Follow the remaining aodv recvreply() function.

V. Simulations and Results

A. Performance Measures Used

- Throughput: It is defined as the amount of data transferred over the period of time expressed in kilobits per second (kbps).
- Packet Drop Rate: It is the ratio of the data lost at destinations to those generated by the CBR sources. The packets are dropped when it is not able to find the valid route to deliver the packets.
- Packet Delivery Ratio: It is the ratio of data delivered to the destination to the data sent out by source.
- Number of Nodes: Total number of nodes within simulated network.

B. Simulation Parameters

- Simulator - NS-2.35
- Simulated Attack - Gray hole attack
- Channel Type - Wireless
- Antenna Type - Antenna/OminiAntenna
- Radio propagation model - Propagation/Two Ray Ground
- interface queue type - Queue/ Drop Tail / PriQueue
- Mac type - Mac/802 11
- Protocols - AODV
- Simulation time - 150 sec
- Pause time - 20 sec.
- Pause time - 1500*1500.

C. Results

It has been analyzed that results are dependent on current position of nodes in the simulation scenario and may vary on next simulation because the gray hole is flashing between good and bad at random time.

TABLE I
PACKET DELIVERY RATIO VS NUMBER OF NODES

Nodes	PDR(Normal)	PDR(attack)	PDR(solution)
30	36.18	69.37	36.89
40	27.02	18.59	26.04
50	39.05	33.08	41.8
60	49.03	31.86	49.03
70	45.33	29	42.88
80	47.9	33.38	47.74

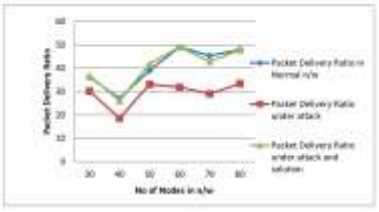

Fig. 6. Packet delivery ratio vs. number of nodes.

TABLE II
THROUGHPUT VS NUMBER OF NODES

Nodes	T(Normal)	T(attack)	T(solution)
30	107495	89538.5	109548
40	80195.4	55174.7	77229.9
50	115487	98064	123872
60	146129	95173.2	146055
70	134271	85965.6	127536
80	141995	99241.3	142594

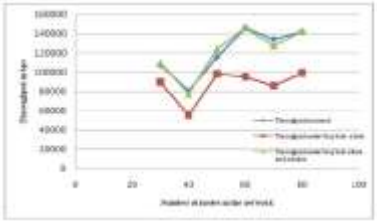

Fig. 7. Throughput vs. number of nodes.

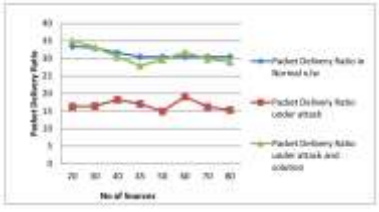

Fig. 8. Packet delivery ratio vs. number of sources.

VI. CONCLUSION

Denial of Services severely impacts any kind of networks. Ad hoc networks are more prone to attacks and Gray hole attack is one of attack and detecting it challenge due to its behavior. Various methods to detect has been studied, disadvantages are observed in DPRAODV, Kurosawas and Jhavaris approach. In which normal node with higher sequence number than threshold value may get in black list. Alarm packets are sent to neighboring nodes which creates routing overhead. It detects only black hole not gray hole nodes.

Algorithm implemented detects gray hole nodes, keeps the information locally, alarm packets are not to neighboring nodes reducing routing overhead and false information, mechanism also checks for false attempts from next hop node before making decision that next hop is malicious .

TABLE III
PACKET DELIVERY RATIO VS NUMBER OF SOURCES

Sources	PDR(Normal)	PDR(attack)	PDR(solution)
20	33.49	16.27	35.13
30	33.01	16.42	33.22
40	31.62	18.22	30.48
45	30.47	17.03	27.94
50	30.47	14.9	29.61
60	30.47	19.1	31.87
70	30.47	16.19	29.84
80	30.47	15.3	29.04

TABLE IV
PACKET DROP RATE VS MOBILITY

Mobility	PDR(Normal)	PDR(attack)	PDR(solution)
10	70.01	79.26	69.39
20	74.32	88.09	77.21
30	76.23	88.79	77.66
40	57.63	82.15	57.38
50	73.51	90.4	74.34
60	80.89	92.04	83.52
70	80.69	95.06	80.23
80	71.87	85.37	73.59

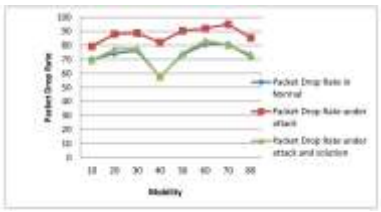

Fig. 9. Packet delivery ratio vs. mobility.

ACKNOWLEDGMENT

I wish to thank Prof. D. C. Mehetre(Guide), Prof. M Nighot, Dr. S. J. Wagh who all have been a constant source of inspiration and guidance. I also acknowledge the research work done by all researchers in this Field.

REFERENCES

[1]P.W.Yau,S.Hu and C.J.Mitchell, Malicious attacks on ad hoc network routing protocol, International Journal of Computer research ,15 no.1 (2007) 73-100.
[2]S.Dokurer,Simulation of black hole attack in wireless ad-hoc networks, Atlm university.
[3]Akanksha Saini, Harish Kumar,Comparision Between Various Black Hole Detection Techniques in Manet, NCCI 2010 -National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 19-20 March 2010.
[4]Marjan Kuchaki Rafsanjani,Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV based MANET,IJCA Special Issue on Network Security and Cryptography NSC, 2011.
[5]Hassen Redwan and Ki-Hyung Kim,Survey of Security Require-ments,Attacks and Network Integration in Wireless Mesh Networks,2008 Japan-China Joint Workshop on Frontier of Computer Science and Technology.
[6]Vesa Krpijoki,Security in Ad Hoc NetworksHelsinki ,University of Tech- nology.
[7]Semih Dokurer, Y. M. Erten, Can Erkin Acar,Performance Analysis of Adhoc networks under black hole attack, ATILIM University Ankara, Turkey.
[8]Shalini Jain,Advanced Algorithm for Detection and Prevention of Coop- erative Black and Gray Hole Attacks in Mobile Ad Hoc Networks, 2010 International Journal of Computer Applications (0975 8887).
[9]S.Marti,Mitigating Routing Misbehavior in Mobil adhoc networks, Stanford University.
[10]Abderrahmane Baadache, Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks, International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.
[11]Sanjay Ramaswamy, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, North Dakota State University.
[12] Yih-Chun Hu,David B.Jhonson, Adrion Perrig, SEAD:Secure Efficient Distance Vector Routing for Mobile Ad hoc Networks,2002
[13]Raj P N,Swades P B, DPRAODV:A Dynamic Learning System Against Blackhole Attack in AODV based MANET,International Journal of Com- puter Science 2:54-59,doi:abs/0909.2371.
[14]Kimaya Sanzagiri, Bridget Dahill, Brian Neil Levine,Clay Shields.Elizabeth M.Beiding Royer ,A Secure Routing Protocol for Ad Hoc Networks, Ad hoc Networks Journal, Vol. 1,pp. 175-192,2003.
[15]Vivek Thaper, Performance analysis of adhoc routing protocols using random waypoint mobility model in wireless sensor networks, Interna- tional Journal on Computer Science and Engineering (IJCSE).
[16]P.Kuppusamy, Scenario Based Performance Evaluation of DSR and AODV Routing Protocols, IJCSET — July 2011 — Vol 1, Issue 6,320- 323.
[17]Kurosawa S.,Nakayama H.,Kato N,Jamalipura A., and Nemoto Y. ,De- tecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning method,International Journal of Network Security ,Vol.5,No.3,P.P338-346,Nov.2007.
[18]Banerjee S,2008, Detection/removal of cooperative black and gray hole attack in mobile ad hoc networksIn Proceedings of the World Congress on Engineering and Computer Science.
[19]Jhaveri R.H.,Patel S.J.,Jinwala D.C., A Novel Approch for Gray Hole and Black Hole Attacks in Mobile Ad Hoc Networks,Advanced Comput- ing and Communication Technologies (ACCT),2012 Second International Conference on 7-8 Jan 2012,IEEE, ISBN:978-1-4673-0471-9.

