Trust Certificate Sequence Exchange (TCSE) for Black Hole Detection in MANET: Reliability Value based Approach

Ashish Patel
Research Scholar,Dept. of CSE
SDBCT, Indore, M.P (India)

Mahendra Kumar Verma
Reader, Dept. of CSE
SDBCT, Indore, M.P (India)

ABSTRACT
A mobile ad hoc network is a temporary network based on movable nodes within a specific range. Due to this motion the information related to nodes is continually changes likewise the addition of new node and its deletion from network is required. Due to this the authenticity of node must be justify to participate in data transmission. In the absence of this verification process some of the unidentified nodes may does malicious act. This type of activity is done by node known as blackhole/grayhole attack.

A black hole node is a malicious node which sends the fake reply for route requests and drops the packets. In this work, a novel approach is proposed to detect blackhole nodes for AODV protocol of MANET. Our solutions find out the safe route between sending node and receiving node through some routing decision which is calculated through proposed Trust Certificate Sequence Exchange (TCSE) mechanism. In this mechanism the trust of each node in a network is calculated on the basis of behavior analysis of nodes & issues a certificate. The trust value is measure as a parameter of reliability & analyses delivery ratio, overhead & delays. This value is stored in a specific certificate & regularly shared with every neighbor. The work also introduces a control node named as watcher node which will monitors the behavior & trust of every other node within its neighbours. Initial results shows that the mechanism proposed will provide an effective solution to the mentioned problem of cooperative blackhole detection & prevention.

KEYWORDS
AODV, BLACK HOLE, MANET, MALICIOUS NODE, TCSE(Trust Certificate Sequence Exchange);

1. INTRODUCTION
Wireless ad hoc networks are a group of computing devices equipped with radio transceivers and interconnected wirelessly through radio frequency without fixed infrastructure or centralized control. Normally, wireless nodes such as sensors, PDA, cell phones are battery-powered. The limited energy budget at the individual node level implies that the transmission range of individual nodes is restricted, which in turn implies that wireless ad hoc networks must be multi-hop. That is, any two nodes that are out of each other's transmission range have to rely on a number of intermediate nodes to rely their messages. In such an environment, nodes are equal, playing both host role and router role; the functionality of the network is subject to node cooperation in relaying messages. Two well-known instances of wireless ad hoc networks are wireless sensor networks and mobile ad hoc networks.

Although wireless ad hoc networks hold promise for a large number of applications in different domains and are expected to revolutionize our everyday life, the problem of securing these networks has been a major roadblock to their large scale deployment in practice. While being vulnerable to the security threats of conventional networks, these networks are susceptible to additional threats stemming from the intrinsic characteristics of ad hoc nodes such as narrow communication bandwidth and limited computation ability, memory and power supply. Wireless ad hoc networks are usually deployed in an open and possibly hostile environment, where an adversary may easily capture nodes and subsequently use them to attack the network. Building tamper-proof nodes is not guaranteed and subject to individual user's decision, for example, in mobile ad hoc networks, while it is not a practical solution in wireless sensor networks which are outsized in scale.

There are several issues in MANETS which addresses the areas such as IP addressing; radio intrusion; routing protocol; power constraints; security; mobility management; bandwidth constraints; QOS; etc;. As of now some hot issue in MANETS can be linked to the routing protocols, attacks, power and bandwidth, which have raise lot of significance in researchers. The paper specifically focuses on the routing security issue in MANETS.

1.1 Characteristics of MANET
A major attribute of MANET is its fully dispersed architecture [2]. It can be set up anywhere on the temporary basis, as there is not as such requirements of infrastructure facilities. There are some major characteristics of MANET are as follows:-

i. Communication via wireless means
ii. Nodes can present the roles of both hosts and routers
iii. Bandwidth-constrained, variable capacity links
iv. Energy-constrained Operation
v. Limited Physical Security
vi. Dynamic network topology
vii. Frequent routing updates
viii. It can set up anywhere
ix. Multi hop Routing
x. Device Heterogeneity

The main goal of the security requirements for MANET is to provide a security that should meet the properties like privacy, reliability, authentication, accessibility and non-repudiation to the mobile users. The identification of a malicious node is the estimated percentage of packets discarded, which is compared against a pre-established misbehavior threshold. Any other node which drops packets in excess of the pre-established misbehavior threshold is said to be misbehaving, while for those nodes having percentage of dropping packets is below the threshold are said to be properly behaving.

The approach TCSE proposed here identifies and prevents misbehaving nodes (malicious), which are capable of launching four routing attacks parallels: the black hole attack, gray hole

attack, eavesdropping of packets attack and message tampering attacks. The proposed architecture will show how effectively malicious node identification is achieved.

The paper will also discuss the framework and a relevant algorithm with AODV protocol implementation to account attacks. The result of these implementation illustrate that an appropriate selection of the misbehavior threshold will be able to identify the misbehaved and well-behaved nodes, also the high level of counter is assured against different degrees of node mobility in a network that is affected especially by black hole and/or gray hole attacks. Finally, we then evaluate our technique for effectiveness and efficiency, against other blackhole detection methodologies.

2. BACKGROUND

MANET security essentials can be classified in to 5 major layers of work given as Application layer; Transport layer; Network layer; Link layer; and Physical layer. However, the center of prime concern is on the network layer, which is the security design perception in MANET. It is considered as it has not got a obvious line of security. Unlike wired networks that have committed routers, each movable node in an ad hoc network may function as a router and forward packets for other neighbor nodes. The wireless medium is accessible to both legitimate network users and maliciously behaved attackers. There is no well distinct place where traffic monitoring or access control mechanisms can be extended. As a result, the line that separates the inside network from the outside world becomes vague. On the other view of existing ad hoc routing protocols, such as (AODV-Ad Hoc on Demand Distance vector protocol) [2] [3], (DSR-Dynamic Source Routing) [4], and wireless MAC protocols like 802.11 [5], usually work in a trusted and cooperative environment. As effect, a malicious attacker node can promptly becomes a router and disrupt network operations by intentionally disobeying the protocol specifications. Recently, several research measures introduced to counter against these malicious attacks.

In this paper we studied AODV protocol & identifies its vulnerability for many attacks; one of them is Black hole attack. Black hole attack is a kind of active attack. In a black hole attack [4], malicious node waits for neighboring nodes to send RREQ (Route Request) messages. When the malicious node receives this RREQ (Route Request) message, without checking its routing table, instantly sends a false RREP message. It shows that malicious node have a route to destination over itself & gives a high priority sequence number to make entry in the routing table of the victim node, before other nodes send a true RREP. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node.

Malicious node attacks all RREQ messages this way and takes access to all routes. So all packets should be sent to a single point when they are not forwarding anywhere. This is called a black hole attack to real meaning which drops all objects and matter.

There are three major behaviors that Black hole node actually possesses. They are as follows:-

• Black hole node advertise itself by showing larger or highest possible destination sequence no. as we know larger the sequence [5] no. means the route is fresh and latest for a particular destination. This way malicious node bluffs the source node, who wants to initiate communication.

• It is an active DoS attack in MANET [5], which intercepts all incoming packets from an anticipated source. A black hole node absorbs the network traffic and drops all packets.

• The malicious node is hypothetical to be positioned in center of the wireless network.

3. RELATED STUDY

During the last few years of research in MANET security various approaches is been proposed and accepted for black hole identification. The mechanism is also capable of preventing this malicious behavior by some decision based methods. These methods are called trust evaluations. Out of these some includes authentication mechanisms for identifying multiple black hole nodes cooperating as a group, which could be potentially exploited by malicious nodes [1]. To address the problems, and cooperative black & gray hole detection without assuming the existence of any authentication infrastructure, such as a Public Key Infrastructure (PKI), which is usually not practical in MANET, authentication mechanisms are constructed based on the concept of the hash value function, the media access control and the PRF.

In 2008, S Ramaswamy et. al. in [3] proposes a methodology for identifying multiple black hole nodes cooperating as a group with slightly modified AODV protocol by introducing data routing information (DRI) table and cross checking. The solution to identify multiple black hole nodes acting in cooperation involves two bits of additional information from the nodes responding to the RREQ of source node S. Each node maintains an additional DRI (Data Routing Information) table.

In 2010 Anita et. al. gives a certificate chaining method for malicious node identification & having self organized PKI authentication by a chain of nodes without the use of a trusted third party [6]. Here authentication is represented as a set of digital certificates that makes a chain. Each node in specific network has similar roles and responsibilities thereby achieving maximum level of node involvement. Each node in the network can generate certificates to every other node within the radio communication range of each other.

In 2011, security solutions are further extended through some newly proposed methods by Defrawy et. al. & Xu Li et. al. in [4, 5] to identify the privacy preserving & side channel monitoring by which we can be sufficiently analyzed the malicious behaviors. The proposed solution can be applied to identify multiple black hole nodes cooperating with each other in a MANET; and discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation.

There are so many other encryption based [7] & robust identification based [8] is given by different authors. They demonstrates an adaptive approach to detecting black and gray hole attacks in ad hoc network based on a cross layer design. In network layer, the paper [9] proposed a path-based method to overhear the next hop's action. This scheme does not send out added more control packets and saves the system resources of the detecting node. In MAC (Media Access Control) layer, a collision process rate monitoring system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. Some approaches developed a novel trust based calculation for malicious node identification is also proposed which is capable of detecting the nodes trust value on the basis of their historical analysis [10]. In [11], the author proposes a solution to identifying and preventing the cooperative black hole attack. The solution discovers the secure route between source and destination by identifying and

isolating cooperative black hole nodes. In this paper the simulation is used to evaluate the proposed solution and compare it with other existing solutions in terms of throughput (Maximum Utilization), packet loss percentage, average end-to-end delay and route request overhead.

In 2012, Jaiswal et. al. suggested that request routing table is an another great option for black& gray hole detection in which the nodes shares their routing table on regular basis network form further malicious behaviour. Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET by identifying the node with their sequence number; check is made for whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not? The solution presents good performance in terms of packet ratio and minimum packet end-to-end delay and throughput [12].

In 2012, Choudhary et. al. identifies acknowledgment as a detection technique of blackhole node [13]. To prove that a node has actually forwarded packets to the next hop, the receiver can send acknowledgment in the reverse direction for multiple hops. Two-hop acknowledgment is suggested. However, it fails when more than two malicious nodes are colluding in a row. For example, three malicious nodes one next to another act as a team to drop packets along a data communication path: the middle one drops packets actually, and the first one does not do the watchdog job and its next hop falsely sends acknowledgment.

There are so many other detection techniques in literature [14, 15, 16]. They aimed at early detection of packet drop attackers during routing process. The general idea is to identify forged routing information by double checking, for example, neighbour information, destination sequence number, or network state, with the nodes after the malicious node or directly with the destination [17]. Due to space limit, we introduce only a few recent proposals.

4. PROBLEM IDENTIFICATION

After analysis of the various paper & their techniques this work found that the existing methods focuses on providing the security to this forged message detection & valid packet dropping by malicious node. So it there must be some procedure which identifies this nodes as early as possible. For that purpose the problem related to malicious or black hole node identification through existing methodology included in AODV on demand protocol is shown in figure 1 below.

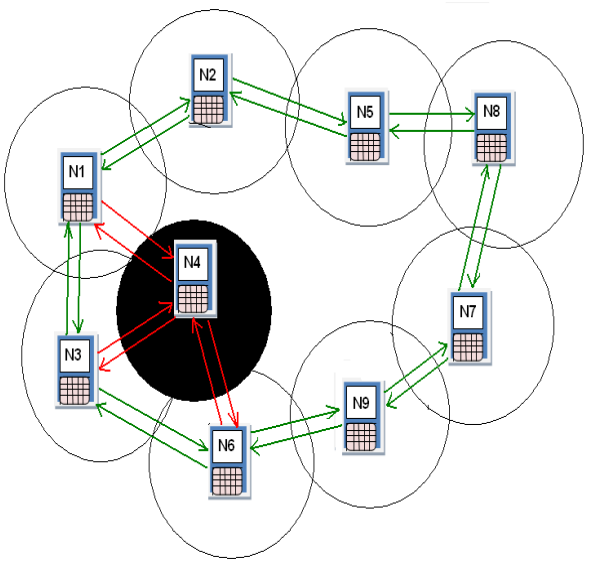

Figure 1: Network Assumption Model for Black Hole Detection through ADOV protocol

In the above network model multiple nodes is connected to each other through specific range of transmission. It has 9 nodes from N1 to N9. Let us assume that before communication start & end node has to finalize. In given model N1 has to send packets to node N8. So it starts route discovery. We also assume the malicious node & apply all its condition & behavior on N4. The N4 has no fresh route for sending the data to N8.

Though, node N4 claims that it has the nearest route to the destination whenever it receives RREQ packets, and sends the reply back to source node N1. The destination node N8 and any other intermediate nodes that have the fresh route to the destination may also give a reply.

If the reply from a genuine node reaches the source node of the RREQ First, everything works as it is supposed to do; but the false reply RREP from malicious node N4 is probable to reach the source node first, in case if malicious node is in close proximity to the source node. A malicious node does not need to check its routing table as it is known that it's sending a false RREP message; its response is probable to reach the source node first. This makes sure that the source node that the route discovery process is complete, then it discards all other reply messages, as it is having the shortest route reply(from malicious node) first and begin to send data packets through it. As a outcome, all the packets through the malicious node are intercepted or dropped. The malicious node could be said to form a black hole in the network. In this way the malicious node can easily gulp a lot of network traffic to itself, and could affect an attack to the network with a big loss of data.

Trust can be consider a well known parameter for node behaviour whose value is continuously exchanged between all the adjacent neighbour nodes. Thus problem related to blackhole detection through trusted & watcher node trust table needs to be maintained. This table exchange & trust value index identification causes an effective detection through our proposed work of Trust Certificate Sequence Exchange (TCSE) & monitoring by watcher node. The TCSE stack will audits & provide the trust to each node at regular intervals. It will also assure that no of the malicious node will able to participate in data transmission. It can only be achieved when the above detection is done at right time.

Apart from the above issues this work finds some more critical descriptive issues in this malicious behaviour detection. If this issues is resolved than the detection & prevention is possible prior to the expected losses.

It also identifies the parameters to define maliciousness or unwanted behaviour of the node. These unwanted behaviour of node can be find out by the trust value of node which is been participated in data transfer previously. Thus this trust value calculation & the exchange of this trust table needs to be secure. The work identifies an invalid trust value due to malicious node behaviour is legitimate at certain condition. In this case the trust value of each node is calculated by a proxy node inside a network & which is further exchange with the data server for aggregation. When a malicious node inside this network will act as the legitimate(Actual) node the calculation of trust value is been disturbed & prompt to somewhere incorrect results. This causes the access gain for this unwanted node in a network & later on will drop the packets & analyze the network for faulty activities. This need to be identified before the table trust value is calculated.

5. PROPOSED APPROACH

Cooperative black hole prevention is a critical issue in mobile ad network. For this purpose this work proposes a novel approach for Trust Certificate Sequence Generation through watcher node for cooperative black hole detection. In this mechanism route discovery can be achieved through a routing decision based on trust sequence certificate exchange through watcher node which is an additional node in node group. This watcher node will act as monitoring node for routing decision based on given steps for blackhole node detection. While discovering the route the sender node will send a RREQ packet to each neighbor node & will expect a RREP packet for existence of route. The node behaving as a malicious node will reply fast irrespective of valid node, due to this misbehaved malicious node seems to have active shortest link. Thus source node S will add this malicious node in its routing table which causes packet drop or denial of service attack. Considering the above problem this work will also adds an additional wait of 20 sec for reply of other nodes.

During this wait period watcher node comes into act for authenticity of each neighbor node through proposed trust certificate sequence exchange (TCSE) mechanism. In this approach firstly the trust of each node is calculated through the previous participation of node in data transmission. This trust must be more than minimum threshold which is decided by the node behavior and issue a specific trust certificate to that node. This certificate is exchange with the entire neighbor nodes in a sequence & routing table of each is updated with the current information. Those nodes who want to participate in data transfer must have at least two trust certificates in a sequence. Now after this routing decision is made on the basis that the node having less than two certificates from previous & next neighbor is identify as the malicious node. After this detection watcher node will transmit a Black Hole (BH) alarm of trust & malicious behavior as a message to entire nodes in a network range. Every node receiving this alarm message must do updates in their routing table with this authenticity detection & deletes the black hole node.

There must be some benefits which we get by applying the proposed TCSE approach like malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process. The delays can also be reduced & blackhole nodes are easily identified. No modification is made in other default operations of AODV Protocol. The approach will give better performance and less memory overhead because only few new things are added.

6. EVALUATION PARAMETER

We have considered four of the network parameters for evaluating the performance with the proposed TCSE approach. Further it can extend to a few more parameters based upon the dense network environment. The algorithm can also be extended to identify and prevent few more network layer attacks.

- *Packet delivery ratio (PDR)* – the ratio of the number of packets received at the destination and the number of packets sent by the source node. PDR of the transmission flow at any given time is calculated as, PDR = (packets received / packets sent)
- *Routing overhead* – The number of routing packets transmitted per data packet delivered at the destination.
- *Power consumption*- the power is calculated in terms of total time taken for transmission of a message from sender node to receiver node. Since this time measured in milliseconds, the power used by a node will be considered as less.
- *Throughput*- It is sum of sizes (bits) or number (packets) of generated/sent/forwarded/received packets, calculated at every time interval and divided by its length. Throughput (bits) is shown in bits. Throughput (packets) shows numbers of packets in every time interval. Time interval duration is equal to one second by default.

Another important fact can be considered with respect to the approach is the power consumption of the nodes in the network. When the proposed TCSE approach is compared to other approaches, scheme represents a simple one-hop acknowledgement and one way trust certificate, termed as semantic security mechanism, significantly reduces overhead in the traffic and the transmission time. The total transmission for sending and receiving data happens in just few milliseconds, overcoming the time constraint thereby reducing power-consumption.

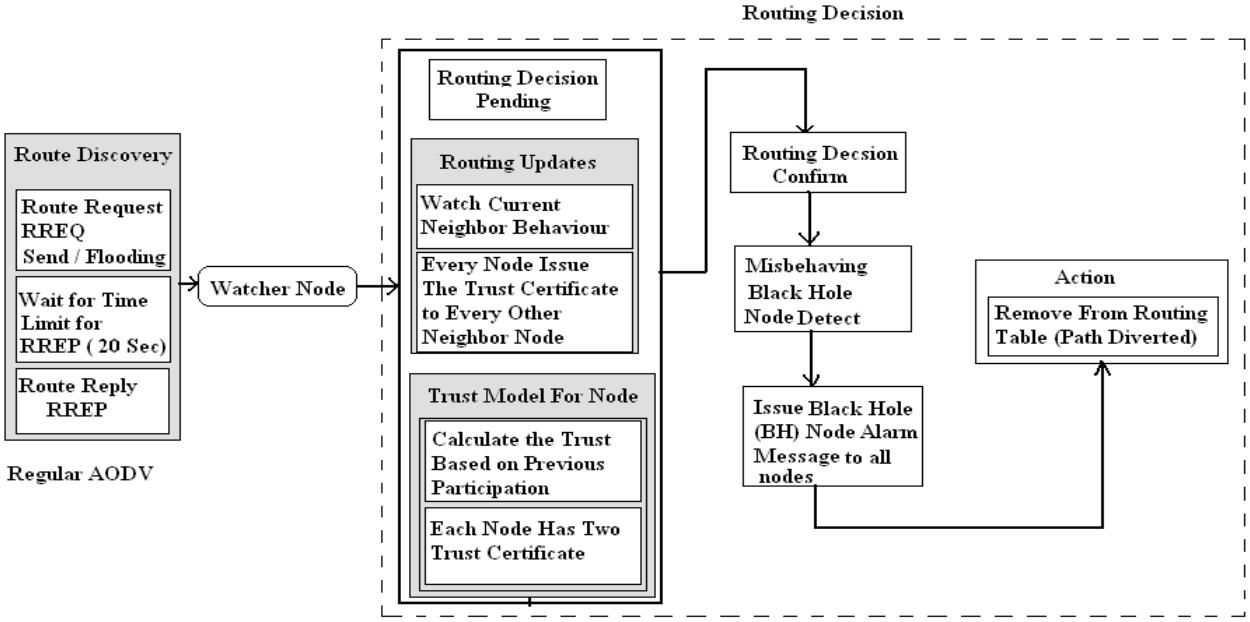

Figure 2: Proposed TCSE architecture for Blackhole node identification in MANET

7. CONCLUSION

In this paper we had analyzed the effects of the Black Hole in an AODV protocol. Thus the effective solution of it tries to remove the Black Hole consequence by making an entry of secure route. This could be a possible way out to make secure entries in the routing table, where each node is recognized to all the other nodes present in the Ad hoc network. If a new node likes to join this network, it has to ensure its authenticity. To this end, we have presented an approach, a network-layer security solution of trust certificate sequence exchange (TCSE) approach which will work on a specific node named as watcher node. This node will work as monitoring node & checks the behaviour of nodes against attacks that protects routing and forwarding operations in the network. As a potential direction for future research work, we are taking into consideration the measurement of more number of network parameters. The work also analyzes the performance of such a network using the proposed approach. In future the results will show the difference between the number of packets lost in the network with and without a Black Hole Attack. This also shows that blackhole attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the number of blackhole nodes are increased then the data loss would also be expected to rise. It is a robust and a very simple proposal, which can be implemented and experienced in future for more number of attacks, by increasing the number of nodes in the network.

8. FUTURE WORK

Some problems and concepts that remain unaddressed can be performed in future. Such as with the help of pre-emptive approach more information can be added for exact timely analysis of malicious node. It can also be used for quantitative & qualitative analysis, rank ordering to each nodes etc. The source code of proposed scheme can also be embed in NS2. So as to use the benefits of approach like open source.

9. ACKNOWLEDGMENT

The authors wish to acknowledge SDBCT administration for their support & motivation while doing this research work. The authors would also like to thank anonymous referees for their many helpful comments, which have strengthened the paper. They also like to give thanks to Mr. Suresh Jain, Mrs. Ruchi Vijayvargiya, and Ms. Jasneet Kaur for discussions in specific domain.

10. REFERENCES

[1] D He, C Chen, S Chen, J Bu & A B. Vasilakos, "ReTrust: Attack Resistant & Lightweight Trust Management for Medical Sensor Network" in IEEE Transaction on IT in vol: - 16, No 4, July 2012.

[2] Z Min & Z Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks" in IEEE Transaction ISBN 978-0-7695-3686-6/09, 2009.

[3] S Ramaswamy, H Fu, M Sreekantaradhya, J Dixon & K Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" in Department of Computer Science, IACC 258, 2008.

[4] K E Defrawy & G Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs" in IEEE Transaction of selected Journal in communication, Vol 29 Issue 10, Dec 2011.

[5] Xu Li, R Lu, X Liang, & X Shen, "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks" in IEEE ICC, 2011.

[6] E. A .Mary Anita & V. Vasudevan, "Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining" in IJCA (0975 – 8887) Volume 1 – No. 12, 2010.

[7] P H. Yu and U W. Pooch, "Chapter on Security and Dynamic Encryption System in Mobile Ad-Hoc Network" in A&M University, Dept of CSE, Texas, USA.

[8] G. S. Mamatha & Dr. S. C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS" in IJCSS Vol 4, Isseu 3, 2010.

[9] J Cal, P Yi, J Chen, Z Wang & N Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network" in IEEE Proceedings, 1550-445X/10, 2010.

[10] R Karandikar, R K Khanuja, S Shukla, "Proposed solution to prevent Black Hole Attack in MANET" in IJRIM ,Vol 2, Issue 2, ISSN 2231-4334, February 2012.

[11] H Weerasinghe and H Fu "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation" in IJCA, Vol 2 ,No 3 July, 2008.

[12] Pooja Jaiswal & Dr. Rakesh Kumar Prevention of Black Hole Attack in MANET in IRACST, ISSN: 2250-3501 Vol.2, No5, October 2012.

[13] Sarita Choudhary & Kriti Sachdeva "Discovering a Secure Path in MANET by Avoiding Black/Gray Holes" in IJRTE ISSN: 2277-3878, Volume-1, Issue-3, August 2012.

[14] M S Ashraf & M Raheel, "RGB Technique of Intrusion Detection in IEEE 802.11 Wireless Mesh Networks" in IJCSI, ISSN (Online): 1694-0814 Vol. 9, Issue 2, No 2, March 2012.

[15] A Kumar & M Chawla, "Destination based group Gray hole attack detection in MANET through AODV" in IJCSI, ISSN (Online): 1694-0814 Vol. 9, Issue 4, No 1, July 2012.

[16] Vishnu K, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks" in IJCA, ISSN 0975 – 8887, Volume 1 – No. 22, 2010.

[17] H P Singh, V P Singh & R Singh, "Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review" in IJCA, ISSN 0975 – 8887, Volume 64– No.3, February 2013.

[18] G. S. Mamatha & Dr. S. C. Sharma, "A New Combination Approach To Secure MANETS Against Attacks" in IJWMN, Vol.2, No.4, November 2010.

[19] S Jain, J Singhai, M Chawla, "A Review Paper on Cooperative Blackhole And Grayhole Attacks in Mobile Ad hoc Networks" in IJASUC, Vol.2, No.3, September 2011.