A Review Paper on Cooperative Blackhole And Grayhole Attacks in Mobile Ad hoc Networks

Sweta Jain[#], Jyoti Singhai[*], Meenu Chawla[#]

[#]*Department of Computer Science and Engineering*
MANIT, Bhopal (M.P.) India
shweta_j82@yahoo.co.in
[*]*Department of Electronics and Telecommunication*
MANIT, Bhopal (M.P.) India
j_singhai@rediffmail.com
[#]*Department of Computer Science and Engineering*
MANIT, Bhopal (M.P.) India
chawlam@manit.ac.in

Abstract:

This paper presents a review on a major category of coordinated attacks i.e. cooperative blackhole / grayhole attack which are a serious threat to ad hoc network security. In cooperative blackhole attack multiple nodes collude to hide the malicious activity of other nodes; hence such attacks are more difficult to detect. In this paper a survey of various security mechanisms that have been proposed in the literature for diction of such attacks is presented.

Keywords:

cooperative, blackhole, grayhole.

1. INTRODUCTION

Routing has been a critical issue in mobile ad hoc networks. A lot of research has been done in the development of specialized routing protocols for mobile ad hoc networks. But none of these protocols take care of security. Hence they are at high risk of being attacked by different kinds of network adversaries. Common types of network attacks are blackhole, wormhole, denial-of-service (DoS), denial-of-messages (DoM), infiltration, and rushing attacks. Moreover the specific characteristics of these networks such as lack of fixed centralized infrastructure, dynamically changing topology, open nature of wireless medium and resource constrained nodes make implementation of security mechanisms a challenging task [5, 8].

A number of secure routing protocols have been proposed in literature in the recent past [2, 3, 6, 7]. These protocols focus on efficient use of digital signatures or shared secret keys to authenticate and confide the data and routing headers. The key management protocols are still

DOI : 10.5121/ijasuc.2011.2305

very expensive and fail in case of internal attacks which result from compromised nodes of the network itself. Also each attack has its own distinct characteristics and solutions have been tailored to defend against specific attacks in isolation. Moreover most of the proposed protocols work against only single node internal attacks. They cannot handle coordinated attacks from multiple malicious nodes working in coordination. The effect of coordinated attacks on network performance could be more devastating as compared to single node uncoordinated attacks

In collaborative attacks multiple malicious adversaries or running processes coordinate their malicious activities against some target organizations or network entities [14]. Detection of collaborative attacks in ad hoc networks is even more challenging for several reasons as stated in [14]:

- Colluding malicious nodes may launch more complex and subtle attacks which may be difficult to identify, detect and prevent.
- They may jointly form a trusted network to mislead other nodes in the network and launch various attacks at the offstage.
- Each participating node may diminish their malicious activities while still hampering the network performance but at a slower rate.

In this paper we have discussed a major category of collaborative network attacks i.e. cooperative blackhole/ grayhole attacks on mobile ad hoc networks and presented a review of the various techniques that have been proposed in literature in the past for prevention and detection of such attacks.

The remainder of the paper is organized as follows. The paper has been divided into five sections. Section 2 describes the cooperative blackhole/ grayhole attack in detail. Sections 3- review the current techniques that have been proposed for detection and prevention of these attacks. Section 4 presents a summary of the various techniques in terms of their effectiveness in preventing such attacks. Section 5 finally concludes the paper and identifies future research directions.

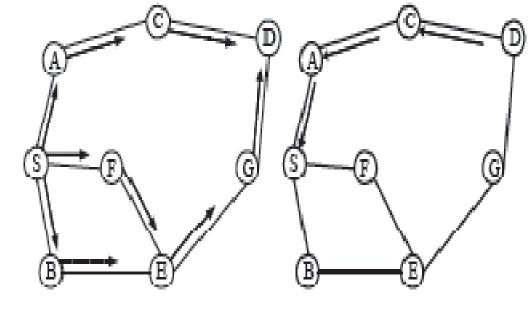
2. COOPERATIVE BLACKHOLE/ GRAYHOLE ATTACK

In the blackhole attack, the malicious node on receiving a route request from any node, falsely replies immediately with the shortest path to the destination. This way the source considers the path through the attacker as the shortest path and uses the path through attacker for all data flow between the source and destination. The attacker node can then drop all the traffic passing through it or selectively drops traffic; hence acts as a blackhole in the network. A grayhole attack is a modified form of blackhole attack in which a node initially behaves non-maliciously but later turns malicious after gaining initial trust of other nodes; hence prevents itself from being detected easily.

Most reactive routing protocols select the shortest route to destination for sending data and this property of routing protocols is exploited by adversary to create a blackhole in the network. For instance, in AODV protocol [1], when a source node S needs to send packets to a destination node D to which it has no available route, it broadcasts a Route Request (RREQ) packet to its neighboring nodes. On receiving RREQ packets, the neighboring nodes update their Routing Tables (RTs) with an entry for the source node, and checks if it is the destination node or has a fresh enough routing to the destination node. If not, then the intermediate nodes receiving a RREQ packet broadcast the RREQ to its neighbors again. The RREQ packet ultimately reaches the destination itself or at an intermediate node that has a fresh routing to the destination, which generates the Route Response (RREP) packet. The RREP packet is propagated along the reverse path to the source node.

Suppose there is a malicious node in the path from source to destination, say B as shown in Fig.

1. Whenever node B receives RREQ packets, it claims that it has the shortest route to the destination node and immediately sends a false RREP packet to the source node, even though it might not be having the route to the destination.

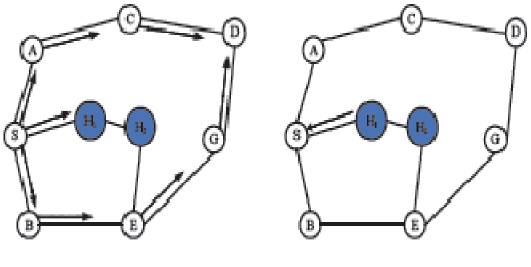


(a) Network Flooding of RREQ (b) Propagation of RREP Message

Fig.1.Route Discovery in AODV Routing Protocol [1]

The destination node may also send the reply but the reply from B could reach the source node first, if B is nearer to the source node. Moreover, B does not need to check its RT when sending a false message; hence its response is more likely to reach the source node firstly. This makes the source node thinks that the route discovery process is completed, ignores all other reply messages, and begins to send data packets through the path containing the attacker node. Subsequently, all the packets through B are simply consumed or lost. B could be said to form a blackhole in the network and this type of attack is known as Blackhole Attack.

Deng et. al. in [3] have proposed some modifications to AODV routing protocol to prevent blackhole attacks called Security Aware AODV. In Security Aware AODV, a source node on receiving a route reply RREP packet, verifies the validity of the path with the next hop node on the route to the destination. If the next hop node either does not have a path to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. However, this technique failed in the presence of multiple malicious nodes cooperating with each other. A shown in Fig.2 when multiple blackhole nodes are acting in coordination with each other, the first blackhole node H1 refers to one of its teammates H2 as the next hop. According to Security Aware AODV, the source node S sends a further request message to ask H2 if it has a route to node H1 and a route to the destination node D. Because H2 is cooperating with H1, its further reply is “yes” to answer both the questions. So source node S starts passing the date packets. In reality, the packets are abstracted by node H1 and the security of the network is compromised.



(a) Network Flooding of RREQ (b) Propagation of RREP message

Fig.2. Cooperative Blackhole Attack [4]

3. TECHNIQUES FOR PREVENTION AND DETECTION OF COOPERATIVE BLACKHOLE AND GRAYHOLE ATTACKS

A number of mechanisms have been proposed for detection and prevention of blackhole / grayhole attacks. A review of these techniques is presented below.

A. In [4], S. Ramaswamy et al have presented an algorithm in which each node maintains an additional Data Routing Information (DRI) table. In the DRI table, 'true' is represented by 1 and 'false' by 0. The first bit "From" denotes that the node has routed data packets *from* the node (in the Node field) while the second bit "Through" denotes that the node has routed data packet *through* the node (in the Node field). The DRI entry is updated when any node received data packet from one of its neighbors or any node that sent data packets through one of its neighbors.

Whenever an intermediate node (say IN) responds to a RREQ, it sends the id of its next hop neighbor (NHN) and DRI entry for NHN to the source. If source node has used IN before to route data, then IN is a reliable node otherwise IN is unreliable. If IN is not a trustable node for source then source sends a further route request (FRq) to NHN. NHN in turn responds with FRp message including DRI entry for IN, the next hop node of current NHN, and the DRI entry for the current NHN's next hop. If NHN is trusted node then source checks whether IN is a blackhole or not using the DRI entry for IN replied by NHN. If NHN is not trustable node then the same cross checking will be continued with the next hop node of NHN. This cross checking loop will be continued until a trusted node is found.

The main drawback of this algorithm is that it is based on a trust relationship between the nodes, and hence it cannot tackle grayhole attacks. Also it is computational intensive as it takes O (n^2) time whenever a node decides to send packets to another node. Moreover as the nodes in ad hoc networks move randomly, a non malicious node which has recently moved in the vicinity of a node may be treated as blackhole as it might not have done nay data transfer through or from the other neighboring nodes. Hence the updation of DRI entry must also take into account the mobility of nodes.

B. P. Agrawal et al in [9] have proposed a technique for detecting a chain of cooperating malicious nodes (black and grayhole nodes) in ad hoc networks. In order to grayhole attacks as well the total traffic volume is divided into a set of small data blocks. In this technique initially a backbone network of strong nodes is built over the ad hoc network. These strong nodes are assumed to be powerful in terms of computing power and radio ranges. Also each strong node is assumed to be a trustful one. Nodes other than strong nodes are considered as regular nodes.

These trustful strong nodes monitor traffic in the ad hoc network and detect the regular nodes if they act maliciously. With the assistance of the backbone network of strong nodes, the source and the destination nodes carry out an end-to-end checking to determine whether the data packets have reached the destination or not. If the checking results in a failure then the backbone network initiates a protocol for detecting the malicious nodes. Fig.3. shows the complete process for detecting cooperating blackhole or grayhole nodes. For detecting malicious node, strong node associated with source node broadcasts a find chain message to the network containing the id of the node which replied to RREQ N_{RREP}, the victim source node S and the destination node D. On receiving find chain message strong node associated with destination node, initializes a list GrayholeChain to contain the id of the node replied to RREQ. It then instructs all the neighbors of that node to vote for the next node to which it is forwarding packets originating from S and destined to D. If the next node id is null then the node is a blackhole node. Then the grayhole removal process is terminated and a broadcast message is sent across the network to alert all other nodes about the nodes in GrayholeChain to be considered as malicious. Else strong node will elect the next node to which N_{RREP} is forwarding the packets based on reported reference counts and again broadcast the find chain message containing the id of the elected node.

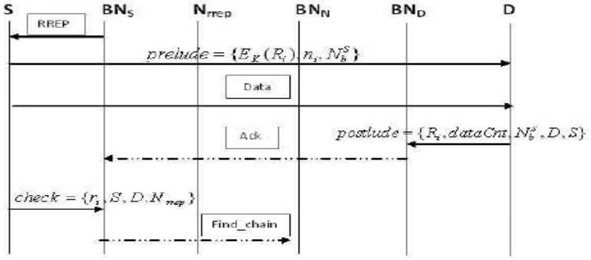

S
BN_S
N_{rrep}
BN_N
BN_D
D
RREP
$prelude = \{E_K(R_i), n_i, N_b^S\}$
Data
Ack
$postlude = \{R_i, dataCnt, N_b^d, D, S\}$
$check = \{r_i, S, D, N_{rrep}\}$
Find_chain

Fig.3. Detection of cooperating blackhole / grayhole in [9]

The major drawback of this approach is the assumption that some strong nodes which are powerful in terms of power, antenna range are available in the network. Such an assumption is not valid for all types of mobile ad hoc network. The optimality of backbone network in terms of minimality and coverage is not proved. Algorithm will fail if the intruder attacks strong nodes because it violates the assumption that strong nodes are always trusted node.

C. In [10], similar to [9], the source divides the data to be transmitted into blocks. Each node in the route monitors the behavior of its neighbors to check if they are forwarding data properly or not. It also assumes that data drop may be due some non malicious reasons also such as lack of CPU cycles, buffer, bandwidth etc. Therefore a threshold on data loss rate μ at each node and total data loss rate threshold μ at the destination is assumed given by $\mu = 1-(1-\mu)^N$ Before starting the transmission of the data packets from the first block, Source node (say S) sends a prelude message to the destination node (say D) to alert the destination node of the incoming data packets and then starts transmission. The destination node sets a timer for the end of the incoming transmission & starts counting the number of data packets received. After the expiration of timer it sends a postlude message to the source containing the number of data packets received by it. At the same time after sending prelude message, source node broadcasts a monitor message to all its neighbors - to monitor the action of the next node in the route i.e to how many data packets the node is forwarding and to whom it is forwarding the data packets. The neighbors of the source node further ask their neighbors to monitor the nodes in the routing path. If source node receive postlude message before timeout expire & the number of the data packets received by destination is equal to the number of data packets sent by source or the data loss is within tolerable range then the source starts the transmission of the next data block; else source starts detection and removal of the malicious nodes.

In the detection process the source node broadcasts a query message to all the neighboring nodes, sets a time out for the receipt of the result message from the monitoring nodes. If the timer has not expired and the node is malicious message is received for any node, it append the malicious node id in its findMalicious table and initializes its voteCount to 1. If other nodes also vote for this node, its voteCount is incremented by one; if the voteCount increases by a predefined number, the node is declared as malicious and broadcasts this information to the entire network. If the timer expires it asks voting for nodes left in findMalicious table.

D. To counteract the cooperative blackhole attack the authors have made use of a Fidelity Table in [11]. Every participating node is assigned a fidelity level that represents a measure of reliability of that node. In case the fidelity level of any node drops to 0, it is considered to be a malicious node, and termed as a blackhole and is eliminated from the routing table of other nodes.

Whenever a node has data to send, it floods RREQ packet to its neighbors and waits for a TIMER period to receive the route replies RREP. The RREP packet contains the fidelity level of the responding node and its next hop on the path. If the average of their levels is found to be above the specified threshold, then the node is considered to be reliable. The source node then selects the path with higher fidelity value. In case two paths have same fidelity value the one with lower hop count is selected.

The fidelity value of participating nodes is updated depending on their faithful participation in packet forwarding.

On receipt of data packets, the destination node sends back an acknowledgement to the source node. On reception of acknowledgement the source node increments the fidelity level of the intermediate nodes as they have faithfully participated in data forwarding. If the source node doesn't receive the acknowledgement within a timer event, the source node will decrement the fidelity level of the intermediate node which sent the Route Reply and also decrements the fidelity level of the node which was given as the next hop of the intermediate node to identify the co-operative attack. The nodes exchange their fidelity tables periodically with each other. If the fidelity level of a node falls to zero level, that node is considered as malicious, declared as blackhole and an alarm message is generated to inform the other nodes about the malicious behavior.

The author have analyzed the performance of proposed scheme PCBHA with AODV in terms of average end-to-end delay, packet delivery ratio and routing overhead. PCBHA achieves higher packet delivery ratio as compared to AODV routing protocol even in the presence of cooperating malicious nodes.

E. In [12] the authors have proposed a slight modification to the technique proposed in [4] for the identification and detection of cooperating blackhole nodes. They have used the same concept of DRI table which keeps track of whether the node has done any data transfer through its neighbors or not in the past. The route reply form the destination is always considered to be valid as the destination is a trusted node. But if a route reply comes from an intermediate node, the source node first checks the validity of the intermediate node by cross checking it with its next hop neighbor in the same manner as in []. But the intermediate nodes between the source and the replying node do not update their route entry for the destination. Only if the replying node and its next hop node is a reliable node then only the source updates the DRI entry for all the intermediate nodes between source and replying node. And at the same time the intermediate nodes also update their route entry for the destination. The process of establishment of secure route is completed and the source starts sending data packets to the destination.

The major contribution of this paper is the implementation of the proposed algorithm and its comparison with the previously existing techniques through simulation which has been skipped in most past works. The performance of the proposed technique has been and compared with the Security Aware AODV in terms of following parameters: throughput, packet loss percentage, average end-to-end delay and route request overhead. The performance analysis has been done for different scenarios generated by varying the number of blackhole nodes, total number of nodes, mobility speed of the nodes and the terrain area. The simulation results show that their proposed scheme is able to achieve higher throughput and low packet loss percentage even in presence of multiple blackhole attacks. While AODV and Security Aware AODV greatly suffer from cooperative blackhole attacks which results in lower throughput and high packet loss percentage. But this performance improvement is achieved at the increased cost of route request overhead.

F. In [13] the concept of the hash function, MAC (Message Authentication Code) and PRF (Pseudo Random Function) are used for identifying multiple blackholes working in a group and for establishing a secure route between source and destination. Each node is assumed to hold a symmetric cryptosystems and it generates the sharing secret key *Ki* by choosing a random number r and recursively applying PRF on *r* by k times where k is the length of the hash chain. MAC is defined by *MAC(Ki ,M)*. All nodes in the network are required to synchronize their time.

They have proposed two solutions for the same. In the first solution, it is assumed that the node divides the transmission time into equal intervals and assigns the ith interval with the ith sharing secret key Ki. Each node also computes the MAC, if it has any message to be transmitted, by applying hash function to the corresponding key and the message. It also generates the key disclosure delay, denoted by d, the time the packet takes to reach destination. As in blackhole attack, the adversary sends an invalid RREP claiming that it has the shortest route to the source. Thus when the destination node sends a RREP packet it forms the following

P= M, MAC(Ki,M) Ki-d
= RREP, MAC(Ki,RREP Ki-d)

Each intermediate node simply forwards the packet to the next node. If the source node receives the RREP packet, it checks the following two conditions:

Condition 1: It checks *K i-d* to find if the key used for the MAC is already disclosed.
Condition 2: It caches the message and checks its authenticity *MAC(Ki,M)=MAC(Ki,RREP)* at the time when *Ki* is disclosed.

If the two above mentioned are all satisfied, this packet is regarded as a valid packet and the route from the destination node to the source node is considered as secure and the source node begins

to send data packets. Otherwise, it either discards the packet or initiates another route discovery process or sends an alarm message to isolate the malicious node in the network.
The second solution is similar to the first one, except that it uses an extra timestamp field while generating the MAC of a message.

The authors have studied and compared the performance of both the proposed solutions with simple AODV under blackhole attack. The have analyzed the performance in terms of packet delivery ratio, delay, detection time and control overhead. The simulation results show that the proposed solutions are able to achieve a high packet delivery ratio as compared to AODV; however there is not much difference in terms of delay and control overhead. This scheme detects that there is a blackhole attack on the network but does not provides mechanism for removal or isolation of the attacking nodes.

G. In [15], similar to [9], it is assumed that a backbone network is present in the ad hoc network. Each backbone node knows the valid IP addresses used in the network. The source node periodically asks for an unused IP i.e. a restricted IP to its nearest backbone node. Whenever a source node has some data to be sent to a destination node to which it has no available route, it floods two RREQ packets, one in search of desired destination and another in search of restricted IP(RIP). As the blackhole/ grayhole node sends RREP for any RREQ it receives, it replies with RREP for RREQ containing RIP as well. If any of the nodes responds positively with a RREP to any restricted IP, then the source node initiates the detection procedure for these malicious nodes. The source node requests the neighboring nodes to enter into promiscuous mode and send feedback to facilitate detection of malicious nodes.

H. In [16], DSR routing protocols has been modified to find secure routes between source and destination. Each node maintains with it the trust value of its neighboring nodes. These trust values are calculated on the basis of its past experiences with its neighbors. The trust value is computed as follows:

$$T = \tanh(R1+R2+A)$$

where R1 is the ratio of total number of packets actually forwarded by a node and the number of packets to be forwarded, R2 is the ratio of total number of packets received by a node and it should forward and the total number of packets sent by its one hop neighbors and are not destined for any other neighbor, and lastly A is used for acknowledgement. The neighbors of a node have been classified as Unknown, Known or Companion in increasing order of the trust values. Thresholds have been used to switch a node from one category to another depending on its behavior.

When a source needs to send data to a destination node it floods RREQ packets in the network. It then collects the RREP from all the nodes which have path to the destination and selects the path with highest trust value as the path to route its data. Nodes having Companion status are given higher priority than Known nodes. If there is a path in which the next node is Known and there is another path in which the next hop node is a Known, then the path with Companion is chosen. Blackhole nodes are identified as unknown nodes and are not given preference in route selection.

4. SUMMARY

From the analysis of the various techniques proposed for prevention and detection of cooperative blackhole and grayhole attack, it is found that most of them are computational intensive; while some mechanisms are based on hypothetical assumptions. For instance certain solutions [] require presence of trusted backbone nodes for detection process which is not a valid assumption in ad hoc networks. False detection rate may be high in some algorithms as they do not consider node mobility. The researchers have presented solutions to various cooperative attacks and proved their correctness theoretically; they have not studied the effectiveness of their proposed solutions in preventing such attacks and their impact on performance of ad hoc networks experimentally. Some techniques fail to detect grayhole attack as they are based on initial trust establishment.

5. CONCLUSION

In this paper we have discussed a major category of cooperative internal attacks on on-demand routing protocols i.e. cooperative blackhole and grayhole attack. In these types of attacks multiple nodes collude with each other to hide the malicious activity of each other. A survey of various security mechanisms that have been proposed in literature for detection and prevention of such attacks is also presented. A lot of work has been done in the detection and prevention of cooperative blackhole attack which are still computational intensive. There is a further need to explore new types of coordinated attacks that can be launched on mobile ad hoc networks and design efficient techniques to detect and prevent them, as coordinated attacks can greatly reduce the system performance in a small amount of time and result in a larger damage. Moreover such attacks are more difficult to detect.

REFERENCES

[1] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing," In Proc. Of IEEEWorkshop on Mobile Comp. Sys. and Apps., Feb. 1999, pp. 90–100.

[2] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", Proc. of IEEE WMCSA 2002, June 2002, pp. 3-13.

[3] H. Deng, W. Li, and D. P. Agarwal, "Routing Security in Wireless Ad hoc Networks," IEEE Communications Magazine, Vol. 40, Number 10, Oct. 2002, pp. 70-75.

[4] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of Cooperative Blackhole Attack in Wireless Ad Hoc Networks," In Proc. of 2003 Int. Conf. on Wireless Networks, ICWN'03, Las Vegas, Nevada, USA, 2003, pp. 570–575.

[5] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security In Mobile Ad Hoc Networks: Challenges And Solutions," IEEE Wireless Communications, pp. 38-47, Feb. 2004.

[6] Huaizhi Li Zhenliu Chen Xiangyang Qin, "Secure Routing in Wired Networks and Wireless Ad Hoc Networks" IEEE, 2004.

[7] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, "Authenticated Routing for Ad Hoc Networks ", IEEE Journal on Selected Areas in Communications, Vol. 23, Number 3, pp. 598-610, March 2005.

[8] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols," Pearson Education, 2007.

[9] P. Agrawal, R. K. Ghosh, and S. K. Das, "Cooperative Black and Grayhole Attacks in Mobile Ad Hoc Networks," In Proc. of 2nd Int. Conf. on Ubiquitous Information Management and Communication, Suwon, Korea, ACM 2008, pp. 310-314.

[10] S. Banerjee, “Detection/Removal of Cooperative Black and Grayhole Attack in Mobile Ad-Hoc Networks,” In Proc. of WCECS 2008, SanFransisco, USA, 2008.

[11] L. Tamilselvan and V. Sankaranarayanan, “Prevention of co-operative blackhole attack in MANET,” Journal of Networks, Vol. 3 Number 5 pp.13- 20, May 2008.

[12] H. Weerasinghe and H. Fu, “Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation,” *International Journal of Softwre Engineering and its Applications Vol* 2, number 3, pp. 39–54, Jul. 2008.

[13] Zhao Min Zhou Jiliu, “Cooperative Blackhole Attack Prevention for Mobile Ad Hoc Networks ,“ International Symposium on Information Engineering and Electronic Commerce, IEEE, 2009

[14] B. Bharagava, R. Oliveria, Y. Zhang and N. C. Idika, “ Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks,” In Proc. of 2009 29th IEEE Int. Conf. on Distributed Computing Systems Workshops, 2009, pp. 447-450.

[15] Vishnu K, A.J. Paul, “Detection and Removal of Cooperative Black/Grayhole attack in Mobile Ad Hoc Networks,” Int. Jnl. of Computer Applications Vol.1, Number 22, 2010, pp. 40-44.

[16] N. Bhalaji, A.V.Kanakeri, K.P.Chaitanya, and A. Shanmugam, “Trust Based Strategy to Resist Collaborative Blackhole Attack in MANET,” In Proc. of International Conference on Recent Trends in Business Administration and Information Processing, BAIP 2010, Trivandrum, Kerala, India, March 26-27, 2010, pp. 468-474.