Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET

Marjan Kuchaki Rafsanjani
Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran

Zahra Zahed Anvari
Science and Research Branch, Islamic Azad University, Kerman, Iran

Shahla Ghasemi
Science and Research Branch, Islamic Azad University, Kerman, Iran

ABSTRACT
Mobile Ad hoc Network (MANET) is constructed from a collection of nodes that can move anywhere and anytime in different areas without any infrastructure. Each node works at the same time as router and host. Lack of a fixed infrastructure, wireless medium and dynamic topology makes MANET vulnerable to different kinds of attacks. In this paper, we investigate different mechanisms that have designed to detect or prevent black or gray hole attacks in AODV protocol. We discuss about advantages and disadvantages of the methods and also compare them.

General Terms
Security, Prevention, Detection, Attacks.

Keywords
MANET, AODV, Black hole attack, Gray hole attack.

1. INTRODUCTION
Different features of Mobile ad hoc networks make these networks susceptible to the security attacks. On the other hand, the traditional security mechanisms that are used for the wired networks are not applicable for Mobile ad hoc networks.

Ad-hoc On-demand Distance Vector (AODV) is one of routing protocols in MANET [2] that we have considered it in this study. It is a reactive routing protocol and creates routes from source to destination at the start of communication. In AODV protocol, source broadcasts RREQ packet to its neighbors to discover route to its destination. After gathering RREP packets from the neighbors, source selects the best route to its destination and sends data packets through that route.

Black hole attack and gray hole attack [1,2] are two kinds of different possible attacks. In black hole attack, attacker replies to each RREQ packet of route discovery with the greatest sequence number that it can. Then source node selects the greatest RREP sequence number and also selects the route contained in that RREP packet. Attacker tries to spoof ID of destination node and by using a high sequence number in RREP, flows all data packets to itself. Gray hole attack is a kind of black hole attack, in which one node occasionally drops packets of a destination. This node sometimes acts like a normal node and sometimes as not normal. Distinguishing of this attack is really harder than black hole attack because of frequently acting normal and frequently malicious.

In the rest of this paper, Section 2 summarizes the basic operation of AODV protocol. In Section 3, we introduce black hole and gray hole attacks with more details. In Section 4, we describe some methods that have proposed for detecting or preventing these attacks. Section 5 comprises the methods and finally, we conclude the paper.

2. AODV ROUTING ALGORITHM
The Ad-hoc On-demand Distance Vector routing protocol [2] is a kind of reactive algorithm. AODV is a simple algorithm which requires less memory than proactive ones. In AODV, source creates route whenever it needs. Route Request (RREQ), Route Reply (RREP), Route Error (RERR) messages are three control packets that are used in AODV. RREQ and RREP are used in route discovery process and RERR is used in maintenance phase.

In route discovery process; first, source sends RREQ packet in the network; each node broadcast this packet to its neighbors until these packets get to destination or to a node with a previous route to destination; after that, source node waits a period of time until receiving all RREP packets. Now, source, first check if it has any entry in its table for that destination, then checks sequence numbers and selects the route with the highest sequence number. If there are more than one RREP packets with the same sequence number, selects the route with the least hop count to destination. In maintenance process, if a link breaks, neighbors of that link broadcast RERR message through the network to alert other nodes about this failure. Maybe some nodes need to reroute again to their destination.

3. BLACK AND GRAY HOLE ATTACKS
Black hole is a kind of active attack. It contains two steps; in first step, attacker spoofed identity of destination that wants to drop its packet. Then, after getting RREQ packet from source node, try reply to that. It then sends RREP that has highest sequence number. In this case, attacker introduces itself as destination or a node that has a route to the destination. In second step, source node initiates a route to destination through the attacker. In this case, source sends data to intermediate node and does not know that this intermediate node is an attacker. Malicious node after receiving data packets drops these packets and doesn't send them to destination.

In gray hole attack, a node that is a member of the network, gets RREQ packets and creates a route to destination. After creating route, it drops some of data packets. This kind of dropping against black hole, does not drop all data packets. Attacker drops

occasionally packets. It means attacker sometimes acts like a normal node and other times as a malicious node [1,2].

4. REVIEW OF THE METHODS

In this section, we review ten different methods for detection and removal of black hole and gray hole attacks.

4.1 First Method

Detection and removing of black/gray hole attacks processes are [3,4]:

- Detection process for black/gray hole attack by source node:
  - Dividing data packets into *k* equal parts.
  - Sending a message to destination containing number of messages.
  - Broadcasting messages to all neighbors of route.
  - After ensuring that destination node knows count of messages, source begins sending of data.
  - Setting up a timer until getting number of data packets that destination receives.
  - If number of announced data packets from destination is less than a limit, initiates removing process of black/gray hole attack.
  - Also if after terminating of timer, did not get any message from destination, starts removing process of black/gray hole attack.

- Detection process for black/gray hole attack by destination node:

After knowing the number of data packets that are sent from source node, setting a timer to zero and starts counting data packets. After a timeout, returns data packet numbers to source node.

- Detection process for black/gray hole attack by neighborhood nodes:

By getting monitoring message from source node, each node starts a counter for counting number of data packets of its neighbors.

- Remove process for black/gray hole attack by source node:
  - Source node gets vote of one node's neighbors about the maliciousness.
  - According to the votes of neighbors, starts counter for malicious node in FindMalicious table.
  - If votes of neighbors about maliciousness exceeds from a limit, source enters that node in Gray/Black hole table and finds a new route to destination. Also announces to the network that node is a malicious one.

- Remove process for black/gray hole attack by neighbor nodes:

When they get monitoring message, they start counting numbers of packets that malicious node sends. If number of passed messages is less than a limit, inform about it to source node.

4.1.1 Advantages

- Using a limit for identifying malicious nodes, decreases number of mistakes in identifying black/gray hole attack. This threshold is the probability of packet dropped by a node through no fault of its own. Packet dropping may occur due to overhead, lack of CPU cycles, buffer space or bandwidth, congestion or collusion to forward packets.
- This method can detect both black and gray hole attacks and also can detect selfish node.

4.1.2 Disadvantages

- In this method, all nodes should always monitor each other; in this case, the network has a high overhead and also each node consumes a lot of energy for monitoring.
- Detection speed for malicious nodes is low, a lot of data lost until malicious node can be detected.

4.2 Second Method

In [5] by using watchdog timer, malicious node can be detected. Each node monitors its next node in the route. If it finds any packet forwarding misbehavior or any packet dropping in a predefined period of time for its next node, it will introduce the next node as a malicious node to the source.

4.2.1 Advantages

- This is a simple method, so that one node should just listen to its next node in the route.

4.2.2 Disadvantages

- In watchdog, each node should always monitor its next neighbors.
- Source node should trust the other node's information about one node's misbehavior.
- It does not use predefined limit to distinguish malicious nodes and as previously mentioned it increases numbers of mistakes to find black/gray hole attacks.

4.3 Third Method

SCAN [6] uses two ideas to protect AODV in MANET: Local collaboration and information cross-validation.

- Local collaboration, nodes monitor each other and also sustain routing tables of each other. Each node uses a token that authenticates itself to the network. If one node is suspected to be malicious, other nodes revoke its token and alert token revocation to all nodes in network and they insert that node in their token revocation list. So, the malicious node does not have any access to the network.
- Information cross-validation, each node checks routing packets comes from its neighbors. Each node knows neighbors' routing tables, can cross-check the overheard transmissions of them. Figure1 shows this action, node M uses routing tables of X and Y, if X or Y announces a new fault routing update, M compares routing tables of two neighbors and if any misbehavior found, announces that node as malicious to the network and revokes its token.

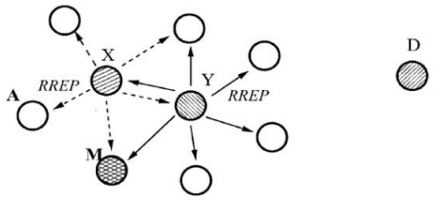

Fig 1: Cross-checking routing updates of neighbors [6].

4.3.1 Advantages

- Each node uses a token which authenticates the node to the whole network. Without a valid token, a node cannot participate in the network and using token to some extend enhances the security of network.

4.3.2 Disadvantages

- Due to mobility of nodes, routing tables change and mistakes in finding malicious nodes will be increased. Also this method needs renewal of table entry of neighbors in certain period of time.
- If there is not any neighbor that can cross-checks the route, this method does not work.

4.4 Forth Method

In [7] there are some additional nodes, strong nodes, which help source and destination to find black and gray hole attacks. These nodes are assumed to be trustful and also capable of tuning its antenna to large ranges as well as short ranges. Each normal node is within the range of one of these strong nodes. With the help of the strong nodes, the source and the destination nodes start an end-to-end checking and can understand whether the data packets have reached the destination or not. If any differences found in number of messages sent from source and received in destination, strong nodes ask the nodes in their areas about the monitoring results of one node's behavior. If the checking results show misbehavior according to the votes, then the backbone network runs a protocol which can detect black or gray hole attack. At the end announces malicious node to the network by broadcasting messages.

4.4.1 Advantages

- Strong nodes decrease the number of monitoring of neighbors, just nodes in particular area of malicious node start monitoring.

4.4.2 Disadvantages

- Differentiate between signal strength of strong and normal nodes in the network, makes this method unsuitable for MANET.
- This algorithm assumes that strong nodes are trustable, but there is no solution considered for attacks.
- There is no limit for detection of maliciousness of one node that increases mistakes to distinguish between normal and strong nodes.

4.5 Fifth Method

Main idea of [9] is using of Merkle tree. 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. Figure 2 shows this process in one Merkle tree.

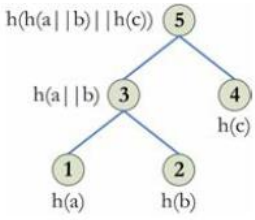

Fig 2: Merkle tree example [9].

For detecting black hole attack, each node contains a hash which is combination of node's 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. The procedure of checking hash values is showed in figure 3. In this figure, 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 method can also find cooperative black hole attacks.

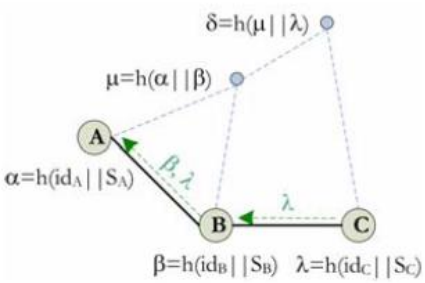

Fig 3: Black hole detection process [9].

4.5.1 Advantages

- In this method all nodes do not monitor each other so a lot of energy is not consumed for monitoring.
- Detecting cooperative black hole attacks is another benefit of this scheme.

4.5.2 .Disadvantages

- If a secure constant value is considered for hash, malicious nodes in the path after a time period can drop packets easily and do not send them to destination, because its hash is constant and does not have any guarantee for detecting attacks.
- This method does not refer to how source node first gathers concatenated hash value of all route values.
- If calculation process of hash is performed all the time, the huge overhead is created.

4.6 Sixth Method

This method [10] uses intrusion detection system (IDS) nodes that protect network from black hole attacks. Each IDS node covers an area of the network that monitors it. Figure 4 shows the coverage area with different numbers of IDS nodes. Different number of IDS affects the coverage area and also detection range for black hole attacks.

Three assumptions are considered in this algorithm:

- IDS nodes are in each other range that can exchange BLOCK messages for detecting black hole messages.
- Authentication mechanism is considered between IDS nodes, so that one IDS node cannot change or drop BLOCK messages.
- Each IDS should overhear its area's routing messages.

- IDS node's actions for RREQ, RREP packets:
  - RREQ: first IDS checks if there is an entry in its table for source and destination. Then IDS adds source, destination and all of the broadcasting nodes in its table. These broadcasting nodes' ID are used for detection of black hole attack.
  - RREP: IDS checks if sender is destination or not. If the answer is yes, it stops checking for black hole attack. If the answer is no, it checks if there is an entry for this node in its table as broadcasting node or not. If it is not a previous broadcasting node starts a counter and named that node as inactive. If its maliciousness exceeds from a predefined value, marks that node as active and sends messages to network that called BLOCK and announces malicious node.

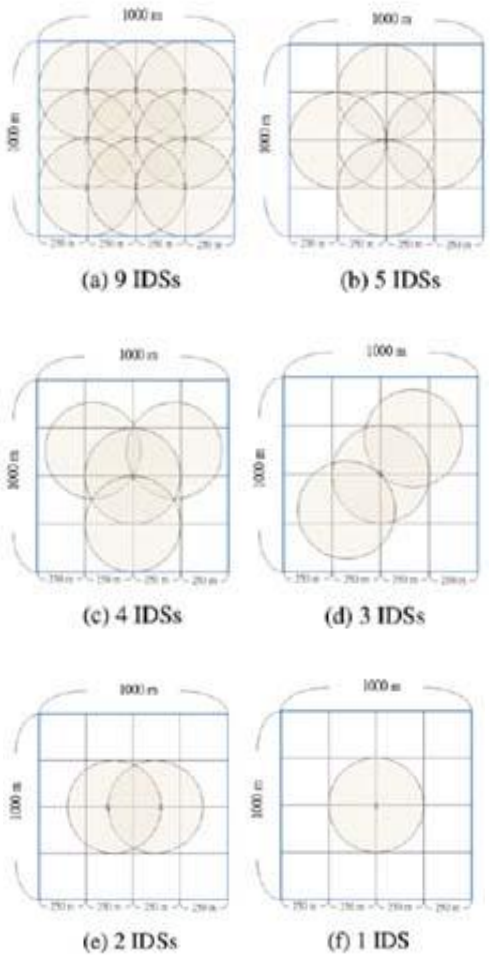

Fig 4: Different number of IDS used for coverage an area [10].

4.6.1 Advantages

- This method uses new nodes called IDS. This usage has two benefits. First, trustfulness of these nodes that makes reporting of black hole attacks more trustable. Second, decreasing overhead for monitoring on all nodes as special nodes just monitor the network.
- Considering a limit for detecting black hole attacks decreases mistakes for detecting malicious nodes and also numbers of BLOCK messages in the network.

4.6.2 Disadvantages

- This system needs some active and constant nodes that always monitor the network. So, these features may make it not very applicable for all MANETs.
- The scheme can only detect black hole attacks not gray hole attack.

4.7 Seventh Method

[11,13] use Data Routing Information (DRI) table for each node that has two fields named 'from' and 'through'. 'From' means that from this node gets a routing message and 'through' means that from current node sends a message to that node or not.

In this method, first, source tries to find a route from source to destination. Source sends RREQ packets to destination. If destination sends back RREP, source trusts to its answer. 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. The same process is done on the next node until source receives a DRI table of a trustable node and then stops this process and just checks DRI table of both neighbor nodes to find maliciousness by checking 'from' and 'through' field of them. If source finds any differences in two neighbors' DRI tables announces all the nodes in the network about maliciousness.

4.7.1 Advantages

- This method finds any cooperative black hole attacks.

4.7.2 Disadvantages

- If there is not any attack in the network, this scheme works very slowly and has a huge overhead for checking all nodes in a route.
- This method does not have any defense against gray hole attack.

4.8 Eighth Method

This method [12] is an extension similar to watchdog design. It categorizes nodes into two groups called trusted and ordinary. Trusted nodes are previously proved their trustfulness to other nodes. Watchdog nodes that monitor the network are selected from these trusted nodes.

Watchdog nodes are selected according to some other criteria such as: energy of each node, enough storage memory and node calculating power. Watchdog tasks exchange between trusted nodes after a period of time. In each watchdog two limit values and counters are considered, ACCEPTANCE threshold and SUSPECT threshold. ACCEPTANCE threshold is a limit that once correct packet sending of one node exceeds it, that node enters in trusted nodes. SUSPECT threshold is used to count maliciousness of one node for packet dropping and after

exceeding that limit, that node enters in malicious nodes and announces that as a black hole node to the network.

4.8.1 Advantages

- Selecting some trusted nodes for monitoring decreases monitoring overhead on all the nodes and also just some special trusted nodes monitor other nodes in network.
- Assuming a limit for maliciousness of a node and entering that node in black hole list, is a reason of decreasing detection mistakes in this method.
- This method also can distinguish cooperative black hole attacks.

4.8.2 Disadvantages

- In this method, if trusted nodes start maliciousness treat and drop packets, like gray hole attack, security of the network is missed and this attack cannot be detected.

4.9 Ninth Method

Another algorithm is considering a limit for sequence number in [8,14]. When source node receives RREP packets, it checks them with a threshold for sequence number of that route and if the received RREP sequence number is higher than that, source enters that node ID in a blocked list and announces that node as malicious to all nodes by broadcasting its ID; because in black hole, attacker starts dropping packets by announcing itself as a node has the freshest route to destination. This sequence number threshold is calculated by average of table's entries sequence numbers in a certain period of time.

4.9.1 Advantages

- Main benefit of this method is simplicity.
- On the contrary of other methods, no energy is consumed for monitoring.

4.9.2 Disadvantages

- This algorithm does not detect any gray hole attacks.
- This method may also make mistake when a node is not malicious, but according to its higher sequence number may be entered into blocked list.

4.10 Tenth Method

The method that introduced in [15] detect malicious nodes in four steps:

- Data collection of neighbors: each node gathers all neighbors' information and enters in its DRI table. If there is a neighbor node in its table with fields of from and through filled with zero, assumes that is a malicious node.
- Local anomaly detection: source selects a Cooperative Node (CN). This is a node with both DRI fields filled with one and is a trusted node as source previously sent to and received data from it. Source broadcasts RREQ to CN as destination, then source asks from CN if it receives RREQ from malicious node, source removes that node from malicious nodes list because it does not drop RREQ packets. But if CN does not receive RREQ packet from malicious node, source increases its maliciousness.
- Cooperative anomaly detection: for avoiding mistakes of malicious node detection, source sends a cooperative detection request to all neighbors of malicious node. These neighbors once received this request, send RREQ message through that node to source node as destination. That node returns RREP to neighbors. Each of these neighbors also sends a probe packet from malicious node to source and also another packet from another path to announce source about that packet, if source does not get probe packet, until three times of sending probe packets from neighbors does not mark that node as gray hole attack and after three times marks that node as an attacker.
- Global alarm sending: after three previous steps, source announces a node to the network as a gray hole attacker.

4.10.1 Advantages

- This method does not force nodes to monitor each other and also does not consume a lot of energy for this.
- Consider a three times of chance for a node before entering that in blocked list decreases mistakes.

4.10.2 Disadvantages

- Speed of distinguishing a node as a gray hole attack increases and overhead for each malicious node detection is high.

5. COMPARISON OF THE METHODS

In this section, we compare discussed methods by different metrics (Table 1).

Table 1. Table captions should be placed above the table

Metrics / Methods	Detection of black hole attack	Detection of gray hole attack	Detection of cooperative black hole attacks	Mistakes in detection of attacks	Detection of misbehavior in source node	Local detection	Overhead
1)Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks	yes	Yes	No	Few (because of using a limit)	According to votes of neighbors	Yes	Find malicious and gray/black hole tables and overhead of voting from neighbors

2)Mitigating routing misbehavior in mobile ad hoc networks	Yes	Yes	Yes	Many (because it does not consider any limit for packets)	No	Yes	No
3)Network-layer security in mobile ad hoc networks Self-organized	Yes	Yes	No	Many (because it does not consider any limit for packets)	No	Yes	Uses a token for each node
4)Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks	Yes	Yes	Yes	Many (because it does not consider any limit for packets)	No	Yes(by using strong and intermediate nodes)	Strong nodes with stronger signal ratio
5)Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks	Yes	No	Yes	Few (just for black hole attacks)	Yes	No	Calculating hash values in each node
6)Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems	Yes(if the region is under coverage of IDS nodes)	No	Yes	Few(using a limit)	No	Yes	IDS nodes and BOLCKs messages
7)Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks	Yes	No	Yes	many(because it does not consider any limit for packets)	Yes	Yes	DRI tables and request packets for monitoring
8)Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks	Yes	No	Yes	less than watchdog timer	No	Yes	Trusted nodes and control packets for exchanging of data
9)DPRAODV: A dynamic learning system against black hole attack in AODV based MANET	Yes	No	No	Few(using a limit)	Yes	Yes	Sequence number limit
10)A mechanism for detection of gray hole attack in mobile ad hoc networks	Yes	Yes	No	Few(using three times chances)	Yes	both	DRI tables, probe packets

6. CONCLUSION

Black hole and gray hole attacks are the most important security problems in MANET. Black hole starts in route discovery phase and gray hole as an attack which drops packets in transmitting step. Detection of gray hole is more difficult than black hole, because the attacker works as normal node then starts dropping of data. In this paper, we introduced some of the proposed works in detecting black and gray hole attacks, pointed out their advantages and disadvantages and at the end, we compared these methods from some aspects. Most of these algorithms suffer from overload and low speed which is a research area for developing a detection system against these attacks. Protection against both attacks in one detection system and decreasing number of errors in detection can be other topics for developing black and gray hole detection systems.

7. REFRENCES

[1] Biswas, K., and Liakat Ali, M. D. 2007 Security Threats in Mobile Ad Hoc Network. Master Thesis. Thesis no: MCS-2007:07., Blekinge Institute of Technology.

[2] Ullah, I., and Rehman, S. U. 2010 Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols. Master Thesis. Thesis no: MEE-2010-2698., Blekinge Institute of Technology.

[3] Banerjee, S. 2008. Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks, In Proceedings of the World Congress on Engineering and Computer Science.

[4] Jain, S., Jain, M., and Kandwal H. 2010. Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. J. Computer Applications, Vol. 1, No. 7, 37-42.

[5] Marti, S., Giuli, T. J., Lai, K., and Baker, M. 2000. Mitigating routing misbehavior in mobile ad hoc networks, In Proceedings of the 6th Annual International Conference on MOBICOM, Boston, Massachusetts, United States, 255-265.

[6] Yang, H., Shu, J., Meng, X., and Lu, S. 2006. SCAN: Self-organized network-layer security in mobile ad hoc networks, J. IEEE Selected Areas in Comm. Vol. 24, No. 2 (Feb. 2006), 261-273.

[7] Agrawal, P., Ghosh, R. K., and Das, S. K. 2008. Cooperative black and gray hole attacks in mobile ad hoc networks. In Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication, Suwon, Korea, 310-314.

[8] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., and Nemoto, Y. 2007. Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method. J. Network Security. Vol. 5, No. 3 (Nov. 2007), 338–346.

[9] Baadache, and Belmehdi, A. 2010. Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks, J. Comp. Sci. and Info. Security, Vol. 7, No. 1, 10-16.

[10] Su, M. Y. 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. J. Comp. Comm., Vol. 34, 107–117.

[11] Weerasinghe, H., Fu, H. 2008. Preventing cooperative black hole attacks in mobile ad hoc networks, Int. J. of Soft. Eng. and Its App., Vol. 2, No. 3 (Jul. 2008), 39-54.

[12] Patcha, A., and Mishra, A., 2003. Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. In Proceedings of the Radio and Wireless Conference (RWCON), VA, USA, 75-78.

[13] Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, j., and Nygard, K. 2003. Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of the International Conference on Wireless Networks.

[14] Raj, P. N., and Swadas, P. B. 2009. DPRAODV: A dynamic learning system against blaackhole attack in aodv based MANET, J. Comp. Sci. Issues, Vol. 2, 54-59.

[15] Sen, J., Chandra, M.G., Harihara, S.G., Reddy, H., and Balamuralidhar, P. 2007. A mechanism for detection of gray hole attack in mobile ad hoc networks, In Proceedings of the 6th International Conference on Information, Communications & Signal Processing, Singapore, 1-5.