Volume-4, Issue-5, October-2014, ISSN No.: 2250-0758
International Journal of Engineering and Management Research
Available at: www.ijemr.net
Page Number: 31-36

Routing Misbehabiour in Mobile Ad Hoc Network

Ashwani Singh[1], Mohd. Haroon[2], Mohd. Arif[3]
[1,2,3]Research Scholar (CSE), Integral University, Lucknow, UP, India

ABSTRACT

MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. Adhoc Network in the presence of nodes that agree to forward data packets but fail to do so, for example a node become selfish and refuse to forward data packets to other nodes or the node fail to forward data packet to the destination node or because of limited power, a node could enter an inactive state. Where routing itself a core challenge in mobile adhoc network, there are still some threats to the existing traditional routing mechanisms as adopted by mobile ad-hoc network. Our work focuses on to improve the performance of on demand routing algorithm in an ad hoc network in the presence of black hole nodes.

In this work, we will address the question how to enable a system to operate in the presence of misbehaviour (black hole). Here I have proposed a bluff probe approach to detect and prevent black hole attacks in the Mobile Ad-hoc Networks. To achieve this we have simulated the Mobile ad-hoc network scenarios which includes Black Hole node using NS-2.34 Network Simulator program.

Keywords— Mobile Adhoc Network, AODV, Black Hole Attack, SQP, FRREQ

I. INTRODUCTION

Ad-hoc in Latin means “for this”. Mobile ad hoc network may be defined as autonomous system of co-operative mobile hosts connected through wireless links to form communication network without support of existing network [1, 2, 3]. As for the mode of operation, ad-hoc networks are basically peer-to-peer multi-hop mobile wireless networks where information packets are transmitted in a store and forward manner from a source to an arbitrary destination, via intermediate nodes. As the node move, the resulting change in network topology must be made known to the other nodes so that outdated topology information can be updated or removed. In MANET nodes are free to move arbitrarily with different speeds thus, the network topology may change randomly and at unpredictable times. There are currently two variations of mobile wireless networks infrastructure and infrastructure less networks.

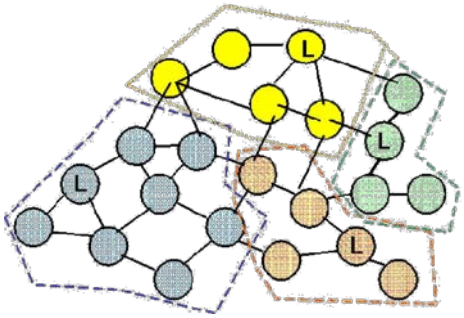


Fig. 1.1
Ccommunication between mobile nodes in Mobile Ad-hoc Network

These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move at will relative to each other. In this type of network, some pairs of terminals may not be able to communicate directly to with each other and relaying of some messages is required so that they are delivered to their destinations. The nodes of these networks also function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices.

***1.1 Characteristics of MANET*:**

Dynamic Topologies: Since nodes are free to move arbitrarily, the network topology may change randomly and rapidly at unpredictable times. The links may be unidirectional bidirectional.

Bandwidth constrained, variable capacity links: Wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple access, fading, noise, and interference conditions etc. the wireless links have low throughput.

Energy constrained operation: Some or all of the nodes in a MANET may rely on batteries. In this scenario, the most important system design criteria for optimization may be energy conservation.

Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping,

spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit the decentralized nature of network control in MANET provides additional robustness against the single points of failure of more centralized approaches

1.2 On Demand Distance Vector (AODV) Protocol

AODV is described in RFC 3561 [4]. AODV belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbours and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbours periodically its whole routing table. So they can check if there is a useful route to another node using this neighbour as next hop. When a link breaks a Count-To-Infinity could happen. AODV is an 'on demand routing protocol' with small delay. That means that routes are only established when needed to reduce traffic overhead. AODV supports Unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently. To characterize the AODV with the five criteria used is distributed, hop-by-hop, deterministic, single path and state dependent.

AODV uses IP in a special way. It treats an IP address just as an unique identifier. This can easily be done with setting the Subnet mask to 255.255.255.255 . But also aggregated networks are supported. They are implemented as subnets. Only one router in each of them is responsible to operate the AODV for the whole subnet and serves as a default gateway. It has to maintain a sequence number for the whole subnet and to forward every package. In AODV the routing table is expanded by a sequence number to every destination and by time to live for every entry. It is also expanded by routing flags, the interface, a list of precursors and for outdated routes the last hop count is stored.It's reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network. There are three types of control messages in AODV which are discussed bellow.

Route Request Message (RREQ):

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP):

A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

Route Error Message (RERR):

Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

1.3 Black Hole Attack

To carry out a black hole attack, malicious node waits for neighbouring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. 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 over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole akin to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack. Black hole attack affects the whole network.

II. RELATED WORK

H. Deng et.al [5] proposed a solution to cope with the black hole attack in AODV. First, they suggest disabling the ability of an intermediate node to send a RREP and allow only the final destination to do that. This technique avoids the black hole problem but increases the route establishment delay, especially in the case of large networks. Furthermore, since no authentication is used in RREP message a smart attacker can forge a RREP message on behalf of the legitimate destination (by spoofing its IP address). As such, this solution is inappropriate for coping with this attack.

To overcome these shortcomings, they have proposed another solution which requires that the intermediate node adds its next hop's information to the RREP packet before sending it. On receiving this packet, the source node sends a special packet (Further Req) to the next hop of the intermediate node in order to verify that it has a route to the destination and also it is a neighbour of the intermediate node. This special packet contains a field dubbed check result which might be filled by the next hop node. When the source node receives the reply (Further Rep) to this packet it extracts the check result information and decide accordingly whether this route is safe or not. If so, it sends out the data packets, otherwise it initiates a new route discovery or waits for subsequent RREPs. While this solution can avoid the black hole attack launched by a single node, it is unable to detect a collusive attack conducted by both of intermediate and next hop nodes. Moreover, its main disadvantage is the induced overhead if the check process is repeated for each intermediate node replying to the RREQ.

Al-Shurman et.al. [6] Proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared

hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive.

Satoshi Kurosawa et. al. [7] uses an anomaly detection scheme. It uses dynamic training method in which the training data is updated at regular time intervals. Multidimensional feature vector is defined to express state of the network at each node. Each dimension is counted on every time slot. It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They calculate mean vector by calculating some mathematical calculation. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack. The updated data set to be used for next detection. Repeating this for time interval T anomaly detection is performed.

Latha Tamilselvan et. al. [8] proposed a better solution with the modification of the AODV protocol, which avoids multiple black holes in the group. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 values is considered as malicious node and is eliminated from the network. The fidelity levels of nodes are updated based on their trusted participation in the network. Upon receiving the data packets, the destination node will send an acknowledgement to the source; thereby the intermediate node's level will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented. The main drawback of this solution is processing delay in the network.

Zhao Min et.al [9] has discussed an authentication mechanism for identifying black hole nodes in MANETs. An authentication mechanism is constructed based on the concept of the hash function, MAC, and PRF, which is used for checking the RREPs at source node to send the data packets. The proposed mechanism eliminates the need for a PKI or other forms of authentication infrastructure, however it needs to be discuses, how to handle unlimited message authentication by switching one-way-hash chains and how to prevent a malicious node cannot forge a reply if the hash key of any node is to be disclosed to all nodes.

XiaoYang Zhang et.al. [10] Introduced a new detection method based on checking the sequence number in the Route Reply packets by making use of a new message originated by the destination. In this method, when an .intermediate node unicasts a RREP packet, the node also unicasts a newly defined control message to the destination node to request for the up-to-date SN. Upon receiving, the destination node unicasts a reply message to inform the source node of the up-to-date SN. This reply from the destination node enables the source node to verify if the intermediate node has sent a faked RREP message by checking if the SN in the RREP message is larger than the up-to-date SN. This method has more network overhead and time delay since node in the network generates new packets.

Payal N. Raj et. al. [11] modifies the behaviour of AODV to include a mechanism for checking the sequence number of the received RREP. As the source node receives the RREP it compares the sequence number of the received RREP to a threshold value. The replying node is suspected to be a black hole if its sequence number is greater than the threshold value. The source node adds the suspected node to its black list, and propagates a control message called an alarm to publicize the black list for its neighbours. The threshold is the computed average of the difference between the destination sequence number in the routing table and the destination sequence number in the RREP within certain periods of time. The main advantage of this protocol is that the source node announces the black hole to its neighbours in order to be ignored and eliminated.

Alem, Y.F et.al. [12] Proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent attacks by the both single and multiple black hole nodes. IDAD assumes every activity of a user can be monitored and anomaly activities of an intruder can be identified from normal activities. To find a black hole node IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data collected and it is given to the IDAD system, which is able to compare every activity with audit data. If any activity of a node is out of the activity listed in the audit data, the IDAD system isolates the particular node from the network. The reduction of the number of routing packets in turn minimizes network overhead and facilitates a faster communication.

Ming-Yang et. al [13] proposed an intrusion detection system called Anti-Blackhole Mechanism (ABM) in which the suspicious value of a node is estimated according to the amount of abnormal difference between RREQs and RREPs transmitted from the node; all nodes perform ABM. With the requirement that intermediate nodes are prohibited to reply to RREQs, if an intermediate node is not the destination and never broadcasts RREQ for a specific route, but forward a RREP for the route, then its suspicious value will be increased in the nearby node's suspicious node table. When the suspicious value of a node goes beyond threshold, a Block message is broadcasted by the node to all other nodes in the network to isolate the suspicious node cooperatively. Though, the solution assumes that an authentication mechanism already exists in MANET.

Lalit Himral et.al [14] have proposed method to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely it is from the malicious node, immediately remove that entry from the RR-Table. The proposed method cannot find multiple black hole nodes.

III. PROPOSED WORK

In our proposed approach we introduced two new special packets.

- *Special Query Packet.*

➢ *Further Route Request Packet (FRREQ)*

3.1 Further Route Request Packet (FRREQ)

Further Route Request (FRREQ) is slightly different from RREQ packet of standard AODV protocol.

- In place of destination address we place an address of a hypothetical node, which actually not exists in the network.
- FRREQ packet also contains a random number in place destination sequence number field.
- During the route discovery phase, once the RREQ packet is broadcasted by the source node, one or more RREP packet (also containing the information of next hop node in case of intermediate node) is generated by either intermediate nodes or destination node itself.
- Unlike AODV protocol, we store all these reply into the Cmg_RREP_Tab table at source node.
- As soon as a source node receive the very first reply (RREP) packet, it assume to be comes from a malicious node and to make a confirmation about the node behaviour, a mechanism is proposed as follows-
- The Source node unicast a Special Query Packet (SQP) to the next node of the very first replying intermediate node in order to verify that it has a route to the destination and also it is a neighbor of the intermediate node.

3.2 Special Query Packet (SQP)

Special Query Packet (SQP) contains two queries-

A Whether node has a route to destination??

B Whether node is a neighbor of the intermediate node (Replying node)??

- This special packet contains a field dubbed check result which might be filled by the next hop node.
- When the source node receives the reply to this packet it extracts the check result information and decide accordingly whether this route is safe or not.
- If the answer for the anyone of the query is 'NO', then it is sure that the replying intermediate node is a black-hole node but if the both answer is 'YES' then there might be a possibility of collusive attack (Black-hole attack performed by cooperation of the node and its next hope).
- To detect a collusive attack we introduced another control packet i.e. Further route request packet (FRREQ).
- So Source node unicast a Further Route Request Bluff RREQ (**packet having similar packet format as in basic AODV, but the source node placed a destination address of a non-existing destination node**) to the next hope of replying intermediate node.
- Upon receiving this Bluff RREQ packet the suspect node either reply or simply forward the packet to its next hope as per of basic AODV mechanism.
- If a reply RREP is generated and arrived to the source, then the replying node surely a black hole node just because it reply to claim that it has a shortest and fresh enough route of a destination that is not exist within a network.
- Else, the replying node is a legitimate node.

TABLE 1: A TABULAR REPRESENTATION OF VARIOUS CONCLUSIONS THAT OUR ALGORITHM DERIVED

CASE	SQP FIRST OUTCOME?	SQP SECOND OUTCOME?	NEED TO CHECK FOR COLLUSIVE ATTACK?	FRREQ REPLY ARRIVED ?	CONCLUSION
1	YES	YES	YES	NO	NO BLACK HOLE ATTACK
2	YES	YES	YES	YES	EXISTS A COLLUSIVE ATTACK
3	NO	NO	NO	N/A	ONLY REPLYING NODE IS BLACK HOLE
4	YES	NO	NO	N/A	ONLY REPLYING NODE IS BLACK HOLE
5	NO	YES	NO	N/A	ONLY REPLYING NODE IS BLACK HOLE

IV. SIMULATION RESULT AND ANALYSIS

We have proposed a bluff probe approach to detect and prevent black hole attacks in the Mobile Ad-hoc Networks. To achieve this we have simulated the Mobile ad-hoc network scenarios which includes Black Hole node using NS-2.34 Network Simulator [15] program. To simulate the Black Hole node in a wireless ad-hoc network we have implemented a new protocol that drops data packets after attracting them to itself.

In [16] Implementation of a New MANET Unicast Routing Protocol in NS-2 is described. To implement our contribution we have used the details explained in this thesis.

At the physical and data link layer, we used the IEEE 802.11 algorithm. The channel used is Wireless Channel with Two Ray Ground radio propagation model. At the network layer, we use AODV as the routing algorithm. Finally, UDP is used at the transport layer. All the data packets are CBR (continuous bit rate) packets. The size of the packet is 512 bytes. The packets transmission rate is 0.2 Mbps. The connection pattern is generated using *cbrgen* and the mobility model is generated using *setdest utility*. *Setdest* generates random positions of the nodes in the network with specified mobility and pause time.

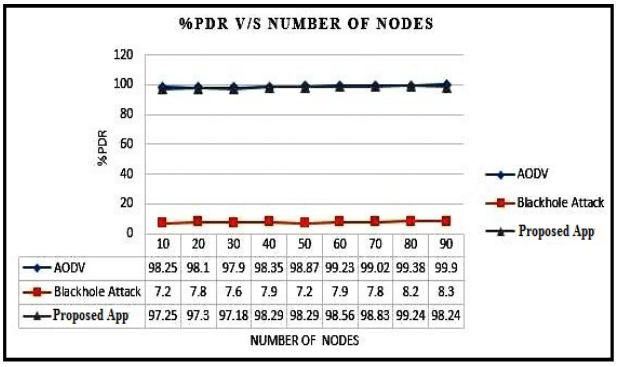
TABLE 2: A tabular representation of Simulation Parameter

PARAMETER	VALUE
Simulator	Ns-2 (ver. 2.34)
Simulation Time	21 s
Number of nodes	10 to 90
Routing Protocol	AODV
Traffic Agent	TCP
Pause Time	2 s
Mobility	10 – 90 m/s
Terrain area	850m × 501 m
Transmission Range	250 m
Type of Attack	Black hole attack

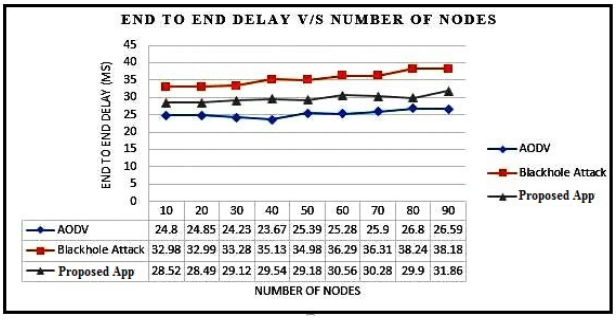
Each data point represents an average of ten runs. The same connection pattern and mobility model is used in simulations to maintain the uniformity across the protocols. The metrics used to evaluate the performance of these contexts are given below.

- **Packet Delivery Ratio:** The ratio between number of packets received by the CBR sink at the final destination and the numbers of packets originated by the "application layer" CBR sources.
- **Average End-to-End Delay:** This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc. It is measured in milliseconds.
- **Throughput:** Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

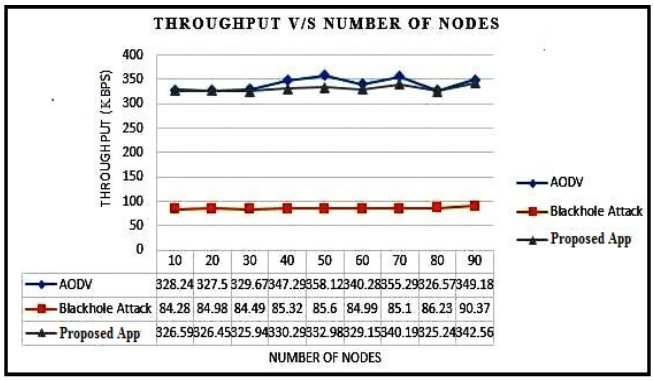
4.1 Results



	10	20	30	40	50	60	70	80	90
AODV	98.25	98.1	97.9	98.35	98.87	99.23	99.02	99.38	99.9
Blackhole Attack	7.2	7.8	7.6	7.9	7.2	7.9	7.8	8.2	8.3
Proposed App	97.25	97.3	97.18	98.29	98.29	98.56	98.83	99.24	98.24



	10	20	30	40	50	60	70	80	90
AODV	24.8	24.85	24.23	23.67	25.39	25.28	25.9	26.8	26.59
Blackhole Attack	32.98	32.99	33.28	35.13	34.98	36.29	36.31	38.24	38.18
Proposed App	28.52	28.49	29.12	29.54	29.18	30.56	30.28	29.9	31.86



	10	20	30	40	50	60	70	80	90
AODV	328.24	327.5	329.67	347.29	358.12	340.28	355.29	326.57	349.18
Blackhole Attack	84.28	84.98	84.49	85.32	85.6	84.99	85.1	86.23	90.37
Proposed App	326.59	326.45	325.94	330.29	332.98	329.15	340.19	325.24	342.56

V. CONCLUSION AND FUTURE WORK

Wireless Ad-Hoc networks are widely used networks due to their flexible nature i.e. easy to deploy regardless of geographic constraints. These networks are exposed to both external and internal attacks as there is not centralized security mechanism. A lot of research work is still need in this area. We tried to discover and analyze the impact of Black Hole attack in MANETs using AODV protocol. There is a need to analyze Black Hole attack in other MANETs routing protocols such as DSR, TORA and GRP. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. They can be categorized on the basis of how much they affect the performance of the network. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack. The detection of this behaviour of Black Hole attack as well as the elimination strategy for such behaviour has to be carried out for further research.

In our thesis, we try to eliminate the Black Hole effect in the network. But detection of the Black Hole Node is another future work. In our work, we assume the black hole node is detected and tried to eliminate its effects. There are many Intrusion Detection Systems (IDS) for ad-hoc networks. These IDSs could be tested to determine which one is the best to detect the Black Hole.

Our solution tries to eliminate the Black Hole effect at the route determination mechanism of the AODV protocol that is carried out before the nodes start the packets. Additionally, we used UDP connection to be able to count the packets at sending and receiving nodes. If we had used the TCP connection between nodes, the sending node would be the end of the connection, since ACK packets do not reach the sending node. This would be another solution for finding the Black Hole Node. This takes place after the

route determination mechanism of the ADOV protocol and finds the route in a much longer period. Our solution finds the path in the AODV level. Finding the black hole node with connection oriented protocols could be another work as a future study.

.

REFERENCES

[1] Hadi SargolZaey, Ayyoub Akbari Moghanjoughi and Sabira Khatun,2009. A Review and Comparison of Reliable Unicast Routing Protocols For Mobile Ad Hoc Networks, International Journal of Computer Science and Network Security,VOL.9 No.1,pp.186-196.

[2] IETF Mobile Adhoc Networks (MANET) Charter http://datatracker.ietf.org /wg/manet/charter/.

[3] J.P. Macker and M.S.Corson,1998. Mobile AdHoc Networking and the IETF.ACM SIGMOBILE Mobile Computing and Communications Reviews, Vol.2, No.1, pp. 9-12.

[4] C. E. Perkins, E. M. Belding-Royer, and S. R. Das,2003 “Ad hoc on-demand distance vector (AODV) routing”, RFC 3561, IETF, MANET working group.

[5] Deng H., Li W. and Agrawal, D.P., "Routing securi ty in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

[6] Mohammad Al-Shurman et. Al” Black Hole Attack in Mobile Ad-Hoc Network” ACMSE’04, Apri l 2-3, 2004, Huntsville, AL, USA .

[7] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipthey, and Yoshiaki Nemoto, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Jtheynal of Network Securi ty, Vol.5, Issue 3, pp: 338–346, 2007

[8] Latha Tamilselvan, V. Sankaranarayanan, “Prevention of Co-operative Black Hole Attack in MANET”, Journal of Networks, Vol 3, No 5, 13-20, May 2008

[9] Zhao Min; Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", Information Engineeri ng and Electronic Commerce, 2009. IEEC '09.International Symposium on, vol., no., pp.26-30, 16-17 May 2009.

[10] XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET," Autonomous Decentralized Systems, 2009. ISADS '09. International Symposium on, vol., no., pp.1-6, 23-25 March 2009.

[11] Payal N. Raj1 and Prashant B. Swadas2, “DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET”, IJCSI International Jtheynal of Computer Science Issues, Vol. 2, 2009.

[12] Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2nd

[13] Ming-Yang Su, “Prevention of Selective Black hole Attacks on Mobile Ad hoc Network through Intrusion Detection Systems”, Computer Communications, 2010. Communications, 2007, pp. 21-26.

[14] Lalit Himral, Vishal Vig, Nagesh Chand, “Preventing AODV Routing Protocol from Black Hole Attack” International Jtheynal of Engineeri ng Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[15] Hoang Lan Nguyen and Uyen Nguyen,2006” Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks”. Proceedings of the International Conference of Networking, International Conference of Mobile Communication and Learning Technologies.

[16] G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006.