International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 1, January- 2013

A New Approach for the Detection of Black hole Nodes in AODV Based Mobile Ad-Hoc Networks

Nisha P John
Mtech Student
Department of CSE, MES College of Engineering Kuttippuram, Kerala, India

Abstract

An ad-hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. Networks are protected using many firewalls and encryption software's. But many of them are not sufficient and effective due to its limited power and mobility. So protecting the mobile ad-hoc network from malicious attacks is very important and challenging issue. In this paper we address the problem of packet forwarding misbehavior and propose a mechanism to detect and remove the black attack using check messages. Also, we simulate the Ad hoc on Demand Vector Routing Protocol (AODV) under blackhole attack by considering different performance metric.

Keywords - MANET, AODV, Black hole attack

I. INTRODUCTION

A mobile ad-hoc network [1] is a self organizing network that consists of mobile nodes that are capable of communicating with each other without the help of fixed infrastructure. On the contrary to traditional wired networks that use copper wire as a communication channel, ad-hoc networks use radio waves to transmit signals. Mobility, an advantage of wireless communication, gives a freedom of moving around while being connected to a network environment. Ad-hoc networks are so flexible that nodes can join and leave a network easily. But this flexibility of mobile nodes results in a dynamic topology that makes it very difficult in developing secure ad-hoc routing protocols. Security being a serious issue, the nature of ad-hoc networks makes them extremely vulnerable to adversarys malicious attacks. First of all, the use of wireless links renders a mobile ad-hoc network to be vulnerable to attacks of various types - black hole attack being one of them [2]. Unlike wired networks where an adversary must gain a physical access to network wires or pass through several lines of defense at firewalls and gateways, attacks on mobile ad-hoc network can come from all directions and target at any node. Compared to traditional wired networks (a network in which network traffic could be monitored at central devices such as switches and routers), mobile ad-hoc networks have no network concentration points to filter traffic.

The use of wireless links, lack of fixed infrastructure and the characteristic of dynamic topology associated with adhoc networks make it impossible to use wired network security mechanism as is.

In the rest of this paper, we summarizes the basic operation of AODV protocol and Black hole attack and describe some methods that have proposed for detecting or preventing these attacks and proposed a new mechanism that effectively prevents the black hole attack and finally, we conclude the paper.

II. AD-HOC ROUTING PROTOCOLS AND BLACK HOLE ATTACK

An ad-hoc routing protocol [3] is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile adhoc network. Being one of the category of ad-hoc routing protocols, on-demand protocols such as AODV (Ad-hoc Ondemand Distance Vector) and DSR (Dynamic Source Routing) establish routes between nodes only when they are required to route data packets.

AODV [4] is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network.

In an ad-hoc network that uses AODV as a routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired destination node. This process is called route discovery. Every neighboring node that receives RREQ broadcast first saves the path the RREQ was transmitted along to its routing table. It subsequently checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQ message. The freshness of a route is indicated by a destination sequence number that is attached to it. If a node finds a fresh enough route, it unicasts an RREP (Route Reply) message back along the saved path to the source node or it re-broadcasts

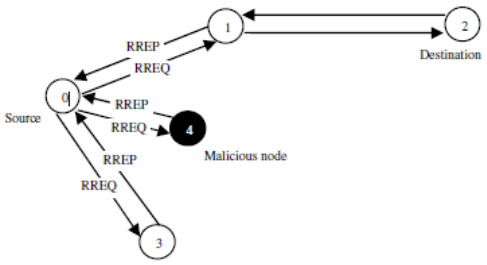

Figure 1. **Black hole attack in AODV**

the RREQ message otherwise. The same process continues until an RREP message from the destination node or an intermediate node that has fresh route to the destination node is received by the source node.

Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, which an adversary can exploit to perform a black hole attack on mobile ad-hoc networks. A malicious node in the network receiving an RREQ message replies to source nodes by sending a fake RREP message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising (by sending a fake RREP to confirm it has a path to a destination node) to source nodes that it will forward data, a malicious node starts to drop all the network traffic it receives from source nodes. This deliberate dropping of packets by a malicious node is what we call a black hole attack [5].

A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As shown in Fig. 1 above, source node 0 broadcasts an RREQ message to discover a route for sending packets to destination node 2. An RREQ broadcast from node 0 is received by neighboring nodes 1, 3 and 4. However, malicious node 4 sends an RREP message immediately without even having a route to destination node 2.

An RREP message from a malicious node [6] is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them.

III. LITERATURE SURVEY

Researchers have proposed various techniques to prevent black hole attack in mobile ad-hoc networks.

H. Weerasinghe and H. Fu [7],introduce the use of DRI (Routing Information) to keep track of past routing information among mobile nodes in the network and cross checking of RREP message from intermediate node by source node.

The main drawback of this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of maintaining their routing table. It is evident that maintaining past routing experiences wastes memory space as well as consuming a significant amount of processing time which contributes to slow communication.

The second drawback is over consumption of limited bandwidth. Cross-checking of the validity of routes contained in RREP message from an intermediate node is implemented by sending a FREQ (Further Request) message to the next-hop of the particular intermediate node. Sending additional FREQ messages consumes a significant amount of bandwidth from an already limited and precious resource. 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.

Kurosawa et al. [8] proposed a dynamic learning method to detect a black hole node. In this approach, the normal state views are updated periodically to adapt to the frequent network changes and clustering-based technique is adopted to identify nodes that deviate from the normal state. It is required to observe if the characteristic change of a node exceeds the threshold within a period of time. If yes, this node is judged as a black hole node, otherwise, the data of the latest observation is added into dataset for dynamic updating purposes. However, it does not involve a detection mode, such as revising the AODV protocol or deploying IDS nodes, thus, it does not isolate black hole nodes. Here adopted anomaly-based detection technique; detecting any deviation from the established normal profile. This technique suffers from a high false-alarm rate especially when the normal behaviour definitions are still unclear and non-standard in wireless ad hoc networks.

P. Raj and P. Swadas [9], proposed an adequate solution by checking RREP messages from intermediate nodes for possible intrusion activities. This technique is successful based on the assumption of cooperation between nodes. If a mobile node discovers a possible attack by an intruder, the discovering node notifies all other nodes the presence of an attack by broadcasting an ALARM message. This process takes a considerable amount of time to notify all nodes for a large network in addition to the network overhead that can be caused by ALARM broadcast. 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.

In [10] authors Alem, Y.F et al.proposed technique intrusion detection using anomaly detection (IDAD) use host base scheme. Network based intrusion detection schema cannot be engaged to MANET where there is no central device that monitor traffic flow, network based intrusion detection system lying on data centric point of a network such as

router and switches but host based intrusion detection system are installed on hosts so that they can oversee the activities of a host and users on the hosts. IDAD assumes every activity of a user or a system can be recognized from normal activities. IDAD needs to be provided with a pre collected set of anomaly activities, called audit data. IDAD system capable to compare every activity of a host with the audit data, if any activity of a host match the activity listed in the audit data, the IDAD system separate the particular node from the network. The drawback of this technique is that, here needs the extra memory to make IDAD system.

In [11] authors Baadache et al. proposed a method to defeat the effect of Black hole attack and this is based on Merkle tree which requires hashing technique to detect the malicious node in the network. For detecting black hole attack, each node contains a hash which is combination of nodes id and a secure value that only the node knows. Source node has concatenation of all hashes of one route to destination in its memory. Each node sends concatenation of its hash and previous nodes in route with RREP packet from destination to source. Source node compares this value with prior saved hash value of this route in its memory and if any differences found, it then informs other nodes about maliciousness of this route. Difference between saved value and new value shows that one node may drops RREQ packets and does not send packets to destination that does not have correct value.

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.

In [13] Authors Ming-Yang Su et.al discussed a mechanism, called an ABM (Anti-Black hole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds a threshold level, the nearby IDS broadcasted a block message with id of IDS, the identified black hole node and the time of identification will place the malicious nodes on their blacklists to isolate the malicious node in the network cooperatively. The advantage of this method is that it can be able to detect cooperative black hole nodes in the MANETs. The main drawback of this technique is that mobile nodes have to maintain an extra database for training data and its updations, in addition to the maintenance of their routing table. 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.

To defend against the black hole attack and to overcome the disadvantage listed above, we proposed a new black hole detection method based on the AODV routing protocol to make it more secure routing protocol.

IV. THE PROPOSED SCHEME FOR BLACK HOLE DETECTION

This proposed system presents a mechanism that prevents the black hole attack without using any special intrusion detection systems. Here an Anti-Blackhole mechanism is performed in each and every mobile nodes, ie each node keeps the required information for monitoring the other node for finding the secure route between source and destination. Self protection principle is used since each node is responsible for protecting itself. The Anti-Blackhole Mechanism is mainly used to find a secure route between source and destination using check messages. After detecting the black hole node and the malicious node ID is added to the Block table and send out a BLOCK message to whole network to isolate the malicious node. Whenever a route reply is coming from a node, it will check its own block table, if it finds the node id in the table, source node will discard that RREP; otherwise the source node stores the RREP in RR(Request Reply) table and the process is repeated until the time exceeds, then performs the antiblack hole mechanism. Thus we avoid black hole problem & also prevents the network from further malicious behaviour. Flowchart for the Antiblack hole mechanism is shown in Fig. 2.

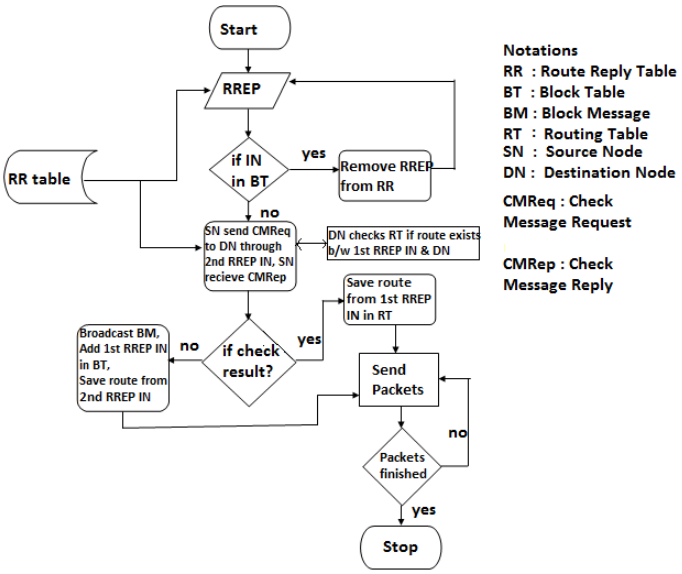

Figure 2. **Flowchart for Antiblack hole mechanism**

AntiBlackhole Mechanism: Our scheme requires only two types of additional control messages, and does not

entail extraneous overhead, for example, operating in promiscuous mode. Since the malicious node(MN) does not have to check its routing table to reply to the route request, the reply from the malicious node will be faster than the reply from a normal node. After a while second RREP message come to source node from the real destination node(DN). Source node(SN) send an additional check message request (CMRq) to the 2nd RREP'ed intermediate node(IN) towards the destination to check whether the route from the 1st RREP'ed IN to the DN exists or not. Then, after receiving CMRq, the destination node looks up its cache for a route to the 1st RREP'ed IN. If it has one, it sends CREP to the source with its route information. When the source node receives the CheckMessageReply (CMRp) from the 2nd RREP'ed IN, it extracts the check result from the reply packets. If the result is yes, then there exists a valid route between 1st RREP IN to DN, so we establish a route to the destination and begin to send out data packets. If the result has no route through the 1st IN, we discard the reply packet from the 1st RREP'ed IN, and use the new route through the 2nd RREP'ed IN to the destination. At the same time, send out the block message to whole network to isolate the malicious node. Thus we avoid the black hole problem, and also prevent the network from further malicious behavior. The proposed solution is explained with an example diagram shown in Fig. 3.

Assumptions

- First RREP message received by source node would normally come from malicious node [14].
- An authentication mechanism exists in MANETs [15], wherein, block messages and check messages sent by Source or Destination node, cannot be modified or counterfeited.
- Nodes are located within each others transmission range in order to forward Block messages to each other.

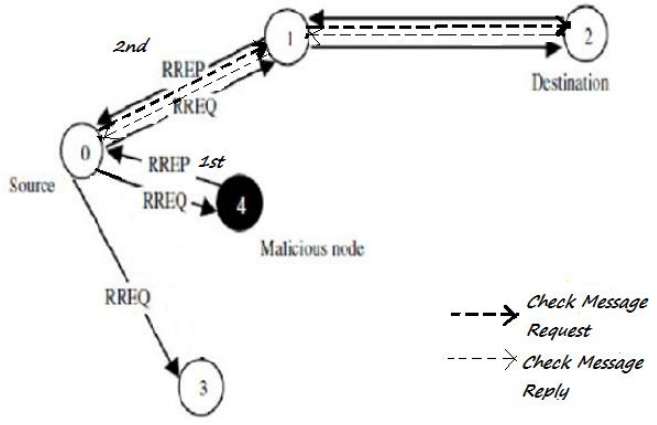

Figure 3. **Solution to Black hole**

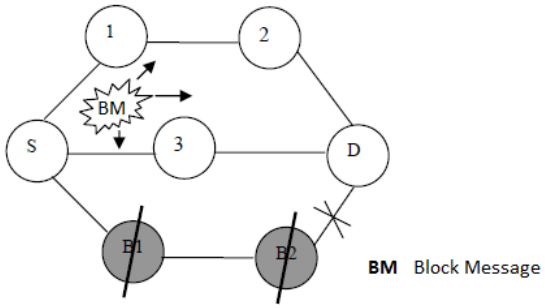

Figure 4. **Block message broadcasting**

The Fig. 4 shows the BLOCK message broadcasting. After detecting the black hole, a block message is broadcasted to its neighbours. Fig. 5 shows the BLOCK table, it contains the fields Detection node ie the node that detects the black hole, Malicious node id and Time of Detection.

The main benefits of proposed solution are: (1) Lower Detection time since the black hole is detected at the beginning stage itself and immediately removed so that it cannot take part in further process and the routing table and the control messages from the malicious node, too, are not forwarded in the network. (2) With no delay the malicious node are easily identified (3) less memory overhead occurs because only few new things are added. (4) Less expensive as there are no special nodes used for monitoring. (5) Continuous replies from the malicious node are blocked, results in less Routing overhead. (6) Generally the malicious node has the highest Destination Sequence number and it is the first RREP to arrive. So the antiblack hole mechanism is made only to the first entry in the table without checking other entries in the RR table. (7) Even though our protocol introduces additional control packets (CMRq and CMRp), extra control messages are kept minimal.

Detection Node	Malicious node	Time
1	1	2012/10/19 12:51
3	6	2012/10/19 12:55

Figure 5. **BLOCK Table**

V. SIMULATION RESULTS

The experiments for the evaluation of the scheme that validate the detection and isolation efficiency of the proposed scheme against black hole nodes have been carried out using the network simulator ns-2 with Linux back-Ground.

The simulations consist of 50 nodes evolving in a region of (1000 m) during 100 seconds. Transmission range is set to 250 meters. Random waypoint movement model[16] is used and maximum movement speed is 20m/s. Packets among the nodes are transmitted with constant bit rate (CBR) of one packet per second, and the size of each packet is 512 bytes.

In these simulations, we used three evaluation metrics. Performance comparison is made on the basis of these three following metrics between existing AODV and proposed AODV.

A. Packet delivery ratio (PDR): PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. This metric shows the reliability of data packet delivery. It is clear from Fig. 6 that PDR of AODV is heavily affected by the malicious nodes where as the PDR of Proposed AODV is immune to it. This graph confirms that while proposed AODV is secure against blackholes, AODV is not.

This is mainly due to the fact that our protocol detects the attacker and allows the source nodes to avoid it. By avoiding the attacker, our protocol finds shortest paths, and so, delivers more packets. On the other hand, the PDR decreases in the case of AODV that is subject to an attack. This is due to the fact that the number of correctly received packet is very less than the number of transmitted packets. Indeed, with the increase of the source nodes, the probability of intrusion increases, and the malicious node absorbs all the data packets passing through it.

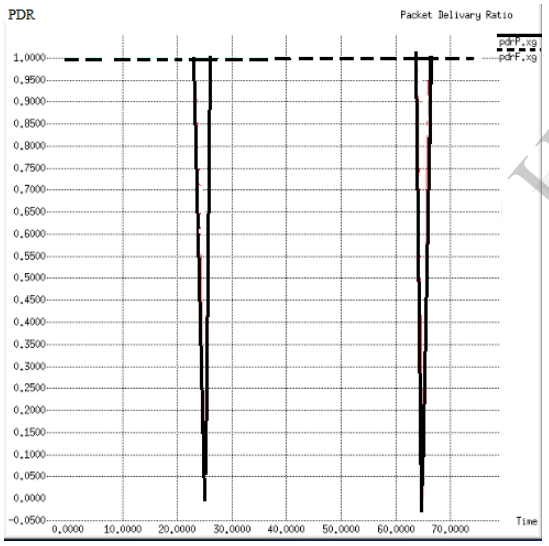

Figure 6. **Packet Delivery ratio vs Time**

B. Packet Loss: This metric informs us about the amount of control packets fails to reach its destination in a timely manner. Clearly, the percentage of packets dropped increases as both the speed and the number of nodes increases. As speed increases, the position of a node will clearly change more rapidly. A source node will still use the last route it has for a destination (if it didnt expire yet), but due to the fast mobility pattern, this route will frequently be invalid which causes the packet to be dropped. This will cause more and more packets to time out before reaching their destinations. This was also noticed in our simulation as shown in the Fig. 7. The graph concludes that there is very less packet lost percentile in the proposed AODV as compared to the AODV.

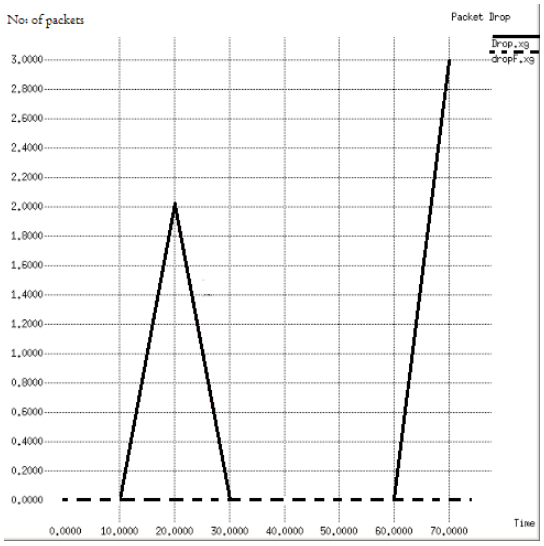

Figure 7. **Packet loss vs Time**

C. Throughput: Throughput is the average rate of successful message delivery over a communication channel. This gives the fraction of the channel capacity used for data transmission. The graph for Throughput is shown in Fig. 8. It shows there is a high throughput in the case of antiblack hole mechanism than normal mechanism under black hole attack.

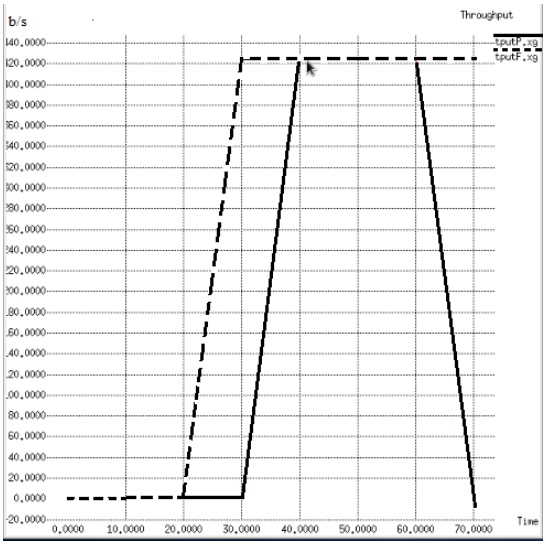

Figure 8. **Throughput vs Time**

From the results we can measure the performance of the secure routing protocol. As we have nullified the effect of black hole in the network, the performance of the network is improved. Figure 6, 7 and 8 shows the graphs which are generated by implementing our solution for black hole attack in ad hoc network. The graphs show that we have improved the packet loss, packet delivery ratio, and throughput of the network. As our solution generates a BLOCK message, there is a slight increase in Normalized Routing Overhead with almost same Delay as normal AODV.

VI. CONCLUSION AND FUTURE SCOPE

In this paper, we have studied the routing security issues of MANETs, described the black hole attack that can be mounted against a MANET, and proposed a feasible solution for it on the top of AODV protocol to avoid the black hole attack, and also prevented the network form further malicious behavior. We have simulated the proposed scheme and analyzed its results. Our solution increases PDR, throughput with less Packet drop and normalized Routing Overhead.

As future work, we intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and also focusing on resolving the problem of co-operative black hole attacks against AODV. We also plan to study the impact of GRAY hole nodes (nodes which switch from good nodes to black hole nodes) and techniques for their identification.

ACKNOWLEDGEMENTS

The authors wish to thank the reviewers and the editors for their valuable suggestions and comments that helped improve the paper.

REFERENCES

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE, vol. 11, no. 1, pp. 38–47, 2004.

[2] P. Goyal, S. Batra, and A. Singh. A literature review of security attack in mobile ad-hoc networks. International Journal of Computer Applications IJCA, 9(12):24–28, 2010.

[3] M. Abolhasan, T. Wysocki, and E. Dutkiewicz. A review of routing protocols for mobile ad hoc networks. Ad hoc networks,
2(1):1–22, 2004.

[4] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on. IEEE, 1999, pp. 90–100.

[5] G. Sandhu and M. Dasgupta. Impact of blackhole attack in manet. International J. of Recent Trends in Engineering and Technology, 3(2), 2010.

[6] EO Ochola and MM Eloff. A review of black hole attack on aodv routing in manet. 2011.

[7] H. Weerasinghe and H. Fu. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In Future generation communication and networking (fgcn 2007), volume 2, pages 362–367. IEEE, 2007.

[8] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato. A dynamic anomaly detection scheme for aodv-based mobile ad hoc networks. Vehicular Technology, IEEE Transactions on, 58(5):2471 –2481, jun 2009.

[9] P.N. Raj and P.B. Swadas. Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. Arxiv preprint arXiv:0909.2371, 2009.

[10] Y.F. Alem and Z.C. Xuan. Preventing black hole attack in mobile ad-hoc networks using anomaly detection. In Future Computer and Communication (ICFCC), 2010 2nd International Conference on, volume 3, pages V3–672. IEEE, 2010.

[11] A. Baadache and A. Belmehdi. Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks. Arxiv preprint arXiv:1002.1681, 2010.

[12] M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in Network Protocols Ninth International Conference on ICNP 2001. IEEE, 2001, pp. 14–23.

[13] M. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Communications, vol. 34, no. 1, pp. 107–117, 2011.

[14] EO Ochola and MM Eloff. A review of black hole attack on aodv routing in manet. 2011.

[15] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated routing for ad hoc networks," Selected Areas in Communications, IEEE Journal on, vol. 23, no. 3, pp. 598–610, 2005.

[16] The Network Simulator - NS-2.
(http://www.isi.edu/nsnam/ns/index.html)