© IJEDR 2018 | Volume 6, Issue 2 | ISSN: 2321-9939

Quality of Service of Black Hole Attack In Manet Using AODV Protocol

[1]K. Praveen Kumar, [2]V. Jai Kumar
[1]PG Scholar, [2]Associate Professor
Department of ECE, QIS College of Engineering & Technology (Autonomous), JNTU-K, Ponduru Road,
Vengamukkalapalem, Ongole, Prakasam district, A.P, INDIA.

Abstract: In this paper, we investigate malicious detection and avoidance of black hole attack for smart meter network. In terms of routing protocol, the reactive routing protocol Ad hoc On-Demand Distance Vector (AODV) is commonly adopted for smart meter network and is considered in our paper. However, the default AODV is vulnerable to black hole attacks. The self configuring and infrastructure less property of MANETs makes them easily deployable anywhere and extremely dynamic in nature. Lack of centralized administration and coordinator are the reasons for MANET to be vulnerable to active attack like black hole. Black hole attack is ubiquitous in mobile ad hoc as well as wireless sensor networks. Black hole affected node, without knowing actual route to destination, spuriously replies to have shortest route to destination and entice the traffic towards itself to drop it. Network containing such node may not work according to the protocol being used for routing. Commonly used protocols like ADOV, DSR, and so forth in MANET are not designed to tackle black hole attack or black hole affected routes. Hence this paper proposes an AODV-based secure routing mechanism to detect and eliminate black hole attack and affected routes in the early phase of route discovery. A validity value is attached with RREP which ensures that there is no attack along the path. The proposed method is simulated in NS2 and performance analysis is carried out.

Keywords- Mobile adhoc network; black hole attack; route reply; validity value; AODV, NS2, Path delay, Packet Delivery Ratio.

I. INTRODUCTION

Mobile ad hoc network is a collection of freely moving, collaborative and wireless nodes. MANET is proposed to configure in battlefield and natural disasters scenarios and salvage operations wherever it is difficult to configure the wired network. There is neither fixed topology nor centralized management in MANET. It consists of easily and rapidly deployable nodes that communicates with one another using wireless links. If the nodes are in the same communication range then they communicate directly otherwise neighboring nodes are used as a router to transmit packets [1] [2]. This process is known as multihop communication. Fig. 1. demonstrate an illustration of multi hop communication. In the former fig. 1. (a) node A and B can communicate directly because node B is in the range of A. But in latter one node B moved out of the communication range of A. So direct communication is not possible hence multihop communication comes into play. To communicate with node B node A has to use an intermediate node as a router. In the given example figure node F is acting as an intermediate router between A and B. Absence of centralized management and unpredictable mobility of nodes [3] are the reasons to make routing process challenging. Routing strategy partitions routing protocols in three types: proactive routing protocols (table driven), reactive routing protocols (on demand) and hybrid protocols.

Fig:1. Mobile Ad-Hoc Network

DSDV, GSR, HSR, and TORA etc are examples of proactive routing protocols. In proactive protocols, complete routing information of the network is maintained at each node. A change in the network topology causes to update routing tables of all the nodes. On the contrary, reactive routing protocols like AODV, DSR, LAR, etc finds the route on demand and only nodes which are part of active route maintains routing information. Hybrid protocols are blend of both proactive as well as reactive routing protocol. AODV is widely adapted and used routing protocol in MANET [4] [5]. Being a kind of reactive routing protocols, it is not intended to handle security threats [5] [6]. Therefore malicious nodes may disrupt the routing process. Black hole is one of those types of attacks and is severe [4]. Effect of this attack becomes more severe if two or more than two nodes collaborate with each other to cause the attack. Most of the researchers focus on single node black hole attack. Also, those focusing collaborative attack require a considerable amount of overhead to mitigate the attack. This paper delivers solution for both single as well as collaborative attack with less overhead.

Remaining paper is composed as follows. Part II presents foundation of AODV and black hole attack followed by literature survey and their limitations. Section III depicts the proposed strategy. Result and analysis is discussed in section IV. Finally in section V conclusion and future work is discussed.

II. BACKGROUND

Frequently altering topology is a challenge to route packets between a pair of nodes [7]. AODV is likely one of a kind pure on demand protocols which suffice the purpose of routing packets between pair of nodes.

A. AODV Protocol Ad hoc On-demand Distance Vector (AODV) has been standardized by IETF and particularly developed for MANET. As it is a reactive protocol, it searches for route on demand. AODV is development over DSDV with introduced benefits of DSR. The basic route discovery and route maintenance mechanism are borrowed from DSR protocol and hop by hop routing and sequence number are borrowed from DSDV. Use of sequence numbers is the reasons to preclude loop freedom and count to infinity problem [9]. Following are the two phases in which AODV works:

1) Route discovery: When a node has data to send to any other node, sending node first polls its own routing table for a route to receiving node. If route is available, data is sent via that route. But if route is unavailable, route discovery phase takes place with the aid of broadcasting RREQ to its neighbors which checks for the requested route in their route table and replies with RREP if available; forward RREQ to their neighbors. This procedure proceeds until a node having route to destination or a destination node itself is discovered. Whenever this happens, RREP is generated and unicasted to the source node. In the meantime, when RREQ and RREP messages travels towards destination and source node respectively, intermediate nodes on receiving them makes an entry towards source node and destination node in their route table. Each entry is associated with timer, on expiry of which an entry is deleted.

2) Route maintenance: During the packet transmission if a link breakage of an active route occurs then other nodes are notified with RRER message. RRER message is sent to all those nodes which are using the failure link for their communication. When a source node receives this RERR message then it has to restart route discovery process.

B. Black hole attack It is otherwise called as packet drop attack and it is a sort of denial of service of attack. An internal or external node can launch this attack [4]. When a route discovery process starts and if attacker node is present in the network, on receiving RREQ message, attacker will send a false RREP message. This RREP will reach the source node well ahead of those sent by other nodes because attacker will send this RREP without checking its route table. This RREP claims to have shortest route to the desired destination; where value of hop count is minimum and has maximum value of sequence number which indicates that fresh enough route to the destination is available. So source node will probably be tricked by this fake RREP and choose this path to transmit data packets. After receiving these data packets, the attacker node will simply drop these packets. An example of black hole attack is portrayed in Fig. 2.

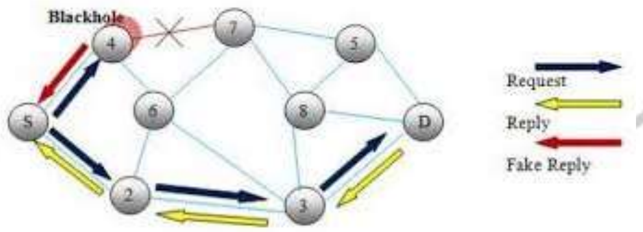


Fig:2. Blackhole Attack

C. Literature Survey

This section talks about prior works done related to black hole attack and even more severe collaborative black hole attack. Pros and cons of the related work are likewise examined. A solution is given by Deng et al. in [1] which states that when an intermediate node send RREP back, it has to add nexthop information in RREP message. Source node, on receiving this RREP, instead directly transmitting data packets it obtains next hop information from RREP and sends Further Request to nex thop to verify route from next hope to destination. A Further Reply is sent by nexthop in the event that it has route to destination. But if the nexthop node is collaborating with the intermediate node sending RREP then this method falls flat. In [10] a framework known as anti-blackhole mechanism (ABM) is proposed where difference between RREQ and RREP are used to find suspicious value of a node. Some of the anomaly based IDS [11] [12] which monitor malicious activities in MANET are proposed. But to have IDS in a network requires a central monitoring. And hence this is not feasible and sometimes impractical in MANET. An approach to negotiate with the nodes claiming to have shortest and fresh route is proposed in [13]. Simulation results shows that this system adds a minimal overhead and delay to mitigate blackhole attack. A method called SAODV is proposed in [14] where source nodes wait for particular period to receive replies from all the nodes. This method adds minimal overhead but due to waiting for replies from other nodes significant delay is added. Payal et al. in [15] proposed to maintain and update threshold value dynamically and routinely. Value of sequence number from RREP is checked with this threshold. What more, higher value of sequence number more than threshold, confirms the RREP sending node as malevolent. An alarm packet is broadcasted to illuminate that malicious node is present in the network. This method adds little bit delay and overhead is also added in the network. In [16], Misbehaving nodes are detected using a table called Data Routing Information. This method uses additional memory to store past routing information which results in expanded overhead and wastage of memory.

III. PROPOSED METHOD

The proposed strategy keeps the basic mechanism of AODV unchanged. In basic AODV, when a node has data addressed to any node, route is discovered by broadcasting route request packet to its neighbors. Neighbors on receiving this RREQ look at their route table for the availability of route requested; replies with RREP if available, forward RREQ to neighbor nodes otherwise. This process is repeated as far as RREQ hit its intended destination. In proposed strategy this basic mechanism of AODV remains untouched with the addition of validity value with RREP message. This is implemented at destination node and checked by intermediate node. Fig. The flow graph of proposed strategy. In proportion to the proposed method, a validity value is attached with the RREP message and is stored in route table at each node of active path. Whenever a node receives route request, if it is the intended destination or possess a legitimate route, then route reply message will be generated by setting value for validity bit in RREP (Here legitimate route refers to the route for which validity bit in route table is set). This RREP then will be sent back to its neighbouring hop from which it obtained RREQ. The proposed route reply message differs in the validity value with the fundamental AODV route reply message. The validity value mechanism is implemented in the RREP message. RREP of AODV will contain an extra header bit in as validity bit. In the fundamental AODV protocol, route table contains following nine fields:

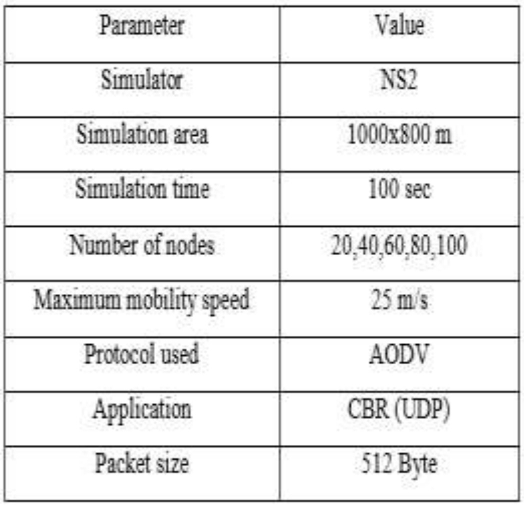
- Destination IP address
- Destination Sequence Number
- Valid Destination Sequence Number Flag
- Other state and routing flags
- Network Interface
- Hop Count
- Next Hop
- Precursor List
- Lifetime

In addition to these nine fields we are proposing an additional field for validity value. This new field will be used to check validity of route. Each time a node receives a route reply, it will be processed if and only if validity bit in that RREP is set. An entry for that route will be made only if validity bit is set. The entry in the route table will consist of above mentioned nine fields plus one proposed in this paper i.e. validity value. As attacker will be unaware about this mechanism; it will reply without looking in its route table. So validity bit will have null value in the RREP sent by attacker node. A node which receives such a reply where validity value is not set will simple drop that RREP without making entry in the route table. Hence route table will be free from fake routes. And hence the term 'legitimate routes' was used earlier.

In proposed strategy as a single bit is used to detect attack, a negligible overhead will be added to the network. Same strategy can be used for single as well as collaborative black hole attack. Although, two or more than two nodes are collaborating with each other in collaborative black hole attack, none of them can set validity bit as they send fake RREP without looking in their route table. In case of collaborative attacks, though nodes in collaboration may be able to forward RREP among themselves. But they cannot forward RREP message to a bode which is not in collaboration with them as, according to proposed strategy, it will be dropped. Hence both single as well as collaborative attacks can be prevented before actual transmission of data.

Simulation environment and parameters used are given in the following table:

Table1: Simulation Parameter



Parameter	Value
Simulator	NS2
Simulation area	1000x800 m
Simulation time	100 sec
Number of nodes	20,40,60,80,100
Maximum mobility speed	25 m/s
Protocol used	AODV
Application	CBR (UDP)
Packet size	512 Byte

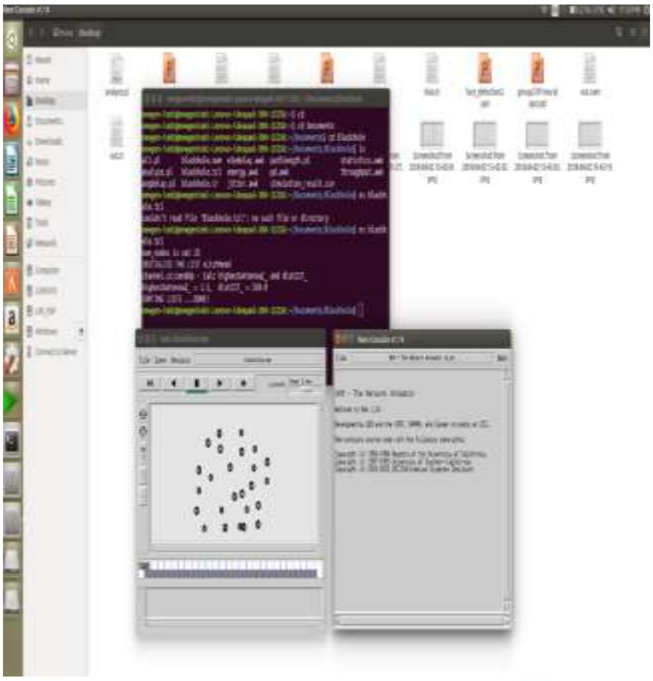


Fig:3. Nam console

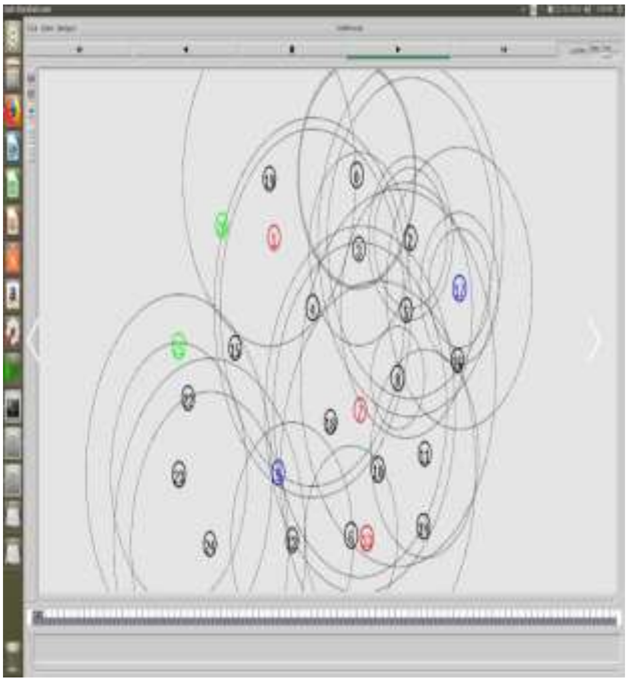


Fig:4. Blackhole Simulation

Table:2.Packet deliver ratio

NODS	AODV	AODV with Blackhole
5	1	1
10	0.9	0.8
15	0.6	0.9
20	1	0.7
25	0.7	0.6
30	0.5	0.7

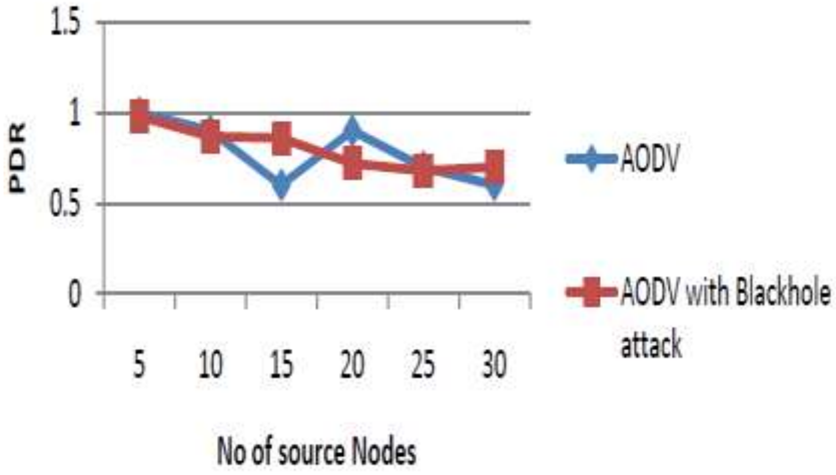
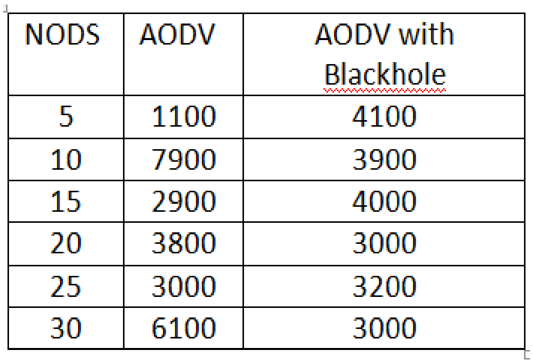


Fig:5. PDR of AODV & AODV With Blackhole

Table:3. Throughput



NODS	AODV	AODV with Blackhole
5	1100	4100
10	7900	3900
15	2900	4000
20	3800	3000
25	3000	3200
30	6100	3000

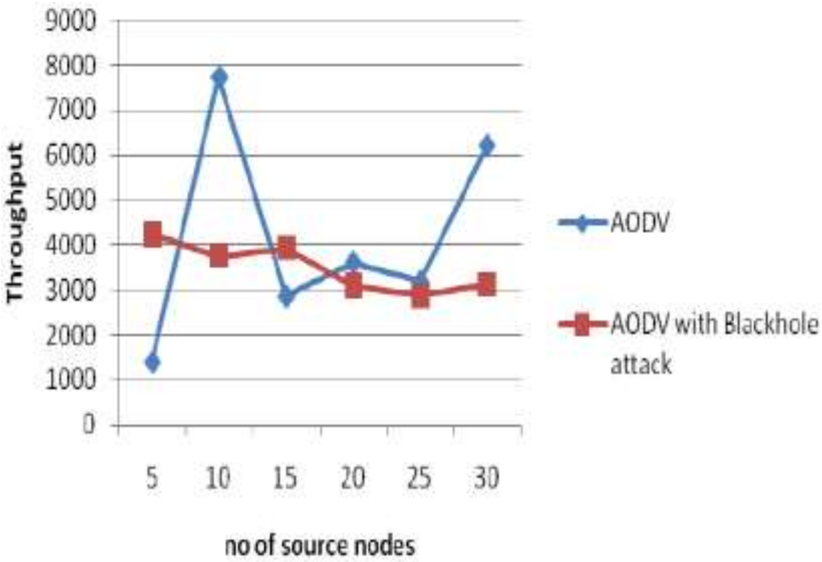
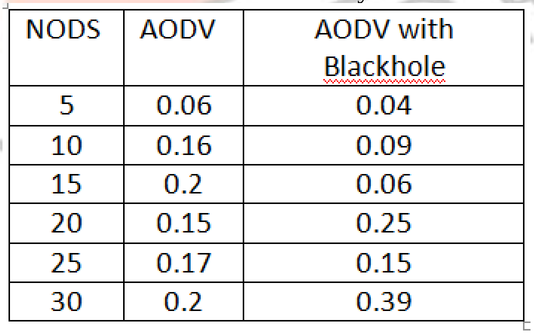


Fig:6. Avg Throughput AODV & AODV With Blackhole

Using the parameter values mentioned in the above table, simulation of proposed strategy has been carried out. Following figures shows the comparison of fundamental AODV and proposed AODV. Packet delivery is compared for AODV, AODV under blackhole attack and Proposed AODV in following fig. 4. With the increase in the amount of nodes in the network causes packet delivery ratio to drop eventually. In presence of an attacker node in the network, there is a significant cut in PDR. But this node can be prevented from participating in the network using proposed protocol which has PDR nearly equal.

Table:4. E2E Delay



NODS	AODV	AODV with Blackhole
5	0.06	0.04
10	0.16	0.09
15	0.2	0.06
20	0.15	0.25
25	0.17	0.15
30	0.2	0.39

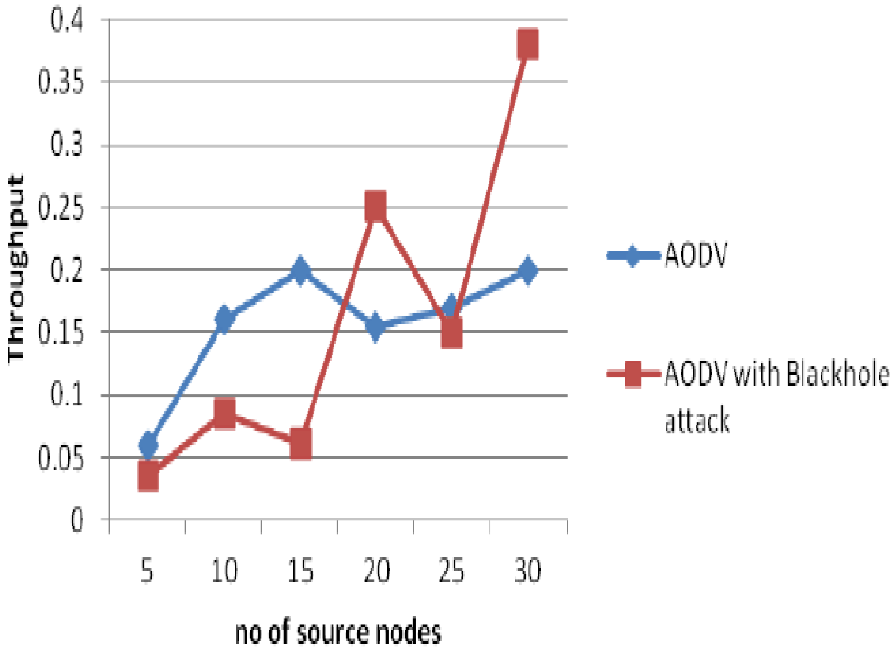


Fig:7. End to End Delay AODV & AODV with Blackhole

Routing overhead is compared in fig.5.where introduction of overhead by proposed method are not eminently altering. Here routing overhead can be seen increasing with the node mobility speed. This is because as nodes will move faster there will be change in the topology resulting in reconstruction of routes. Hence routing overhead increases with node mobility speed. Average end to end delay is depicted in fig. 6. Also like PDR, number of nodes affects average end to end delay. As number of nodes increases there is increase in average end to end delay.

IV. CONCLUSIONS AND FUTURE WORK

Mobile wireless networks like MANET are more likely to be suffered from security threats due to their characteristic like open medium. This paper discusses one of the security threat known as black hole attack and proposes an efficient solution for the same. Proposed system neither requires heavy processing nor extra memory. With the addition of negligible overhead, black hole attack is prevented before actual data transmission phase, even before the participation of malevolent node in the network. Hence the legitimacy of route is confirmed. Proposed strategy is compatible with other reactive routing protocols. The proposed method will be implemented for other reactive routing protocol as a part of future work.

REFERENCES

[1]. Hongmei Deng; Li, W; Agrawal, D.P., "Routing security in wireless ad hoc networks", Communications Magazine, IEEE, vol. 40, no. 10, pp. 70-75, October, 2002.

[2] Rajesh Yerneni, and Anil K. Sarje, "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks, " ICCCNT' 2012 26th 28th July 2012, IEEE-20180, Coimbatore, India.

[3] K.Mahamuni and Dr.C.Chandrasekar," Mitigate Black Hole Attack In Dynamic Source Routing (DSR) Protocol By Trapping ", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 2, July 2013.

[4] Sarita Mandala, Abdul Hanan Abdullah, Abdul Samad Ismail, HAbibollah Haron, Asri Ngadi and Yahaya Coulibaly, "A review of blackhole attack in mobile Adhoc network", ICIC I-BME

[5] Nirbhay Chaubey, Akshai Aggarwal, Savita Gandhi, Keyurbhai A Jani, "Performance Analysis of TSDRP and AODV Routing Protocol under Black Hole Attacks in MANETs by Varying Network Size" 2015 Fifth International Conference on Advanced Computing & Communication Technologies, pp. 320 - 324, 21-22 Feb. 2015.

[6] Seryvuth Tan, Keecheon Kim, 'Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs', IEEE International Conference on Telecommunication , pp. 1027-1032,2013.

[7] M. N. Alslaim, H A. Alaqel, S. S. Zaghloul, " A Comparative Study of MANET Routing Protocols ", Third International conference on eTechnologies and Networks for Development (ICeND), 2014, pp. 178182.

[8] Vahid Nazari Talooki, Jonathan Rodriguez, "Quality of Service for Flat Routing Protocols in Mobile Ad-hoc Network," ICST, September 7-9, 2009.

[9] Morshed, M.M.; Rahman, M.U.; Rahman, M.H.; Islaml, M.R. "Performance comparison of TCP variants over AODV, DSDV, DSR, OLSR in NS-2", Informatics, Electronics & Vision (ICIEV), 2012 International Conference on, On page(s): 1069 – 1074.

[10] Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on , vol., no., pp.162,167, 6-9 Sept. 2010.

[11] B. Sun; K. Wu; U. Pooch; “Towards Adaptive Intrusion Detection in Mobile Ad Hoc Networks”, In Proceedings of IEEE Global Telecommunications Conference (GLOBECOM), Vol. 6, pp. 3551– 3555, 2004.

[12]. Yibeltal Fantahun Alem, Zhao Cheng Xuan, "Preventing Black Hole Attack in Mobile Adhoc Networks using Anomally Detection", 2nd International conference on Future Computer and Communication 2010.
[13] M. Medadian, A. Mebadi and E. Shahri, "Combat with Black Hole Attack in AODV Routing Protocol", in Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications, pp 530-535, 2009.
[14]. Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), IEEE, 2007.
[15]. P. N. Raj and P. B. Swadas, "DPRAODV: A dyanamic learning system against blackhole attack in aodv based manet," IJCSI International Journal of Computer Science Issues, vol. 2, pp. 54–59, 2009.
[16] H. Weerasinghe, H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation", Proc. of Intl.Conference on Future Generation Communication and Networking (FGCN'07), Jeju Island, Korea, pp. 362-367, 2007.