ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 49-54 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

A Secure Probabilistic Rebroadcast Routing Protocol based on Neighbor Coverage in Mobile Adhoc Networks

Hafeesa M Habeeb[1], Selin .M[2]
[1]Department of CSE ,KMEA Eng .College, India.
hafeesa6@gmail.com

[2]HOD, Department of CSE
KMEA Eng. College, India

***Abstract*—**Mobile Adhoc Networks leads to frequent path failuresand route reconstructions, which causes an increase in the routingcontrol overhead. This is because of the frequent topology variations and arbitrary mobility of nodes as compared to other adhoc networks like VANETs. There are many existing routing protocols namely AdhocOn Demand Distance Vector (AODV), Dynamic Source Routing (DSR) for adhoc networks. AODV is an on-demand reactive routing protocol for mobile adhoc networks. DSR is a simple and efficient routing protocol mainly for mesh networks. Eventhough these mentioned protocols improve the scalability and reduce the routing overhead to an extent they are all on demand and cause broadcast storm problem.To avoid these problems a new secure routing protocol based on neighbor knowledge is proposed. Based on the neighbor information a Rebroadcast delay and then a rebroadcast probability is calculatedwhich can significantly decrease the number of retransmissions so as to reduce the routing overhead. This paper also proposes a solution for identifying the malicious node in Neighbor coverage probabilistic protocol (NCPR) suffering from Black Hole attack. Black hole detection in NCPR protocol results in much secure routing protocol in adhoc networks.

***Keywords*—**MANETs, AODV, DSR,Neighbor coverage,Probabilistic rebroadcast, Black Hole attack

INTRODUCTION

In Mobile Adhoc Networks there is a frequent path failure due to the arbitrary movement of mobile nodes. Each device in a MANET is free to move independently in any direction and will change its links to other devices abruptly. There are many routing protocols in adhoc networks which increase the scalability of the networks and reduce the routing overhead. AODV is a reactive on demand routing protocol ,which finds a route on demand by flooding the network with Route Request Packets(RREQ).DSR is another reactive on demand routing protocol , in which the destination node on receiving a RREQ back to the source ,which carries theroute traversed by the RREQ packet received. These routing protocols find the route by flooding the RREQ packets and hence there is a chance of broadcaststorm problem.Somemethods have been proposed to optimize the broadcast problem in MANETs in the past few years.They categorized broadcasting protocols into four classes:1) simple flooding 2) probability-based methods 3)area based methods and 4) neighbor knowledge methods.There are many other classifications of routing protocols in the network scenarios as shown.

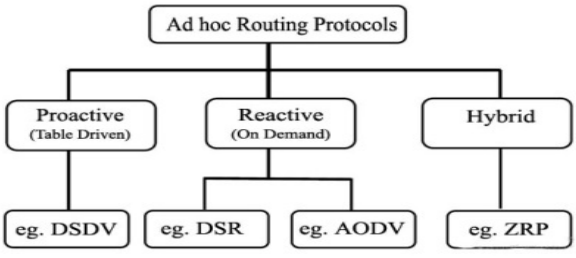


Fig.1. Hierarchy ofRouting Protocols [2]

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 49-54 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

The current proposal is a routing protocol purely based on the neighbor coverage knowledge. Each RREQ packetcarry the uncovered neighbor list and with the neighbor information rebroadcast delay and rebroadcast probability is calculated.Towards the end of the paper the proposed protocol is compared with the conventional routing protocols in MANETs .The paper also deals with the black hole detection in the NCPR protocol.Black holes aremalicious nodes agree to forward packet to destination but do not forward packet intentionally .The malicious node intercept the packet and have the availability in replying to the route request .On receiving the reply the source thinks that it is from the intended destination but truly it is from the attacker node.NCPR protocol implementation in this paper also checks for the presence of black holes and there by securing the protocol.

MOTIVATION

There are many existing works related to the routing in adhoc networks. The routing protocols namely AODV [10]DSR [9] are few among them. AODV is an adhoc on demand reactive routing protocol which discovers the route to the destination only when a transmitter node requests for it.Also it finds the route with the help of routing table maintained in each node.It is one of the traditional routing protocols mainly for adhoc networks like VANETs and MANETs.DSR is also an adhoc reactive protocol but it varies from AODV in the sense that it is source routing.On-demand routing protocols have the potential to achieve high levels of scalability in mobile ad hoc networks.However, before these protocols can be realized two major issues need to be resolved. These are high levels of control overhead due to route request packets and also additional delay. There is a chance of broadcaststorm problem also[8],[13].Several approaches have been proposed to reduce the routing overheads of on-demand routing protocols such asstable routing, multi-path routing, load balance routing, and routing based on previous knowledge[3]. There are many existing works related to the categorization of routing protocols.There are works related to route discovery in the absence of previous route information[9].Several techniques are used to reduce the overhead of HELLO packets to discover or gather the neighbor information[7],[5].

Research works indicated that the performance of neighbor knowledge methods is better than that of area-based ones, and the performance of area-based methods is better than that of probability-based ones[1]. The proposal is neighbor coverage based routing protocol taking into consideration the security concern also.Black hole detection [2], [6] is discussed in many research papers and how the routing protocols like AODV behaves in the presence of black holes as well. The proposed method takes care of the presence of malicious node and how the proposed protocol behaves during black hole detection.

SYSTEM OVERVIEW

The proposed method is a secure routing protocol based on neighbor coverage knowledge and detection of black holes in thenetwork.The formal description of the Neighbor coverage-based Probabilistic Rebroadcast for reducing routing overhead in route discovery is given.

ALGORITHM

The proposed routing protocol can be implemented as mentioned in the algorithm.

NCPR Algorithm
RREQv: RREQ packet received from node v.
Rv:id: the unique identifier (id) of RREQv.
N(u): Neighbor set of node u.
U(u,x): Uncovered neighbors set of node u for RREQ whose
id is x.
Timer(u, x): Timer of node u for RREQ packet whose id is x.
{Note that, in the actual implementation of NCPR protocol,
every different RREQ needs a UCN set and a Timer.}

1: if $n_i$receives a new RREQs from s then
2: {Compute initial uncovered neighbors set U(ni,Rs.id) for RREQs:}
3: U(ni,Rs.id) =N(ni) _ [N(ni)∩N(s)]-{s}
4: {Compute the rebroadcast delay T_d(ni):}

5: $Tp(n_i) = 1 - \frac{|N(s)\cap N(ni)|}{|N(S)|}$
6: T_d(ni) =MaxDelay*$Tp(n_i)$
7: Set a Timer(ni,Rs.id) according to T_d(ni)
8: end if

9:
10: while $n_i$receives a duplicate $RREQ_j$from $n_j$before Timer(n_i,Rs.id) expires do
11: {Adjust U(n_i,Rs.id):}
12: U(n_i,Rs.id)=U(n_i,Rs.id) _ [U(n_i,Rs.id)∩N(n_j)]
13: discard($RREQ_j$)
14: end while.

15:
16: if Timer(n_i,Rs.id) expires then
17: {Compute the rebroadcast probability P_{re}(n_i):}
18: $R_a(n_i) = \frac{|u(ni,Rs.id)|}{|n(ni)|}$

19: $F_c(n_i) = \frac{Nc}{|N(ni)|}$
20: $P_{re}(n_i) = F_c(n_i) . R_a(n_i)$
21: if Random(0,1) <= P_{re}(n_i) then
22: broadcast($RREQ_s$)
23: else
24: discard($RREQ_s$)
25: end if
26: end if

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 49-54 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

The proposal can be done in five steps.The steps involve setting up of an adhoc network with dynamic node density.There are provisions to dynamically add nodes remove nodes and search for nodes as obvious in an adhoc mobile network. Once the nodes are added for simulation,they need to be configured. That refers to assigning name,IP addresses,port no and its location. The nodes can be stored in a database for further implementation purposes.The activities performed in a network can be tracked using a log which will be useful at later point of time .Since the protocol is purely neighbor Coveragebased,neighbor information collection is significant steps involved in the algorithm.Each RREQ packet contains the Uncovered Neighbor List (UCN) and based on the UCN,each node decides to discard or rebroadcast the packet there by reducing the flooding of the packets.The scheme considers theinformation about the uncovered neighbors (UCN),connectivity metric and local node density tocalculate the rebroadcast probability.The rebroadcast probability is based on the rebroadcast delay calculated.Based on the delay a timer is set in such a way that a node receives all the duplicate RREQ packets from its neighbor nodes. Implementation of Neighbor Coverage Probabilistic Routing Protocol takes into consideration the security concern also. During the process the protocol also checks for the presence of malicious nodes.Detection of the blackholes in AODV is existing in Mobile adhoc networks. But because of the overhead,need for blackhole detection in NCPR is arisen. Once the protocol is implemented,it can be evaluated with the traditional routing protocols.This can be done interms of varying node density,packet delivery ratio and the packet loss. AODV and DSR behave almost similar in terms of the simulation parameters.

A. Setting up of a Network

MANET is a self-configuring infrastructure less network of mobile nodes. The nodes can be added or removed from the network at any time. Such an environment is simulated with dynamic node density. Broadcasting is a fundamental and effective data dissemination mechanism for many applications inMANETs. In this paper, only one of the applications: route request in route discovery iscovered.In order to evaluate the performance of the routing protocols, AODV and DSR were also taken into consideration.In the network model, eachnode moves to a random selected destination with arandom speed from a uniform distribution .After the node reaches its destination; it stops for a pausetimeinterval and chooses a new destination and speed. Inorder to reflect the network mobility, set the max-speedto 5 m/s and set the pause time to 0. The MaxDelay used todetermine the rebroadcast delay is set to 0.01 s, which isequal to the upper limit of the random jitter time of sendingbroadcast packets in the default implementation of AODV. In the simulation environment, provision for adding,deleting and searching for a node is also given to make the network an adhoc in nature .The number of nodes can be varied to know the behavior of the protocol in varying node density. The flow of control messages is as shown figure 2.

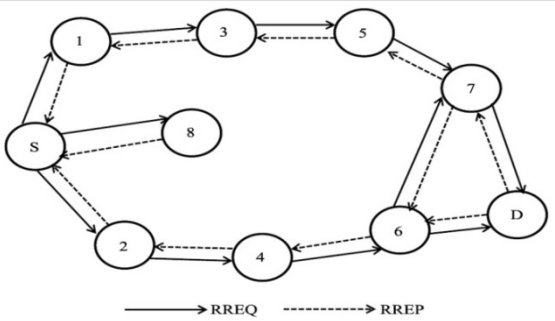


Fig.2.Flow of control messages.[2]

B. Node Configuration

Once the network is set up for the simulation, the next step is configuring the mobile nodes which are the key components of an adhoc network. Configuring a node indicates assigning each node its name,IP address,port number, and its location.For further process to calculate or for identification these nodes can be stored into a database.While an RREQ packet is send from the source todiscover a route,the actions can be tracked in a log.The RREQ packets,RREP packets are of constant sending rate to avoid collisions.The configuration should be done such that the neighbor information is highly significant in this implementation.Each node should know its neighbors.This can be obtained using periodic HELLO packets. But there is a great overhead in periodicHELLOpackets.Other techniques like sending the acknowledgment, in response to the RREQ packets,or considering the range of each node etc. can be used to identify its neighbors. Each node checks the incoming RREQ packetsto determine the UCN list and then calculate the rebroadcast delay.

C.Neighbor Information collection and Data Transfer

The current proposed protocol is a broadcasting protocol categorized into neighbor coverage based protocol. Hence this step of neighbor collection is highly significant for the implementation of the current proposed method.The method takes care of the uncovered neighbors set and then it calculates the rebroadcast delay. When node n_i receives an RREQ packet from its previous node s, it can use the neighbor list in the RREQ packet to estimate how many of its neighbors have not been covered by the RREQ packet from s. If node n_i has more neighbors uncovered by the RREQ packet from s, which means that if node n_i rebroadcasts the RREQ packet, the RREQ packet can reach more additional neighbor nodes.Uncovered Neighbors set U (n_i) of node n_i is given as follows

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 49-54 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

$$U(n_i) = N(n_i) \_ [N(n_i) \cap N(s)] - \{s\},$$

Where N(s) and N (n_i) are the neighbors sets of node s and ni, respectively is the node which sends an RREQ packet to node n_i Due to broadcast characteristics of an RREQ packet, node ni can receive the duplicate RREQ packets from its neighbors in the network. Node n_i could further adjust the U(n_i) with the neighbor knowledge. In order to sufficiently exploit the neighborknowledge and avoid channel collisions, each node shouldset a rebroadcast delay. The success of the proposed protocol relay on the choice of the proper rebroadcast delay.

D.Implementation of NCPR protocol with Black hole detection.

In NCPR protocol,each nodecalculates the UCN set and then a timer is set for the rebroadcast delay. Based on the rebroadcast delay, the protocol decides to discard the packet or to broadcast it.If the duplicate RREQ packet is received before the timer exceeds, then modify the UCN set and discard the packet.If the timer is received after timer expires then calculate the rebroadcast probability and verify it with random values to check whether to discard the packet or to broadcast it.In the meantime, italso checks for the malicious nodes. Based on the neighbor set of the source node and the current node, rebroadcast delay is calculated.

If there is a black hole detected, i.e.; in this protocol ,a black hole can be detected by assigning an integer variable say STATUS to value one and then check for the value ,that route shouldn't be chosen.In other protocols namely AODV and DSR,a black hole can be detected in the following ways ;1) if any node modifies the source ID in the RREQ packet or 2)if there is any node which doesn't send the acknowledgement.
UCN set is significant because the node with more number of elements in the UCN set can broadcast the packet without any delay .Once node nk rebroadcasts the RREQ packet, there are more nodes to receive it, because node nk has the largest number of common neighbors. Then, there are more nodes which canexploit the neighbor knowledge to adjust their UCN sets.

E. Performance Evaluation ofAODV,DSR and NCPRrouting protocols

The evaluation of the implemented protocol NCPR is compared with the existing protocols DSR and AODV.The AODV and DSR behave similar whereas NCPR varies as it is a neighbor coverage knowledge based protocol. A graph is to be plotted to evaluate its performance. The performance involves time taken, the packet delivery ratio and the packet loss. The packet delivery ratio takes into account the packets received to the packets sent. The NCPR protocol takes into consideration the neighbors and once the neighbor information is collected, it decides to send the packet or to discard it. So time taken is less and the chance of packet loss is also reduced. Hence packet delivery ratio is guaranteed.

But the black hole detection in NCPR allows the protocol not to choose the route with the black hole. Hence there is a great packet delivery ratio and the packet loss can be reduced to an extent.

In the case of AODV, it simply broadcast the packet with no neighbor information and there is a great overhead of routing also. The time taken is also high for broadcasting to all the neighbors irrespective of whether they are valid nodes or not

In case of DSR, the routing overhead is comparatively less but the black hole detection with fake RREQs cause broadcast storm problem. The packet loss also cannot be guaranteed.The transfer log shows the various values of the data transmission with respect to the three routing protocols.

SIMULATION RESULTS

The implementation of the method initiates with the simulation of an adhoc network with mobile nodes. The network contains dynamic number of nodes and each node can easily move out of the network and can also join the network .The simulation provides the facility of adding nodes ,removing nodes and searching for a node.Also while configuring the node, each node is assigned with its name,IP address, port number and its location in X, Y coordinates.There is also an intervention of the database for storing the nodes in a network for further processes.

The simulation also shows the neighbor nodes of each node during the traversal of the RREQ packets.As the proposed method is based on the neighbor coverage knowledge, neighbor information collection or gathering is important. A transfer log indicates the activities in the network inorder to track the nodes. The simulation during the implementation of the protocol also taken into account the presence of black holes there by securing the protocol.Black holes are those malicious nodes that behave as original nodes but cause attack to the network and deceive the sending node. The implementation also evaluates the proposed protocol with the traditional routing protocols for performance valuation.

Once the nodes are configured, the data can be transferred. A source and destination is selected and the message can be send.The activity log indicates the actions during the transmission and also the neighbor list.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 49-54 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

The performance evaluation of the three routing protocols are plotted based on the values obtained in the transfer log.The simulation parameters include node density,time taken or the delay and the packet loss due to black holes.

a) Node density

The number of nodes determines the efficiency of a protocol. But as the number of nodes cannot be restrained in an adhoc networks, node density varies and need to evaluate the proposed protocol based on it.Among the nodes few can be malicious as well. Also the packet delivery ratio is also affected by the number of black holes. Hence the protocol implemented is taking care of the malicious nodes on the routes and the best or as to say the shortest path is selected.

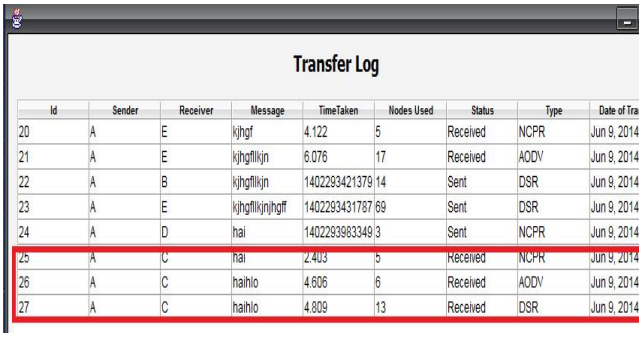
b) Time taken for the data transmission

The time required for the transmission of data is calculated based on the current system time in milliseconds.Also before the data packet is to be transmitted ,UCN set,the rebroadcast delay and the rebroadcast probabilities are calculated.

c) Packet loss due to the presence of black holes

When a black hole is found to be in the route discovered, it shouldn't be chosen .Therefore there may be some packet loss due to the malicious nodes. It is an important parameter which decides the performance of the proposed protocol.

Once the simulation is started each data transmission is tracked in the transfer log for the evaluation purpose. The log is as shown below in the figure 3.



Transfer Log

Id	Sender	Receiver	Message	TimeTaken	Nodes Used	Status	Type	Date of Tra
20	A	E	kjhgf	4.122	5	Received	NCPR	Jun 9, 2014
21	A	E	kjhgfllkjn	6.076	17	Received	AODV	Jun 9, 2014
22	A	B	kjhgfllkjn	1402293421379	14	Sent	DSR	Jun 9, 2014
23	A	E	kjhgfllkjnjhgff	1402293431787	69	Sent	DSR	Jun 9, 2014
24	A	D	hai	1402293983349	3	Sent	NCPR	Jun 9, 2014
25	A	C	hai	2.403	5	Received	NCPR	Jun 9, 2014
26	A	C	haihlo	4.606	6	Received	AODV	Jun 9, 2014
27	A	C	haihlo	4.809	13	Received	DSR	Jun 9, 2014

Fig 3.Transfer log

The transfer log contains records with information of the sender,receiver, message, time taken and the number of nodes used.Based on the transfer log,few records are selected and are compared.

The Graph indicates that the protocol NCPR outperforms the traditional routing protocols as per the values in the transfer log. AODV and DSR behave similar as per the transfer log. Presence of Black holes affects the protocols performance. Hence once black hole is detected the route with that the node should not be selected.The performance in percentage is in the Y-axis and the data transmission in the X-axis. The performance is calculated with the consideration of the time taken the number of nodes and the message send in bytes .The graph indicates that the proposed protocol outperforms the traditional protocol namely AODV and DSR.

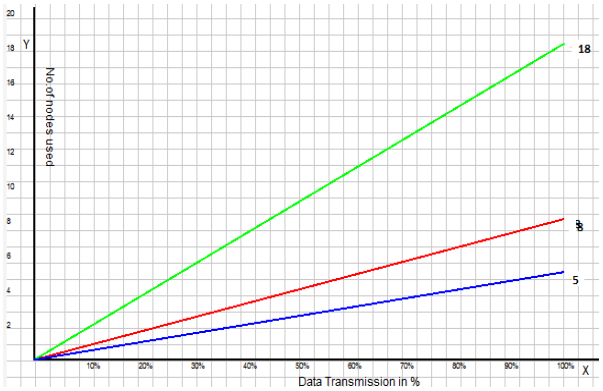


Fig 4.Data transmission with varying node density

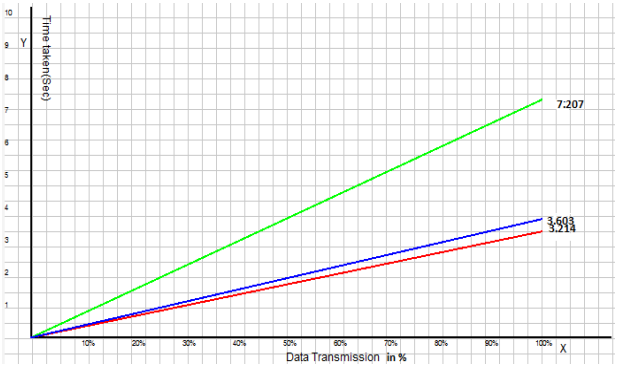


Fig 5.Data transmission with time taken

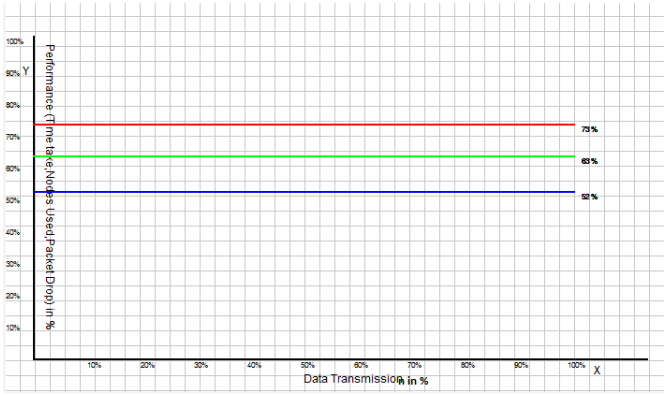


Fig 6.Performance evaluation of NCPR,AODV and DSR routing protocols

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 49-54 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

CONCLUSION

The current proposed method deals with a secure routing protocol to reduce the broadcast storm problem and the routing overhead in the adhoc networks. It is secure in the sense it detects the black holes in the network along with the implementation of route discovery. Now since malicious node is identified, the routing table and the control messages from the malicious node, too, are not forwarded in the network. The protocol is based on neighbor coverage knowledge and hence the implementation calculates the rebroadcast delay and then the rebroadcast probability. This is on the basis of additional coverage ratio and the connectivity factor.In this paper, black hole detection is also discussed. The performance evaluation of the routing protocols namely AODV,DSR and NCPR is to considered based on the simulation parameters packet loss, node density and packet delivery ratio. NCPR protocol is considered to outperform other routing protocols, and also it is secure enough in an adhoc network from black hole attacks.

REFERENCES

[1]Xin Ming Zhang, En Bo Wang, Jing Jing Xia, Dan Keun Sung, "A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, vol.12, no. 3, pp. 424-433, March 2013, doi:10.1109/TMC.2011.277

[2]Vipan Chand Sharma , Atul Gupta, VivekDimri,"Detection of Black Hole Attack in MANET under AODV Routing Protocol", International Journal of advanced Research in Computer science ,vol 3,no .6, June 2013

[3]Khanvilkar,T.S ,Patil ,K.P. "Performance evaluation and comparison of routing protocols in MANETs ",International Conference on Communications and Networking Technologies ,July 2013.

[4]Jaspal Kumar, M. Kulkarni, Daya Gupta "Effect of Black Hole Attack on MANET Routing Protocols", I. J. Computer Network and Information Security, 2013

[5]Mostajeran .E,Md Noor R, Keshavarz.H"A Novel Improved neighbor discovery method for an intelligent –AODV in Mobile Adhoc Networks", IEEE conference .Information and communication technology, March 2013.

[6]LijaJoy,SheenaKurian K "Black Holes Detection in Ad-Hoc Wireless Networks",2014

[7]Hafeesa M H abeebSelin M ,"VANET GBM"In the Proceedings of National Conference On Information and Communication Technologies (NCICT 2014)held at Baselious Poulose II Catholicos College ,Baselios Mount ,Piravom ,4.3.2014

[8]X.M. Zhang, E.B. Wang, J.J. Xia, and D.K. Sung, "An Estimated Distance Based Routing Protocol for Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 60, no. 7, pp. 3473-3484, Sept.2011

[9]Leu.S,Chang R,"Simple algorithm for solving Broadcast storm in Mobile adhoc Networks.",IEEE Trans.Communications,Vol.5 no.16,pp 2356-2363,Nov 2011

[10] H. AlAamri, M. Abolhasan, and T. Wysocki, "On Optimising Route Discovery in Absence of Previous Route Information in MANETs," Proc. IEEE Vehicular Technology Conf. (VTC), pp. 1-5,2009

[11]IETF Trust D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routingprotocol for mobile ad hoc networks (DSR) for IPv4," RFC 4728, IETFTrust, Feb. 2007

[12]C. Perkins, E. Belding-Royer, and S. Das, Ad Hoc On-Demand Distance Vector (AODV) Routing, IETF RFC 3561, 2003.

[13] W. Peng and X. Lu, "On the Reduction of Broadcast Redundancy in Mobile Ad Hoc Networks," Proc. ACM MobiHoc, pp. 129-130,2000

[14]S.Y. Ni, Y.C. Tseng, Y.S. Chen, and J.P. Sheu, "The Broadcast Storm Problemin a Mobile Ad Hoc Network," Proc. ACM/IEEE MobiCom, pp. 151-162, 1999