Australian Journal of Basic and Applied Sciences, 9(27) August 2015, Pages: 366-372

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Detecting Collaborative Blackhole Attack in MANET Using Sequence Number Mitigation Mechanism

[1]R. Somasundaram and [2]Dr. P. Sivakumar

[1]*M.Tech Student, Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.*
[2]*Professor, Department of Information Technology, Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.*

ARTICLE INFO

Article history:
Received 23 June 2015
Accepted 25 August 2015
Available online 2 September 2015

Keywords:
MANET, Blackhole, Grayhole, Wormhole, Route Reply (RREP), Packet Delivery Ratio (PDR), End To End Delay, Packet Drop, Sequence Number Mitigation.

ABSTRACT

Mobile ad hoc network (MANET) is a self-configuring network that is formed automatically via wireless links by a collection of mobile nodes without the help of a centralized management or fixed infrastructure. Due to dynamic infrastructure-less nature and lack of centralized monitoring point, the mobile ad hoc networks are vulnerable to many attacks such as Blackhole, Grayhole, wormhole, rushing attack, Information Disclosure attack, etc. The network performance and reliability is broken by the attacks on ad hoc routing protocols. Many methods have been proposed to come across the Black hole Attack. A Blackhole node or malicious send Route Response (RREP) incorrectly of having route to destination with minimum hop count and when sender sends the data packet to this malicious node, it drops the whole packets in the network. The proposed work is Sequence Number Mitigation-AODV (SNM-AODV) mechanism is used to avoid the collaborative blackhole attack. The proposed technique performance can be observed by using PDR, End to End delay and Packet Drop.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: : R. Somasundaram, Dr. P. Sivakumar., Detecting Collaborative Blackhole Attack in MANET Using Sequence Number Mitigation Mechanism. ***Aust. J. Basic & Appl. Sci.,*** *9(27): 366-372, 2015*

INTRODUCTION

A MANET is an independent collection of mobile users that communicate through wireless links without any base station or access point. Meanwhile the mobiles are node; the network topology may change randomly over time. The network is decentralized, where delivering messages and discovering the topology must be performed by the nodes them self. Some characteristics of MANET are distributed operation, multi hop routing, autonomous terminals, dynamic topology, and light-weight terminals. The wireless mobile ad hoc nature of MANET brings new security challenges to the network. Equally the wireless medium is vulnerable to many attacks such as Blackhole, grayhole, wormhole, etc and MANET is basically exposed to numerous security attacks.

An Ad hoc routing protocol is an agreement that regulates how nodes choose which way to route packets among computing devices in MANET. There are 3 routing approaches in MANET they are: Proactive or Table-driven Protocols, Reactive or On-demand Protocols, Hybrid Routing Protocols. In Table Driven routing protocols each and every node preserves one or more tables including routing information to every other node in the network. Every node saves on updating these tables to sustain most recent view of the network. Example: DSDV, OLSR. In On-Demand protocol, routes are created as and when essential. When a transmission occurs from source to destination, it appeals the route discovery process. The route remains valid till destination is achieved or until the route is no longer needed. Example: AODV, DSR. Hybrid protocols combine features from both reactive and proactive routing protocol, normally trying to exploit the reduced control traffic overhead from proactive systems whilst reducing the route discovery delays of reactive systems by maintaining some form of routing table. Example: ZRP. AODV is one of the reactive routing protocols with weaker design, which is prone to numerous security threats including Denial-of- Service (DoS) attacks such as Black hole. In existing new routing protocol called Modified AODV is proposed. This new protocol modified AODV is designed from the existing AODV routing protocol. In Watchdog mechanism (Surana, K.A., *et al.*, 2012), each node maintains 2 extra tables namely: Pending Packet Table and Node Rating Table.

In Pending Packet, Table each node maintains tracks of the packet , this table consists of 4 fields they are Packet ID, Next Hop, Expiry Time, Packet

Corresponding Author: R. Somasundaram, M.Tech Student, Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.
E-mail: somu15.diamond@gmail.

Destination. In Node Rating Table, each node maintains rating of nodes which are next to it, this tables consists of 4 fields they are Node Address, Packet Drops, Packet Forward, Misbehave. If the packet drop ratio is greater than a given threshold value then this node is malicious, otherwise it is considered as a genuine node. After detecting a misbehaving node, a node will try to do local repair for the routes which are crossing through the malicious node. This process tries to prevent a misbehaving node from dropping packets, and also prevent blackmailing of genuine nodes.

The Watchdog mechanism is suitable for single black hole attack but it is vulnerable to cooperative black hole attack. If mobility of the node is increased it is not so accurate i.e. if number of node is increased throughput value is decreased. To avoid the drawback in the existing approach to prevent blackhole attack, we proposed a Sequence Number Mitigation Mechanism. Sequence Number Mitigation mechanism significantly improves performance of MANET and detect the multiple blackhole attack. Therefore, further research work focusing on introducing security into AODV protocol has been carried out.

Related works:

There are many existing result for detecting and mitigating the malicious node in the network. They are analysed them in the following. T. Ghosh *et al* 2005 designed a secure routing solution to find an end-to-end route free of malicious nodes with collaborative effort from the neighbors. Any malicious entity, trying to inject wrong routing information either independently or acting in collusion, is effectively singled out. Next-hop's behaviour is measured with the local evaluation record which defined as a 2- tuple: packet ratio and byte ratio, forwarded by the next-hop neighbor. Local evaluation records are broadcast to all neighbors. The trust level of a node is the combination of its local observation and the broadcasted information. Trust level is inserted to the RREQ (Route Request). Route is selected in the similar way to AODV. But drawback is if there is no accusation from all malicious nodes, the protocol does not find a secure end-to-end path.

The authors Douglas S. J. De Couto 2003 proposed a novel idea to find the black and Grayhole nodes. The sender infrequently check through all available routes to find out if the destination received every of its messages antiseptic. In order to dodge any black hole node that might obstruct with message traffic, the sender broadcasts a "check" request message and the destination's reply would pursue the similar route as the request.

The Author Moumita Deb 2008 proposed a Two-Step Cooperative Detection mechanism. Two-Step Cooperative Detection mechanism that would detect potential multiple black hole node.(i) First Phase detects the malicious node by comparing the sequence no. of the current node with the sequence number of the destination node , if node sequence number found to be greater it may be malicious. (ii) In this Phase voter table mechanism to detect the malicious node by flooding the ack and test packet via the attacker node, if test packet is received it is genuine and vice versa. Drawback in this proposed work is each node should maintain numerous tables and additional packets such as test packet, acknowledgement packet and warning message.

The Authors Zhaoyu Liu *et al* 2004 proposed a Dynamic Trust Model. Each node is assigned a trust value. Using IDS the trust level of node is predicted, the neighboring nodes to a node is exhibits a suspicious behavior , the trust reports will be sent over the network. By using the trust levels of a node paths are established and messages are transmitted. Drawback in this method is Detection of false positive and false negative is difficult

The Authors S.Vijayalakshmi *et al* 2011 proposed, one approach is based on packet leashes technique. There are two types of leashes geographical and temporal. Geographical is used to limit in the distance of packet travel and temporal leash is used to check whether the packet has travelled from a longer distance. Another approach is by using directional antenna for connecting information like packet arrival direction and accurate information about neighbors. This process is mainly used in wormhole attack.

MATERIALS AND METHOD

Blackhole Attack:

Blackhole attack is an active attack and a kind of denial of service attack where malicious nodes can falsely claiming a fresh route to the destination and absorbing all packets, then engage them without forwarding them to the destination. The Black hole Attack works in 2 steps: (i) Black hole advertises itself as it has fresh route to reach the destination node. (ii) It drops the data packet without forwarding it. The nodes B1 & B2 are malicious node.

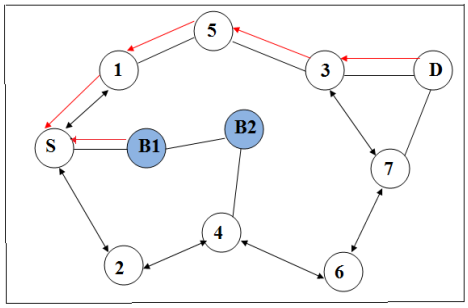

Fig. 1: Blackhole Attack

The Black hole Attack can be categorized into 2 types: Single Blackhole Attack: In this attack, only one node will act as malicious node in a zone. The other nodes of the zone will be genuine. Collaborative Blackhole attack: In this Attack more than one node act as malicious node in a group. It is also known as blackhole attack with multiple malicious nodes.

Proposed Methodology:

Sequence Number Mitigation mechanism (SNM-AODV) is used to detect the collaborative blackhole attack in MANET. SNM-AODV prevents the joining of an attacker node by discarding the RREP having extremely high destination sequence number. This could be done with the help of the Source node, which does not accept every first RREP but waits for Pre_ReceiveRREP procedure during which it stores all the RREPs in the freshly created table until a time stamp.

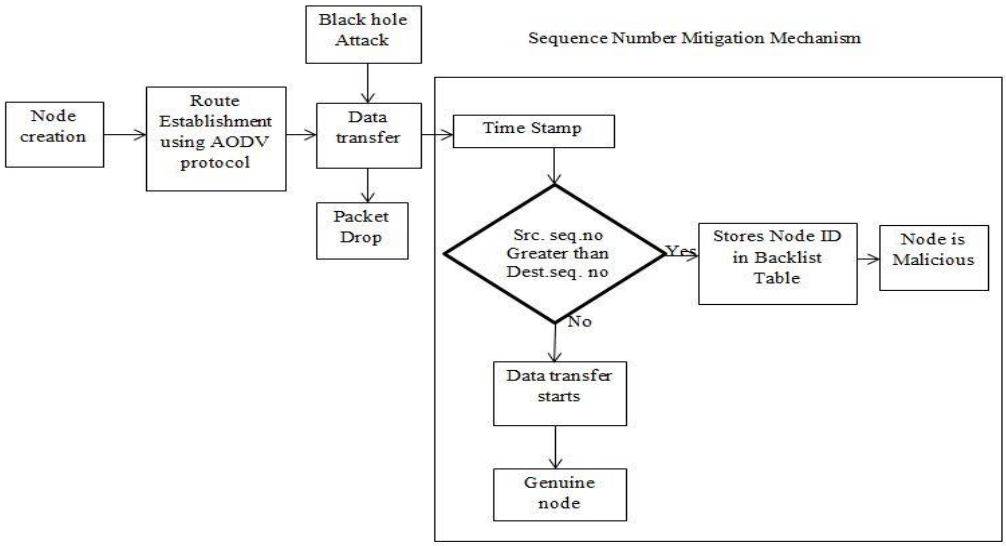

Fig. 2: Architecture Diagram of Sequence Number Mitigation Mechanism.

The path can be recognized by comparing the node sequence number with the destination sequence number. If the node is found to have higher sequence number when compared with the destination node, it is considered as malicious and no further route replies are recorded in the route reply table and the nodes corresponding to the entries are removed from the table. The solution involves detection of the malicious node which acts as normal node by accepting the RREP which has higher sequence number than the destination sequence number. Thus the malicious node is identified and the normal working of the protocol is regained to a maximum extent explains the sequence number mitigation technique to find the malicious node and eradicate from the multicast group.

In the above architecture diagram the overall working of the proposed work is explained. First the nodes are created and source node, destination nodes are assigned. If the source node wants to communicate with the destination node, first source should send the route request (RREQ) message to its neighboring node until it reaches the destination node. Then the destination node sends the route reply (RREP) message after receiving the RREQ message, this process is called route establishment. Then the data is transferred from source to destination. During

data transfer the malicious node will attack the packets, so packet drop will occur.

To avoid the problem, Sequence Number Mitigation mechanism (SNM-AODV) is proposed. In this mechanism timestamp is used and sequence number compassion is done, using timestamp the route reply time is calculated. If reply message is received within particular time interval store the source sequence number and node-id in the protocol RREP table otherwise reply message is rejected and the table will be empty. Then select the destination sequence number from the table and compare with the source sequence number. If the source sequence number is greater than the destination sequence number, the node-id is stored in the back list table and declared as malicious node so further response from that node is rejected. If source sequence number is lesser than the destination sequence number, then data transfer will continue and the node is considered as genuine node.

The Sequence Number Mitigation algorithm as follows:

```
At Source Node: PROTOCOL
Pre_ReceiveRREP (Packet P)
{
t0 = get(current time value) + settimer(t0 + PROTOCOL_WAIT_TIME)
Stores Src_Seq_No and
P.NODE_ID in PROTOCOL_RREP_Tab table
while (PROTOCOL _RREP_Tab is not empty)
{
Select Dest_Seq_No from table
if (Src_Seq_No > Dest_Seq_ No)
{
Malic_Node=Node_Id
discard entry from table
} }
Node_Id having
Lowest value of Dest_Seq_No
ReceiveRREP(Packet q)
}
```

Initially the source node does not accept every first RREP but waits for Pre_ReceiveRREP(Packet p) which stores all the RREPs in the newly formed (PROTOCOL_RREP_Tab) table till PROTOCOL_WAIT_TIME. Then it evaluates all the stored RREPs from PROTOCOL _RREP_Tab table and discards the RREP having very high destination sequence number. The node that sends this RREP is assumed to be the malicious node. The protocol maintains the uniqueness of the malicious node as Malic_node so that in future it can remove any RREPs from that node. After identifying malicious node, no further data packets or control packets can be transmitted by the malicious node to the next hop node as the node's identity has been recorded in the route reply table and has been refreshed to the participating nodes in the group.

Simulation Model and Parameter:

Table 1: Simulation Parameters

PARAMETER	VALUE
Simulator	NS2.33
No. of Nodes	50
Area	500m x 500m
Traffic Type	CBR
Signal Propagation Model	Two Ray Ground
MAC Type	802.11 MAC Layer
Packet Size	128 Bytes
Antenna Type	Omni Directional
Routing Protocol	AODV
No of Attacker node	1 & 5
Transmission Speed	10 m/sec

The experiment uses NetworkSimulator-2 and version is NS2.33. Our simulated network consists of 50 mobile nodes placed randomly within a 500 m x 500 m area. Each node has a transmission speed of 10Mbps.The mobility model chosen for a mobile node was the two-ray ground model and traffic type is constant bit rate (CBR). The MAC type is IEEE 802.11 MAC Layer is used and the packet size is 128 bytes, the omni directional antenna is used for this work. The comparison is shown by variation attacker as 1 and 5 shown in Table 5.1 lists the values of the common parameters used in all the experiments.

A. Performance Metrics:

i. Packet Delivery Ratio:

It is the ratio of the total numbers of packets received by the destination node to the total number of packets generated by the source node.

$$PDR = \frac{\sum \text{Number of data packets received}}{\sum \text{Number of data packets sent}}$$

ii. Average End-to-End Delay:

Average time consumed by data packets to reach to respective destinations.

Delay = Receiving time – Sending time

iii. Packet Loss:

Packet loss is the failure of one or more transmitted packets to arrive at their destination.

B. Simulation Experiment:

Case 1: *If there is only 1 Attacker node:*

By keeping single attacker node, the performance metrics are calculated. The graph is drawn between Time (in ms) in X Axis and respective metrics Y Axis. Here the output SNM-AODV graph is compared with the normal AODV working, the result will be better for the SNM-AODV. In this graph only one attacker node is present so the damage is low and performance metrics value varies slightly better.

Case 2: *If there is more than one Attacker node (5 nodes):*

By increasing the number of Attacker node, the performance metrics (such as PDR, Average End-To-End Delay, and Routing Overhead) are calculated, so the mentioned performance metrics is not affected. The Graph is drawn between Time (in ms) in X Axis and respective metrics in Y Axis.

RESULT AND DISCUSSION

These two implementations made the approach very secure and efficient. The comparison graphs show the results in both the cases, i.e., when there are more than one attacker nodes and when there are only one attacker node.

Packet Delivery Ratio (PDR):

Basically this graph is used to describe the Packet delivery ratio which is the ratio of total incoming packets and actual received packets by the destination. The Graph is drawn between Time (in m/sec) in X Axis and PDR in Y-Axis.

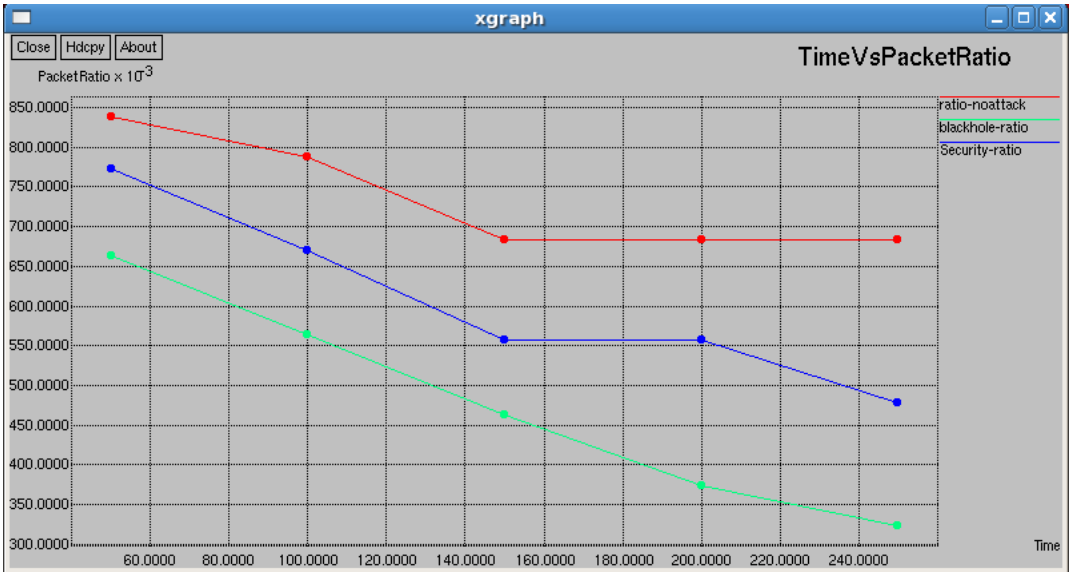

Fig. 3: Packet Delivery Ratio

The figure-3 shows the Packet Delivery Ratio which increases on an average by **13%** when solution is provided to prevent the Blackhole attack in AODV.

Average End –To-End Delay:

This graph is used to describe the average end-to-end delay which is the Average time consumed by data packets to reach to respective destinations. The Graph is drawn between Time (in m/sec) in X Axis and in Average End-to-End Delay Y-Axis.

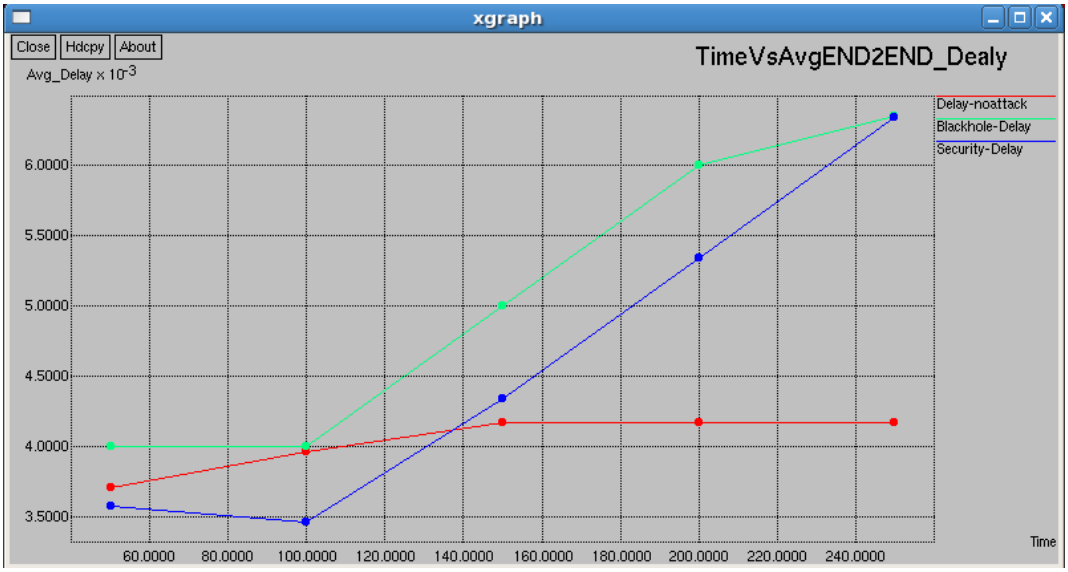

Fig. 4: Average End-to-End Delay

The figure-4 shows the End to End Delay which decreases on an average by **10%** when solution is provided to prevent the Blackhole attack in AODV.

Packet Drop:

This graph is used to describe the packet drop which is the failure of one or more transmitted packets to arrive at their destination. The Graph is drawn between Time (in m/sec) in X Axis and Packet Drop in Y-Axis.

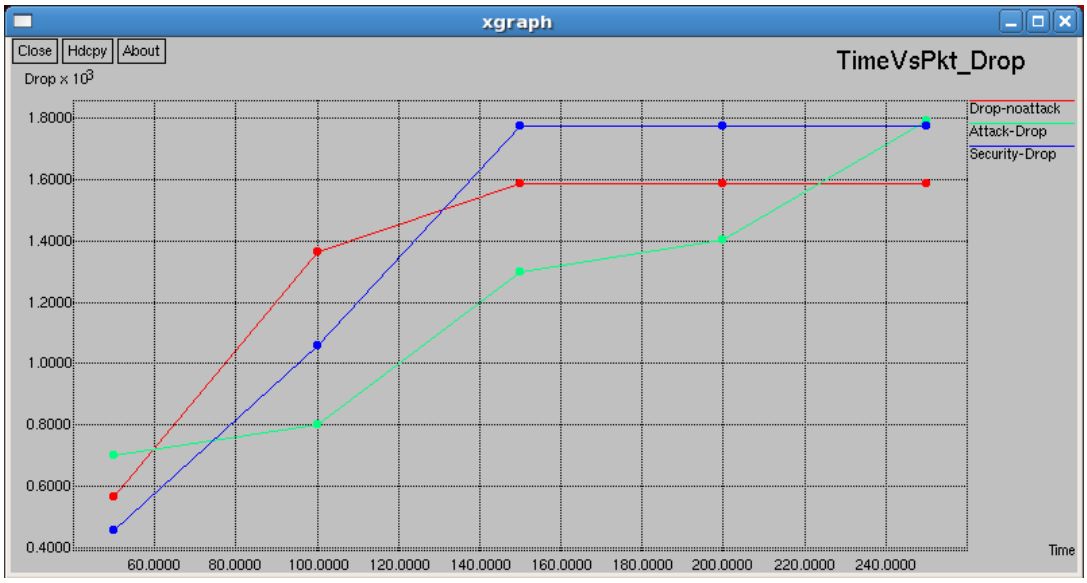

Fig. 5: Packet Drop

The figure-5 shows the Packet Drop which decreases on an average by **3.7%** when solution is provided to prevent the Blackhole attack in AODV.

Conclusion:

The nodes in the MANETs are dynamically formed with no need for an existing infrastructure or pre-configuration, such as, base station or access point. MANETs can be deployed and operated without depending on a fixed backbone. However, their features of open medium, lack of centralized monitoring and management point, no infrastructure, dynamic changing network topology, cooperative algorithms, resource constraints and lack of a clear line of defence, they are vulnerable to many attacks. Therefore, there is a major concern about their security.

An in-depth analysis is done on the AODV protocol and the vulnerabilities of the protocol are identified such as blackhole attack. A Sequence

number based approach has been proposed to mitigate collaborative blackhole attack. This solution achieves a very good rise in PDR (Packet Delivery Ratio) and a reduced Average End-to-End Delay and Packet Loss. This solution can be applied irrespective of the protocol and on any routing attacks and a good convincing result can be achieved.

REFERENCES

Surana, K.A., S.B. Rathi, T.P. Thosar and Snehal Mehatre, 2012. Securing Black Hole Attack In Routing Protocol Aodv in Manet With Watchdog Mechanisms, World Research Journal of Computer Architecture – 1: 1.

Tirthankar Ghosh, Dr. Niki Pissinou, Dr. Kami (Sam) Makki, 2005. Towards designing a trusted routing solution in mobile ad hoc networks, Springer Mobile Networks and Applications, 10: 6.

Douglas, S.J., De Couto, Daniel Aguayo, John Bicket, Robert Morris, A High-Throughput Path Metric for Multi-Hop Wireless routing, MobiCom'03 Proceedings of the 9th annual international conference on Mobile computing and networking, ACM, pp: 134-146.

Moumita Deb, 2008. A Cooperative Blackhole Node Detection Mechanism for ADHOC Networks, World Congress on Engineering and Computer Science.

Zhaoyu Liu, Antony, W., 2004. A Dynamic Trust Model for Mobile Ad Hoc Networks", FTDCS. Proceedings. 10th IEEE International Workshop on Future Trends.

Vijayalakshmi, S., S. Albert Rabara, 2011. Weeding Worm hole Attack in MANET Multicast Routing using two novel Technique, International Journal of Computer Applications., 16(7): 26-33.

Natasha Tomar, Arun Kumar Singh, 2014. Study Of Blackhole Attack Focusing On Aodv Protocol In MANET, International Journal of Computer Engineering and Applications, VII: I.

Mr. A. Amuthan and D. Nagamani Abirami, 2012. Multicast security attacks and its counter measures for puma protocol - Int. J. Comp. Tech. Appl., 2(3): 594-600.

FaridNa¨ıt-Abdesselam, BrahimBensaou, and Tarik Taleb, 2005. Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks - (IEEE WCNC).

S.Vijayalakshmi and S. AlbertRabara, 2011. Weeding Wormhole Attack in MANET Multicast Routing using Two Novel Techniques - LP3 and NAWA2- International Journal of Computer Applications (0975 – 8887) 16: 7.

Chi-Sung Laih and Wen-Chung Kuo, 2009. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET - Shang-Ming Jen , ISSN 1424-8220.