ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Detection and Prevention of Black Hole Attack on MANET Routing Protocols

[1]S. Amutha and [2]Kannan Balasubramanian

[1]*Department of Information Technology, P.S.R. Engineering College, Sivakasi, Tamilnadu.*
[2]*Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu.*

ARTICLE INFO

Article history:
Received 12 November 2014
Received in revised form 26 December 2014
Accepted 29 January 2015
Available online 10 February 2015

Keywords:
AODV, Black hole attack, DSR MANET, NS 2, Routing, Security.

ABSTRACT

Due to the mobility, MANET has the dynamic, continuously changing network topology. This feature makes it difficult to perform routing in a MANET. In the presence of malicious nodes, one of the main challenges in MANET is to design a robust security solution that can protect the MANET from various routing attacks such as flooding, black hole, link spoofing, warm - hole attack. The proposed system deals with the detection and the prevention of Black Hole Attack in on- demand routing protocols such as AODV, DSR. The goals of this proposed work are to find the stable, shortest routes and to decrease the routing related overhead. The simulation is achieved by the Network Simulation (NS 2) Tool and the Xgraph is used to plot the network performance of the system.

To Cite This Article: S. Amutha and Kannan Balasubramanian., Detection and Prevention of Black Hole Attack on MANET Routing Protocols. ***Aust. J. Basic & Appl. Sci.,*** *9(5): 281-289, 2015*

INTRODUCTION

Recently, both academia and industry have paid momentous attention in the field of security for MANETs achieving seamless communication for mobile nodes. Each node in the MANETs must forward traffic unrelated to their own purpose, and therefore be a router. The main challenge of constructing a MANET is equipping each node to constantly uphold the information required to properly route traffic.

MANETs are self- organized, decentralized and infrastructure-less networks. So they can form arbitrary topologies depending upon their connectivity with each other in the network. Because of their self configuration ability, these nodes are able to configure themselves and they can be deployed immediately without the need of any infrastructure. MANET Working Group (WG) of Internet Engineering Task Force (IETF) is dedicated for developing the IP routing protocols. Routing protocols have the great deal of attention in today's interesting research area of MANET. Many routing protocols have been made for MANETs such as proactive and reactive routing protocols.

Security in Mobile Ad-Hoc Network is the most significant concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by declaring that security issues have been met. Due to the nature of open medium, dynamic changing of its topology, lacking in central monitoring and management cooperative algorithms and ambiguous defense mechanism, MANETs often suffer from security attacks. These things have changed the conflict field condition for the MANETs against the security threats. In MANETs, the mobile nodes work without a centralized administration on the basis of mutual trust among the decentralized nodes. This characteristic of MANETs make it more vulnerable to be exploited by an inside attacker in the network. Wireless links between the mobile nodes also make the MANETs more vulnerable to attacks, which allows the attacker inside the network and grants the right to use the ongoing communications.

Mobile nodes in the MANETs must have the secure transmission and communication. Secure transmission plays a vital issue as there is increasing threats of attacks on the MANETs. In order to provide secure communication and transmission, the technicians must understand different types of attacks and their effects on the MANETs. A MANET is more open to Black hole attack because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, dynamically changing topology and limited resources. The black hole attack involves malicious node(s) formulating the string number, hence imagination of having the shortest and freshest route to the destination. A

Corresponding Author: S. Amutha, Department of Information Technology, P.S.R. Engineering College, Sivakasi, Tamilnadu.
E-mail: rndamutha@gmail.com

Number of studies have tried to develop the effective detection methods for black-hole attack. The main goal of this paper is to examine the black-hole attack and to develop the detection with in the span of both proactive and reactive protocols such as AODV (Tamilarasan-Santhamurthy, 2011; Bounpadith Kannhavong, 2007), DSDV. These different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

The rest of the article is organized as follows: Section II describes the security requirements for the work which includes the overview of Routing Protocols and Black hole attack. Taxonomy of Existing techniques is detailed in the Section III. Section IV describes the proposed algorithm to detect and prevent the black hole attack on routing protocols. Section V shows the effective simulation results and analysis. Finally, the Section V draws the conclusions and the future work of this article.

2. Security Requirements:

2.1 Routing Protocols:

The key goal of routing protocols in ad-hoc network is to establish optimal path with minimum numbers of hop between source and destination, with minimum overhead and minimum bandwidth consumption so that packets are transported in a timely manner. A MANET routing protocol should work successfully over a broad range of networking environment from small ad-hoc group to larger mobile Multi-hop networks. Routing protocols in MANETs are categorized by proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table-driven. This work deals with secure routing using proactive protocol such as OLSR and reactive or on-demand protocols such as AODV and DSR protocols.

1. Proactive Protocols:

Proactive protocols are also known as Table driven protocols. These protocols keep up the new list of destinations and their routes by periodically distributing the routing tables throughout the network (Tseng, Y.C., 2003). OLSR needs large amount of data for route maintenance and it reacts slowly on restructuring and failures of the network.

2. *Reactive Protocols:*

Reactive Protocols are also known as On-Demand Routing Protocols. This protocol finds the route on demand by flooding the network with route request packets (RREQ). DSR has a higher overhead as each packet holds the entire route, and does not support multicast (Perkins, C., 2003). AODV is a source initiated on-demand routing protocol. Every node in the network maintains a routing table that maintains the information of the next hop node for a route to the destination node. This protocol uses the precise route if a new sufficient route to the destination node is present in its routing table, when a source node needs to route a packet to a destination node.

2.2 Black hole attack:

In MANET, one of the active Denial of Service (DoS) attacks is Black hole attack. In order to pose itself as a destination node or an immediate neighbor to the actual destination node, a malicious node sends a false RREP packet to a source node that initiated the route discovery. The black hole node responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination without delay, when a source node broadcasts the RREQ message for any destination.

The source assumes that the destination is at the rear of the black hole and rejects the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination (Mistry, N., 2010). As a result, therefore, the source and the destination nodes became unable to communicate with each other.

These requirements are needed primarily to deal the black hole attack on selected proactive and reactive protocols in terms of detection and prevention.

3. Taxonomy of Existing Techniques:

Many of the researchers have addressed the problem of black hole attack on AODV. Some of them are as follows:

Lakshmi k et al proposed the solution for Black hole attack on AODV protocol (Lakshmi1, K., 2010). The main goal of this scheme is used to detect the secure routes and prevent the malicious node in the MANET. The concept of proposed method is that requires a source node to wait until a RREP packet arrives from more than two nodes. In the lead of receiving multiple RREPs, the source node verifies whether there is a shared hop or not. If there is, the source node jury that the route is safe. The main problem of this solution is that it initiates time delay, since it must wait until multiple RREPs arrive.

Satoshi Kurosawa et al proposed the statistical based anomaly detection approach for analyzing the black hole attack and that a malicious node must increase the destination sequence number adequately to prove the route provided by the source node is sufficient enough (Satoshi Kurosawal, 2007). Through this analysis, the black hole attacks are detected based on the differences between the destination sequence numbers of the received RREPs. The benefit of the proposed scheme is that the black hole attack detection at low cost without

the need of extra routing traffic, and one more benefit is that it doesn't require the alteration of the existing protocol. Due to the open nature of anomaly detection, this approach had the problem of false positives.

Latha Tamilselvan et al (2008) proposed an enhanced solution on AODV protocol which evades numerous black holes in the cluster. The idea of the technique is to provide the identification of multiple black holes assist with each other and to find out the safe route by avoiding the attacks. Nodes are participated in the communication, since it was assumed as authenticated. The solution leads to the reliability of the node by using the fidelity levels of each node that entered on the fidelity table.

Mohammad Al-Shurman et al proposed two different approaches to solve the Black hole attack (Mohammad Al-Shurman, 2004). The first approach is that the sender node needs to check the authenticity of the node that instigates the RREP packet by using the idleness of the network. The idea of this solution is to discover more than one route to the destination. The SN uni-cast the chink packet using different routes. The IN or destination node or malicious node will peal requests. The SN verifies the acknowledgment checks which one is having malicious node or safe. In this period, the packets are buffered by the SN until it found the safe route. After the identification of safe route, the buffered packets will be transmitted to it. The problem of this solution is the time delay. The second approach is to accumulate the sequence number of the last sent packet and the last received packet in the table. It is automatically updated when any packet is arrived or transmitted. It checks the last sent and received sequence number, when node receives reply from another node. If there is any variance then an ALARM designates the survival of a Black hole node. This results as faster and more reliable and has no overhead.

Though many of the existing techniques are presented against black hole attacks in MANET routing, it needs to be more secure on routing paths and require better performance on the network.

4. Proposed Algorithm:

The proposed solution is proposed to prevent the black hole attacks on routing protocols such as AODV, DRS protocols in the MANET. This solution is principally to alter the working of the source node without sporadic intermediate nodes and destination nodes by using a method called Early-Receive-Reply Method.

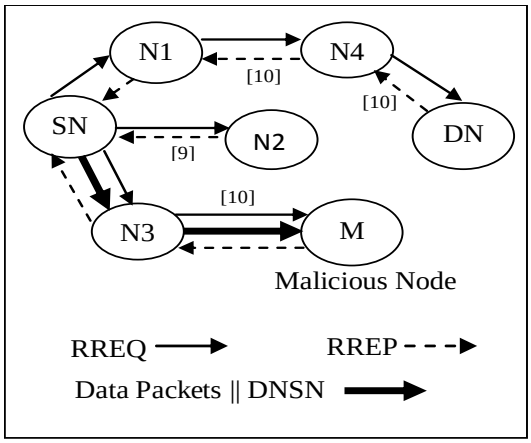

Fig. 1: Routes of control messages in routing protocol.

In this method, we can add the following:

- A new Request Reply Table,
- A variable to identify Malicious Node ID(MN-ID),
- A timer to know Waiting Time.

In this method, the checking method involves to check the differences between the sequence number of source node and the intermediate node, where intermediate node has sent back RREP. In general, the reply from malicious node with the high destination sequence number routes in the RR Table. At the moment, the first destination sequence number is compared with the source sequence number. If there is much more differences between source and destination sequence number, then the destination node is malicious node, the proposed system could immediately remove that entry from the RR-Table. The destination sequence number is a 32 bit integer related with every route. This number is used to find the route as more novel. If the destination sequence number is larger than others, then this number is considered as DNSN from the malicious node. Now, N3 will send RREQ message to the source and eminent it to DN, they would again transmit the RREQ control message. When the node N3 broadcasted the RREQ control messages, the malicious node M also received that RREQ.The malicious node create fake RREP message and send it to node N3 with very high destination sequence

number. Then the node N3 would send it to source node SN.

In AODV, as the destination sequence number is high, the route node N3 will be considered to be novel and hence node SN would start sending data packets to node N3. Therefore, the proposed algorithm deals with the novel idea of sequence number difference checking i.e., source node first checking the difference between the sequence number of source node and the sequence number of intermediate nodes before sending the data packets from source to destination. The node will be considered as malicious node, if the sequence number is too larger than others, and it will be isolated from the network.

The Early _Receive Reply has the following detailed steps to identify and remove the malicious node, when the routing protocols in the MANETs are attacked with the black hole attack.

4.1 Early_Receive Reply (RREP) Method:

Step 1: Low_Level Formating Process

- Discovery Phase starts with the Source node SN.
- Current time and Execution time required executing the prior-Receive Reply (RREP function).

Step 2: Garnering Process

- To store all the Route Replies DNSN and NID in the RR (Request Reply) Table.
- Repeat the above process until the time exceeds.

While ((current time <= (current time + wait time))
{
Store the route replies DNSN and NID in the RRTable.
}

Step 3: Discover and Eradicate Malicious Node

- Retrieve the first entry from RR Table.
- Check the DNSN with SNSN, if DNSN is greater than SSN, then discard the first selected entry from the RR Table.

If (DNSN > SNSN)
{
MN_ID = NID;
Discard entry from table
}

Step 4: Node Assortment Process

- Sort the contents of RR Table entries according to the DNSN.
- Select the NID having highest value of DNSN among the RR Table entries.

Continue step 3 and step 4 until we have to find the destination node.

Step 5: Prolong Default Process

- Call Receive Reply method of default AODV Protocol

Parameters:

Source Node Sequence Number (SNSN), Destination Sequence Number (DNSN), Nod ID (NID), Malicious Node ID (MN_ID)

5. Simulation Results and Analysis:

This section deals with the simulation results of the solution against black hole attack on routing protocols in MANETs.

5.1 Average Delay:

The end-to-end delay is the time taken for a data packet to reach the destination node. The delay for a packet is the time taken for it to reach the destination. And the average delay is calculated by taking the average of delays for every data packet transmitted. The parameter comes into play only when the data transmission has been successful. The following figure depicts the delay analysis by the network. Equation (1) and (2) are used to calculate the average packet delay. The analysis of average delay using AODV and DSR is depicted in the following Fig. 2(a) and 2(b) respectively. The red line indicates the measurement of delay for the presence of 20 MNs, blue line for the presence of 5 Malicious Nodes (MNs), and green line for presence of 10 MNs in the delay analysis using AODV. By the same analysis of delay using DSR the red line indicates the measurement of 20 MNs, green line for 5 MNs and yellow line for 10 MNs.

$$pd = rt_{destn} - tt_{source} \quad (1)$$

$$d = \sum \frac{pd}{n(rp)} \quad (2)$$

Where
pd - packet delay
rt_{detn} – receive time at destination
tt_{source} – transmit time at source
d – average delay
n(rp) – total number of received packet

5.2 Packet Delivery Ratio:

PDR can be derived from the ratio of the number of received packets by the number of transmitted packets to be received and sent from/to the server respectively. By using the equation (3), the PDR is calculated for this MANETs scenario.

The analysis of packet delivery ratio for the presence of 5, 10, 15 malicious nodes (MNs) using AODV and DSR is depicted in the following Fig. 3(a) and 3(b) respectively.

$$pdr = \frac{n(rp)}{n(tp)} \quad (3)$$

Where
Pdr- packet delivery ratio
n(rp) – number of received packets
n(tp) – number of transmitted packets.

5.3 Throughput:

In this case, attacker present at the network will degrade the network performance. The analysis of total throughput with the presence of 5 MNs, 10

MNs and 20 MNs are depicted in the Fig. 4(a), 4(b),4(c) respectively. The total throughput can be calculated by using the following equation (4).

$$Throughput = \sum \frac{t(nodes)}{N} \quad (4)$$

Where
t(nodes) – throughput of nodes involved in data transmission
N- Number of nodes

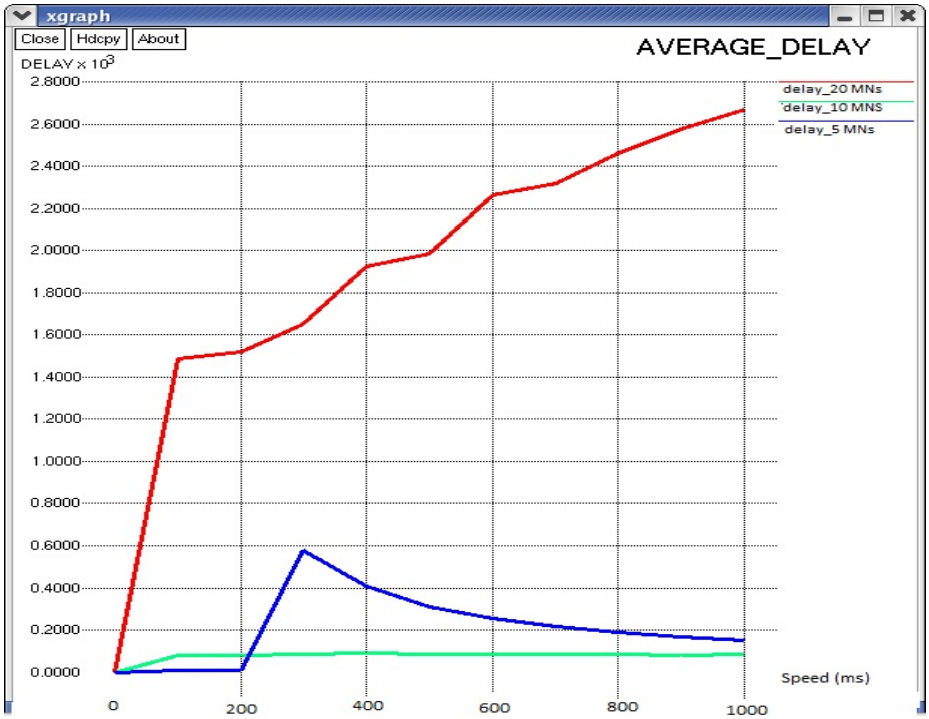

Fig. 2 (a): Analysis of Average Delay (In the Presence of 5, 10, 20 MNs) Using AODV.

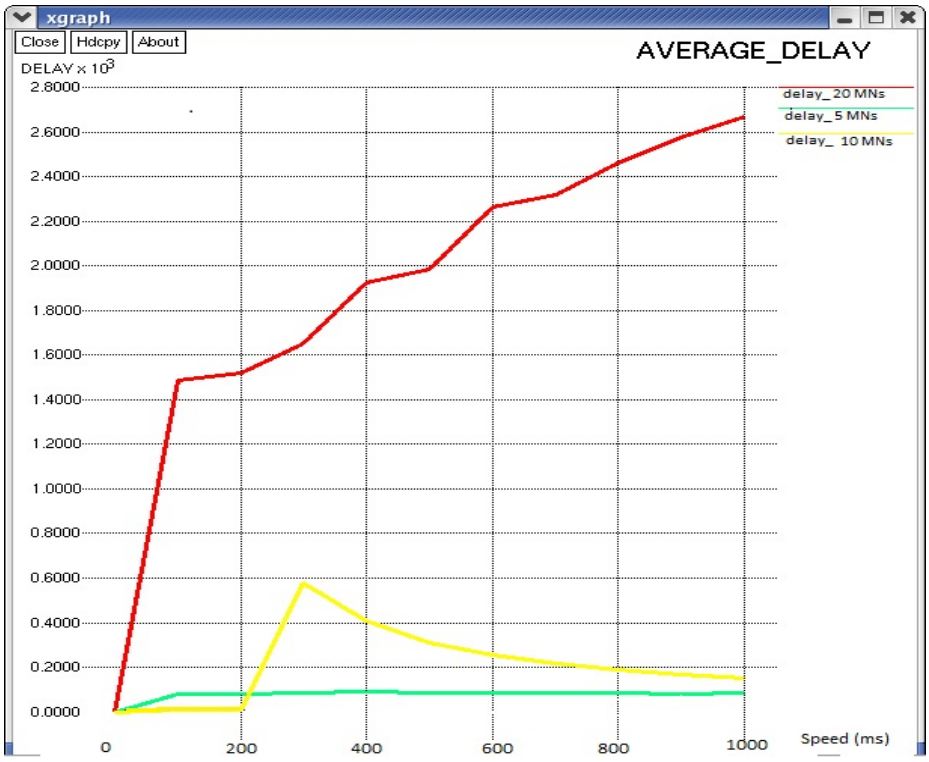

Fig. 2(b): Analysis of Average Delay (In the Presence of 5, 10, 20 MNs) Using DSR.

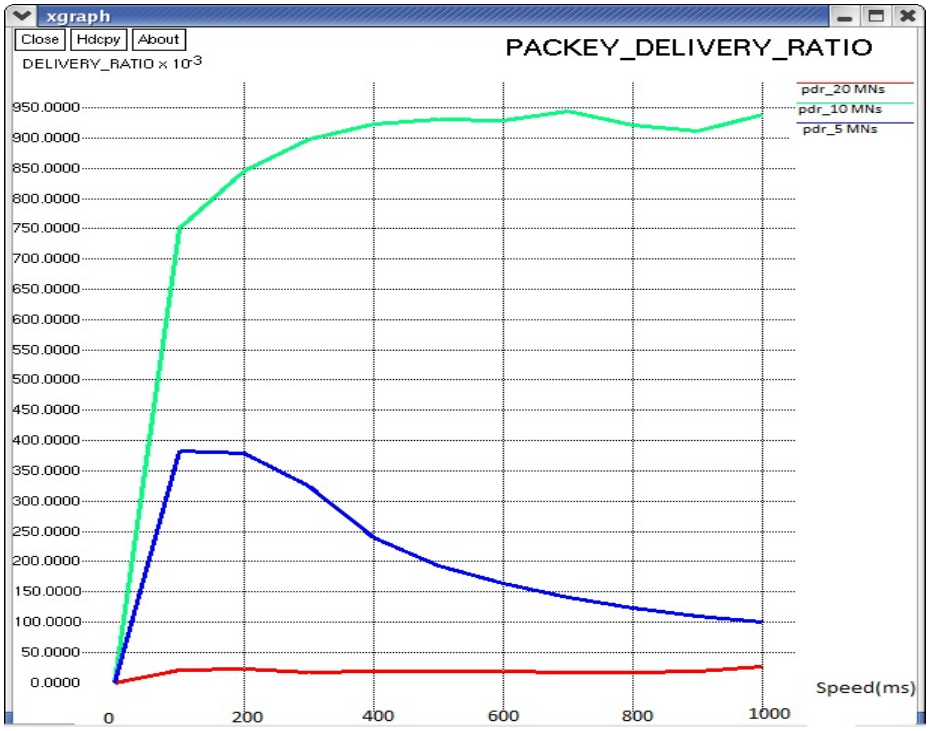

Fig. 3(a): PDR Analysis in the presence of 5,10,20 MNs using AODV.

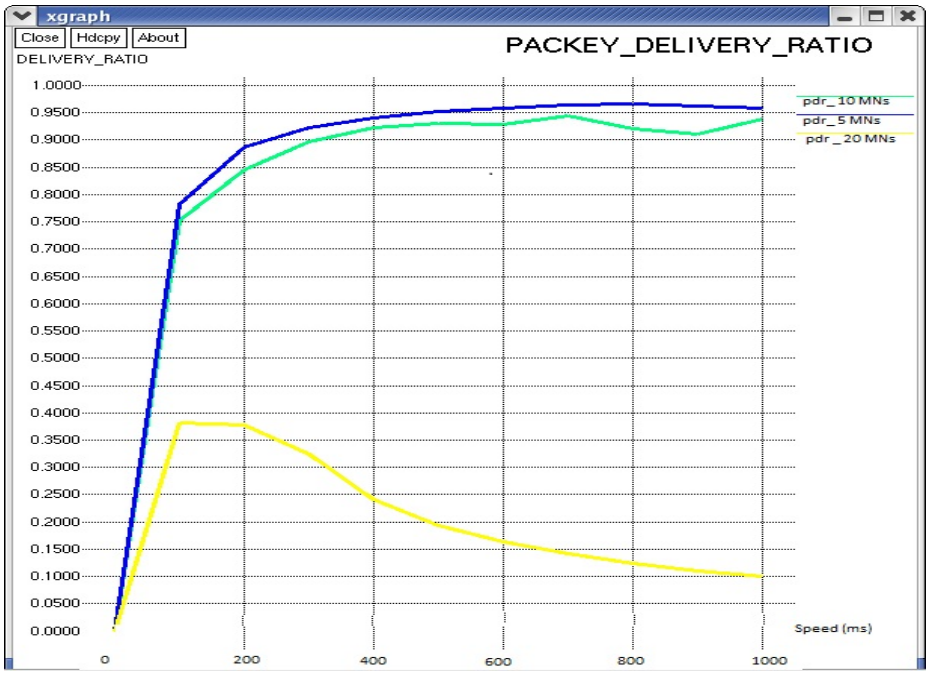

Fig. 3(b): PDR Analysis in the presence of 5,10,15 MNs using DSR.

The analysis of throughput expresses the exclusive results of higher throughput for minimum presence of malicious nodes in the network, since it will affects the network performance as low level compared to the effect of maximum number of malicious nodes can do for the performance.

Fig. 4(a): Total throughput in the presence of 5 malicious nodes.

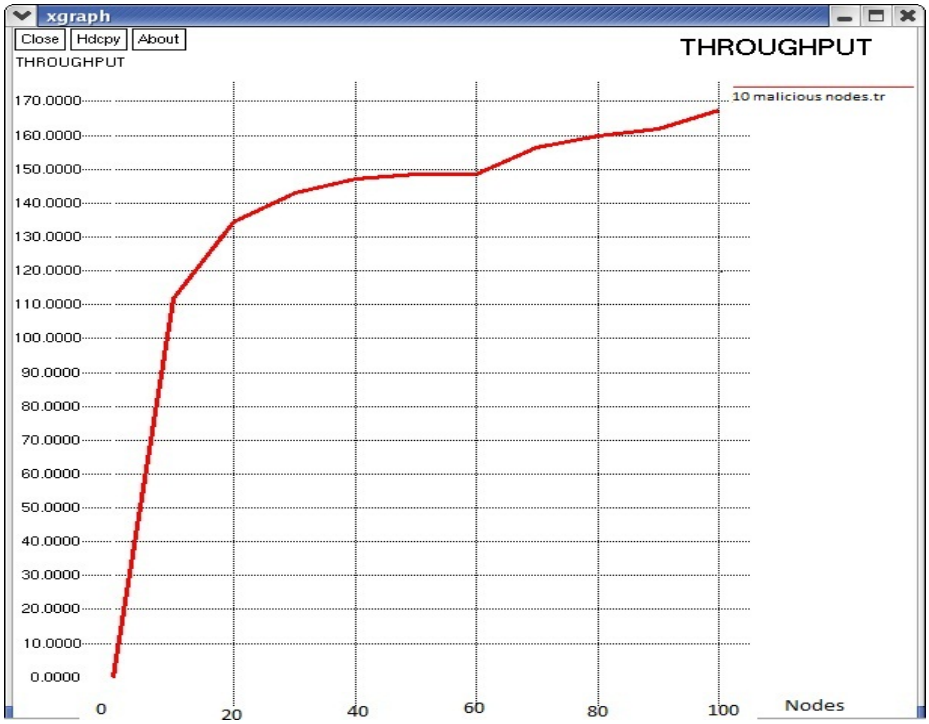

Fig. 4(b): Total throughput in the presence of 10 malicious nodes.

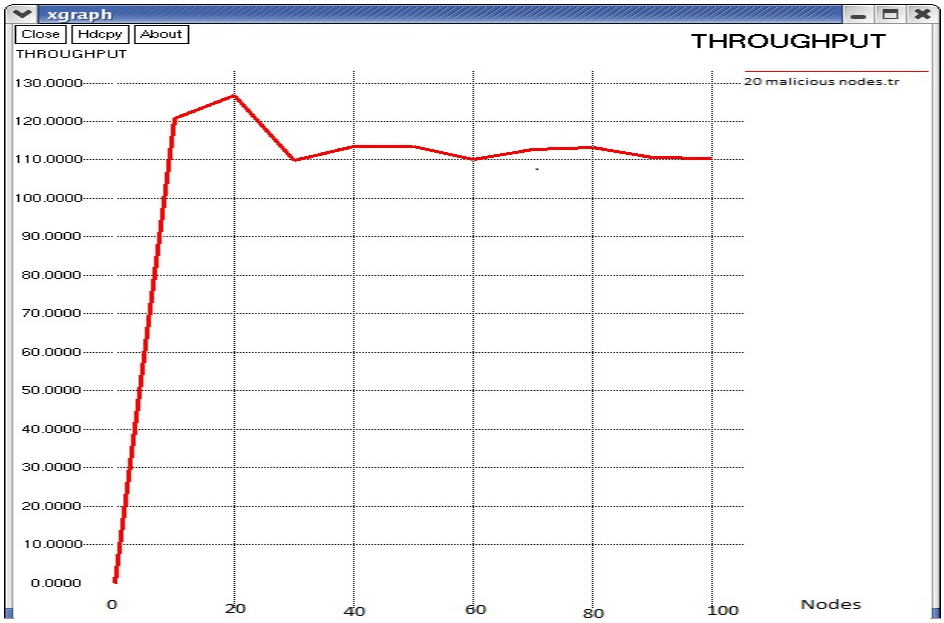

Fig. 4(c): Total throughput in the presence of 20 malicious nodes.

6. Conclusion and Future Work:

This paper gives an efficient approach for preserving the routing protocols against Black hole attacks. The proposed algorithm thwarts the black hole attack in the MANET by identifying the malicious node and also removes it from the network with their sequence number.

The novel algorithm has two steps such as checking the difference between the sequence number of source and destination node, and passes the packets in secure routing. If the first route reply will be from the malicious node with high destination sequence number, then that is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table.

In addition, the proposed algorithm may be used to preserve the identity of the malicious node as MN-Id, so that in future, it can discard any control messages coming from that node. Now since malicious node is identified, the routing table and the control messages from the malicious node, too, are not forwarded in the network. Finally we can conclude that our proposed algorithm has achieved good improvement in PDR with permissible end-to-end delay and lower overhead in DSR. Furthermore, the proposed solution does not require any overhead on either the destination node or any intermediate node on AODV routing protocol.

In future, this secure routing on MANETs against black hole attack will be enhanced with the cryptographic techniques such as AES, ECC encryption and decryption techniques. The network performance will be improved with the future enhancement techniques such as authentication verification and integrity checking.

REFERENCES

An Adaptive Approach to Detecting Black Hole Attacks in Ad Hoc Network, 2010. 24th IEEE International Conference.

Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto and Nei Kato, 2007. “A Survey of Routing Attacks in Mobile AD HOC Networks”, IEEE Wireless Communications, 85-90.

Dokurer, S., Y.M. Erten, Can Erkin Acar, “Performance analysis of ad-hoc networks under black hole attacks”, Turkey.

Lakshmi1, K., S. Manju Priya, A. Jeevarathinam, K. Rama, K. Thilagam, 2010. “Modified AODV Protocol against Blackhole Attacks in MANET by Lecturer, Dept. of Computer Applications”, Karpagam University, Coimbatore. International Journal of Engineering and Technology, 2(6).

Latha Tamilselvan and V. Sankarnarayana, 2008. “Prevention of Black Hole Attack in MANET. Journal of Networks”, 3(5): 13-20.

Mistry, N., D.C. Jinwala and M. Zaveri, 2010. “Improving AODV protocol against black hole attacks. International multiconference of engineers and computer scientists”, Hong Kong.

Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, 2004. “Black Hole Attack in Mobile Ad Hoc Networks”, ACM SouthEast Regional Conference.

Perkins, C., 2003. “(RFC) request for Comments-3561”, Category: Experimental, Network, Working Group.

Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, 2003. "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", International Conference on WirelessNetworks (ICWN 03), Las Vegas, Nevada, USA.

Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto, 2007. "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", In: International Journal of Network Security, 5(3): 338-346.

Tamilarasan-Santhamurthy, 2011. "A Comparative Study of Multi-Hop wireless Ad-Hoc Network Routing Protocols in MANET", IJCSI International Journal of Computer Science Issues, 176-184.ISSN(online):1694-0814.

Tamilselvan, L., V. Sankaranarayanan, 2008. "Prevention of Blackhole Attack in MANET", Journal of Networks, 3(5).

Tseng, Y.C., C.C. Shen and W.T. Chen, 2003. "Mobile ip and ad hoc networks: An integration and implementation experience". Technical report, Deptartment. of Computer Sci. and Inf. Eng., Nat. Chiao Tung Univ., Hsinchu, Taiwan.

Yibeltal Fantahum Alem, Zhao Hheng Xaun from Tainjin, 2010. "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", China, IEEE.