Deployment of Black hole attack using DYMO in MANETs

Ms.Fahmina Taranum[1], Khaleel Ur Rahman Khan[2]
[1]*Muffakham Jah College of Engineering and Technology,* [2]*ACE Engineering College*
(*[1]*ftaranum@mjcollege.ac.in, [2]khaleelrkhan@gmail.com)

***Abstract*—** MANETs is a collection of mobile nodes acting as routers or terminal or relay to liaise via radio communication by dynamically configure itself. Black hole is a security threat to the network since it is an active attack in which attacker either stop or drop packets transmitted to the destination. The attacker tries to direct traffic to itself by advertising in the network with the shortest path to destination or by pretending to have extra privileges sufficient to be treated and trusted as a leader. The paper portrays on deploying an internal active black hole attack using DYMO in MANET. Dymo is a power aware routing algorithm works on the concept of selecting the shortest path to destination for transmitting data. Black hole usually assimilates traffic of the network around it and tries to harm the network by reducing the performance metrics of the system. The aim is to enhance different characteristics for diverting the traffics towards a black hole node. For the transmission of packets CBR is used. Beacon nodes are transmitted to do the handshake. Route requests (RREQ), route reply (RREP) and route error (RERR) are the three types of messages being used in DYMO for communication. Performance metrics is measured using Utilization, Transmission delay, Jitter, Control packet delivery rate, etc and comparative analysis of a network with and without black hole is highlighted.

Keywords—DYMO- DYnamic On-demand routing protocol; CBR; Black hole; RREQ; RREP

I. Introduction

A network is created with multiple nodes viz. source, destination and malicious in addition to intermediate and gateway nodes. A gateway node uses IP address to route packets to external network. Node in QualNet can represent any of the several devices that connect to a network, such as radio devices, desktop computers, routers, satellites, etc. In the current scenario nodes are selected as default mobile devices with three network interfaces, each of which has its own IP address and subnet mask. Nodes communicate with each other through connected network interfaces and collection of nodes in network is referred as subnet. A node can be a member of multiple subnets and has an interface to each subnet it belongs to. An example of a network IP address is 192.168.0.0, and an example of a corresponding subnet mask is 255.255.255.0. The subnet mask indicates that 8 bits are used to determine host IP addresses. Dymo is applicable for both IPv4 and IPv6 protocols with dynamic or reactive nature. Here control packets are generated only when the node receives data packet and does not contain routing information. The basic operation of DYMO protocol is route discovery, the route request (RREQ) routing message is generated for a target node for which it does not have any routing information. Source node floods the RREQ message to find the target node. During flooding each intermediate node records a route to the originating node by adding the routing information into routing table. When the target node receives the RREQ, it responds with a route reply (RREP) message which is sent as a unicast message toward the originating node. Each node that receives the RREP records a route to the target node and forwards the RREP to next hop. When the originating node receives the RREP, routes are established between the originating node and the target node in both directions. In order to react to the changes in the network topology nodes maintain their routes and monitor their links. A route error (RERR) message is generated by a node whenever it receives a data packet for a destination to which it has no route in its routing table. This RERR broken notifies other nodes that the current route is broken.

The rest of the paper is organized as follows: Section II provides a brief description of related work; Section III describes about methodology; Section IV discusses the result analysis; Section V portrays on conclusion and future research scope.

Section II
Related Work

Black hole detection and prevention scheme using DYMO is proposed by Dhiraj et. al [1]. The parameters like transmission power and Antenna height are used to deploy a malicious node in the network. For detection and prevention a threshold is set to check the suspicious value for the neighboring node, if it exceeds then the node is declared as suspicious and is eliminated from transmission. The malicious node may or may not belong to the network and may also be a hidden node. Suspicious node advertises in the network by promising with the shortest path, thereby attracting traffic and dropping packets; hence preventing it to reach the destination node. Parameter used under result analysis includes number of nodes, speed, pause time and terrain size.

Rakesh Ranjan et. al discusses security issues of Black Hole attack in MANETs [2].The paper focuses on a single and cooperative black hole attack and concluded the identification of malicious node is more difficult in case of cooperative attack. Author has explored and discussed types, issues and solutions of multiple types of network attacks and concluded that security is a major concern for the network layer attacks.

Prevention of Black hole on AODV is highlighted in [3] by comparing the sequence number, if the destination sequence number is greater than source sequence number then the node is identified as malicious and is removed from the route request table. Performance evaluation is done using packet delivery ratio and End to End delay. Author has also analyzed the behavior and challenges to security threats in MANET.

The formulas used to measure the performance metric in the paper are listed below, which are inherited from [2].

$$Packet\ delivery\ ratio = \frac{Number\ of\ data\ packets\ received}{Number\ of\ data\ packets\ sent} * 100 \quad (1)$$

$$End\ to\ End\ Delay = D = \sum_{k=1}^{n} \frac{x^k}{n} \quad (2)$$

Where x represents types of delays like route discovery queuing, processing at intermediate nodes propagation time, data acquisition and n represents the number of delays considered in transmission. Formulas (1) and (2) have been adapted in the proposed scenarios along with other performance metrics.

[4] Author has examined the performance by deploying a black hole in AODV and concluded that the deployment of a black hole reduces the packet deliver rate to a greater extent.

[5] The node misbehavior under varying degree is analyzed for AODV and DYMO. The three types of node misbehavior discussed include type1, 2 and 3.Type 1 nodes drop some or all data packets which has source or destination node address, but it participates in route discovery and route maintenance phases. Type 2 uses energy for its own communication; it does not participate in route discovery and route maintenance phases and acts as passive eavesdropper snooping the information in the network. Type 3 is similar to type 1 and behaves in a selective manner i.e. it start dropping the data packets when the energy is below the set threshold to conserve the energy and with an attempt to disrupt the communication.

[6] The analysis of different parameters for wireless routing protocols is done using qualnet 5.2. The simulation was conducted using CBR and under extension of the paper the author has proposed using FTP. The packet delivery rates of some wireless protocols were compared.

[7]Author has proposed a solution that is an enhancement of the basic AODV routing protocol to avoid black holes by waiting and checking the replies from all the neighboring nodes to find a safe route. After receiving the first request it sets timer in the Timer Expired Table. It will store the sequence number and the time at which the packet arrives in 'Collect Route Reply Table' (CRRT). The waiting time is proportional to nodes distance from the source. It calculates the 'timeout' value based on arrival time of the first route request. It then checks in CRRT for repeated next hop node. If any repeated next hop node is available in the reply path then chance of malicious paths is limited, thereby eliminating the possibility of malicious node.

[8] The proposal is to measure the performance analysis of the routing protocols of network layer and Application layer based protocols used for IPv4 and IPv6 standards. The performance metrics is calculated using unicast offered load, Average delay, Average jitter overhead and throughput. The analysis proves that RIPng out performs network layer protocols. RIP and RIPng works at the application layer whereas other routing protocols are operational at the network layer.

Section III
Methodology

Black hole attack is a security threat, which is explicitly deployed in the proposed system. Black hole node advertises itself as having a valid route to destination which is spurious and facilities with other characteristics required to divert traffic forwarded to destination node towards itself. The malicious node tries to capture the packets of the network with the intention to harm the network by decreasing the performance, packet delivery rate, throughput and efficiency of the network and thereby increasing the delays. The detection and prevention strategies need to be handled by using some mechanism. For detection mechanism the traffic at the destination is monitored to check whether the packets are delivered or not, if the packets are not delivered after the set threshold then; other nodes of the network are checked to find a node with the maximum packet drop and this node is referred as a malicious node. The aim of the prevention mechanism is to eliminate this malicious node from data transmission after waiting for some duration for the acknowledgement and confirmation. It is observed from fig. 1 that if the link near the black hole node is broken, then even though it does not have the route to destination it sends back fake replies to source node (indicated by mustard color links). The route discovery and route reply using DYMO with an orange color malicious node absorbing traffic and sending fake reply to the source node is depicted in fig. 1.The subnet 1 and subnet 3 are IPv6 based and subnet 2 is IPv4 based containing four nodes each, which are mobile in nature.

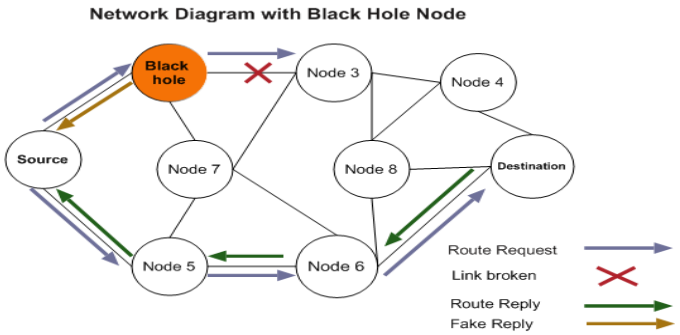

Fig. 1: Deployment of Black hole node

The hardware configuration used to design the scenario is shown in Table 1, these are set at the different layers in the configuration.

Parameter	Value
Qualnet version	7.4
Terrain Size	1500*1500 meters
Physical Layer	802.11b Radio
Mobility model	Random waypoint
Routing Protocol	DYMO
Network Layer	IPv4, IPV6
Simulation Time	60 seconds
Pause Time	30 seconds
Frequencies	2.4 GHz
No of Channels	3
Packet size	100

Table 1: Parameters used in the scenario

Architecture

The architecture shows three subnets with IPv6-IPv4-IPv6 configuration, source node- node 1, destination node- node 16, and malicious node- node17 are shown in fig. 2. The three dimensional architecture is shown in fig. 3.

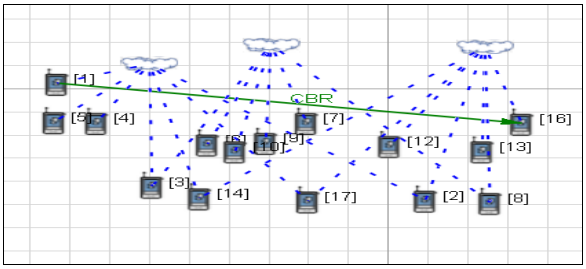

Fig. 2: Network Architecture with subnet & mobile nodes

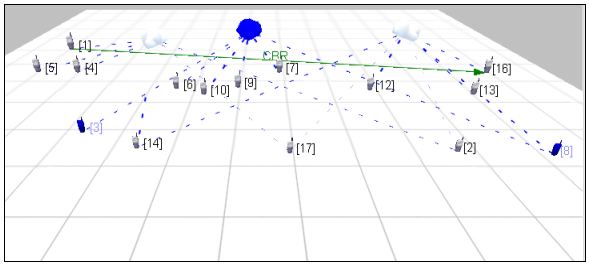

Fig. 3: 3D Architecture with 3 subnets

The transmission of data using DYMO routing algorithm is shown in fig. 4 and the architecture with a black hole node is depicted in fig. 5.

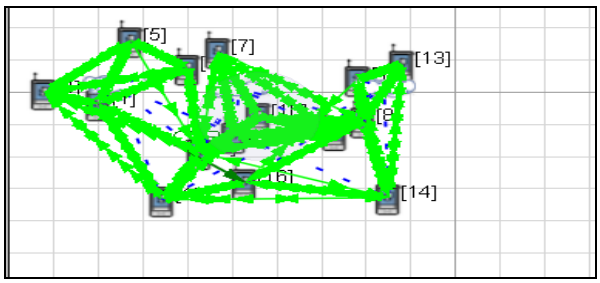

Fig. 4: Transmission using DYMO

The nodes move within the terrain size allocated in the scenario properties with a minimum speed of 0 mps to maximum 10mps using random waypoint model.

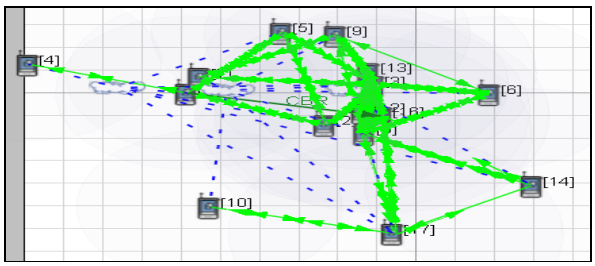

Fig. 5: Transmission in DYMO with a malicious node

Node 17 is deployed as a malicious node by modifying the hardware level features like reception transitivity at 2Mbs is set as -69; Antenna height is 30m; maximum speed is 6mps; noise factor is 20 and maximum hop limit is 20.The packets sent through other routes are forwarded to the destination using shortest distance algorithm except the route containing a black hole node. The transmission acceptance power becomes more for malicious node as the antenna height is increased to capture more packets in the designed scenario. The changes done layer-wise to deploy a malicious node is demonstrated.

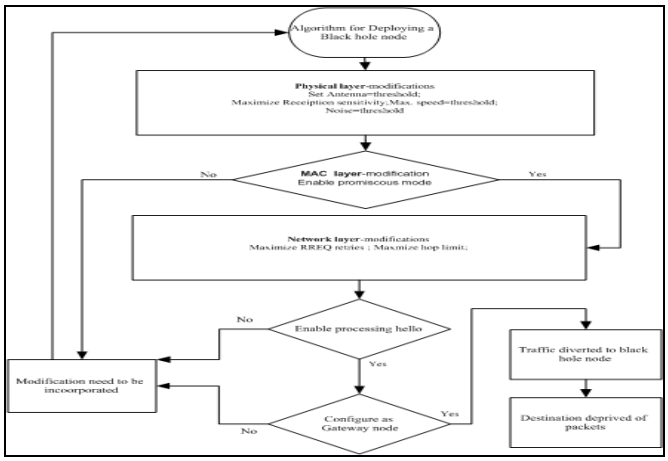

Fig. 6: Algorithm to deploy Black hole node

Nodes 3 and node 8 are configured as gateway and dual Ip. CBR traffic connects the source node to destination node for sending 100 data packets of 512 bytes from node 1 to node 16.The simulation time varies. Source node will continuously send data packets to the target node till the end of simulation time. The tunneling concept is used to make the IP versions compatible and is applied to the second subnet. Black Hole is created by facilitating a node with extra features as highlighted in fig. 6 algorithm. The proposed scenario is created to deploy a black-hole node in the network and detection plus prevention are the enhancement to be incorporated. The basic DYMO routing protocol is used as it is power aware routing algorithm and a comparison of this algorithm is done with a malicious node deployed in DYMO to check the characteristically differences in the normal network to a malicious network

Section IV
Result Analysis

The analysis of deploying a black hole node in DYMO is discussed in the result analysis using generated file statistic (.stat) file in qualnet 7.4 and is graphically depicted from fig. 7 to fig. 14.

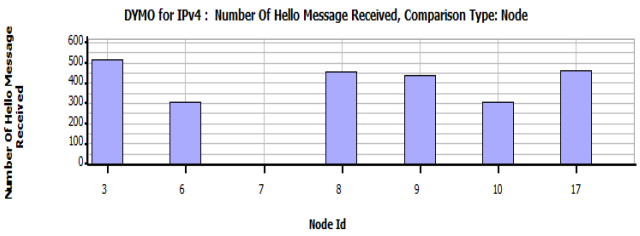

Fig. 7: Beacon messages at Subnet 2

The CBR traffic is transmitted from the source node-1 to the destination node-16. Hello messages are activated to do the handshake for all the connected and active nodes. As shown in fig. 7 more hello messages are received by the black hole node 17 and gateway nodes-node 3 and node 8.

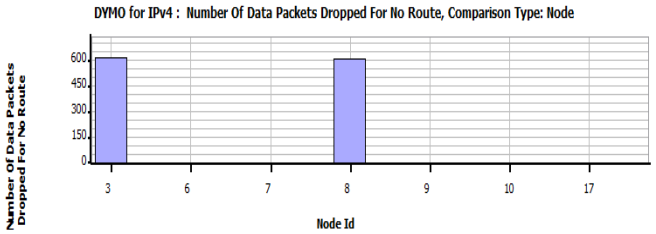

Fig. 8: Packet drop rate at Gateway node

The number of packets dropped is more at the gateway node for no route explored since the nodes from different IP configuration are connected by gateway nodes as shown in fig. 8.

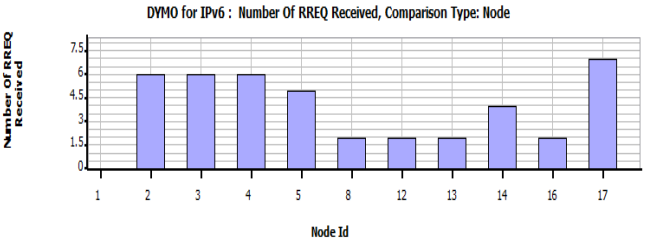

Fig. 9: No. of RREQ received for IPv6

The route request for the nodes connected to IPv6 is shown in fig. 9 and the nodes connected to IPv4 is not depicted in fig.9

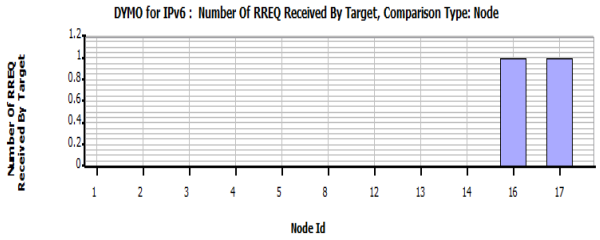

Fig. 10: No. of RREQ received by target

Because of the extra privileges assigned to the black hole node, its reception probability increases and has the highest RREQ received value among all the nodes connected to IPv6 as shown in fig. 9 and fig. 10. The destination node-16 and black hole node-17 receives almost same RREQ because of the extra facilities enabled at the malicious node.CBR is used to connect source with destination node thereby enabling traffic to be directed to the sink.

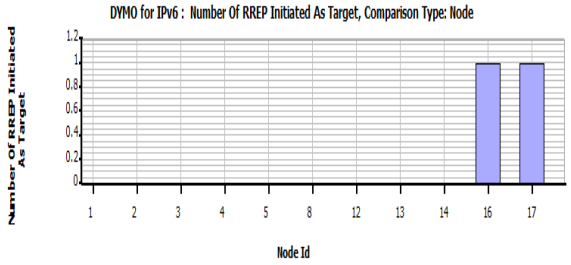

Fig. 11: No. of RREQ initiated as target

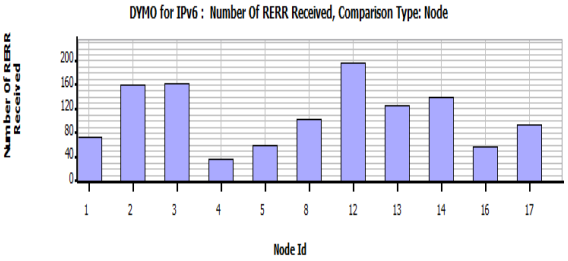

Fig. 12: No. of RERR received for IPv6

The analysis of DYMO at the network layer for RREQ and RERR for the IPv6 subnets-[subnet 1 and subnet 3] is depicted in fig. 11 and fig. 12.The RREQ initiated for black-hole node is almost same as destination node. RERR messages received through control packet for a black-hole node are more than the destination node, which is because of link failure or unavailability of node being discovered through RREQ in fig. 12. A packet consists of user data and control information which is also referred as payload. A packet header carries certain types of metadata along with routing information. IP data packets have a header containing an IP address of origin and destination IP address. Data packets may also have trailers that help refine data transmission whereas control packets do not store routing information; it contains monitoring information like RTS, CTS, RREQ, RREP and RERR. The statistics in fig. 13 and fig. 14 shows that the black-hole node and destination node receives data and control packets in the same proportion.

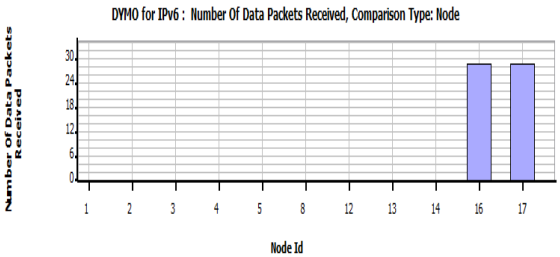

Fig. 13: No. of Data packets received

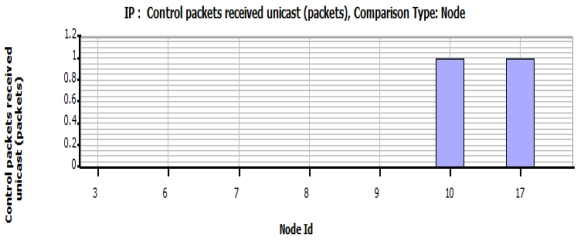

Fig. 14: No. of Control packets received

Comparison of DYMO and Black-hole node

The analysis is made in between DYMO without malicious node to DYMO with malicious node at different layers like Network, Mac and Physical and are depicted from fig. 15 to fig. 26

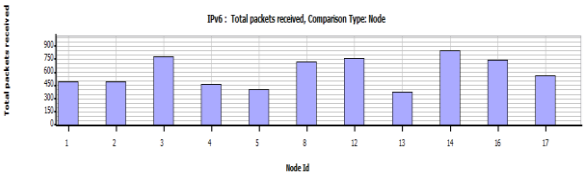

Fig. 15: Total packets received- without Black-hole

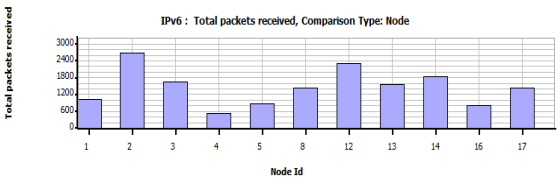

Fig. 16: Total packets received- with Black-hole

The total packet received by the IPv6 subnets is shown in fig.15 with a conclusion that the destination node receives more packets in a normal network to malicious network in fig.16. Hence, it is proved from fig. 16 that a black-hole node [node 17] imbibes traffic of the network and the destination node [node 16] is being deprived of transmission.

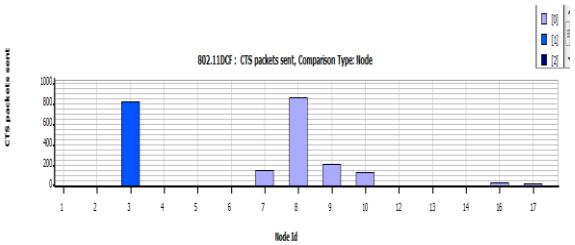

Fig. 17: Clear to Sent packets-without Black-hole network

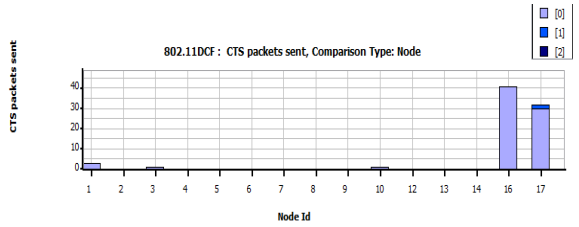

Fig. 18: Clear to Sent packets- Black-hole Network

CTS/RTS (clear to sent/request to sent) are approaches to implement virtual carrier sensing in IEEE 802.11b standards for avoiding collisions at the MAC layer. The CTS packet sent in fig 17 for destination node is almost negligible, whereas it is largely noticeable in fig.18 for both destination and malicious node.

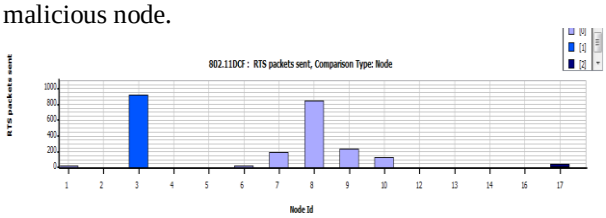

Fig. 19: Request to sent packets-without Black-hole Network

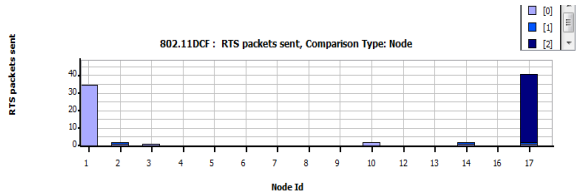

Fig. 20: Request to send packets- Black-hole Network

The gateway nodes- node 3 and node 8 in fig. 19 sends maximum number of RTS in a non malicious network whereas in fig. 20 the sender and the malicious node have the maximum RTS packets sent.

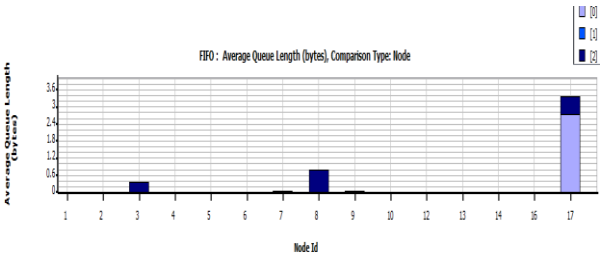

Fig. 21: Network layer-FIFO- without Black-hole

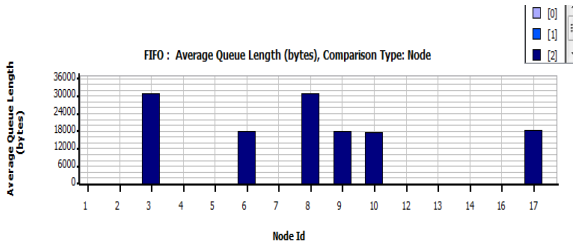

Fig. 22: Network layer-FIFO- with **B**lack-hole

The proportion of average queued length in bytes using FIFO for without black hole to with black hole network is in the ratio of 1.53:: $22*10^3$ as shown in fig. 21 and fig. 22,the peak values are observed at gateway nodes.

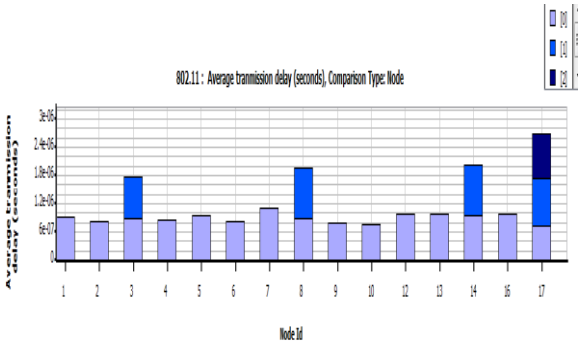

Fig. 23: Physical layer-Transmission delay- without Black-hole

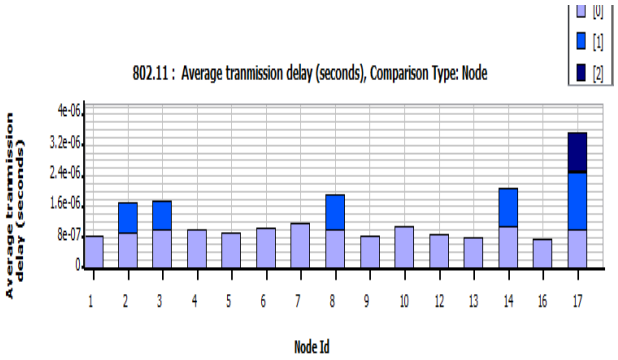

Fig. 24: Physical layer-Transmission delay- Black-hole

The delay in network terminology is used to specify the time it takes for a bit to travel from source to destination .At the physical layer the average transmission delay is calculated for all the nodes of the network and it has been observed that the transmission delay is slighter more in case of malicious network as shown in fig. 23 and fig. 24. The utilization refers to effective use of different parameters that helps in transmission to improve performance metrics as shown in fig 25 and it is observed that the non black-hole has better utilization when compared to black-hole. The jitter estimate is computed taking absolute values of IP delay variation sequence as shown in fig. 26 for all dual-Ip configured and gate way nodes.

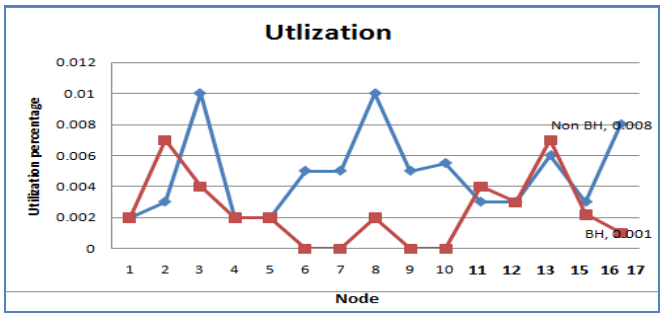

Fig. 25: Physical layer- Utilization

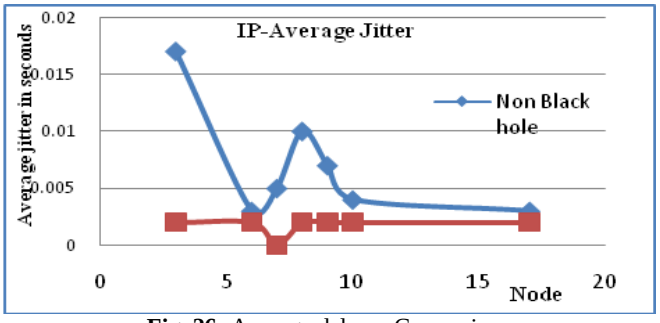

Fig. 26: Average delay – Comparison

Enhancement

The main challenge in MANET after deployment of black hole is to design a robust security solution to detect and protect the network from various types of routing attacks- viz. black-hole, worm-hole and grey-hole**.** Further FTP, dynamic CBR, FTP and telnet can be used to check the best traffic flow in the network and comparative analysis can be made.

References

[1] Dhiraj Nitnaware,Anita Thakur, "Black Hole Attack Detection and Prevention Strategy in DYMO for MANETS", 3rd International Conference on Signal Processing and Integrated Networks (SPIN)-2016.

[2] Rakesh Ranjan, Nirnemesh Kumar Singh and Ajay Singh, "Security Issues Of Black Hole Attacks in MANET", International Conference on Computing, Communication and Automation, IEEE 2015.

[3] Pooja Jaiswal, Rakesh Kumar, "Prevention of Black Hole Attack in MANET", International Journal of Computer Network and Wireless Communication, October 2012.

[4] Mangesh Ghonge,S.U.Nimbhorkar, "Simulation of AODV under Blackhole Attack in MANET",International Journal of Advanced Research in Computer Science and Software Engineering ,vol. 2,Issue 2, February 2012.

[5] Sudhir Agarwal,Sanjeev et al, "Mobility based Performance Analysis of AODV and DYMO under Varying Degree of Node Misbehavior, International Journal of Applications, vol. 30,September 2011.

[6] Jogendra Kumar, Annaurna Singh, "Study AND Performance Analysis of Routing Protocol Based on CBR", Science Direct, Procedia 2016.
[7] Tamilselvan, L.Sankaranarayana,"Prevention of Blackhole attack in MANET", Journal of Networks, Vol.3, No.5 May 2008.
[8] Fahmina Taranum, Khaleel Ur Rahman Khan, "Performance analysis of routing protocol based on IPv4 and IPv6", and IPv6", International Conference on Innovative Technologies in Engineering, April 2018.

Author's Biography

Ms. Fahmina Taranum is an external research scholar of Jawaharlal Nehru Technological University, Hyderabad registered with a title "Transaction Management in Mobile Adhoc Network" and has published some papers in conferences and journals. Presently working as an Associate Professor in Muffakham Jah College of Engineering, Hyderabad.