IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

To Study the Impact of Black Hole Attack in MANET using AODV & DYMO Protocols

Manju[1], Mr. Kapil Kaswan[2]

M. Tech, CSE, CDLU, Sirsa, India[1]

Asst Professor (CSE), CDLU, Sirsa, India[2]

Abstract: A Mobile Ad-hoc Network (MANET) is a dynamic wireless network that can be formed without the need for any pre-existing infrastructure in which each node can act as a router. Mobile ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links. Wireless Networks enable users to communicate and transfer data with each other without any wired medium between them. The main classes of routing protocols are Proactive, Reactive and Hybrid. In this work an attempt has been made to compare the performance of prominent on demand reactive routing protocols for MANETs: - Ad hoc On Demand Distance Vector (AODV), OLSR (Optimized Link State Routing) and Dynamic Manet on demand (DYMO). AODV is a reactive protocol: the routes are created only when they are needed. The simulation is carried out using the ns-2 network simulator. The Blackhole attack has been implemented on the routing protocol. The Research proposal considered five different simulation environments with different number of nodes which are 5, 10, 15, 20 and 25 and results are compared in a graphical representation. There are number of parameters considered for compare the performance among these protocols. The parameters are Throughput (Good put), packet delivery ratio and Routing Overload. The results presented in this work illustrate the importance in carefully evaluating and implementing routing protocols in an ad hoc environment.

Keywords: AODV (Ad hoc On-Demand Distance Vector); OLSR (Optimized Link State Routing); Dynamic Manet on demand (DYMO), MANET (Mobile Ad Hoc Networks), PDR (Packet Delivery Ratio), Throughput.

I. INTRODUCTION

Wireless Networks enable users to communicate and transfer data with each other without any wired medium between them. One of the reasons of the popularity of these networks is widely penetration of wireless devices. Wireless applications and devices mainly emphasize on Wireless Local Area Networks (WLANs). This has mainly two modes of operations, i.e. in the presence of Control Module (CM) also known as Base Stations and Ad-Hoc connectivity where there is no Control Module. Ad-Hoc networks do not depend on fixed infrastructure in order to carry out their operations. These networks exhibits the same conventional problems of wireless communications i.e. bandwidth limitations, battery power, enhancement of transmission quality and coverage problems. Wireless networks can be classified in two ways:

a. Infrastructured networks
b. Infrastructureless networks

Infrastructures networks consist of a network with fixed and wired gateways. A mobile host communicates with a bridge in the network (called base station) within its communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This is called handoff. In this approach the base stations are fixed.

Infrastructure less networks in contrast to infrastructure based networks, in ad hoc networks all nodes are mobile and can be connected dynamically in an arbitrary network. This may be done either because it may not be economically practical or physically possible to provide the necessary infrastructure or because the situation does not permit its installation. Users may not be sparse or dense that the appropriate level of fixed is not an economical investment. Sometimes fixed infrastructure exists but cannot be relied upon, such as during disaster recovery. Finally, existing services may not provide adequate service, or may not be too expensive. Ad hoc mobile networks are attracting a lot of attention these days due to little efforts needed to deploy them. These networks prove to be economical in sparse areas. In emergency services such as disaster recovery these networks are the only possible options. There are no dedicated routers, access points and cables. They are speedy, low cost and efficient.

Features:

1. Dynamic network topology

Each node in a mobile ad hoc network is free to move randomly. This feature makes the network topology change dynamically. Also an ad hoc network may be comprised of both bi- directional or uni- directional link.

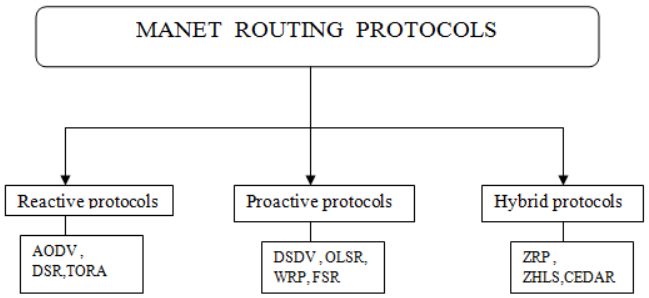
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

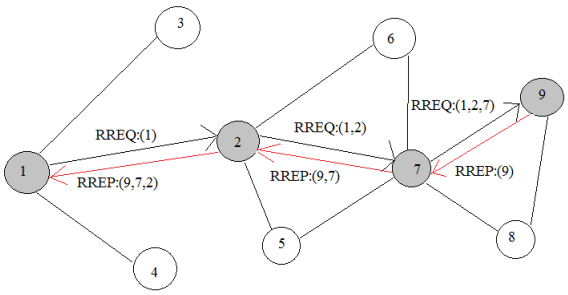
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

2. Bandwidth Limited and Fluctuating capacity Links
Wireless links will remain to have substantially lower capacity compared to their hard wired counter parts. The throughput of the wireless communications is often less because there may be effects of multiple access, fading, noise and interference conditions.
3. Low – power and Resource limited operation
In most cases, the network nodes in a wireless ad hoc network may depend on batteries and other means of energy. This feature makes the power budget tight for all the power consuming components in a mobile device.
4. Constrained Physical security
In general mobile wireless networks are more likely to be vulnerable to physical security threats than are fixed cable nets. For example, there is the increased possibility of eavesdropping, spoofing, and denial of service attack that should be carefully considered.
5. Decentralized Network Control
As an advantage the decentralized nature of network control in mobile ad hoc networks supports extra robustness against the single points of failure of more centralized approaches.

Hierarchy of Routing Protocols
Routing is a technique which gives proper direction to which any communication between one or more networks can take place. Routing protocol specifies how the communication is carried between nodes.
Routing in MANETs is a critical issue, since each node acts as a router. To preserve the security of MANETs from different types of attacks, a routing protocol must fulfil certain requirements. A routing protocol specifies how particular communication is carried between different routes. Thus, the routing algorithm helps in selecting the choices of routes that can be followed. Accordingly there are three major types of routing protocols – reactive (on – demand), proactive (table – driven) and hybrid. In the paper the reactive routing protocols and DYMO routing protocol has been discussed in details. Routing protocols of mobile ad hoc network is divided into three different categories:-
1) Reactive routing protocols
2) Proactive routing protocols
3) Hybrid routing protocols



DYMO routing protocol
DYMO (dynamic MANET on-demand routing protocol) is a newly proposed routing protocol. It has been proposed by Perkins and Chakeres and its first internet draft was released in 2005. Currently it is in its 26th version and still in process. It is considered as a successor of AODV routing protocol which is a reactive routing protocol. It shares many features of AODV routing protocol and is also named as AODVv2.
It adds no special feature to itself, the basic operations of DYMO are similar to that of AODV i.e. route discovery and route maintenance, it just simplifies it. It also handles features from DSR routing protocol which is source routing. DYMO was designed to handle the dynamic nature of mobile networks. It also contains sequence number logic, hop count and control messages from AODV.



IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

II. LITERATURE REVIEW

[1] P. Pham, S. Perreau, and A. Jayasuriya(2005), "New Cross-Layer Design Approach to Ad Hoc Networks under Rayleigh Fading", IEEE.
The author has been assimilated the knowledge about design approach of Ad-hoc network and proposed a new cross-layer design employing the predictability of Rayleigh channels to improve the performance of ad hoc networks. They also explain a Markov model for Rayleigh channels and an innovative Markov model for IEEE 802.11 distributed coordination function. By combining these two models, they derive the theoretical expressions for network throughput, packet processing rate, packet loss probability, and average packet delay under Rayleigh channels. The simulation of the proposed cross-layer design is also carried out. They shown that the new approach improves the network throughput, reduces unnecessary packet transmissions and therefore reduces packets lost. They also show that there is a close match between the analytical and the simulation results which confirms the validity of the analytical models.
[2] Osama H. Hussein, Tarek N. Saadawi (2005), "Probability Routing Algorithm for Mobile Ad Hoc Networks Resources Management", IEEE.
Author has been introduces a resource management application of a probabilistic-based ant routing algorithm for mobile ad hoc networks (ARAMA) that is inspired from the ant's life . Mobile ad hoc networks (MANETs) are highly dynamic, self-configured and self-built networks. The goal of this paper is to present ARAMA ability to manage MANET's resources by achieving fair network resources distribution, while considering the dynamic characteristics of MANETs and the need for low control overheads. This paper provides a description for the algorithm. In this algorithm, the nodes' (node's energy, processing power,) and links' (bandwidth,) parameters are measured and collected in the nodes' indices. A path index is used to measure the path total resources and serves to minimize the forward control packet (ant) size. More, the results show the general ability of the algorithm to solve MANET's routing problem.
[3] Mei-yu Feng, Sheng Cheng, Xu Zhang and WeiDing (2007), "A Self Healing Routing Scheme Based on AODV in Adhoc Networks", IEEE.
The author has explained the routing schemes and many routing protocols have been proposed for ad hoc networks and many research works have been done to improve the performance of routing protocols. They explained that this cannot overcome the problems of edge effect and route break at same time without incurring heavy control overhead. In this paper, based on the analysis of routing problem, a self-healing routing scheme based on AODV (SHAODV) is proposed. In this scheme, routes can be constructed with long lifetime and unstable route can be self-heal to stable one before being broken absolutely. Simulation shows that the scheme wins lower average route overhead and lower times of route break than AODV.
[4] Satoshi Kurosawa (2007), "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security.
This paper analyzes the Blackhole attack which is one of the possible attacks in ad hoc networks. In a Blackhole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. In conventional schemes, anomaly detection is achieved by defining the normal state from static training data. However, in mobile ad hoc networks where the network topology dynamically changes, such static training method could not be used efficiently. In this paper, they propose an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. The simulation results show the effectiveness of our scheme compared with conventional scheme.
[5] Vishnu K, and Amos J .Paul (2010), "Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks", International Journal of Computer Applications.
The author has explained the Blackhole and grayhole attack in Mobile adhoc network. Mobile ad hoc networks (MANET) are widely used in places where there is little or no infrastructure. A number of people with mobile devices may connect together to form a large group. This dynamically changing network topology of MANETs makes it vulnerable for a wide range of attack. In this paper they proposed complete protocol for detection & removal of networking Black/Gray Holes.
[6] K. Lakshmi, S. Manju Priya (2010), "Modified AODV Protocol against Black Hole Attacks in MANET", International Journal of Engineering and Technology.
The author has been explained the AODV routing protocol and modified the AODV file for Blackhole attack implementation and analysis. In Mobile Adhoc Network (MANET), it consists of a collection of wireless mobile hosts without the required intervention of any existing infrastructure or centralized access point such as base station. The dynamic topology of MANET allows nodes to join and leave the network at any point of time. Wireless MANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and constrained capability. So security in MANET is a complex issue. There are many routing protocols that establish the routes between the nodes in the network.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

III. OBJECTIVES

There are number of routing protocols used in MANET for Nodes Communication but correspondingly, the number of problems exists in the communication. The Research Work has shown that reactive protocols are more adaptable to MANET environments than proactive protocols. DYMO is new member to the protocol family and is under development period. It is mandatory to study all the relating effects of DYMO with and without any particular type of attack. To render the network function normally in the presence of misbehaving nodes is a challenging task and demands it necessary to consider "fault tolerance" as a main objective at the design level of routing protocols. It seems imperative to provide a simulation study that measures the impact of misbehaving nodes in order to provide protocol designers with new guidelines that help in the design of fault tolerant and attack tolerant routing protocols for MANETs.

For resolve the issues in the Problems, the following objectives has been designed to study the affect of Attacks in Routing Protocols. The Objectives has been discussed in the Review paper and are explained as:

1. Literature review of MANET Routing protocols.
2. Analyse the selected protocols through simulation via ns2.34 and verify it on the basis of literature review.
3. Review and understanding of black hole attack on routing Protocols.
4. To implement black hole attack on DYMO and AODV routing protocol.
5. To evaluate and conclude the result of the proposed work using different parameters.
6. To conclude which protocol between AODV and DYMO works better under the effect of attack.

IV. RESEARCH METHODOLOGY

Implementation Tool NS2, ns is an object oriented simulator, written in C++, with an OTcl interpreter as a frontend. The simulator supports a class hierarchy in C++ (also called the compiled hierarchy in this document), and a similar class hierarchy within the OTcl interpreter (also called the interpreted hierarchy in this document). Each mobile node makes use of a routing agent for the purpose of calculating routes to other nodes in the ad hoc network. Packets are sent by the application and received by the routing agent. The routing agent decides which path of nodes to travel to reach its destination and stamped the node with this information. It then sends the packet down to the link layer. The link layer uses ARP (address resolution protocol) to determine the hardware addresses of neighboring nodes and map IP addresses to their correct interfaces.

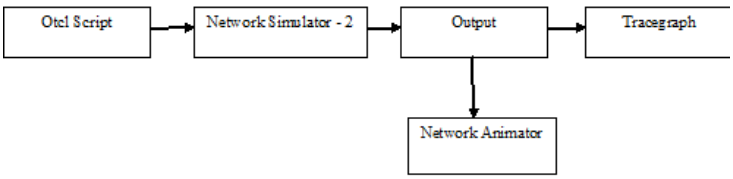


Fig: Simplified view of ns

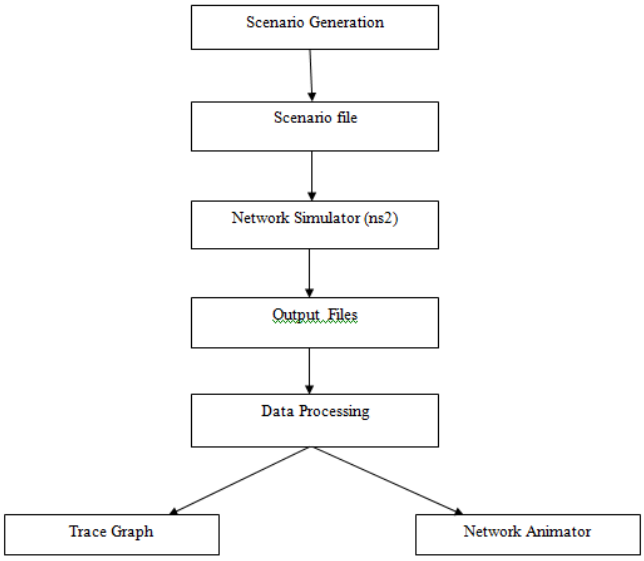


Fig: Flow Chart

DOI10.17148/IJARCCE.2017.6859

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

A file that describes the movement pattern of nodes and the traffic in the network called scenario file. This file is then used for the simulation and as a result of it a trace file is generated as output. The trace file can then be scanned and analyzed for the various parameters that we want to measure

V. RESULTS

This Section Explains the results generated by the mentioned Objectives and Methodology and show the accuracy of the Work. This Explains the various performance metrics required for evaluation of protocols. To reiterate the black hole attack, we begin with the overview of performance metrics that includes End-to-end delay, Throughput, packet delivery ratio and Routing Overload. These matrices are important because of the performance analysis of network.

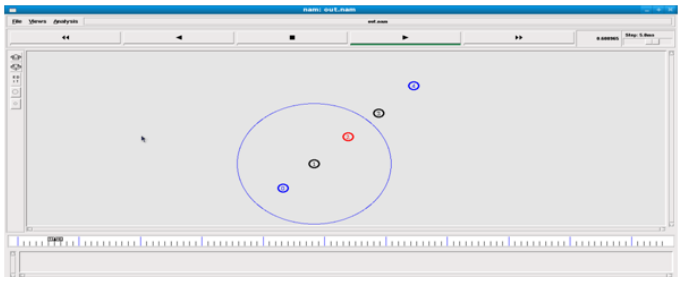


Fig NAM files for DYMO with 5 nodes

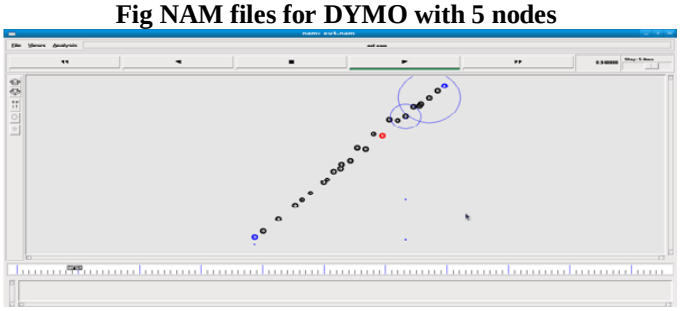


Fig NAM files for DYMO with 25 nodes

The above mentioned figures explained the research work and results has been shows in images format. As per the behaviour of black hole attack the red colour node is the black hole node and it doesn't allow the packets to reach the destination successfully. According to the specification of the target routing protocol, the manner with which the malicious node fits in the data route differs. Main task is to hinder the data forwarding between source and destination.

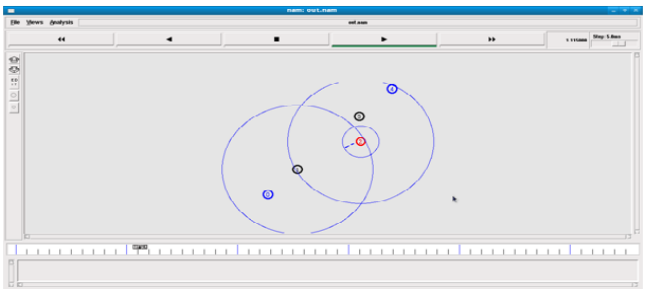


Fig NAM files for AODV with 5 nodes

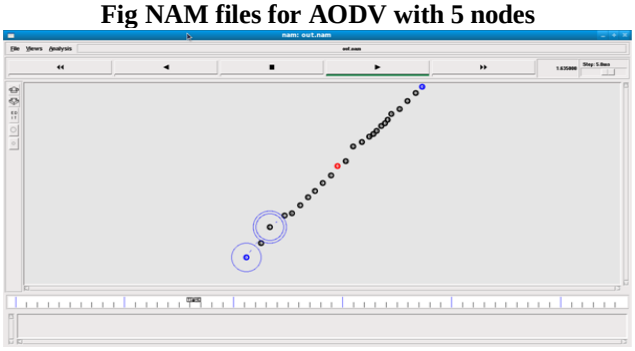


Fig NAM files for AODV with 25 nodes

DOI10.17148/IJARCCE.2017.6859

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Since we have considered five different simulation environments with different number of nodes which are 5, 10 ,15, 20 and 25. All four metrices are measured on these simulations and results are compared in a graphical representation.

END TO END DELAY

This parameter comprises all kind of delay i.e. delay that occurs when the packet is stored in a buffer before the node transmits it to other node , transmission delay etc.

THROUGHPUT

It is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. As per the simulation throughput for AODV and DYMO is calculated in all 5 nodes conditions under the effect of blackhole attack. As per figure below the throughput of both AODV and DYMO can be calculated and compared.

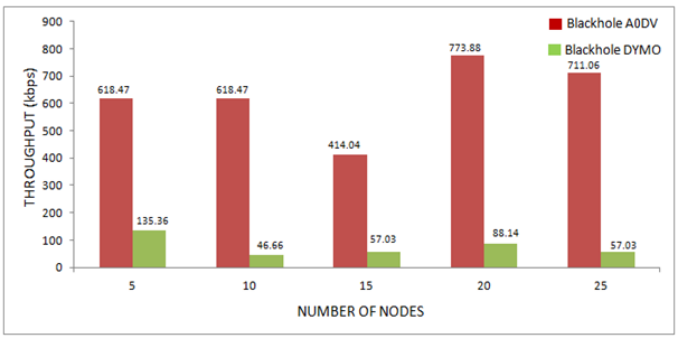


Fig: Throughput versus number of nodes

ROUTING OVERLOAD

It represents the total data traffic in bits per seconds received by the entire network from higher layer accepted and queued for transmission. Routing overload for both AODV and DYMO is calculated under each simulation environment. Fig shows graphical description of routing overload.

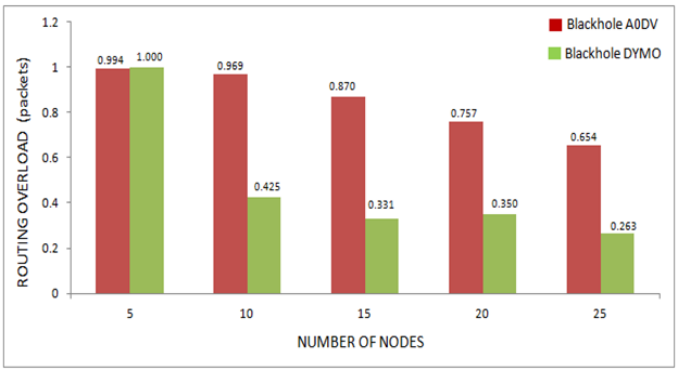


Fig: Routing Overload versus number of nodes

PACKET DELIVERY RATIO

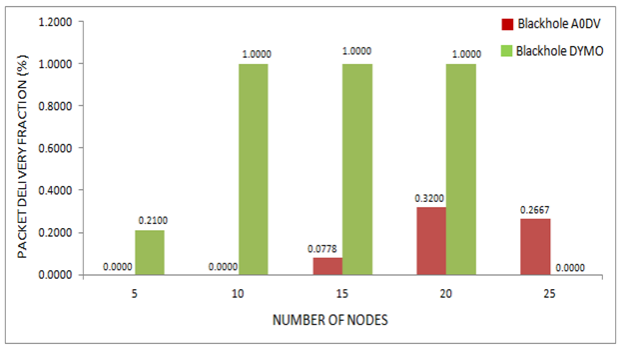


Fig: Packet Delivery Ratio versus number of nodes

DOI10.17148/IJARCCE.2017.6859

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

It is the ratio of the amount of data packets delivered to the destination and total number of data packets sent by source. Packet delivery ratio for both AODV routing protocol and DYMO routing protocol is calculated and are presented graphically. All these calculations are done using awk scripts and are calculated on ns2. Packet delivery ratio gives the ratio of successful packets delivered. Figure shows the packet delivery ratio of both DYMO and AODV routing protocol under the effect of blackhole attack.

Performance Metric Computations

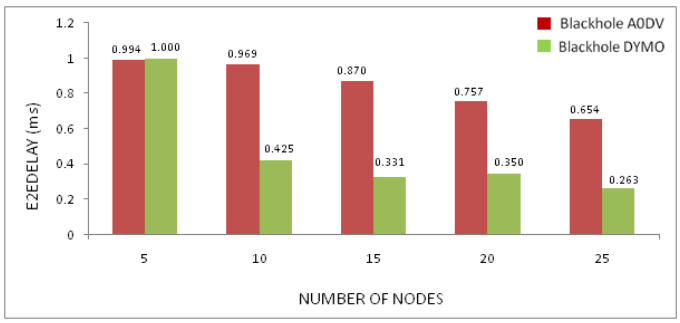


Fig: End To End Delay versus number of nodes

VI. CONCLUSION AND FUTURE WORK

All four graphical representations show that even under the harmful effect of blackhole attack DYMO shows better performance than AODV routing protocol. The reasons behind this behavior of DYMO may be one of the following –
1. DYMO has a special path accumulation function which makes it different from AODV routing protocol.
2. DYMO has multipath characteristics which allows source to have more route options.
3. It is also clear that DYMO, though a derivative of AODV is more efficient than the latter since it takes advantage of its salient features carefully pruning its weaknesses.
In this we have studied the performance parameters and Results of implemented work of the routing protocols i.e. AODV, DYMO and OLSR and tool proposed ns-2 simulator. In Future Work, The different parameters will be analyzed and detailed in the research paper. The above work will be conducted at the real time platform and it should also be tested on cross layer. The tool will be used NS-2 Simulator.

REFERNCES

[1] P. Pham, S. Perreau, and A. Jayasuriya(2005), "New Cross-Layer Design Approach to Ad Hoc Networks under Rayleigh Fading", IEEE.
[2] Osama H. Hussein, Tarek N. Saadawi (2005), "Probability Routing Algorithm for Mobile Ad Hoc Networks Resources Management", IEEE.
[3] Mei-yu Feng, Sheng Cheng, Xu Zhang and WeiDing (2007), "A Self Healing Routing Scheme Based on AODV in Adhoc Networks", IEEE.
[4] Satoshi Kurosawa (2007), "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security.
[5] Vishnu K, and Amos J .Paul (2010), "Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks", International Journal of Computer Applications.
[6] Devendra Singh, Vandana Dubey, Shipra Sharma,(2012),"Performance Analysis of DSR and AODV in Manets: Using WLAN Parameters", International Journal of Computer Applications (0975 – 888).
[7] Swati Jain, Dr Naveen Hemrajani, Dr. Sumit Srivastava,(2013),"Simulation And Analysis Of Performance Parameters For Black Hole And Flooding Attack In MANET Using AODV Protocol", International Journal Of Scientific & Technology Research, Volume 2, Issue 7, July 2013, ISSN 2277-8616.
[8] A.Moravejosharieh, H.Modares, Rosli Salleh (2013),"Performance Analysis of AODV, AOMDV, DSR, DSDV Routing Protocols in Vehicular Ad Hoc Network", International Science Congress Association.