Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549919

PERFORMANCE ANALYSIS OF IMPROVED DYMO ROUTING PROTOCOL USING ENERGY & TRAFFIC PARAMETERS WITH PERMUTATION SCHEME IN MANET

[1]Ankush Shrivastava, [2]Dr. Sandeep Dubey
[1]Phd Scholar, [2]Assistant Professor
[12]Department of Computer Science Engineering, RKDF University, Bhopal, India
[1]ankushshrivastava19@gmail.com, [2]sandeepdubey1981@gmail.com

Abstract- The routing protocol plays a vital role in mobile ad-hoc networks (MANETs). So, the designing of effective and secure routing protocol in MANETs is a crucial challenge. In current scenario, the mobile ad-hoc networks (MANETs) shows the dynamic behaviour in communication networks. Due to this, researchers face more problem during implementation of secure and effective routing protocol in networks. In this paper, authors have taken numerous factors to design the effective routing protocol for mobile ad-hoc networks in a unified manner. The main motive of this paper is to make some improvement in on-demand multicast routing protocol i.e. DYMO on the basis of energy and traffic pattern parameters with encryption scheme. In this paper, present an enhanced or modified on demand multicast secure routing protocol mechanism i.e. Enhance secure DYMO routing mechanism which follows the efficient energy and minimum traffic load concept to reach out the destination of the message control packet from the source host with encryption. This improved secure DYMO routing protocol mechanism also reconsider the route or path selection procedure as per the energy available at nodes and traffic at nodes with message encryption process using permutation method. For simulation of this system module used NS2 with VM-Ware workstation. A comparative analysis with other on demand routing protocol such as DYMO self-forwarding node, Improved DYMO based on energy and traffic parameter also presented in this paper.
Keywords: WSN, MANET, DYMO, AODV, NS2.

I. INTRODUCTION

Wireless ad hoc networking is a field that includes several areas such as wireless sensor networks [WSN], wireless mesh networks [WMN], and mobile ad hoc networks. Wireless networks are particularly attractive, especially in applications such as military-assisted automation control, intelligent traffic management systems, security checks, and more. [1]. Wireless networks are generally divided into two categories, as infrastructure-based networks and infrastructure less networks.

In the current scenario, wireless ad hoc networks are the most popular field for researchers, wireless ad hoc networks are essentially is the area where all devices or nodes participate in communication with each other without a dedicated link or path, i.e. all nodes are connected via radio or radio modem [2].

Two types of devices are used in this network, the first types of devices operate on fixed infrastructures providing the control to others, the second types of devices operate on mobile stations in the networks [1]. Infrastructure-based network types have a centralized system [1]. In this network, each device is connected to a central access point. Therefore, each device is controlled from a central point [2]. These types of networks are the opposite of infrastructure-based networks in that there is no centralized control over network devices and no single point of access. Each device is connected in peer-to-peer mode [1]-[2]. All devices are self-configuring and self-organizing nodes, they can communicate directly with each other [1]-[2].

In the last scenario, the increased demand for a computer increases the limit of data transmitted from one station to another or from source terminal to destination terminal, as the Internet is a more common term for the exchange of information and data in today's world [3]. Higher demand for devices requires more security features or equipment's for the network and the nodes participating in the network, since the network must always be protected from an attacker and other intruders [4]-[5].

II. RELATED WORK

The significantly contribution of mobile ad-hoc network towards research & development of wireless sensor network has been observed in the last two decades. Basically, the mobile ad-hoc network is a wireless ad-hoc network that makes communication between the devices without any link or dedicated path. The components connected through this network can share their data whenever needed. This paper section presents a recent development on detection and prevention of attacks in mobile ad-hoc network as per the protocol used i.e. DYMO, AODV, and DSR etc. These protocols have been used to quick and reliable communication between components and devices and also provide us a secure quick communication and safe data or information transfer through deducing overhead traffic and eliminates intruder activities. This comprehensive survey gives us a detailed insight about the mechanism of detection and prevention of attacks present in the mobile ad-hoc network and also discusses the several overhead control mechanisms using different ad-hoc network protocol that consist of their internal and external methods available in wireless sensor networks.

Authors introduced a on demand protocol-based mechanism that detected and prevented the attacks such as black hole attacks presented in the mobile ad-hoc network that consisted the dynamic topology [1]. The mechanism totally mitigated the attacks like black hole presented in the network and also deduced the possibility of malicious node in the network through mitigation algorithm based on DYMO protocol and also prevented the remaining non effected node available in the network [1].

The paper introduced an analysis of protocols such as DYMO the self-forwarding node performance in term of congestion control present in a MANET [2].

The paper introduced a comparative analysis of protocols such as DYMO and AODV performance in term of congestion control present in a VANET [3]. The protocol DYMO is an enhance or better version of AODV [3].

The paper introduced an optimization search algorithm namely CUCKOO SERACH to simulate the protocols such as AODV and DYMO and determined the performance in term of

Packet Delivery Ratio [PDR], End to End Delay [EDR], Throughput and Consumption of Energy [COE] at distinguished simulation parameters [4]. The authors got better results in term of performance metrics for DYMO and AODV protocol with optimization search algorithm i.e. CUCKOO SEARCH as compared to the simple DYMO and AODV protocol [4].

The paper introduced an optimization search algorithm namely Ant Colony Optimization to simulate the protocols such as AODV and DYMO and determined the performance in term of Packet Delivery Ratio [PDR], End to End Delay [EDR], Throughput and Consumption of Energy [COE] at distinguished simulation parameters [5]. The authors got better results in term of performance metrics for DYMO and AODV protocol with optimization search algorithm i.e. ACO as compared to the simple DYMO and AODV protocol [5].

In this article author presented few modifications in on demand protocol DYMO and got better performance results in term of PDR, EDR, and Throughput as compare to the simple DYMO protocol [6].

The authors proposed a distributed algorithm that created a Delaunay Triangulation [7]. In this paper authors also presented a comparative analysis between DYMO and AODV protocol for arbitrary sensor network using distributed algorithm and got better results in term of performance metrices for DYMO with distributed algorithm [7].

In this paper, authors introduced the comprehensive review of literature and also presented a comparative assessment among distinguished protocol used in this study in term of performance metrices such as types of protocol, their routing mechanism etc. [8].

This paper introduced an invincible AODV protocol for MANET and also proposed a mechanism for discovery routing procedure that was By-Pass mechanism which detected and prevented the attacks in nodes of network such as black hole and grey hole attacks [9].

The authors introduced the fuzzy logic in AODV protocol for mobile ad-hoc network to improving their performances [10]. This proposed technique was more efficiently secure in data routing and provided more reliability in military assistance. The proposed mechanism was also capable to detect and prevent the black hole attacks in network's node and also had numerous features such as providing authorities certificates, handling of energy, and test data package [10].

In this paper, introduced two algorithms, first one was D-MBH and second one is D-CBH algorithm [11]. The authors used D-MBH algorithm for detecting the single and multiple black hole attacks presented in the nodes of mobile ad-hoc network. But in the case of non-existence of the address of destination node, need an additional route request, to mitigate this problem authors were introduced new algorithm i.e. D-CBH [11].

In this paper, introduced MBDP algorithm for AODV protocol in mobile ad-hoc network and also used value of threshold for dynamic sequence number to determine the impact of black hole attack presented in the mobile ad-hoc network and also determined the performance parameters such as PDR, EDR and Throughput [12].

In this paper, introduced MBDF algorithm for AODV protocol in mobile ad-hoc network and also used network simulator to determine the impact of black hole attack presented in the mobile ad-hoc network and also determined the performance parameters such as PDR, EDR and Throughput [13].

In this paper, introduced a comprehensive assessment of impact of black hole attacks presented in infrastructure less mobile ad-hoc network [14]. For this assessment used CUSUM (Cumulative Sum) test to detected the change in natural behaviour of AODV protocol in terms of parameter such as protocol sequence number [14].

In this paper, suggested the use of extended routing data information table for data control packets to test the selected link or path of nodes for approaching the destination in the networks [15]. The authors had presented a detection and prevention mechanism to mitigate the malicious node in AODV protocol based mobile ad-hoc network. To simulate this mechanism and system module used OPNET-14 and got simulated results in term of performance parameters such as Throughput [15]. The value of throughput much better than the previous existing system module [15].

An introduction of novel new modified secure mechanism for AODV protocol that secure the nodes of mobile ad-hoc network from the black hole and grey hole attacks [16]. This new modified secure mechanism for AODV protocol simulated on Network simulator [NS-2] and got results in terms of performance metrices [16]. At last of the paper, the authors had drawn a comparative assessment between proposed and previous mechanism of AODV protocol [16].

In this paper, authors proposed a enhance algorithm to identified the malicious nodes presented in the mobile ad-hoc network and then mitigate all these identified malicious node form the route discovery and routing process [17]. This proposed modified algorithm for AODV protocol in MANET has given more secure communication. NS-2 software was used by the author to simulate the environment and got results in term of PDR, EDR, and throughput [17].

III. PROPOSED METHODOLOGY

3.1 DYMO Protocol (The Self-forwarding Node)

DYMO is an on-demand multicast reactive routing protocol that advance version of AODV protocol referred as AODV-v2. The DYMO routing protocol is transmitting or routing the control message packet using routing process schedule or transmitting task process as hop by hop. A simple transmitting process flow or routing process of control message packet to destination node from the source host node shown in the *figure 1.* As depicted below in the flow chart, the source node starts to send the control message and the route has known to reach destination then this reactive protocol used that known route to reach the destination node of control message packet. If there is no route information or failure occurs using stored route then the DYMO reactive routing protocol mechanism starts route discovery and route selection process via broadcasting the route request (RREQ) with nodes address to neighbouring and its intermediate nodes. Whenever, the destination node gets this route request (RREQ), it replies against this route request as (RREP) with node address. When source host node received this

RREP with node address, a route has been established between source host and destination node after that the communication starts in both ways.

The main advantage of DYMO over AODV is that, it allows the all neighbouring and its intermediate nodes to store the information or address of routes which occurs between source to destination that also help in lesser the route overhead.

Algorithm 1: Step by step process flow follows by dynamic DYMO protocol (on demand multicast routing protocol);

Step 1: Begin with initialization of the system module.

Step 2: Source host node starts or need to send the information containing message.

Step 3: Identify that is it control message or not, if it is not a control message then delete the message, if it is control message then send a route request RREQ with address of source node to the all neighbouring nodes.

Step 4: Identify whether it is destination node or not, if it is destination node then send reply against route request as RREP with node address and establish link between source and destination and make communication to each other in both ways.

Step 5: Otherwise, resend control message packet, send a reply RREP to the source host and sent a destination route request RREQ to the neighbouring nodes.

Step 6: END.

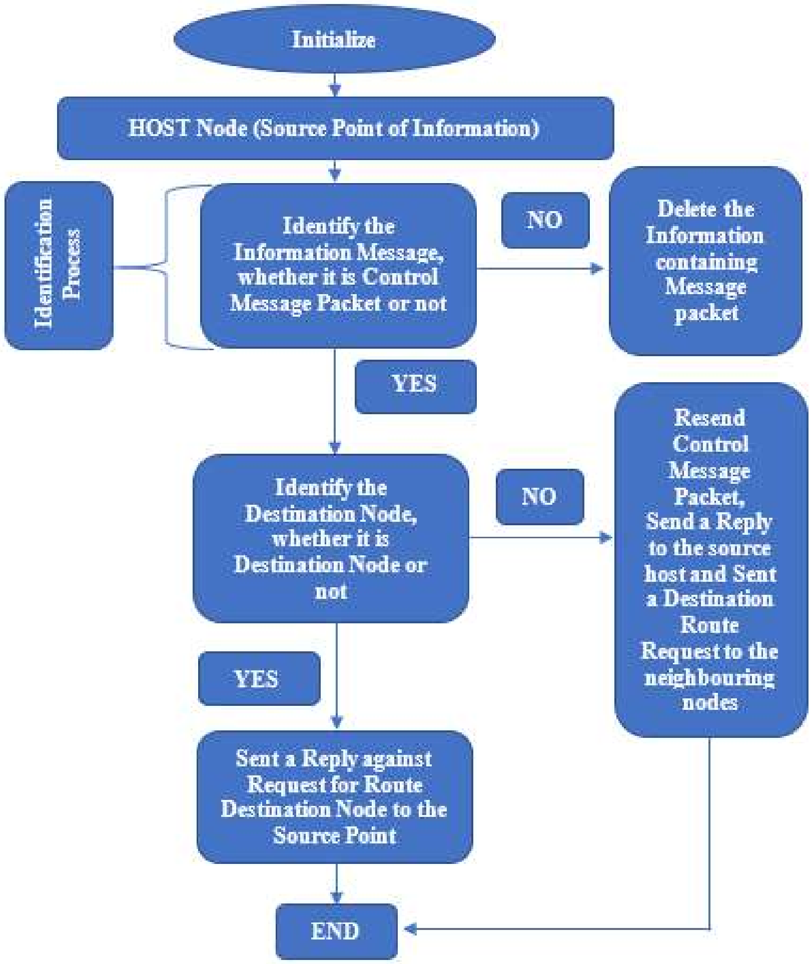


Figure 1: Process Flow Module for DYMO the Self Forwarding Protocol

3.2 Improved DYMO with Energy and Traffic Pattern Parameters with Partial permutation Encryption [PPE] Scheme

The DYMO is an on-demand multicast, reactive and dynamic protocol that have several advantages over the existing dynamic, reactive protocol but there is also needs of numerous intended factors which also help to improves the performances of the particular protocol in term of throughput, packet delivery ratio and end to end delay. Here, proposed improvement in DYMO protocol as per energy and traffic pattern parameters as shown in the *figure 2.*

3.2.1 Determination of Energy Pattern Field

An improved DYMO a dynamic, reactive and on-demand multicast protocol introduced a new intended field i.e. energy pattern field determine as follows;

Assume that for an establishment link between source host node and destination node; There are R number of routes to reaching destination node, the number of nodes in Q^{th} route is $N_{(Q)}$, referred as Route $_{(Q)}$.

In improved DYMO with energy pattern field, each and every node such as J^{th} node in Route $_{(Q)}$ having power in battery is [Battery Power = BP_J] level, (from 0 to 15) total 16 quantified distinguished value referred as [BP_J].

If any node such as J^{th} node in Route $_{(Q)}$ having power in battery less the critical battery power level [CBPL] which generalize in our system module as numeric value two. So, if the condition such as [BP_J] < CBPL occurs then node is considered as depleted energy and also considered as critical node in term of power in battery. Hence, this critical node has not been selected for transmitting the message. The route request RREQ from improved DYMO with energy pattern field consisting three factors such as Total Battery, Minimum Battery and Critical Battery.

The summation of total battery power level of all nodes [$N_{(Q)}$] of route [Route $_{(Q)}$] is referred as Total Battery Level [BP_J] shown in the equation 1.

$$\boldsymbol{Total\ Battery_{(J)} = \sum_{J=1}^{J=N_Q} BP_J} \qquad \textbf{Equation 1}$$

The minimum battery [Minimum Battery $_{(J)}$] cell in energy field of $RREQ_{(Q)}$ is the minimum value of power in battery for all nodes in Route $_{(Q)}$. The critical battery [Critical Battery $_{(J)}$] shows that the power in battery less the numeric value of CBPL in Route $_{(Q)}$.

3.2.2 Determination of Traffic Pattern Field

If the interface queue size of node J situated in Route $_{(Q)}$ is AQ_J and the interface maximum size of node J in Route $_{(Q)}$ is MQ_J, then the traffic pattern parameter of node J in Route $_{(Q)}$ can be determine as TP_J;

$$\boldsymbol{TP_{(J)} = \frac{AQ_J}{MQ_J}} \qquad \textbf{Equation 2}$$

The total traffic and maximum traffic are the two cells of traffic field of RREQ. The total traffic [Total Traffic $_{(J)}$] is the traffic pattern parameter summation of all nodes $N_{(Q)}$ as follows;

$$\boldsymbol{Total\ Traffic_J = \sum_{k=1}^{k=N_Q} TP_J} \qquad \textbf{Equation 3}$$

The maximum traffic **[Maximum Traffic $_{(J)}$]** is the maximum traffic pattern parameter of Route $_{(Q)}$.

In improved DYMO mechanism based on energy pattern parameter, Once the RREQ received by the intermediate node J, the process updates the total traffic and maximum traffic on the traffic field of RREQ and then again send forwarding RREQ to the next intermediate node.

3.2.3 Selection Process of Route

Once the several route request RREQ from distinguished routes received by the destination node then it acquires the selection process of appropriate route in term of energy and traffic pattern parameters.

3.2.3.1 Pattern Parameter of Energy

The Route $_{(Q)}$ energy pattern parameter referred as E $_{(J)}$, indicates the Route Priority [Route Priority $_{(J)}$], as per the power level of battery:

$$E_{(J)} = \frac{Total\ Battery_J}{N_Q \times Initial\ Battery} \qquad Equation\ 4$$

At some instances, some node in the route may have very low in power means power in battery less than the critical battery power but overall battery power of route is high. In that case the transmission through such route has been avoided due to the negative effect of minimum battery. So, revised the equation the E $_{(J)}$.

$$E_{(J)} = \frac{Total\ Battery_J \times Minimum\ Battery_J}{N_Q \times Initial\ Battery^2} \qquad Equation\ 5$$

At some instances, some node in the route may have very low in power means critical battery power but overall battery power of route is high. In that case the transmission through such route has been avoided due to the negative effect of minimum battery. So, revised again the equation the E $_{(J)}$.

$$E_{(J)} = \frac{Total\ Battery_J \times Minimum\ Battery_J}{N_Q \times Initial\ Battery^2 \times [Critical\ Battery_{(J)} + 1]} \qquad Equation\ 6$$

Once the destination node gets a notification such as RREQ, the process system module able to determine the final value of energy pattern parameter E $_{(J)}$.

3.2.3.2 Pattern Parameter of Traffic

As know that the optimal traffic route is lower traffic route, always considered as priority route in the routing process routine. The traffic pattern parameter of **Route $_{(Q)}$** define as **[T $_{(J)}$]**.

$$T_{(J)} = \frac{Total\ Traffic_J \times Maximum\ Traffic_J}{N_Q} \qquad Equation\ 7$$

3.2.3.3 Route Priority

$$Route\ Priority\ (J) = \frac{E_J}{T_J} \qquad Equation\ 8$$

3.2.3.4 Improved DYMO Routing Behaviour of Nodes

The routing behaviour of nodes in improved DYMO consisting the three steps namely source node, intermediate nodes and destination node.

Algorithm 2: Step by step process flow follows by dynamic Improved DYMO protocol (on demand multicast routing protocol) with energy and traffic pattern parameters;

Step 1: Begin with initialization of the system module.

Step 2: Source host node starts or need to send the information containing message.

Step 3: Identify that is it control message or not, if it is not a control message then delete the message, if it is control message then send a route request RREQ with address of source node to the all neighbouring nodes.

Step 4: Initialize the energy and traffic parameter with this route request RREQ with address of source node to the all neighbouring nodes.

```
##BEGIN,
        #Initial_strength = 10
                #Max_energy = 0;
                #n = 0;
                #Node_id = 999;
                #Total_energy = 0;
                #Event = @1
        #If_(occasion == "N")
                        #node_id = @5;
                        #Energy = @7;
                        #Final_power_[node_id] = energy;
        #If_(n < node_id)
                # n = node_id;
END

##Compute the energy for each node given as input;
        #For_(I in final_energy)
                #Consume_strength[i] = initial_energy – final_energy [i]
                #Total_energy = eat_energy[i]
        #If (max_energy < devour_power[i])
                        #Max_energy = eat_electricity[i]
                        #Node_id = I,
        #Average_electricity = total_energy/(n+1);
        #Printf ("%5.4fn", average_energy)}
        }
END
```

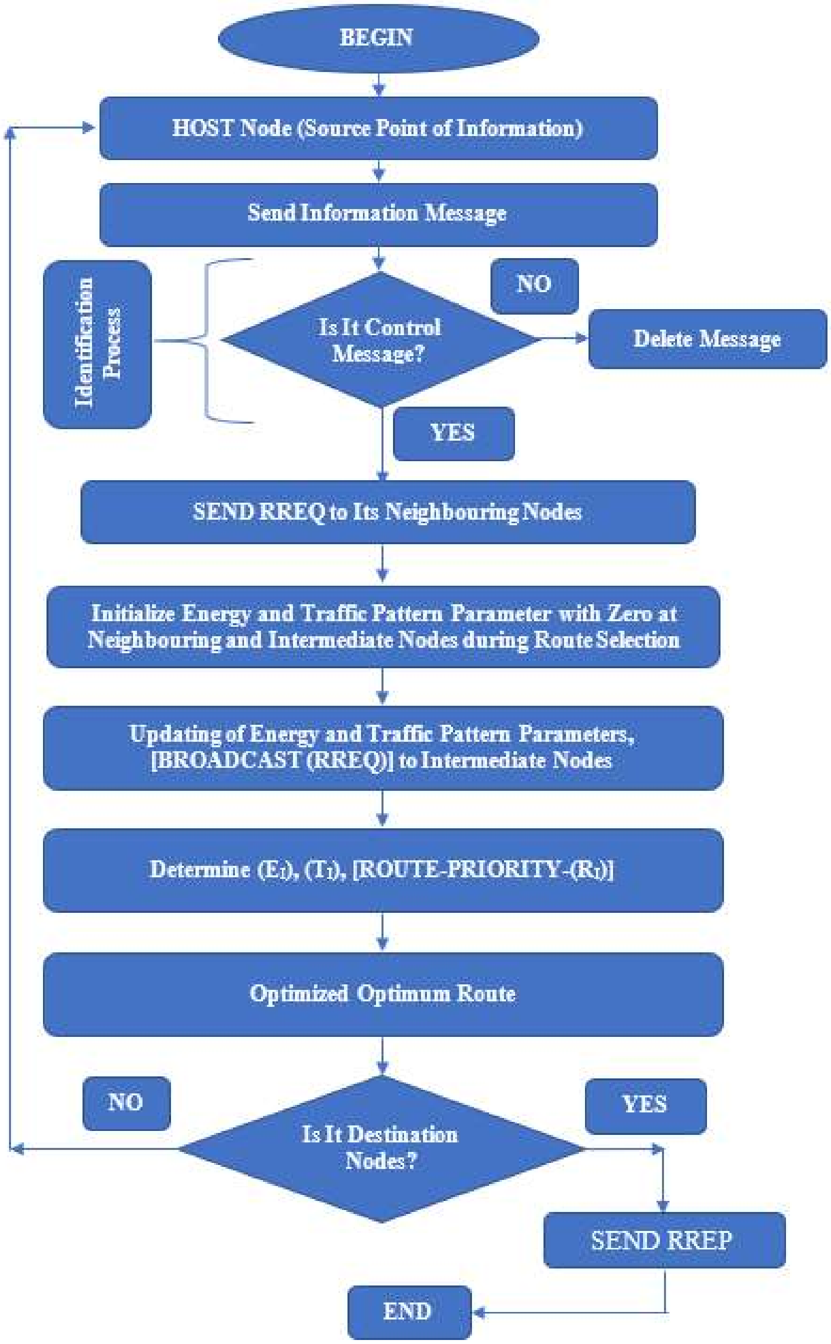


Figure 2: Improved DYMO with Energy and Traffic Pattern Parameters

Step 5: If any known route store in the data then a RREP send by the neighboring nodes with its node address. Otherwise send a broadcast route request RREQ to its intermediate nodes with previous nodes address.

Step 6: Updating of Energy and Traffic Pattern Parameters, [BROADCAST (RREQ)] to Intermediate Nodes.

Step 7: If several route information received by the intermediates nodes then determine the route energy and traffic pattern present in identified route.

Step 8: Optimized optimal route i.e. minimum energy and minimum traffic.

Step 9: Send a RREP to the source host as follows optimal route and established connection between source and destination.

Step 10: End.

3.2.4 Encoding Encryption using PPE

The concept of proposed mechanism {i.e. partial permutation encryption scheme [PPE]} is very smooth, it just permutated the global encoding vector [GEV] in place of entire message packet. As know that the initiation of message packet starts from source host node towards destination node. The proposed PPE scheme makes significant confusion to the attackers to get a records of message packets and also find the global encoding vector. So that, the PPE scheme has a great mechanism to secure the routing protocol and also it shows lesser complexity.

In Addition, here we add a process to proposed PPE scheme for more reliable secure routing i.e. generation of random encryption key. Nomenclature used in Improved DYMO Routing Protocol based on PPE with Random Encryption Key Generation shows in the *table 1.*

Table 1: Nomenclature Improved DYMO Routing Protocol based on PPE with Random Encryption Key Generation

Symbol	Explanation
[X_I]	Msg. Packet at Host or Source
[X]	Source Packets Vector Matrix
[L]	Number of Msg., Length of Permutation
[Y_(e)]	Coded Packet at Link (e)
[B_(e)]	Local Encoding Vector [LEV] Link (e)
[G_(e)]	Global Encoding Vector [GEV] Link e
[G]	Global Encoding Matrix [GEV]
[a]	GEVs Sequence
[K]	PEF Key
[C]	Cipher-Text
[DG]	Data-Generation
[f (h)]	Function of Confusion Key
[k']	Data Generation Confusion Key for Each Generation

As below depicted *figure 3* shows that the improved Dymo routing protocol process flow for coded message with PPE scheme. The process flow of proposed PPE scheme on improved Dymo routing protocol follows steps as below;

[1] Starts the scheme.

[2] Initiation of source host message packets [Msg. M_1, Msg. M_2, Msg. M_3, ……….Msg. M_L] and there are total number of message packets [L] and their individual length of message packet is [N – L].

[3] Initialize the permutation to $GEV\__S$ of message packets.

[4] Each message packet has been stuffed with [UV] unit vector as header. Because of the stuffing, system module has been performing a linear combination on the message data packets and creates the independent or individual message data packets where total number of independent or individual packets are [L].

[5] The permutation key [k] based permutation of $GEV\__S$ of data packets has created and done complete process to each individual data packets.

[6] An encryption has been done with the help of key encryption mechanism on data packets using random key encryption on improved DYMO routing protocol and end the encoding encryption process i.e. PPE with random key encryption on data message packets.

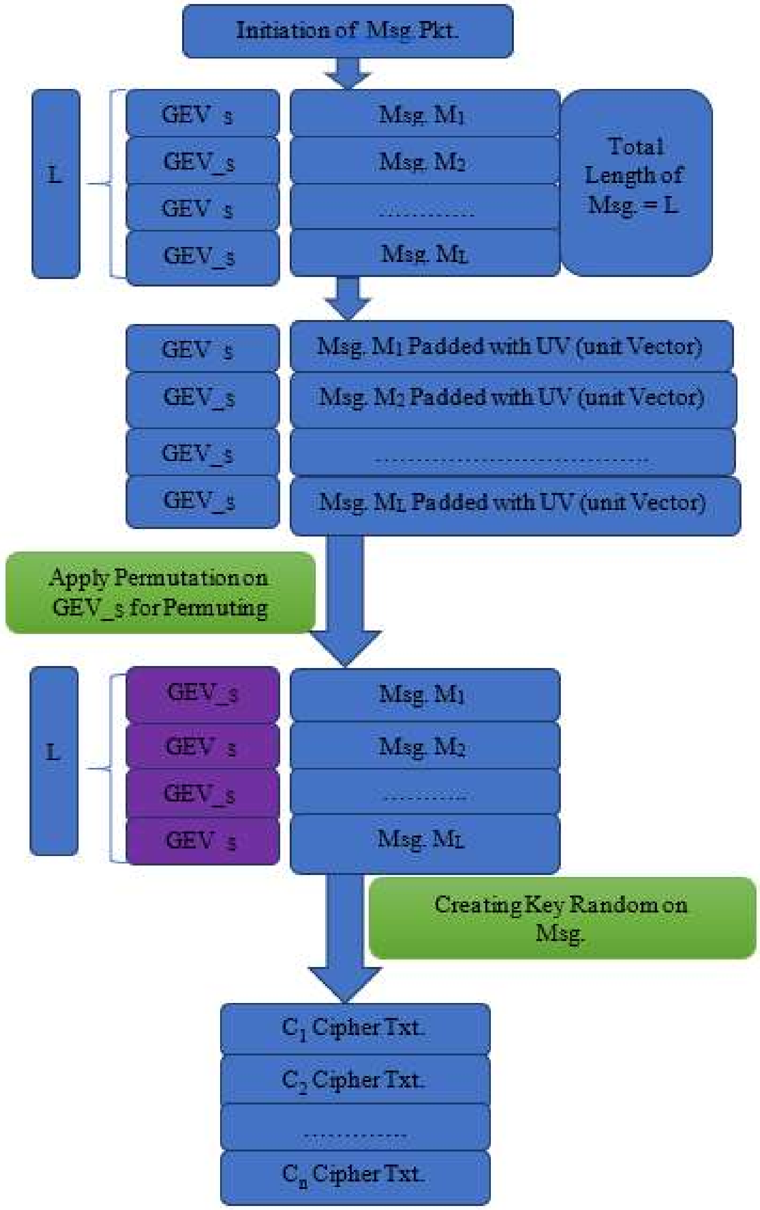


Figure 3: Improve DYMO Routing Protocol Process Flow for Coded Message with Proposed PPE

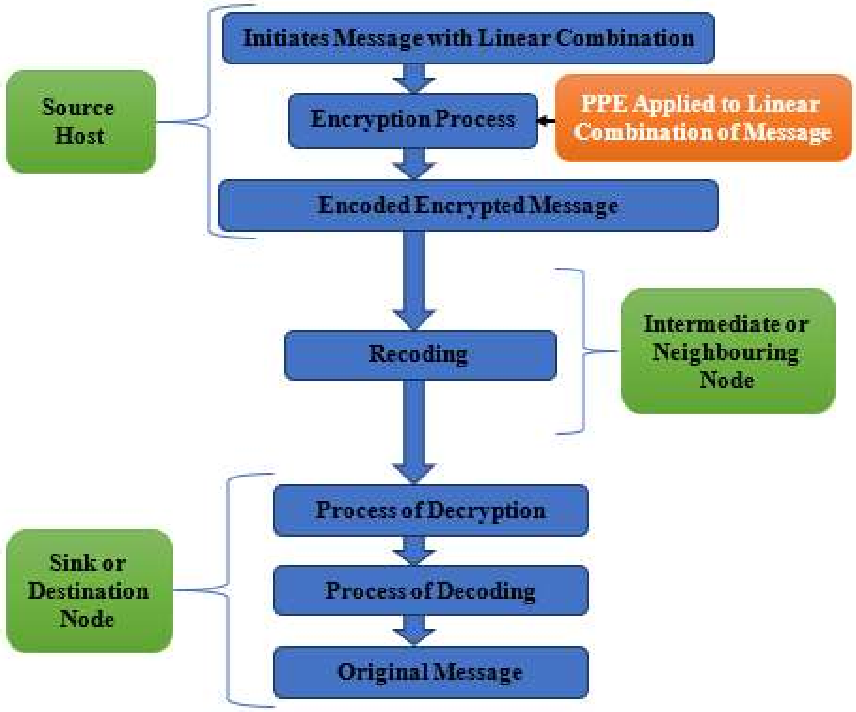


Figure 4: Process Flow Module of Improve DYMO using Coded Message based on PPE with Generation of Random Encryption Key

As above depicted figure 4 show that the process module of improved DYMO routing protocol using coded message based on PPE with generation of random encryption key. This process module consists source host node, intermediate node and sink or destination node. At source host node, the process module performs three tasks i.e. linear combination, permutation, and encryption of data message packets using random encryption key generation. In this process, the recoding has been done at intermediate or neighbouring nodes. At last sink or destination node, decoding decryption process has been done and get a original data message.

IV. SIMULATION RESULTS

This improved DYMO routing protocol mechanism also reconsider the route or path selection procedure as per the energy available at nodes and traffic at nodes. For simulation of this system module used NS2 with VM-Ware workstation as shown in the figure 5 depicted below. A comparative analysis with other on demand routing protocol such as AODV also presented in this paper. The simulation of proposed system module has been simulated on network simulator and determine the performance metrics in term of throughput, packet delivery ratio and end to end delay. The parameter of mobile node for the networks shown in the figure 6 as depicted below and detailed parameter of mobile node for the networks shown in the table 2 as depicted below.

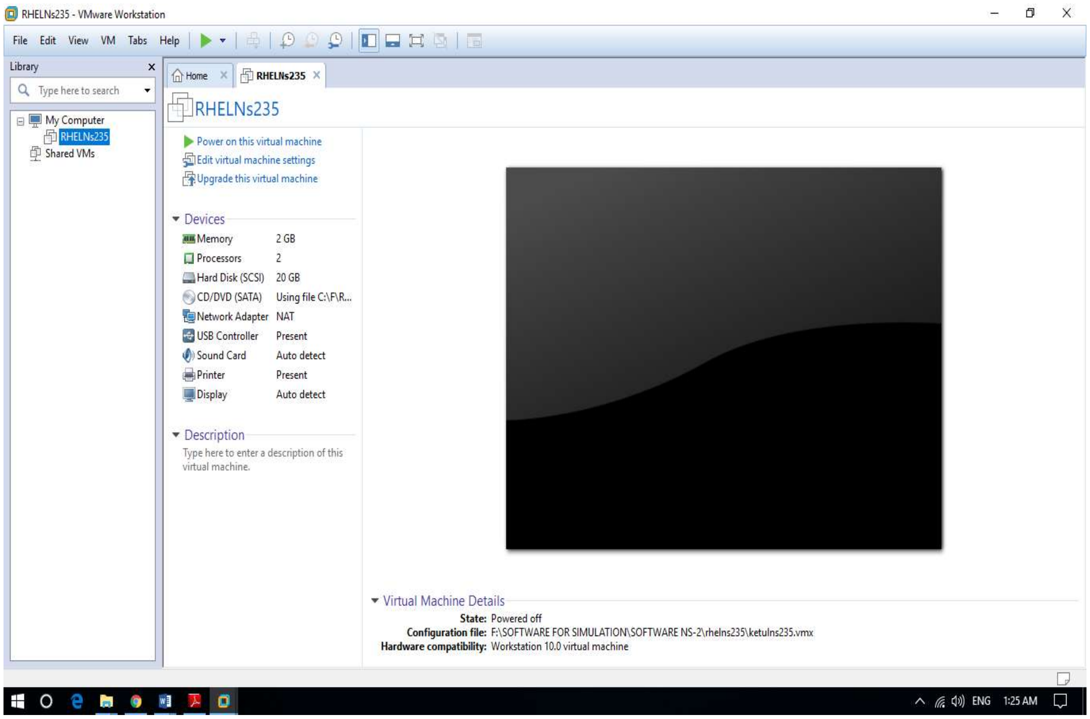


Figure 5: VM-Ware Platform and Network Simulator NS2.35 Environment (An Open Virtual Machine)

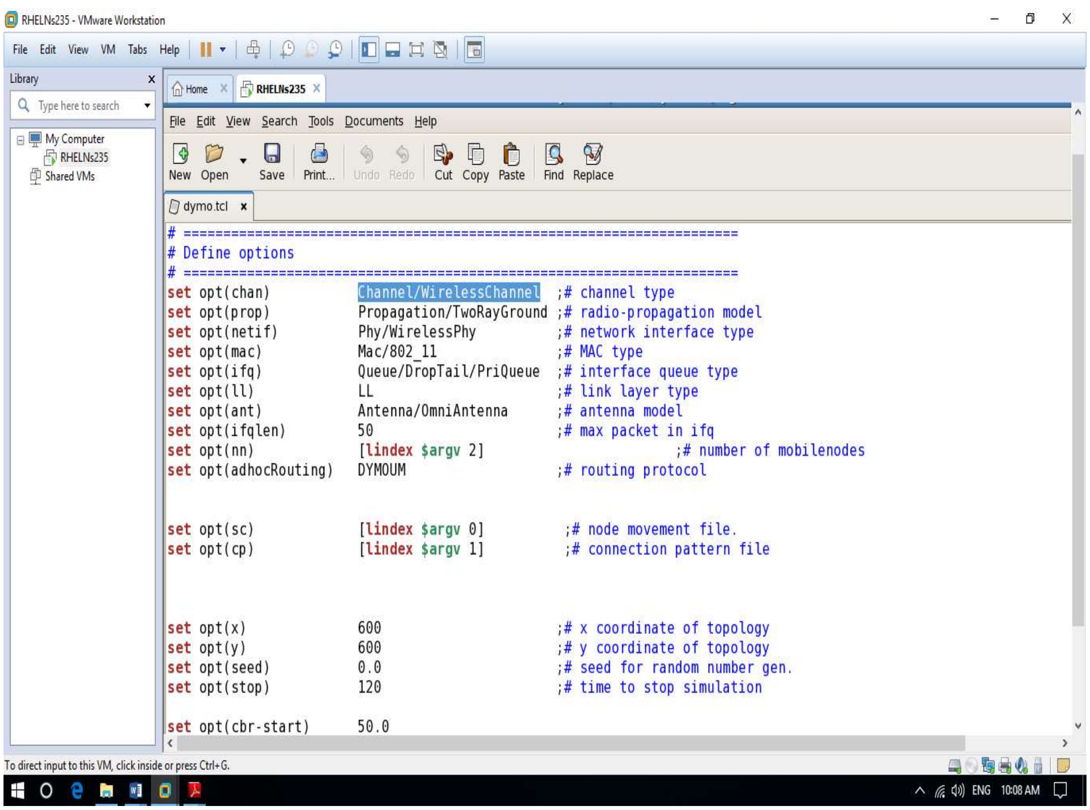


Figure 6: Parameter of Mobile Node for the Networks

Table 2: Parameter of Mobile Node for the Networks

S.	Parameter	Value
1	Type of Channel	Channel Wireless [WSN]
2	Version of Simulation Software	Network Simulator [NS-2.35]
3	Propagation of Radio Link	Direction in Both Way [Two-Way-
4	Used Number of Nodes	50 [Fifty]
5	Protocol for Routing	DYMO, Improved DYMO
6	Used MAC-Protocol	802.11
7	Type of Queue Interface	[Queue-(Drop)/(Tail)] [Queue-
8	Type of Network Interface	Physical/Wireless-Physical
9	Type of Link Layer	L-L
10	System Model of Antenna Model	Antenna of Omni-Antenna
11	Size of Frame	512 [Five-One-Two]
12	System Module for Mobility	Way-Point [Random]
13	Radius of Coverage	[Seventy-One] 71-Meter
14	Shadowing	(0) Zero-dB
15	Band of Frequency	2.4-GHz
16	Rate of Sending Message Control	One frame every 250 Milli-Second
17	Rate of Bit (For Message Control	54-Bit per Second [bps]

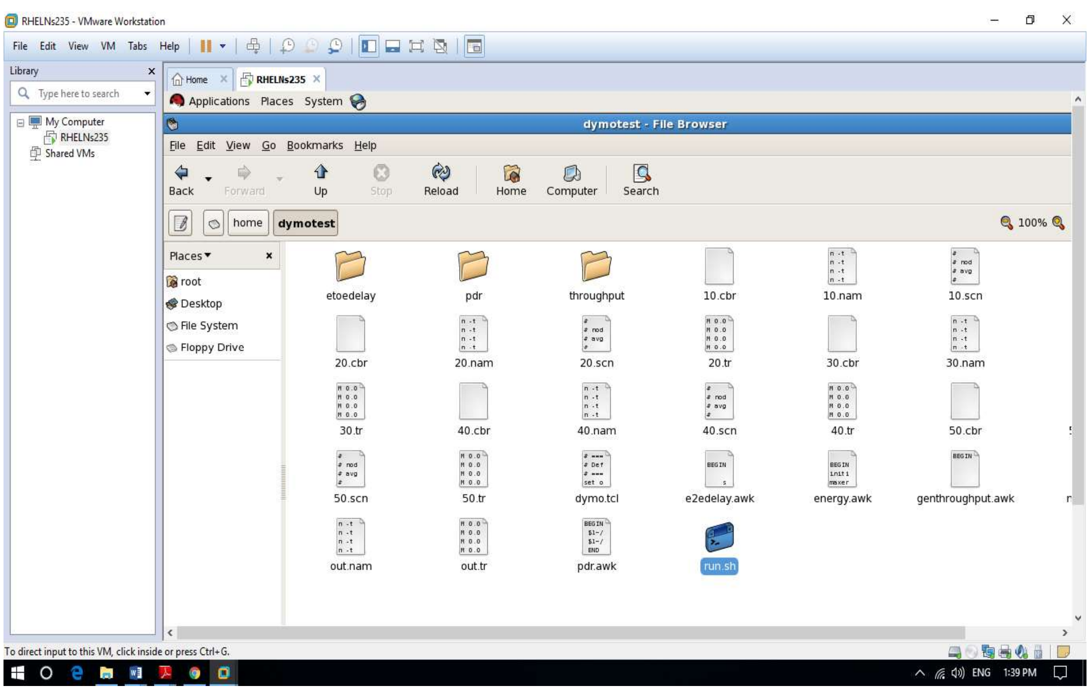


Figure 7: Dynamic, Reactive Routing Protocol DYMO in Simulation Environment (DYMO-TEST)

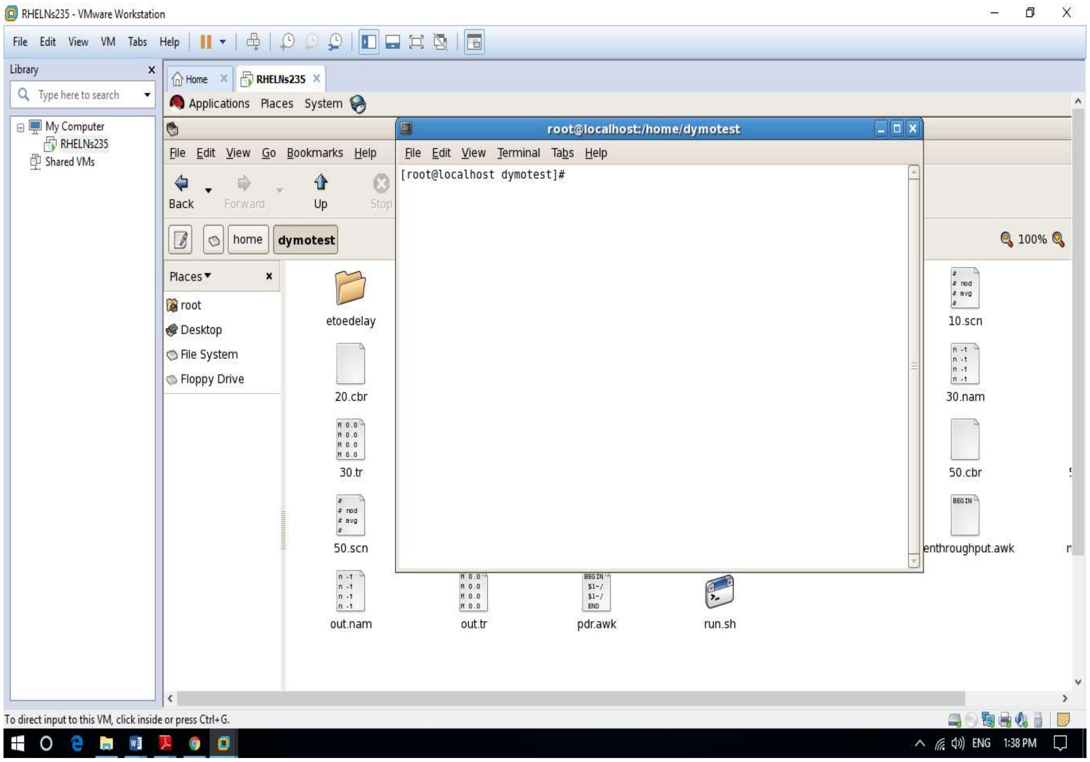


Figure 8: Run the Terminal for DYMO, Improved DYMO in Simulation Environment

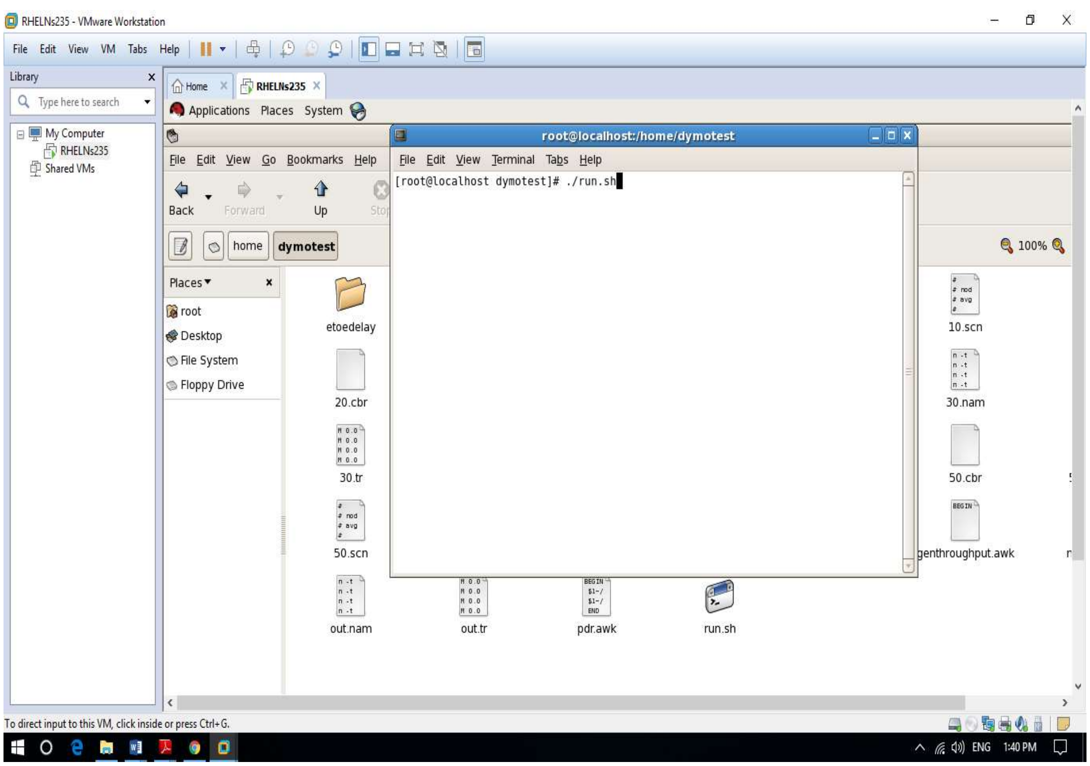
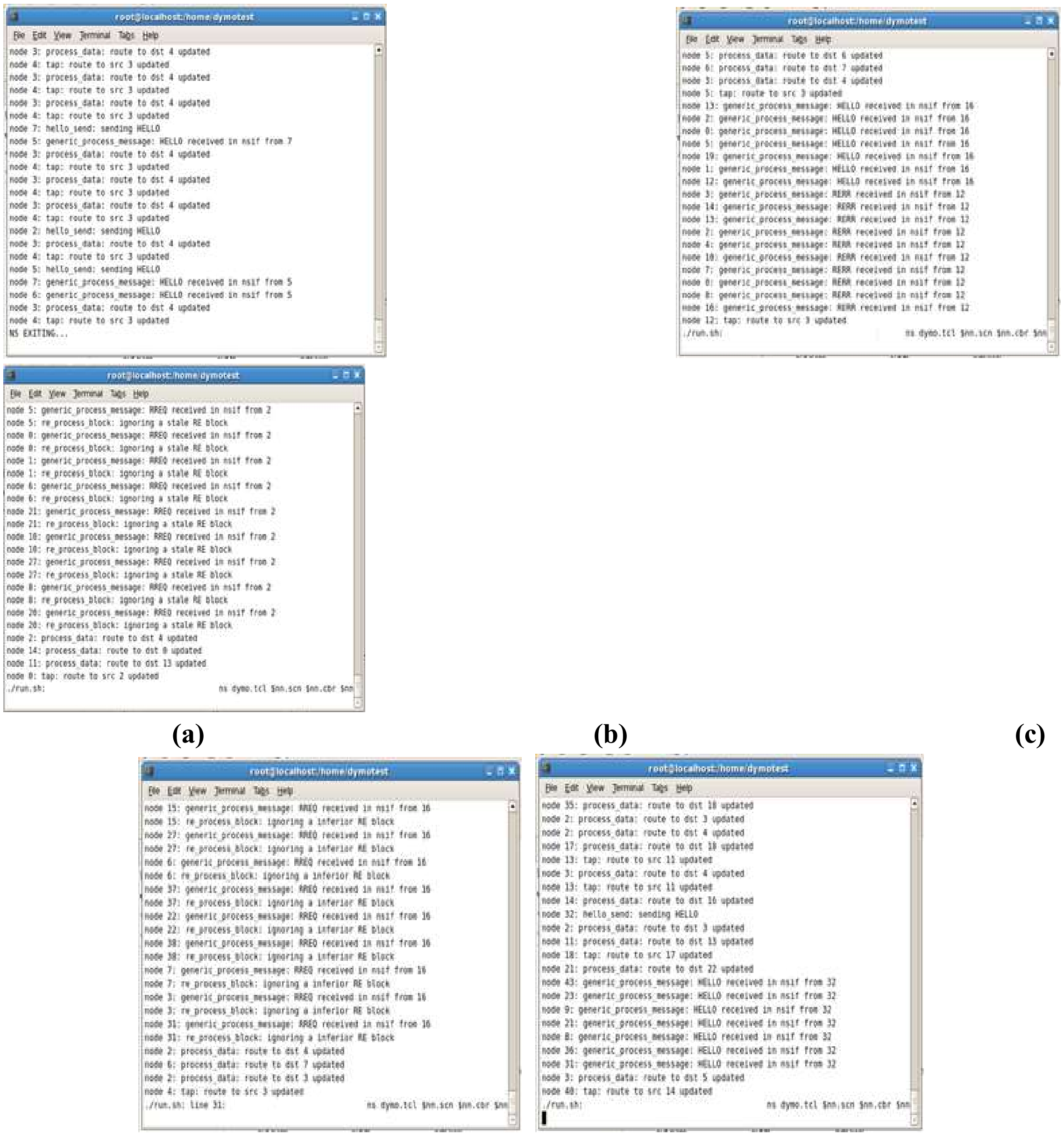


Figure 9: Run the Terminal for DYMO, Improved DYMO in Simulation Environment (./run.sh)



(a) (b) (c)

(d) (e)

Figure 10: Routing scenario and updating Process pattern (The Simulation Results Window)

As above depicted figure 7, figure 8, figure 9 and figure 10 shows that the dynamic, reactive routing protocol DYMO in simulation environment (DYMO-TEST), run the terminal for DYMO, improved DYMO in simulation environment, run the terminal for DYMO, improved DYMO in simulation environment (./run.sh) and the routing scenario and updating process pattern (the simulation results window) respectively.

4.1 Evaluation of System Performance

The simulation of proposed system model using dynamic reactive routing protocol such as DYMO the self-forwarding node concept and DYMO routing with energy and traffic pattern parameter in term of performance parameter like throughput, packet delivery ratio and end to end delay define the system performance. The simulation at predifined system network node parameter and performance metrics shows the simulation effect towards the observer in term of consumption of power in battery during routing the control message from source to destination, adaptability and scalability of DYMO and improved DYMO routing protocol.

4.1.1 Throughput of DYMO (the self-forwarding Node)

Table 3: Throughput Values with Increasing Number of Nodes for DYMO the Self-Forwarding Protocol

Number of	Throughput
10	249.156
20	502.126
30	367.750
40	610.922
50	316.160

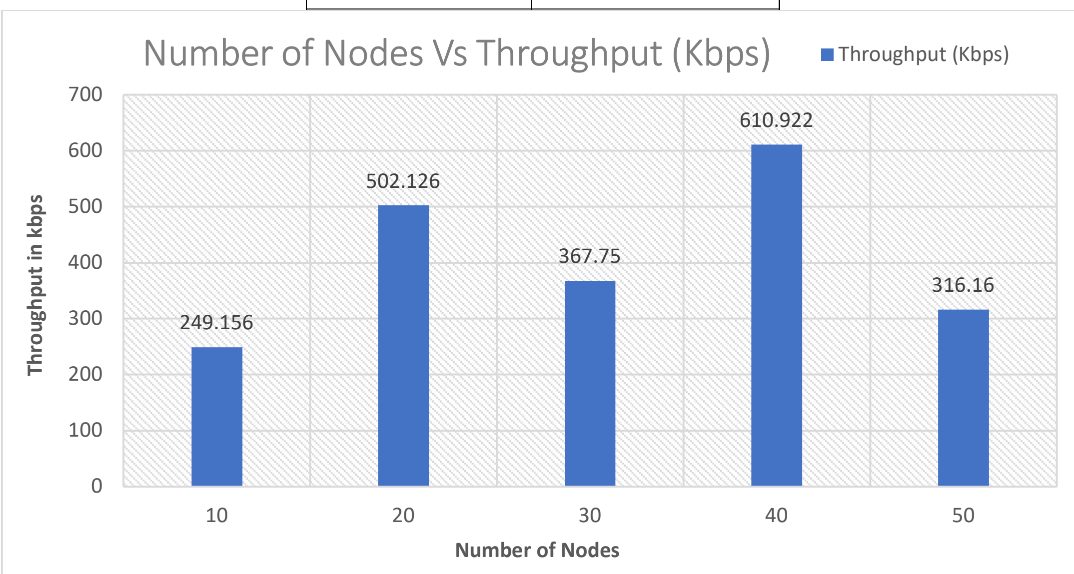


Figure 11: Throughput Values with Increasing Number of Nodes for DYMO the Self-Forwarding Protocol

4.1.2 Packet Delivery Ratio (PDR) of DYMO (the Self-Forwarding Node)

Table 4: PDR Values with Increasing Number of Nodes for DYMO the Self-Forwarding Protocol

Number of	PDR
10	0.331
20	0.538
30	0.479
40	0.495

50	0.320

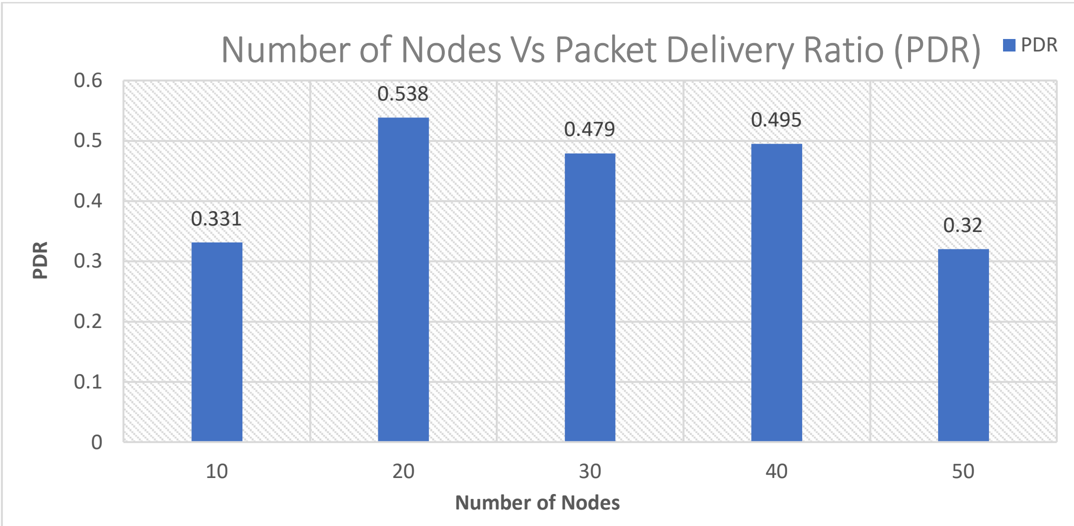


Figure 12: PDR Values with Increasing Number of Nodes for DYMO the Self-Forwarding Protocol

4.1.3 End to End Delay (ETE Delay in msec.) of DYMO (the Self-Forwarding Node)

Table 5: Throughput Values with Increasing Number of Nodes for DYMO the Self-Forwarding Protocol

Number of	End to End Delay ETE Delay (m.
10	81.394
20	270.018
30	276.058
40	264.326
50	206.065

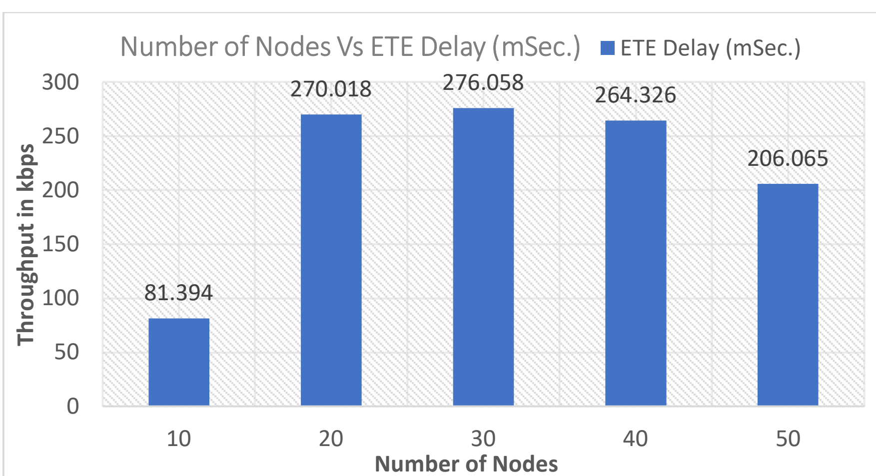


Figure 13: Throughput Values with Increasing Number of Nodes for DYMO the Self-Forwarding Protocol

As above depicted tables 3, 4 and 5 shows that the throughput, PDR and End to End Delay value with increasing number of nodes respectively. Similarly the values of throughput, PDR and end to end delay with increasing number of nodes presented graphically in the figures 11, 12 and 13 respectively. The value of thoughput for DYMO routing protocal maximum at 40 nodes and minimum at 10 nodes due to their dynanism topology and also because of dynamic traffic pattern, it clearly shown in the figure 11 and table 3 depicted above. Similarly, the value of packet delivery ratio for DYMO protocol maximum at 20 and 40 nodes respective as shown in the figure 12 and table 4 depicted above. There is no such significant difference observed in end to end delay for the DYMO routing protocol after 10 nodes.

4.1.4 Throughput of Improved DYMO (Routing Protocol with Energy and Traffic Pattern Parameter)

Table 6: Throughput Values with Increasing Number of Nodes for Improved DYMO

Number of	Throughput
10	259.251
20	511.352
30	371.681
40	610.480
50	322.089

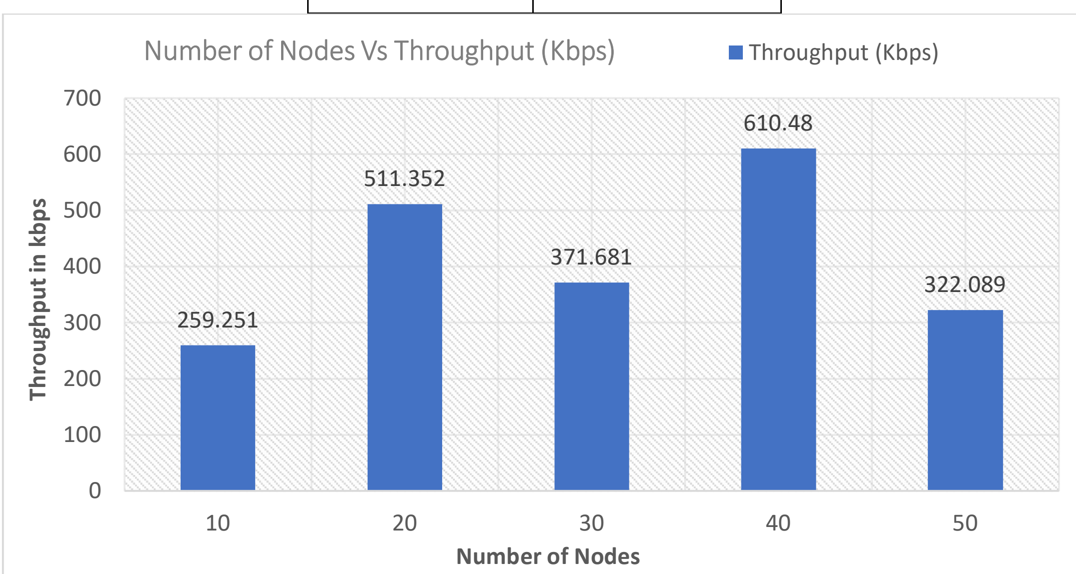


Figure 14: Throughput Values with Increasing Number of Nodes for Improved DYMO

4.1.5 Packet Delivery Ratio (PDR) of Improved DYMO (Routing Protocol with Energy and Traffic Pattern Parameter)

Table 7: PDR Values with Increasing Number of Nodes for Improved DYMO

Number of	PDR
10	0.451
20	0.625
30	0.515
40	0.648
50	0.336

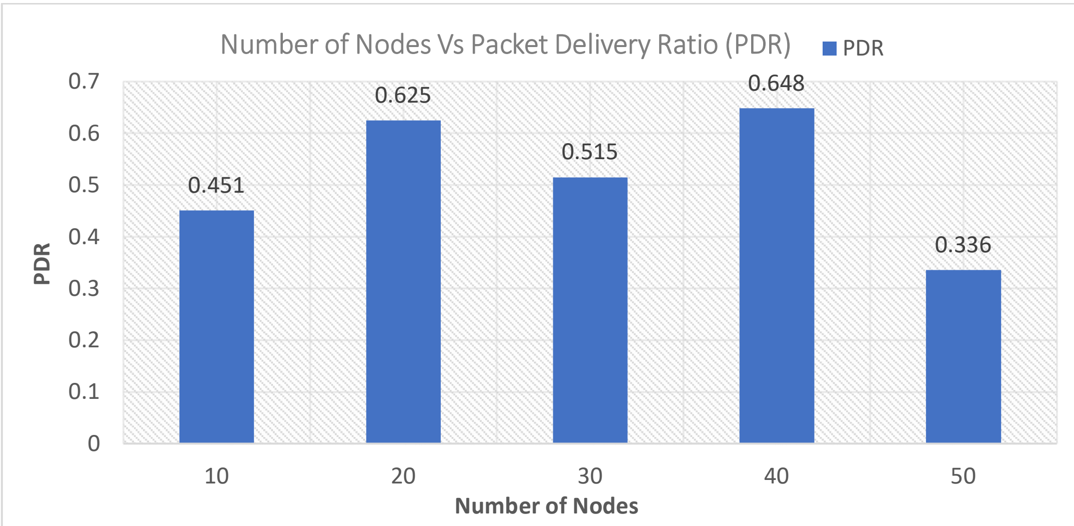


Figure 15: PDR Values with Increasing Number of Nodes for Improved DYMO

4.1.6 End to End Delay (ETE Delay in msec.) of Improved DYMO (Routing Protocol with Energy and Traffic Pattern Parameter)

Table 8: ETE Delay Values with Increasing Number of Nodes for Improved DYMO

Number of	End to End Delay ETE Delay (m.
10	80.251
20	268.058
30	255.895
40	241.325
50	190.268

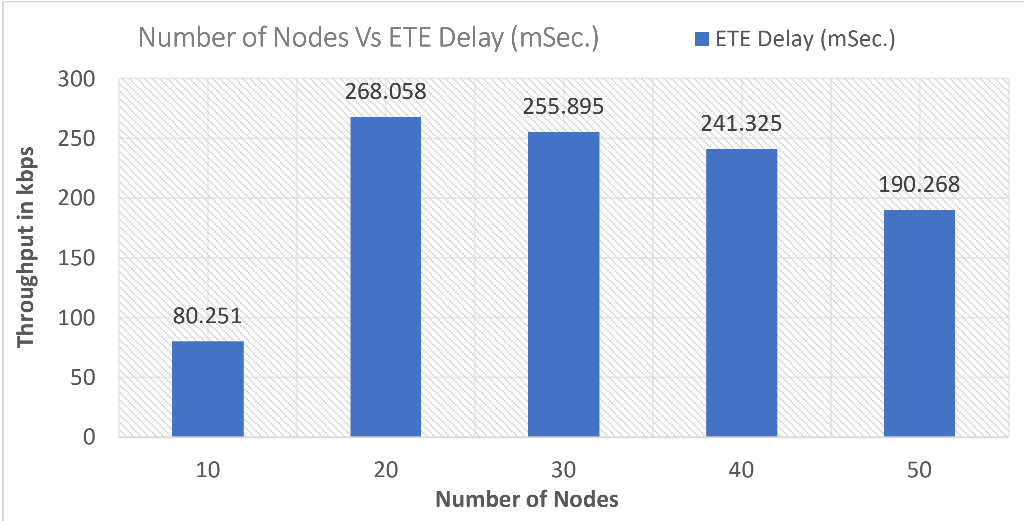


Figure 16: ETE Delay Values with Increasing Number of Nodes for Improved DYMO

As above depicted tables 6, 7 and 8 shows that the throughput, PDR and End to End Delay value with increasing number of nodes respectively. Similarly the values of throughput, PDR and end to end delay with increasing number of nodes presented graphically in the figures 14, 15 and 16 respectively. The value of thoughput for Improved DYMO routing protocal maximum at 40 nodes and minimum at 10 nodes due to their dynanism topology and also because of dynamic traffic pattern, it clearly shown in the figure 14 and table 6 depicted above. Similarly, the value of packet delivery ratio for DYMO protocol maximum at 20 and 40 nodes respective as shown in the figure 14 and table 7 depicted above. There is no such significant difference observed in end to end delay for the DYMO routing protocol after 10 nodes.

A Comparative analysis in terms of performance parameters such as thoughput and PDR for DYMO (the self-forwarding node), improved DYMO routing with energy and traffic pattern parameter and AODV reactive routing protocol present in the figures 18 and figure 19 respectively. It is clear from the figure 17 and figure 18 and table 9 and table 10, the value of throughput and PDR better for the improved DYMO routing with energy and traffic pattern parameter as compare to the DYMO (the self-forwarding node) and secure improved DYMO using PPE with random key encryption generation.

4.1.7 Comparative analysis in terms of performance parameters such as thoughput, PDR and ETE Delay for DYMO (the self-forwarding node), improved DYMO routing with energy and traffic pattern parameter and Improved DYMO using PPE with Random Key Generation.

Table 9: Throughput Values with Increasing Number of Nodes for DYMO, Improved DYMO and Secure Improved DYMO

Number of Node	Average Throughput (kbps)		
	DYMO (Self-forwarding)	Improved DYMO (Energy & Traffic	Secure Improved DYMO (PPE with
10	249.156	259.251	253.561
20	502.126	511.352	508.568
30	367.750	371.681	370.258
40	610.922	610.480	610.511
50	316.160	322.089	320.895

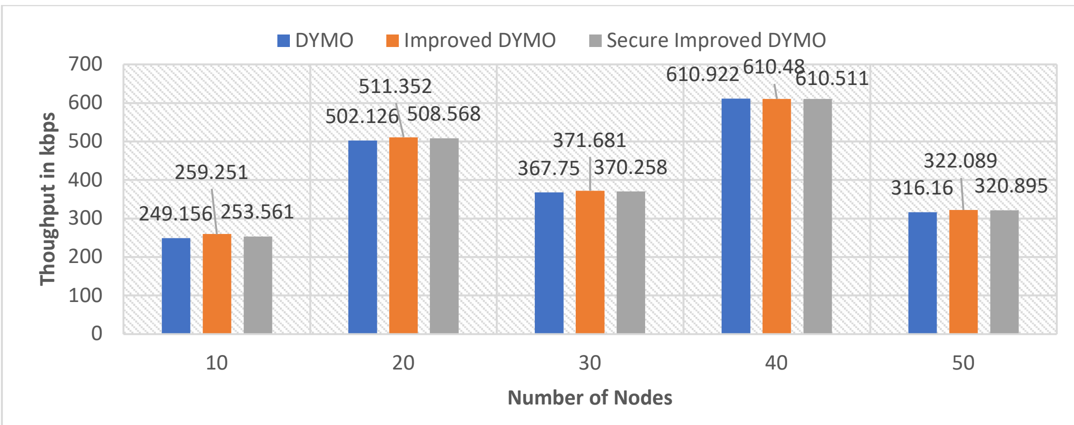


Figure 17: Comparison of Throughput Values with Increasing Number of Nodes betwwen DYMO, Improved DYMO and Secure Improved DYMO

Table 10: Packet Delivery Ratio (PDR) Values with Increasing Number of Nodes for DYMO, Improved DYMO and Secure Improved DYMO

Number of Node	Packet Delivery Ratio [PDR]		
	DYMO (Self-forwarding)	Improved DYMO (Energy & Traffic	Secure Improved DYMO (PPE with
10	0.331	0.451	0.435
20	0.538	0.625	0.598
30	0.479	0.515	0.505
40	0.495	0.648	0.545
50	0.320	0.336	0.30

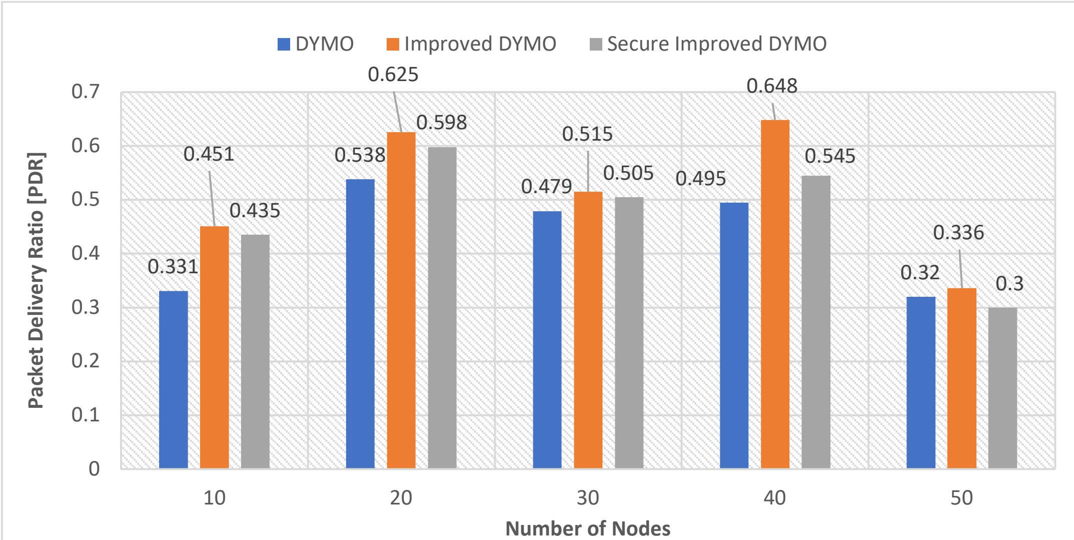


Figure 18: Comparison of PDR Values with Increasing Number of Nodes betwwen DYMO, Improved DYMO and Secure Improved DYMO

VI. CONCLUSION

The significantly contribution of mobile ad-hoc network towards research & development of wireless sensor network has been observed in the last two decades. Basically, the mobile ad-hoc network is a wireless ad-hoc network that makes communication between the devices without any link or dedicated path. The components connected through this network can share their data whenever needed. This paper presents a performance analysis of mobile ad-hoc network as per the protocol used i.e. DYMO, Improved DYMO and AODV. These protocols have been used to quick and reliable communication between components and devices and also provide us a secure quick communication and safe data or information transfer through deducing overhead traffic and eliminates intruder activities. The routing protocol plays a vital role in mobile ad-hoc networks (MANETs). So, the designing of effective and secure routing protocol in MANETs is a crucial challenge. In current scenario, the mobile ad-hoc networks (MANETs) shows the dynamic behaviour in communication networks. Due to this, researchers face more problem during implementation of secure and effective routing protocol in networks. In this paper, authors have taken numerous factors to design the effective routing protocol for mobile ad-hoc networks in a unified manner.

The main motive of this paper is to make some improvement in on-demand multicast routing protocol i.e. DYMO on the basis of energy and traffic pattern parameters. In this paper, present an enhanced or modified on demand multicast routing protocol mechanism i.e. Enhance DYMO routing mechanism which follows the efficient energy and minimum traffic load concept to reach out the destination of the message control packet from the source host. This improved DYMO routing protocol mechanism also reconsider the route or path selection procedure as per the energy available at nodes and traffic at nodes. For simulation of this system module used NS2 with VM-Ware workstation. A comparative analysis with other on demand routing protocol such as AODV also presented in this paper. A Comparative analysis in terms of performance parameters such as throughput and PDR for DYMO (the self-forwarding node), improved DYMO routing with energy and traffic pattern parameter and secure improved DYMO using PPE with random key encryption generation present in the figures 17 and figure 18 respectively. It is clear from the figure 17 and figure 18 and table 8 and table 9, the value of throughput and PDR better for the improved DYMO routing with energy and traffic pattern parameter as compare to the DYMO (the self-forwarding node) and secure improved DYMO using PPE with random key encryption generation.

REFERENCES

[1] Nitnaware D. and Thakur A. et al. (2016). Black Hole Attack Detection and Prevention Strategy in DYMO for MANET. IEEE 3rd International Conference on Signal Processing and Integrated Networks, pp 279-284.

[2] Zola E. and Escalona I. M. et al. (2017). DYMO Self-Forwarding: A Simple Way for Reducing the Routing Overhead in MANETs. Hindawi Mobile Information Systems, pp - 10-17.

[3] Dutta R. and Thalore R. et al. (2017). Performance comparison of AODV and DYMO Routing Protocols, for Congestion Detection in VANET. International Journal of Advance Research Ideas and Innovations in Technology, Pp 447-454.

[4] Kaur J. and Kaur R. et al. (2014). Performance Analysis of AODV and DYMO Routing Protocols in MANETs Using Cuckoo Search Optimization. International Journal of Advance Research in Computer Science and Management Studies Volume 2, Pp. 236-247.

[5] Gupta A. K. and Sadawarti H. et al. (2014). Performance Enhancement of DYMO Routing Protocol with Ant Colony Optimization. International Journal of Electronics and Electrical Engineering Vol. 2, Pp 188-193.

[6] Deb S. K. and Banerjee P K et al. (2014). Modified Dynamic MANET On-demand (DYMO) Routing protocol. International Journal of Emerging Trends & Technology in Computer Science, Pp 139-144.

[7] Pandey A. and Thalore R. et al. (2017) Performance Comparison of AODV and DYMO Routing Protocols for Boundary Detection in 3-D Wireless Sensor Networks. International Journal of Advance Research, Ideas and Innovations in Technology, Pp 429-436.

[8] Yadav A. K. and Kush A. et al. (2016) Assessment of Routing Protocols in MANET. IJCSC, Volume 07, Pp 252-257.

[9] Nayak D. and Kiran Y C et al. (2017) Malicious Node Detection by Identification of Gray and Black Hole Attacks using Control Packets in MANETs. Imperial Journal of Interdisciplinary Research, Vol-3, Pp 494-498.

[10] Arulkumaran, G and Gnanamurthy R.K. et al. (2017) Fuzzy Trust Approach for Detecting Black Hole Attack in Mobile Ad-hoc Network. Mobile Network. Application, 1–8.

[11] Arathy, K.S and Sminesh C.N. et al. (2016) A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET. Procedia Technology-25, Pp. 264–271.

[12] Gurung, S. and Chauhan S. et al. (2017) A dynamic threshold-based algorithm for improving security and performance of AODV under black-hole attack in MANET. Wireless Network, Pp. 1–11.

[13] Gurung, S. and Chauhan, S. et al. (2018) A dynamic threshold-based approach for mitigating black-hole attack in MANET. Wireless Network-24, Pp. 2957–2971.

[14] Panos, C. and Xenakis C. et al. (2017) Analysing, quantifying, and detecting the black holeattack in infrastructure-less networks. Computer Network-113, Pp. 94–110.

[15] Dorri, A. (2017) An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. Wireless Network-23, Pp. 1767–1778.

[16] Dhende, S. and Najan A. et al. (2017) SAODV: Black hole and grey-hole attack detection protocol in MANETs. (WiSPNET) In Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking, Chennai, India, 22–24 March, Pp 2391–2394.

[17] Shahabi, S. and Bakhtiarian, M. et al. (2016) A modified algorithm to improve security and performance of AODV protocol against black hole attack. Wireless Network-22, Pp. 1505–1511.