Investigation Misbehavior Configuration Nodes with Secure Neighborhood on Energy Consumption for DYMO Routing Protocol in MANETS

Upp nanaji, S. P. Setty

Abstract*: *We calculate misbehavior of energy consumption during configuration nodes between neighborhood nodes with specific investigation on secure environment with DYMP routing Protocol. An experimental analysis of DYMO, M-DYMO (misbehavior DYMO), S-DYMO (Secure-DYMO) has been carried out using QualNet 5.1 simulator. The simulation results have been derived using self-created network scenarios by incorporating secure neighborhood in de-facto DYMO by varying the network size as small, medium and large, Node Traversal Time, ART, Buffer Size. From the experiment results, it has been concluded that energy consumption increases as security is incorporated in the existing routing protocol. From the results, the variance of total energy consumed in all modes of energy (transmit, receive and idle) for nodes in DYMO,M-DYMO and S-DYMO under Random waypoint Mobility Model is maximum for larger network size which is 3.380037 mj , 3.363414 mj and 3.612123 mj. For random waypoint mobility model the variance of total energy consumed in all modes of energy is maximum at 0.2320866668 at 115 nodes. In this research paper, an effort has been made to investigate the impact of secure neighborhood on energy consumption and QoS metrics of Dynamic MANETs On-Demand (routing protocol) (DYMO) in MANETS.

Keywords: MANETs, DYMO, M-DYMO, S-DYMO, Energy Consumption, secure neighborhood.

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a group of two or more autonomous nodes that connect without any centralized node administration. MANETs have few prominent structures, such as dynamic topology, restricted storage as well as bandwidth, which make them attractive for certain applications, and at the same time create difficulties for effectively and accurately routing packets to a specific destination. From figure 2 there is a shortage of defined topology in these forms of networks, because they are sometimes referred to as fewer network infrastructure, because every node has the potential to act whether as a router otherwise host or mutually. MANET routing is a daunting activity and has generated exceptional interest from researchers all over the world. From the literature survey it was found that none of the current protocols are the strongest to justify the functionality and are ideal for effective routing. By improving its achievement of different metrics such as throughput, end to strangle, packet delivery ratio, etc., investigators strive to reveal the effectiveness of the existing routing protocol. The wireless networks can be infrastructure based and infrastructure-less. The infrastructure-less wireless network is described as “ad hoc” networks. MANETs are special type of Wireless ad hoc networks. A MANET is a collection of autonomous mobile nodes linked by wireless links. Figure 1 demonstrates mobile ad hoc scenario.

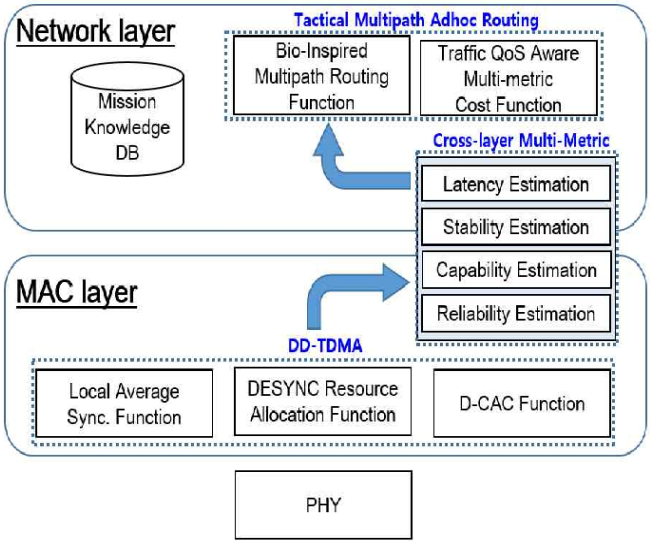

Figure.1: Mobile Ad hoc Network Architecture

MANET carries the hope of the future, with the potential to create networks at any time and wherever. MANET is a wireless network containing mobile nodes that have a complex topology and no networks or centralized control already in place. For multiple systems as well as settings, like emergency situations (e.g. catastrophe recovery), military environments and people, MANET is a workable solution. MANET can be quickly implemented, since traditional wireless networks do not require costly facilities.

Figure.2: Mobile Ad hoc network scenario

Revised Manuscript Received on January 05, 2020.
***** Correspondence Author
Uppe Nanaji*, Research Scholar, Department of CS&SE, Andhra University, Visakhapatnam, India, nanajistiet@gmail.com.
Dr. S.Pallam Setty, Research Guide, Department of CS&SE, Andhra University, Visakhapatnam, India, prof.spsetty@andhrauniversity.edu.in

One of the difficult issues in the MANET [1][2] is to course the bundles commencing basis to objective securely in occurrence of aggressors. The nodes in MANETs can join or leave the network at anytime. So it possesses dynamic topology. In MANETs, every hub goes about as both host and switch. This implies that each hub advances bundles and along these lines, each hub takes an interest in steering measure. in MANETs, the hub's assets like battery lifetime, processor handling abilities are restricted. By and large, the remote channel isn't s protected. Due to these features, routing firmly is difficult. The MANET directing conventions [3][4][5][6] can be characterized into different sorts practical , imprudent and hybrid.

In this paper, the figure 3, we studied DYMO [7][8] and S-DYMO [20] the directing convention in presence of an unstable climate. The simulations are accomplished for 35, 75, and 115 numbers of hubs utilizing QualNet5.1 network simulator [9]**.** Organization of the paper: In this paper section-I manages the presentation of MANETs and their qualities. Review of literature related to DYMO, secure neighborhood, security attacks etc., is given in section-2. The methodology and the replication environment are located in section-III. The results are graphically denoted and analyzed in section-IV. Section-V offers conclusion & future extent of this work.

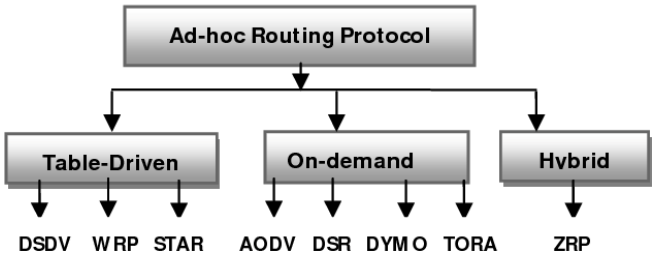

Figure.3: Mobile Ad hoc network scenario

II. LITERATURE REVIEW

2.1. **Dynamic Manet On-Demand (routing protocol) (DYMO):** Routing is the way toward finding a way to the planned objective.

DYMO is Dynamic Manet On-Demand (routing protocol) for versatile impromptu organizations conveyed in antagonistic conditions. DYMO addresses two intently related issues, the first one is route anonymity in which DYMO keeps solid enemies from following a bundle stream back to its source or objective and the subsequent one is area protection. DYMO guarantees that enemies can't find the genuine characters of neighborhood transmitters. The plan of DYMO depends on "broadcast with hidden entrance data", a novel organization security idea that incorporates highlights of two existing organization and security instruments, specifically "broadcast" and "secret entryway data". DYMO utilizes the ideas of the Trap door work. DYMO steering resolution has been planned by Perkins & Chakeres [3] as headway to the current AODV convention. It is likewise considered to as replacement of AODV/ ADOVv2 also continues refreshing till date. DYMO works like its archetype for example AODV and doesn't add any additional adjustments to the current usefulness however activity is besides very less difficult.

DYMO is a simple-responsive convention where for example, courses are processed on interest as necessary. Not at all like AODV, DYMO doesn't uphold superfluous HELLO notifications, & operation is clearly focused on sorting numbers to all packages. It is a responsive steering system that displays unicast courses on demand or when necessary, using grouping statistics to guarantee circle opportunities. It empowers interest, multi-bounce unicast steering among hubs in a specially selected portable organization. The basic duties are disclosure and assistance. Course revelation is done at source hub to an objective towards which it has no valid path. In addition, courses are assisted to evade the existing catastrophic courses commencing the guiding table also to decrease the package drop in the event of any course break or hub disappointment.

M-DYMO is misconduct configuration to transform from normal node to malicious node to change behaviour from normal node to degrade QOS efficiency. It is complicated for them to follow the amount of hubs in the territory, who has been the sender or recipient, where a stream of parcels came since and where it goes (i.e. what are the past hops as well as the subsequent bounces on course), not to mention the source transmitter and the target receiver of the stream. The pseudonymity strategy relies on an organizational protection concept called "broadcast with secret entry data"".

Advantages and Disadvantages of DYMO Protocol

DYMO adds new structures over AODV. Production evaluation demonstration that DYMO defeats AODV as MANET. The procedure can be outlined:

• The protocol is energy-efficient while the system is wide and mobile

• DYMO's routing table is relatively less memory-consuming than AODV's Route Aggregation.

• Protocol overhead reduces with expanded network sizes and high versatility.

Even then, DYMO protocol is not doing well with low mobility. The workload for such situations is very large and needless. Another weakness is the protocol's applicability as described in the DYMO draft, which specifies that DYMO achieves well when traffic is guided beginning 1 section of the network to alternative.

It indicates poor efficiency when random traffic is very tiny, and overhead routing outstrips real traffic.

A) Packet Distribution Fraction (PDF): Percentage of data packets sent to aim & overall number of knowledge packets sent through basis.

B) End-to-End Latency (AEED): Length between the source node and destination node, including loading period and queue duration.

C) Overhead routing (RO): complete routing packets exchanged through simulation. Routing overhead is significant since it tests a protocol's scalability, the degree it can operate in congested or limited bandwidth environments. Complete number of signals successfully delivered, i.e. total digit of bits transmitted per second. Also denotes to the amount of data transmission from source to endpoint in a specified time.

2.2 Security Attacks: MANET attacks[11] can be loosely divided into 2 main category-passive attacks and aggressive attacks, so according means of attack[12][13].

2.2.1 Passive Attacks: A passive attack obtains data exchanged in the network without disrupting the operation of the communications. Eg. : eavesdropping, traffic analysis, and traffic monitoring.

2.2.2 Active Attacks: An active attack involves information interruption, modification or fabrication. Eg: jamming, impersonating, modification, denial of service (DoS), and message replay.

2.2 Eavesdropper: Eavesdropping is accidental receivers able to intercept and translating communications and interactions. Eavesdropping's aim [14, 15] is to collect any classified details that should be held secret through contact. Confidential details can involve node position, public key, private key, or even passwords.

2.2.1. Passive Eavesdropping: In this the noxious hubs recognize the data by tuning in to the message transmission in the telecom remote medium.

2.2.2. Active Eavesdropping: In this, the malevolent hubs effectively snatch the data by means of sending questions to transmitters by masking themselves as a benevolent hub. The eavesdropper can drop all parcels (dark opening assault) [16]or burrow the bundles starting with one area then onto the next (wormhole attack)[17].

2.3 Secure Neighbor: To prevent this eavesdropper, we have employed secure neighborhood [9] using pair-wise secret key authentication method.

This method is used when IPSec is absent [20]. In secure neighbor confirmation (SNAuth), each portable hub builds up a confirmed neighborhood moving. Intermittently, every portable hub X transmissions its character parcel <SNAuth-HELLO, X> to its area. Here, Y is neighbor of X.

This method is pictorially depicted in figure 4.

Step 1a.) Y selects a random nonce n1.

Step 1b.) Y encrypts n1 with k and sends the encrypted result to X i.e. **<CHALLENGE, Y, ENC_k (n1)>.**

Step 2a.) X receives the encrypted message sent by Y.

Step 2b.) Since X knows k, it decrypts Y's message with k and obtains n1, the nonce of Y.

Step 2c.) X creates another nonce n2.

Step 2d.) X encrypts (n1 XOR n2) with the same key k and sends the encrypted result as response to Y i.e. **<RESPONSE1, X, n2, ENC_k (n1 XOR n2)>.**

Step3a.) Y receives the encrypted message sent by X.

Step 3b.) Y decrypts X's message with key k gets (n1 XOR n2).

Step 3c.) If Y gets the same consequence commencing XORing n2 in the reply & its own challenge n1, then X passes the test . GOTO step 3e.)

Step 3d.) Else Y neither sends any packet to X nor receives any packet from X ; Y only receives the reaction packets from X untill a accurate <RESPONSE1> packet from X passes the test.

Step 3e.) Y puts X in its secure neighbor list.

Step 3f.) Y selects a random nonce n3

Step eg.) Y encrypts (n1 XOR n2 XOR n3) with k and sends this as a confirmation response to X as **<RESPONSE2, Y, n3, ENCk (n1 XOR n2 XOR n3)>**.

Step 4a.) X receives the encrypted message from Y.

Step 4b.) X decrypts Y's message with key k and obtains (n1 xor n2 Xor n3)

Step 4c.) If this matches the consequence of XORing n1 that is earlier decrypted, its own n2 and n3 in the RESPONSE2 packet , GOTO step 4d.)

Step 4d.) X puts Y into its secure neighbor list.

This 3rd-way handshake is compulsory because X needs to confirm that Y actually knows "k".

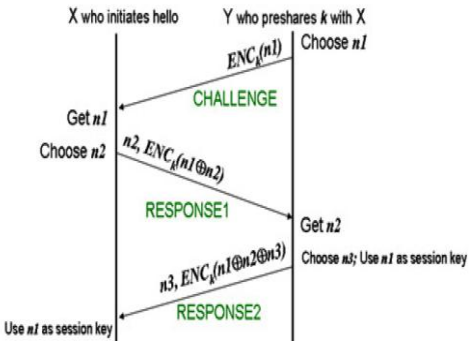

Figure 4: Secure neighbor method using pair wise secret key

2.3.1. Dynamic Source Routing (DSR): DSR is a routing protocol that is still required, in which the data sender may specifically specify the sequence of nodes used to transmit a packet. The packet header includes multiple average routing nodes. To seize the source route learned, each node job is to preserve the route cache. It is demonstrated that "Route Discovery and Route Maintenance" are the two major components of DSR, which both preserve and evaluate routes to random destinations.

Limiting the massive bandwidth usage incurred by MANET control packets is the explanation for creating such a protocol. By omitting messages from the time updates required, this phase is accomplished, which normally occurs in the table-driven method. DSR is an auto-maintaining routing protocol which provides networks. The protocol will also utilize wireless telecommunications services and broadband networks of up to 200 nodes. A complex source routing network may be individually managed and configured by managers. In DSR, each trigger resolves the route for use in conveying its samples to destinations picked.

There are two big components called road management and path exploration. Transmission route remains optimal and loop-free when network requirements shift. Path management means that even though the route is changed during transmission. The optimal path amongst a given basis & destination is defined by route discovery.

This safe neighborhood protocol is placed in the current Anonymous On Demand routing protocol.

III. METHODOLOGY AND BACKGROUND RESEARCH WORK

Most of the safe specially appointed directing conventions proposed so far will in general zero in on the insurance strategies instead of computational expense and energy utilization. The principle destinations have been to explore the materialness of the current secure plans for MANETS by limiting the energy utilization to upgrade the organization life and add to the improvement of asset effective and secure to upgrade the organization.

Any experts indicated some answers for help
Dynamic MANET atmosphere QoS. Yet they're not dealing with having defense necessities near to hold gadgets, where reserves are scarce. This is because the security arrangement costs additional assets and reduces network life.
It might likewise unfavorably influence the QoS. In this way, it could be important to think about the provisioning of security to limit energy utilization in order to give network life in a coordinated way.
To assess the plans proposed in this work and to pick the most appropriate assessment approach, three assessment techniques were recognized

1. Simulation,
2. Experimental and
3. Mathematical

Simulation is picked, as the exploratory system isn't practicable while the numerical procedure is exceptionally prohibitive. This reproduction strategy is to assess the assortment of outcomes. The outcomes are broken down and contrasted and DYMO alongside S-DYMO. Ends are drawn from assessments of the proposed steering convention (S-DYMO).

3.1 Simulation Scenarios: All the Simulation are finished utilizing QualNet 5.1 organization test system. The Simulation boundaries are clarified beneath.

From the table 1 shows the parameter configuration for all the hubs move [9] with speeds going from 0m/s to 10m/s with high mobility. In this scenario, node deployment model used is random. Constant Bit Rate traffic (CBR) [19] model is utilized to create traffic at a deterministic rate with some randomizing vacillate empowered on the between bundle takeoff span. Bundle size was set to 512 bytes is shown in the figure 5 and 6. The following simulation parameters are used:

TABLE 1. SCENARIO PARAMETERS

Routing Protocol	DYMO, S-DYMO
SECURE-NEIGHBOR-TIMEOUT	5sec
Terrain	1000m x 1000m
Pause Time	0 sec
Simulation Time	300 sec
Mobile Nodes	35,75,115
Node Placement Model	Random
Propagation Model	Two-ray
Mobility Model	Random Way Point
Energy model	Generic
Minimum Speed	0 m/s
Maximum Speed	10 (m/s)
Traffic	CBR
Packet size	512 bytes
MAC layer	802.11
Antenna Type	Omni directional

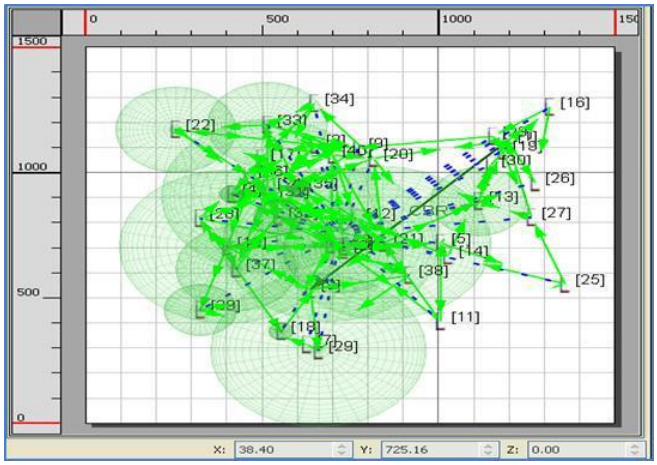

Figure 5: Simulation scenario for 35 nodes

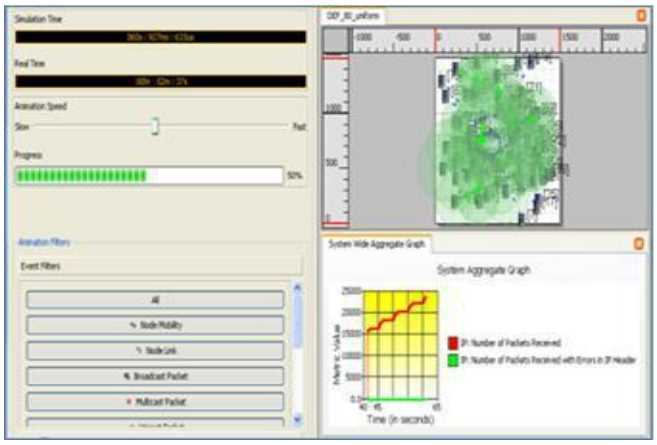

Figure 6: Simulation scenario for 75 nodes showing dynamic environment

The simulation environment screen shots of DYMO protocol is presented in figure 5

3.2 What happens in S-DYMO: From figure 7, all the sending node should check its neighbor nodes to know whether neighboring nodes are reliable or not. This is done by the sender by sending a challenge to its neighbor nodes. If the response is received within 5 sec, it is considered to be a safe node; otherwise, the node is exempted from routing process. The anonymous routing scheme of DYMO is then used.

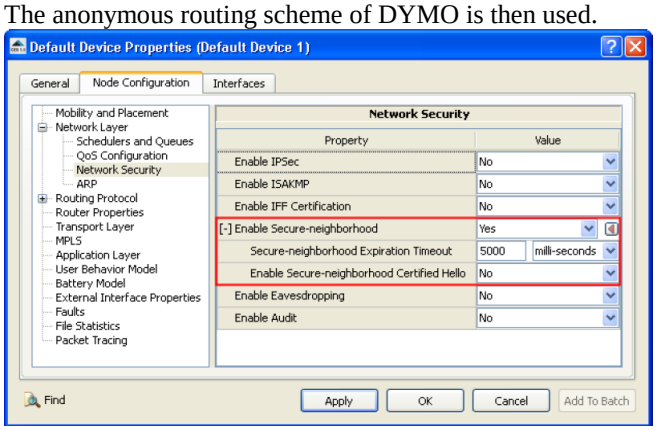

Figure 7: Selection of S-DYMO in QualNet

IV. RESULTS AND ANALYSIS

Initially, we present consequences of QoS measurements – throughput, normal start to finish deferral and normal jitter. Finally, we present measurements identified with energy utilization [18].

4.1Throughput (bits/s): The rate of effectively sent information every second in the organization during reproduction. The variety of throughput under two-ray propagation models for nodes in DYMO, S-DYMO is given in figure 8. The throughput for DYMO in random waypoint is maximum for larger network size at 2678 and is minimum at 850 for smaller network size. The throughput for S-DYMO is maximum for larger network at 3687 and is minimum at 1002 for smaller network.

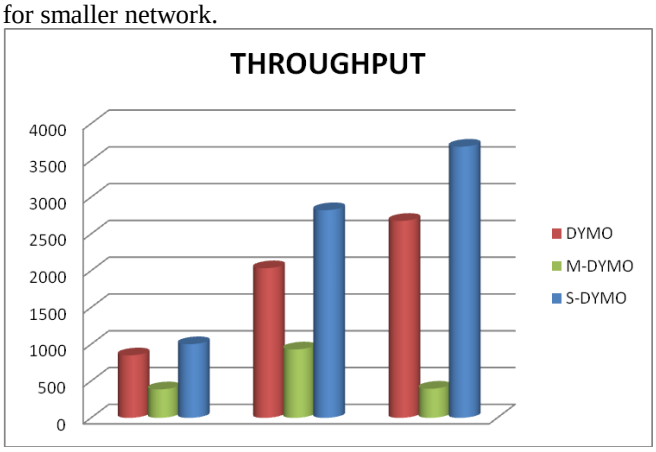

Figure 8: Variation of throughput with network size under random waypoint mobility model for DYMO &S-DYMO

4.2 Average end-to-end delay(s): The time is taken on behalf of a bundle to go from a basis to an objective. The variety of normal start to finish delay under the irregular waypoint portability model for hubs in DYMO, S-DYMO is given in figure 9.

The end-to-end postponement for DYMO in random waypoint is maximum for larger network at 0.085262 and is minimum at 0.048958 for smaller network. The end-to-end deferral for S-DYMO in random waypoint is maximum for larger network at 0.130941 and is minimum at 0.095626 for smaller network.

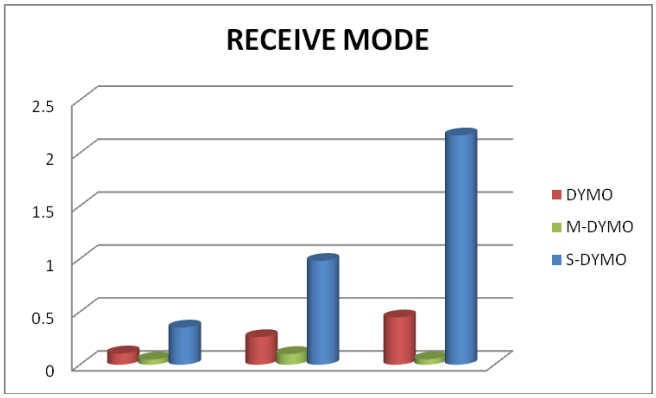

Figure .9: Variation of delay with network size under random waypoint mobility models for DYMO &S-DYMO

4.3. Average jitter (s): The variance of minimum and maximum interruption is jitter. The dissimilarity of average jitter under random waypoint mobility models for nodes in DYMO, S-DYMO is given in figure 10. The jitter for DYMO in random waypoint is maximum for medium network at 0.061417 and is minimum at 0.101682 for smaller network. The jitter for S-DYMO in random waypoint is maximum for larger network at 0.173246 and is minimum at 0.1187 for smaller network.

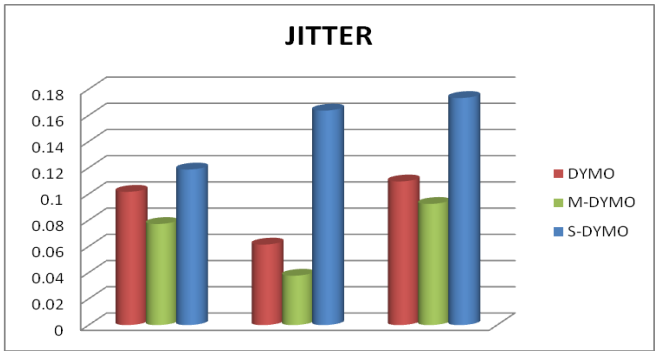

Figure 10: Variation of jitter with network size under random waypoint mobility models for DYMO &S-DYMO

4.4. Energy consumed in transmit mode: A hub should be in transmission mode as it sends knowledge bundles to organizational hubs. These hubs anticipate capacity to transmit knowledge packets and Transmission Resources (Tx). The variance of energy absorbed in transmit mode in DYMO, S-DYMO node mobility models is shown in Figure 11. DYMO's random waypoint energy usage in transmit mode is 0.148124 overall for larger networks and 0.106884 minimum for smaller networks. S-random DYMO's waypoint energy usage in transmission mode is 0.730888 limit for larger network and 0.358859 for smaller network.

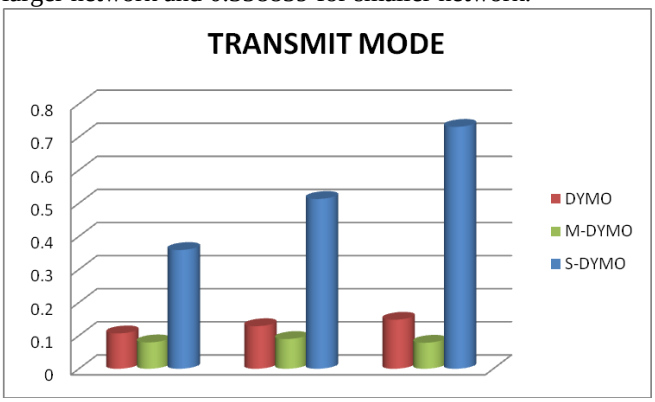

Figure 11: Variation of energy consumed in transmit mode mode with network size under random waypoint mobility model for DYMO &S-DYMO

4.5. Energy expended in receiving mode: When a hub collects a packet of knowledge from various hubs, it is said to be in receiving mode and the energy is used to get the parcel is called Reception Energy (RX). The variance of energy absorbed in receive mode in DYMO, S-DYMO node mobility models is shown in Figure 12. DYMO's random waypoint energy usage in receive mode is 0.446787 overall for larger networks and 0.106843 minimum for smaller networks. Energy usage in receiving mode for S-DYMO in random waypoint is 2.16518 overall for larger networks and 0.350962 minimum for smaller network.

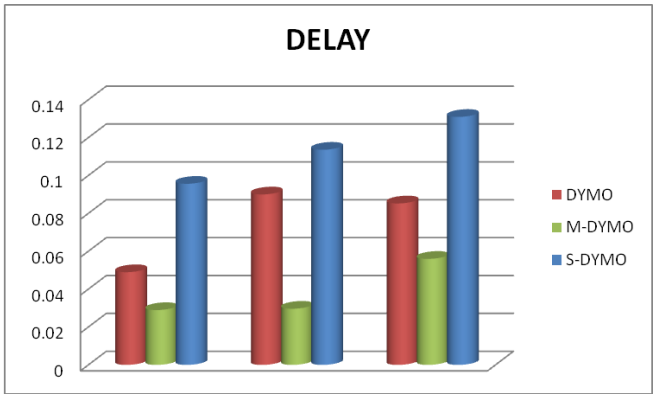

Figure 12: Variation of energy consumed in receive mode with network size under random waypoint mobility models for DYMO &S-DYMO

4.6. Energy consumed in idle mode: In this mode, for the most part, the hub is neither sending nor accepting any information parcels. However, this mode devours power on the grounds that the hubs need to tune in to the remote medium constantly to distinguish a bundle that it ought to get so the hub would then be able to switch into get mode from inert mode. The variety of energy devoured in the inert mode under random waypoint mobility models for nodes in DYMO ,S-DYMO is given in figure 13.The energy consumption in idle mode for DYMO in random waypoint mobility model is maximum for smaller network at 9.89245 and is minimum at 9.5452 for larger network. The energy consumption in idle mode for S-DYMO in random waypoint is maximum for smaller network at 9.64605 and is minimum at 7.9403 for larger network.

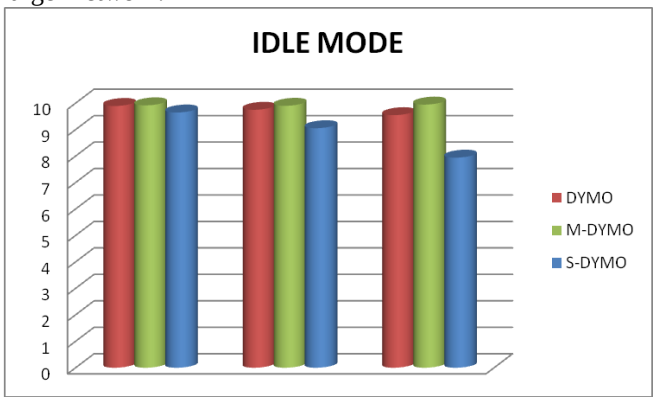

Figure 13: Variation of energy consumed in idle mode with network size under random waypoint mobility models for DYMO &S-DYMO

4.7. Total Energy (mJoule): Complete energy is the sum of all various energies. The variance of total energy absorbed under random waypoint mobility systems for nodes in DYMO,S-DYMO is seen in Figure 12. For DYMO in random waypoint, overall energy usage in send, receive and idle modes is 3.380037 limit for larger network and 3.368726 minimum for smaller network. For S-DYMO in random waypoint, overall energy usage in send, receive and idle modes is 3.612123 limit for larger network and 3.451957 minimum for smaller network. We specifically observed that M-DYMO degrades efficiency with regular DYMO. Figure 6 to Figure 14.

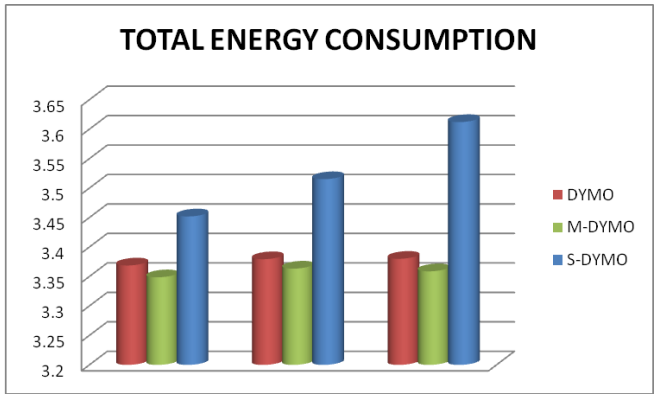

Figure 14: Variation of total energy with network size in all modes under random waypoint mobility models for DYMO &S-DYMO

V. CONCLUSION

From the findings of the trial, energy usage improved as encryption was integrated into the current routing protocol. Network size raises energy usage declines in random waypoint for DYMO in idle mode. In idle mode, no effect of network size raises energy consumption arbitrarily for M-DYMO. Whereas in the case of S-DYMO, as network size grows energy usage declines randomly in idle mode. It is stated that increased network size energy usage is lower for S-DYMO.

REFERENCES

1. D. P. Agrawal and Q-A Zeng. “Introduction to Wireless and Mobile Systems,” Brooks/Cole Publishing, ISBN No. 0534-40851-6, 436 pages, 2003.
2. S. Giordano and W. W. Lu, “Challenges in mobile ad hoc networking,” IEEE Communications Magazine, vol. 39, no. 6, pp. 129–181, June 2001.
3. J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva. “Multi- Hop Wireless Ad Hoc Network Routing Protocols.”ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM‟98), pages 85-97, 1998.
4. Latiff, L. A. and Fisal, N. 2003.„Routing Protocols in Wireless Mobile Ad Hoc Network – A Review‟.The 9th Asia-Pasific Conference on Communication (APCC 2003), vol. 2, pp. 600- 604.
5. [5]S. Lee, M. Gerla, and C. Chiang. “On-Demand Multicast Routing Protocol.”IEEE Wireless Communications and Networking Conference (WCNC‟99), 1999.
6. J. Broch, D. Maltz, D. B. Johnson, Yih-Chun Hu, J. Jetcheva. “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing protocols.”Proceedings of the Fourth Annual ACM/IEEE on Mobile Computing and Networking, MOBICOM 98, October 1998.
7. C.E. Perkins, E.M. Royer & S. Das, Ad Hoc On Demand Distance Vector (DYMO) Routing, IETFInternet draft, draft-ietf-manet-DYMO-08.txt, March 2001
8. C. E. Perkins, and E. M. Royer, “Ad-Hoc On-Demand Distance Vector Routing,” in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp. 90-100, February 1999.
9. QualNet 5.1Developer Model Library, Scalable Network Technologies, Inc.,http://www.scalable-networks.com
10. Jiejun Kong, Xiaoyan Hong. DYMO: anonymous on demand routing with untraceable routes for mobile adhoc networks. MobiHoc‟03, June 1–3, 2003, Annapolis, Maryland, USA
11. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”,

12. WIRELESS/MOBILE NETWORK SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp.,2006 SpringerS. Yi and R. Kravets, Composite Key Management for Ad Hoc Networks.Proc. of the 1st Annual International Conference on Mobile and Ubiquitous
13. R. Oppliger, Internet and Intranet Security, Artech House, 1998.
14. Qiu Wang and Hong-Ning Dai and Qinglin Zhao,
15. "Eavesdropping Security in Wireless Ad Hoc Networks with Directional Antennas"
16. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour2, and Yoshiaki Nemoto, "Detecting Blackhole Attack on DYMO-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007
17. Anuj K. Gupta1, Harsh Sadawarti and Anil K.Verma, "Implementation of Dymorouting Protocol", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol.1, No.2, May 2013.
18. Viren Mahajan, Maitreya Natu, and AdarshpalSethi, "ANALYSIS OF WORMHOLE INTRUSION ATTACKS IN MANETS", 2008 IEEE
19. Neeraj Tantubay, Dinesh Ratnam Gautam and Mukesh Kumar Dharjwal , "A Review of Power Conservation in Wireless Mobile Ad hoc Network (MANET)",IJCSI Vol.8, Issue 4, No.1 , July,2011.
20. Ayyaswamy Kathirve,and Rengaramanujam Srinivasan, "Analysis of Propagation Model using Mobile Ad Hoc Network, Routing Protocols", International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 1, No. 1
21. Muhammad Inayat Ullah,Nasir Nawaz, "Measuring the Effect of CBR and TCP Traffic Models over DYMO Routing Protocol", Global Journal of Computer Science and Technology Volume 11 Issue 14 Version 1.0 July 2011, Global Journals Inc. (USA),Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

AUTHORS PROFILE

Uppe. Nanaji received the B. Tech CSE degree from JNTU, Hyderabad, and M. Tech degree in Computer Science Technology from Andhra University, Vishakhapatnam and he is currently pursuing Ph. D in Computer Networks from Andhra University, Visakhapatnam. He is Research Scholar from department of CSSE, Andhra University, and Visakhapatnam. 15 years teaching experience in various engineering college.

Sri S Pallam Setty is presently working as Professor, Department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam. He has completed M.Phil., M.Tech, and Ph.D, from Andhra University. His areas of specialization are Mobile Ad Hoc Networks, Sensor Networks, and Wireless Networks. Total 30 years of teaching experience.