Analysis of the Effect of Routing Protocols on a Network

B Rama Devi,[1]

[1]Asst. Professor, Department of Computer Science and Engineering

QIS College of Engineering and Technology

ChennaReddy Manoj Kumar[2], Bethapudi Tarun[3], KavuriGidhyon[4], PurimitlaMaruthi Prasad[5]

Student, Department of Computer Science and Engineering
QIS College of Engineering and Technology

***Abstract**-As the name suggests, this system is made up of a number of computers that share the resources that the network's nodes have. The computers interact with each other using the same protocols across digital links. There are several network topologies that may be used for these linkages, which are made up of telecommunication network technologies, such as physically wired, optical, and wireless radio-frequency means. Personal computers, servers, networking devices, and other specialised or general-purpose hosts are all examples of nodes in a computer network. Network addresses and hostnames may be used to identify them. Hostnames serve as node identifiers that may be easily remembered and are seldom modified after being assigned. For communication protocols like the Internet Protocol, network addresses are necessary.Computer networks may be categorised in a variety of ways, including by the medium used to transmit signals, bandwidth, the protocols used to arrange network traffic, the scale of the network, topology, traffic management mechanisms, and the purpose of the organisation.Access to the World Wide Web, digital video and music, shared usage of application and storage servers and printers/fax machines, as well as use of email and instant messaging programmes are all supported via computer networks. Protocols that define how routers interact with one other are known as routing protocols. These protocols let routers determine the most efficient path between two nodes on a computer network.We may say that routing algorithms are in charge of finding the most efficient route for communication. The language a router uses to communicate with other routers about the reachability and state of a network is known as a routing protocol. Routing and bridging are frequently used interchangeably.The main distinction between the two is that they are functioning in different layers. To get to a certain location, routing algorithms consider a variety of factors, including the present load on a route, its dependability, latency, and other metrics. First, it exchanges data with its local neighbours, and subsequently with everyone else on the network as a whole.*

Keywords—Routing Protocols,OSPF, RIP, RIP2, IS-IS, BGP.

I. INTRODUCTION

As the world strives for a speedier and more efficient medium of expression, further mechanical advancements in connection are expected, leading to a more seamless method of information exchange. Communication demands of the public may be met by using wireless adhoc networks. In a local area network, WANET (Wireless Adhoc Network) creates a network of wireless devices on-the-fly that allows them to communicate with each other continuously or intermittently. As a result of the point-to-point wireless methods used to connect the connected devices, the devices may communicate with one another in a dispersed network.This one sort of data transmission was developed by author Raj, Jennifer S., and colleagues [1] to deal with the problem of power consumption in sensor systems owing to their battery power and inability to focus simply on delivering a suitable configuration. while focusing their efforts on identifying and developing a routing that takes into account both power consumption and optimal web usage, they neglected to consider the security of data sent from the photomultiplier tube to the iiot schema. Similarly, Manshahia, et al [2] used swarm intelligence to route their wireless link, but the researcher used the based algorithm and CNN to do so. One of the most challenging tasks in vanets is the creation of routing capacity, which is essential for fundamental network activities. Transit in ad hoc networks fascinates because of the unique subsets of variables. A primary benefit of an ad-hoc network is the freedom of nodes to roam around. As a consequence of this node movement, the network experienced regular network dynamics and route failures.

This network's dynamic nature necessitates a routing system that can dynamically adapt. For one thing, the base transceiver has a far lower and more changeable band width than on wired networks. The amount of bandwidth available to each node is severely constrained when the wireless transmitter is used as a shared medium. As a consequence, relays should be low-cost and staff-intensive to generate routes, allowing the additional bandwidth to be put to good use for data transfer. Third, nodes are powered by electricity, which has a finite amount of power available. Routing protocols must be energy efficient if they are to keep nodes connected and connected for an extended length of time. This seems to be even another motivation for keeping costs as low as possible. In order to achieve high overall performance, routing systems must meet the attractive objectives of dynamic flexibility and minimal latency. As a result of their heavy reliance on lead topology and their high overhead, routing protocols designed for wired networks like the wired Internet are woefully insufficient. Because of this, there are several routing concepts specialised to ad-hoc networks.Even if some of these theories are improved wired network implementations, the bulk of them incorporate unique concepts like "on-demand routing," in which routes are only kept "reactively" when they are necessary. On the other hand, standard Internet-based protocols take an active role. Other new paradigms, such as using routing location information and energy efficient routing, have also arisen. The underlying network architecture may be regarded of as an undirected graph in all of our talks. This may not be the case in practise due to the possibility of unidirectional connections.

When the transmission powers of the network's nodes diverge, this is a common occurrence. Links may benefit from geographically varying wireless channel distortion even in a fully homogeneous network. However, empirical [38] and theoretical [3] data suggests that continuous networks may not be useful for routing. On the other side, using these kinds of connections might take a lot more time and cost a lot of money. On the other hand, ignoring unidirectional linkages when they do exist is a simple matter. A simple two-way message exchange between neighbouring nodes may do this. Routing systems often send "beacons" (also known as "hello" messages) in order to find the nearby node set (neighbour discovery).ADhoc is a busy and scattered species because the nodes are powered by limited-capacity batteries. It is thus a huge task to develop energy-efficient routing methods. Due to the limited lifetime of different energy sources, the ad hoc network's ability to function is severely limited in terms of its ability to deliver energy. Various sources of energy are used to power an ad hoc network node. Energy has been wasted by sending a packet, receiving a packet, putting the node in a waiting state and putting the router in deep sleep, all of which occur when the wireless network on the node is switched down. A node's ability to relay packets on behalf of others, as well as the network's overall lifespan, are both impacted by a power outage. This means that when it comes to energy-efficient routing, short distances and average ratings are preferable over extended durations and low energy consumption.Therefore, in order to maximise network performance, nodes should choose the best route based on their remaining lifetime. It's impossible to calculate the remaining lifespan of the route in a systematic way since the elements affecting route lifetime vary.With the proposed protocol's foundations based on energy and distance, intelligent fuzzy logic approaches may be used to assess its performance in this situation. These two parameters allow to initiate various implications, which are then passed to the inference engine, which analyses the many rewards related with each route.. Based on simulations and a comparison of the proposed routing protocol to other existing protocols, it has been shown that the proposed routing protocol contributes to performance benefits.

II. RELATEDWORKS

Routing protocols are concerned with finding the most direct route across the network in order to maintain the network's connection. Routing protocols use many metrics to evaluate the quality of a route, such as the number of next hops, bandwidth, and latency. Use of Cisco packet Tracer and several routing protocols is presented in this paper. EIGRP is the best protocol to utilise since it has a faster convergence time than RIPv2 and OSPF, according to our study.OSPF outperforms RIP in terms of average throughput and instant latency in various network sizes. The OSPF protocol transmitted the most traffic and was the last to send routing traffic, whereas EIGRP was the first to send traffic and RIP was the least trafficful since it simply communicates the number of hops.Distinguishing faulty routing data from the rest of the OSPF system by dividing it into separate autonomous routing zones reduces route overhead, reduces table size, and speeds up convergence. On the contrary, regions limit connectivity while increasing the complexity of routing, the length of routing paths, and the concentration of traffic. The OSPF routing protocol is extensively used in the computer networking industry.Data transfer through a network is not specified. network's behaviour under real-world conditions can't be predicted by a single set of routing protocols since such protocols don't take into account things like data flow, which the present system does.

Using an ad hoc network of wireless smart tags, Gil Zussman and Adrian Segall [11] suggested to collect data from incarcerated survivors using this method. The authors study the energy-efficient routing dilemma in such a networks, showing that "smart badges" have limited power sources and poor data speeds, both of which are inadequate in an emergency. Like any other cast routing problem, the goal of this work is to maximise the amount of time until the first battery dies.Yu et al. [12] examines and categorises the suggested MANET energy-aware routing methods. They minimise the amount of continuous feedback energy required to transmit and receive packets, as well as the amount of collaborative negotiation energy spent when a mobile node is inactive but listens to the wireless media for any future particular status from other nodes. According to the authors, the results are classified into two categories:

In the first category, transmission power regulation and load distribution are included, while in the second, sleep/power-down mode is used. When it comes to choosing the best algorithm for a certain case, it might be hard to identify which one is the best fit. Consequently, the authors make it simple for scientists to combine current approaches to develop a more energy-efficient system.In mobile ad hoc networks, Su et al. [13] presented the fuzzy logic modified AODV routing (FMAR) protocol. The primary goal of this system is to employ fuzzy logic weighted multi-criteria to dynamically analyse active routes. The poor throughput of mobile devices may be managed with its assistance. In addition, the suggested protocol does not establish rating values for all possible routes; rather, it selects one, making it impossible to discern which pathways are most valuable. These solutions do not address the challenges of energy-efficient routing and network lifetime depending on factors such as energy and distance. Therefor two metrics based on these issues are taken into consideration in the suggested technique.

III. PROPOSED SYSTEM ARCHITECTURE

Static Routing, Dynamic Routing and Default Routing would be tested in the Proposed System instead of certain Routing Protocols.Analyzing the impact of routing protocols is possible using Cisco Packet Tracer.Cisco Corporation created it as a simulation tool.

Static Routing Module

Using a static routing protocol, an administrator may choose a direct route from one network to another by hand. It enhances the network's security.It is the responsibility of a network administrator to establish, maintain, and update a static routing table. Every router must have a static route to every network in order to have complete connectivity. This allows for fine-grained control over routing, but it rapidly becomes infeasible on big networks.Network traffic will not be clogged up by routers sharing the same static routes. Because every update to the routing infrastructure (such as a broken connection or the addition of a new network) must be made by hand, static routing is not fault-tolerant. If a link goes down, routers in a static environment can't automatically switch to a new path.

Dynamic Routing module

Another sort of routing technique to consider is dynamic routing. It makes it easier for routers to automatically update their routing tables with information from other connected routers. When the network's topological structure changes, these protocols also send out topology updates.A total of five distinct Dynamic Routing Protocols are in use today.First, Take the Shortest Route (OSPF)(EIGRP) Route Information Protocol (RIP). A Border Gateway Protocol for Inter-System Interoperability (IS-IS) (BGP).

Default Routing Module

If a router cannot find a way to a certain network, it will drop all traffic to that network. Traffic may be redirected via a default route or gateway of last resort even when there is no specified route to the desired network.The following would be included in the project's Function Design, given that we are running it via a simulation tool.If a router cannot find a way to a certain network, it will drop all traffic to that network. It is possible to forward traffic even when no specific route to a particular network is specified by using a default route, or "gateway of last resort."All zeros in the network and subnet mask identify the default route (0.0.0.0 0.0.0.0). The gateway of last resort is the least specific route possible, so it will only be used if a more specific route is unavailable.How to set up a default routeip route command on the router Node number for the 0.0.0.0/0 networkOn a Cisco device, it is possible to designate a default network:ip default-network network octet number: Router(config)# ElementsRouter(s)Switche(s), Servers(s), Cables Made of Pure CopperCrossover, Cables made of copperFiber, Optic Cables, PC(s).

Computer networks use routers to exchange data packets between one other. The Internet's traffic is directed by routers. Internet data, such as a web page or an email, is sent in the form of packets of data. Typically, a packet is sent from one router to another until it reaches its final destination node in an internetwork.Packet switching is used by network switches to link devices on a network so that data may be received and sent to its respective destinations.

As a data link layer (layer 2) OSI model network bridge, a network switch employs MAC addresses to route traffic. Routing capabilities may be added to certain switches so that data can be routed at the network layer (layer 3). Layer-3 or multilayer switches are the most popular names for these types of switches.It is a computer that serves as a repository for other computers in the network and provides them with a variety of resources such as hardware access, disc space, printer access, and so on.A form of CAT5 with RJ-45 connections at both ends, straight-through cable is a type of CAT5 with the same pin out. The T568A or T568B specifications are followed. For the sake of uniformity, the LAN use the same colour code. In a local area network (LAN), this twisted-pair cable is used to link computers and network hubs like routers. Network cables of this sort are rather prevalent.

Copper Cross-Over Cables (CCCs):

A CAT 5 crossover cable has one end configured as T568A and the other as T568BC. Pin 1 is crossed with Pin 3 and Pin 2 is crossed with Pin 6 in this type of cable connection.Two or more computers can be linked together with the help of a crossover cable. Transmission and reception signals are reversed in crossover cables. Devices of the same type, like computers or switches, can be connected to each other using this method of connection.It is a network cable that is made up of glass fibres that are wrapped in an insulated casing. They're meant for long-distance, high-performance data networking, and telephony. Fiber optic lines have a greater bandwidth and can carry data over longer distances than traditional wired cables. The internet, cable television, and telephone services of most of the globe are all supported by fibre optic cables.PCs are multi-purpose microcomputers that are small enough, powerful enough, and affordable enough to be used by individuals. Instead of relying on a computer specialist or technician, personal computers are meant to be controlled by the end user. Unlike huge, expensive minicomputers and mainframes, time-sharing by several users at the same time is not employed with personal computers.At a minimum, a router must be able to do the following:

The address to which a packet is headed. This is handled by layer 3 protocols like IP.Packets can be routed to neighbouring routers from which remote networks can be discovered and learned of.It's possible to discover the optimum path between faraway networks.A method for acquiring, verifying, and maintaining route information. Even worse than not having any routing information at all is having information that is inaccurate, incomplete, or otherwise unstable. Packets are dropped and the source is informed if a router does not have routing information. Incorrect routing information can lead to loops, which can disrupt networks.

Open Shortest Path First (OSPF)

Only IP packets are routed using the link-state routing protocol OSPF (Open Shortest Path First). Multi-vendor network devices are supported via the inner gateway protocol (IGP). With the exchange of link-state announcements, OSPF routers develop and maintain a global topology database (LSA). Using LSAs, routers with OSPF enabled may broadcast their topology and routing information to one other. It is possible to save bandwidth by only sending event-triggered updates when there is a change in the topology (link failure).

Enhanced Interior Gateway Routing Protocol (EIGRP)
In order to route various network layer protocols, Cisco created the proprietary routing protocol EIGRP. Monolithic IP-only network design, with open internet and cloud connection standards, has gained popularity more lately. It's no secret that OSPF is taking the place of EIGRP since it's open source and more scalable. EIGRP is a non-hierarchical routing technology that is challenging to debug because of its complexity.EIGRP is an enhanced distance vector protocol that combines the features of both distance vector and link state protocols into a single system. Unlike other routing protocols, EIGRP does not have a comprehensive network map. Like link state protocols, EIGRP forms neighbour adjacencies and provides event-driven updates instead of periodic complete routing table updates. Subnet information is provided in routing updates for this classless protocol, which is similar to OSPF in design. Variable length subnet masks (VLSM) allow for classless subnetting and route summarization on any bit boundary, making this a significant benefit. Contrast this with distance vector protocols, which only support subnetting in the class of a given IP address. The variance feature of EIGRP allows for unequal cost path load balancing, which is unique to EIGRP.

Routing Information Protocol (RIP)
An earlier routing system, Routing Information Protocol (RIP), predates the internet age by many decades. Smaller networks with simple routing and no subnetting were the target audience for this product. RIP is a non-scalable distance vector protocol with delayed convergence and classful addressing as its sole addressing mechanism. The benefits of this approach are that it is simple to implement and debug. The route metric for a distance vector protocol is the number of hops. Distance from source to destination is measured in hops (distance). As a result, the path with the fewest router hops is chosen as the optimal route. RIPv1 does not provide message authentication, which makes it less appropriate for internet connections. Except for EIGRP, most inner gateway protocols exclusively use equal-cost pathways for load balancing.

Routing Information Protocol 2(RIP2)
RIPv2 is an upgrade to the protocol standard that was aimed to alleviate some of the difficulties of RIPv1. RIPv2 is a classless protocol that incorporates subnet mask information into routing updates, while RIPv1 is a class-based system. That provides the same classless subnetting that OSPF, EIGRP, IS-IS and BGP support. There is also support for authentication of communications between RIPv2 neighbours through text password or MD5 hash. A basic degree of security is provided by this across current network domains.RIPv2 transmits routing changes to multicast 224.0.0.9 instead of the traditional 255.255.255.255 broadcast technique where all routers would have to digest messages. For backwards compatibility, RIPv2 routers may transmit broadcasts to RIPv1 routers. The difficulty is that RIPv1 will summarise any classless routes on a classful border.

Intermediate System to Intermediate System(IS-IS)
The IS-IS link state routing protocol resembles OSPF in that it is a protocol that connects intermediate systems. Routing inside big service provider network domains is a primary use of this IGP (internal gateway protocol). An external gateway protocol is required for any routing

via the Internet (BGP). Among the benefits are scalability, rapid convergence, and security. As an OSI Layer 2 protocol, IS-IS packets are not subject to IP spoofing or DDOS assaults. Any multiprotocol payload, including IP packets, may be transported using CLNS.It uses Dijkstra's method to determine which route is shortest for each destination in a topology database. A topology table may be built using LSPs that are promoted as being comparable to OSPF LSAs. The IS-IS addressing protocol uses interface cost to determine the optimum route metric (bandwidth). A route's cost is calculated as the sum of all expenses encountered along the way. An end system (ES) or an intermediate system (IS) is how IS-IS categorises all nodes (routers).Level 1 routers (intra-area), Level 1/Level 2 routers (ABR), and Level 2 routers (inter-area) form a two-level hierarchy (backbone). Because each router may only be assigned to one area, the router serves as the border between areas rather than an interface in OSPF... There is no such thing as an OSPF-style backbone that connects all of the regions. The routing architecture of certain Level 2 routers allows them to link locations through L1/L2 routers.

Border Gateway Protocol (BGP)

Interdomain routing between private IGP routing domains is handled by Border Gateway Protocol (BGP), the de facto internet routing protocol. A route vector protocol is one that uses an external gateway protocol (EGP). In essence, BGP is a distance vector protocol that broadcasts the AS route to neighbours with every change to the routing table.Path attribute regulations allow for load sharing rather than load balancing. Classless routing protocols don't automatically summarise routes that are offered. Internal BGP (iBGP) and external BGP (eBGP) connections are given autonomous system numbers (ASNs) in this non-hierarchical design. In contrast to iBGP peers, eBGP neighbours are all allocated to the same autonomous system.Either a private or public BGP autonomous system number (ASN) exists. A service provider's assignment of a public ASN is required for Internet access. BGP internet routable connections are allowed to use a public range of 1 to 64511. The iBGP and/or eBGP network uses the private AS number range from 64512 to 65535. iBGP and/or eBGP autonomous systems are used in several big business network domains.

IV. RESULTS AND DISCUSSION

When a packet travels from its source to its destination, its average end-to-end delay is measured. It also includes the time it takes for a node to discover a route when it is initially unavailable.A communication channel's throughput is the average rate of successful message delivery. Figure 1 shows the average end-to-end throughput for typical routing protocols, which shows how much network resources are being utilised. Maximum throughput is approximately 6kbps with an offered load of 1 packet/sec. With fewer nodes, throughput for DSR and DYMO improves quickly. When the number of nodes increases, OLSR, on the other hand, performs better. In particular, DSR outperforms the other protocols when the number of nodes is less than or equal to 75 as shown in figure 2. Packets from the source will arrive at the destination with varying delays, as indicated by the average jitter value. When a packet is queried by routers along its path from source to destination, its delay varies as shown in figure 3. It is the number of packets that are lost due to incorrect or unavailable routes and MAC layer collisions that is the average loss rate. Network size and average packet dropped are shown in this graph to show how reliable each protocol is in comparison to others as shown in figure 4. When the network is smaller, all protocols except DSR see fewer data packets dropped (with the number of nodes 25, 50, 75). The higher reliability of AODV and DYMO can be attributed to their strong performance.However, as the number of nodes grows, more packets are dropped for both protocols, but more so for DSR.With 75 nodes, DSR's average packet loss is 60% closer as shown in figure 5.

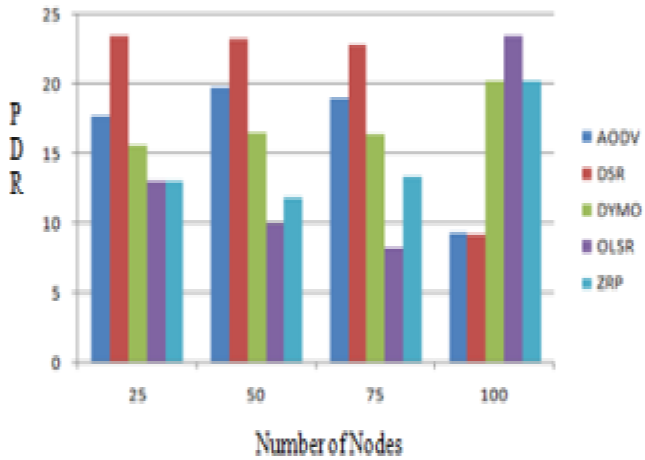

Fig. 1 Packet delivery ratio

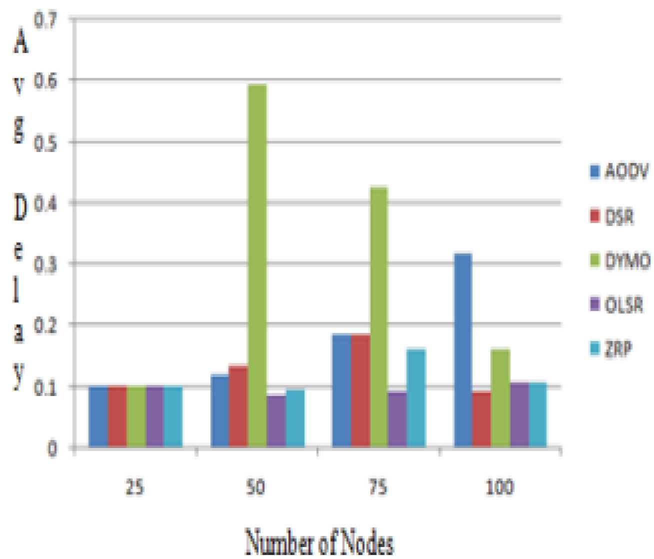

Fig.2 Average End-to End Delay

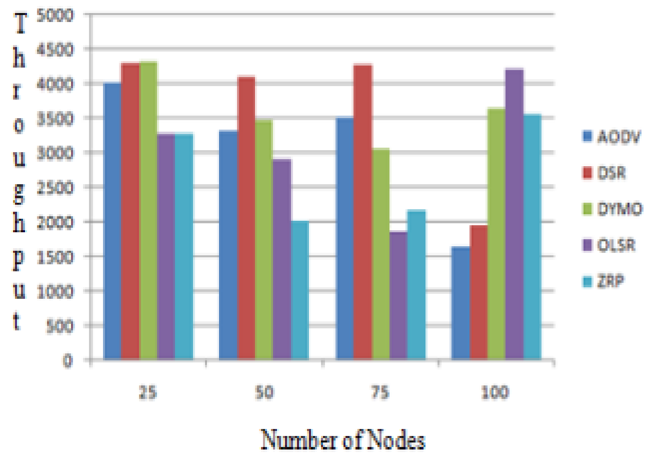

Fig. 3Throughput

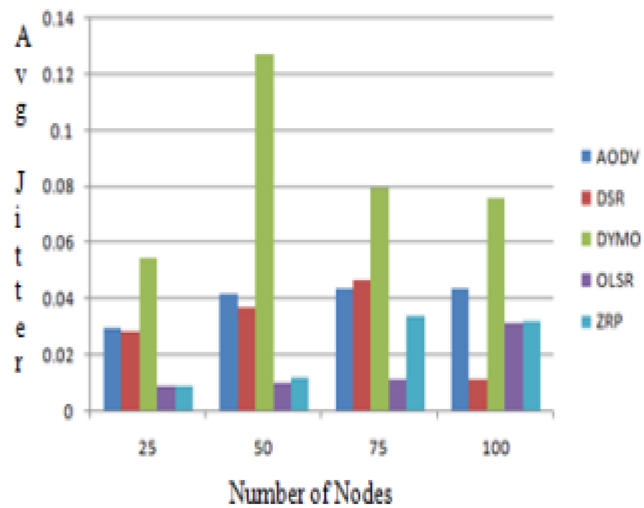

Fig. 4 Average JitterValue

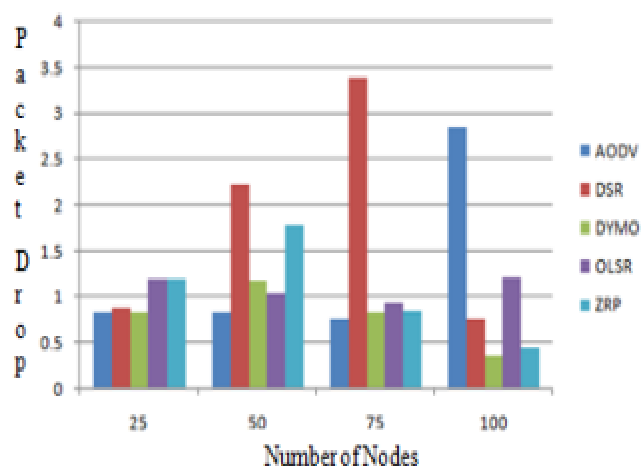

Fig. 5 Average Packet loss

V. FUTURE SCOPE AND CONCLUSION

It has been shown that for low traffic and low mobility, proactive routing techniques perform better than on-demand routing. Minimal delay from beginning to finish. On the fly High traffic variety and mobility make routing techniques more effective. OSLV and RIP Protocols have the greatest rate of packet delivery. BGP and RIP2 are both capable of producing identical outcomes, however RIP2 has a bigger over-head. With regards to transportation, outcomes vary depending on the type of model being used. Based on the application's requirements, the routing protocol and mobility are chosen. When compared to the IS-IS and OLSR protocols, BGP and EIGRP provide superior performance. It is more common to use the Manhattan Mobility Model than the Random Waypoint or Random Group Mobility Models because it provides a higher packet delivery ratio while requiring less management overhead.

REFERENCES

[1] P. Kalamani, M. Venkatesh Kumar , M. Chithambarathanu, Reji Thomas, Comparison of RIP, EIGRP, OSPF, IGRP Routing Protocols in Wireless Local Area Network (WLAN) by using OPNET Simulator tool - A Practical Approach-IOSR-JCE,e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. VI (Jul- Aug. 2014).

[2] Rajan, R., Shipra, S.“WLAN Performance Improvisation by Fine Tuning IEEE 802.11Parameters”, International Journal of Computer Applications, April 2012.

[3]Tanenbaum, Andrew s. Computer Networks. s.l.: Pearson Education, 2003.[4]R.Devi, B.Sumathi, T.Gandhimathi, G.Alaiyarasi,Performance Metrics of MANET in Multi-Hop Wireless Ad-Hoc Network Routing Protocols, International Journal of Computational Engineering Research (IJCER) ISSN: 2250-3005.

[5]V.Vetriselvan, Pravin R.Patil, M.Mahendran, Survey on the RIP, OSPF, EIGRP Routing Protocols, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1058-1065.

[6] Y. Zhang and Y. Shi, "Tactical Wireless Network Visualization: Requirements and Representations," 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 2018, pp. 740-743

[7] Wan Aida Nadia Wan Abdullah et al, “Impact of clustering in AODV routing protocol for wireless body area network in remote health monitoring system”, Indonesian Journal of Electrical Engineering and Computer Science Vol. 13, No. 2, February 2019, pp. 689~695

[8] P. Bellavista, G. Cardone, A. Corradi and L. Foschini, "Convergence of MANET and WSN in IoT Urban Scenarios," in IEEE Sensors Journal, vol. 13, no. 10, pp. 3558-3567, Oct. 2013.

[9] W. A. Hussein, B. M. Ali, M. F. A. Rasid and F. Hashim, "Design and performance analysis of high reliability-optimal routing protocol for mobile wireless multimedia sensor networks," 2017 IEEE 13th Malaysia International Conference on Communications (MICC), Johor Bahru, 2017, pp. 136-140

[10] T. T. Son, H. Le Minh, G. Sexton and N. Aslam, "Self-adaptive proactive routing scheme for mobile ad-hoc networks," in IET Networks, vol. 4, no. 2, pp. 128-136, 3 2015.

[11] Rahul Desai, B P Patil, “Analysis of Reinforcement Based Adaptive Routing in MANET”, Indonesian Journal of Electrical Engineering and Computer Science Vol. 2, No. 3, 2016, pp. 684 ~ 694

[12] N. Meghanathan, "A Location Prediction-Based Reactive Routing Protocol to Minimize the Number of Route Discoveries and Hop Count per Path in Mobile Ad Hoc Networks," in The Computer Journal, vol. 52, no. 4, pp. 461-482, July 2009

[13] Y. Fengjie, Y. Hui and Z. Ying, "Research on DSDV routing protocol based on wireless Mesh network," 2018 Chinese Control And Decision Conference (CCDC), Shenyang, China, 2018, pp. 4292-4297.

[14] Zhihao Ding, Pinyi Ren, Qinghe Du, "Mobility Based Routing Protocol with MAC Collision Improvement in Vehicular Ad Hoc Networks", Communications Workshops (ICC Workshops) 2018 IEEE International Conference on, 2018.

[15]Yujun Zhang, Guiling Wang, Qi Hu, Zhongcheng Li, Jie Tian, "Design and performance study of a Topology-Hiding Multipath Routing protocol for mobile ad hoc networks", INFOCOM 2012 Proceedings IEEE, pp. 10-18, 2012.

[16] A. Garcia-Santiago, J. Castaneda-Camacho, J. F. Guerrero-Castellanos and G. Mino-Aguilar, "Evaluation of AODV and DSDV routing protocols for a FANET: Further results towards robotic vehicle networks," 2018 IEEE 9th Latin American Symposium on Circuits & Systems (LASCAS), Puerto Vallarta, Mexico, 2018, pp. 1-4.

[17] A. K. Yogi and J. Surana, "An implementation of Modified AOMDV routing protocol in different wireless networks," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, 2016, pp. 1-5.

[18] Manijeh Keshtgary, Negar Rikhtegar, "Performance evaluation of routing protocols for wireless sensor networks in forest fire detection application", Information and Knowledge Technology (IKT) 2013 5th Conference on, pp. 248-251, 2013

[19] Rahul Desai, B P Patil, “Routing protocols for Mobile Ad Hoc Network - A Survey and Analysis”, Indonesian Journal of Electrical Engineering and Computer Science Vol. 7, No. 3, 2017

[20] S. K. Srivastava, R. D. Raut and P. T. Karule, "Analyzing the performance of routing protocols based on evaluation of different parameters in MANETs," 2015 International Conference on Communication Networks (ICCN), Gwalior, 2015, pp. 258-261.

[21] U. Draz, T. Ali, S. Yasin and A. Shaf, "Evaluation based analysis of packet delivery ratio for AODV and DSR under UDP and TCP environment," 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, 2018, pp. 1-7

[22] Wan Aida Nadia Wan Abdullah et al, “Corrupted packets discarding mechanism to alleviate congestion in wireless body area network”, Indonesian Journal of Electrical Engineering and Computer Science, Vol. 14, No. 2, May 2019, pp. 581~587

[23] Nur Aishah Bt. Zainal, Mohamed HadiHabaebi, Israth Jahan Chowdhury, Md Rafiqul Islam, Jamal I. Daoud, “Gateway sink placement for sensor node grid distribution in lora smart city networks”, Indonesian Journal of Electrical Engineering and Computer Science, Vol 14, No 2: May 2019, pp. 834-842

[24] Nabeena Ameen, Najumnissa Jamal, L. Arun Raj, “Comparative analysis of energy based optimized dynamic source multipath routing protocol in WSNs”, Indonesian Journal of Electrical Engineering and Computer Science, Vol. 16, No. 1, October 2019, pp. 441~455