ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1262

Design of Dynamic Routing Mechanisms in Wireless Local Area Networks Using Cisco Packet Tracer Tool

Momodu Kabiru Sanu[1]; Biralatei Fawei[1]; Diripigi Briyai Okolai[1]

[1]Department of Computer Science, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria

Publication Date: 2026/01/08

Abstract: The study examines the impact of different routing protocols on WLAN performance. This research is motivated by the increasing reliance on WLANs in both personal and professional domains, highlighting the need to optimize data transmission efficiency for various network demands. The study focuses on three well-known routing protocols: Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Destination-Sequenced Distance-Vector (DSDV). Each protocol was selected for its distinct characteristics in handling network changes, making them relevant for comparison in dynamic WLAN environments. Using Cisco Packet Tracer network simulation software, the study modeled each protocol within a WLAN framework, evaluating key performance metrics such as hop count, throughput, end-to-end delay, network congestion, packet delivery ratio, delay (latency) and packet loss rate. This approach enabled the simulation of real-time data transmission scenarios, providing insights into each protocol's responsiveness and adaptability. Results indicate that AODV and DSR are well-suited for dynamic high-mobility WLANs, showing strong adaptability and efficient path-finding capabilities under changing conditions. In contrast, DSDV a table-driven protocol, demonstrated stable performance in static environments but showed limitations in adaptability within rapidly changing network conditions. Overall, AODV demonstrated the best balance of stability and adaptability, making it a favorable choice for WLANs that require flexibility. This study contributes valuable insight into protocol selection for WLANs, underscoring the importance of aligning protocol capabilities with specific network demands. Based on these findings, we recommend adopting AODV for WLANs in need of flexibility and adaptability, while DSDV may be more suitable for static, low-mobility environments.

How to Cite: Momodu Kabiru Sanu; Biralatei Fawei; Diripigi Briyai Okolai (2025) Design of Dynamic Routing Mechanisms in Wireless Local Area Networks Using Cisco Packet Tracer Tool. *International Journal of Innovative Science and Research Technology*, 10(12), 2731-2740. https://doi.org/10.38124/ijisrt/25dec1262

I. INTRODUCTION

➤ *Background to the Study*

Wireless local area networks (WLANs) currently plays a vital role in present day communication infrastructure. WLANs provide wireless access to devices within a particular geographical location, thereby making them suitable for use in residential, office, or public places. However, it is challenging to design WLAN that is capable of transmitting data efficiently in a complex and dynamic environment. Moreover, the design of a WLAN require selecting a relevant and applicable routing protocol and metric that enables network performance optimization. This is important in that the transmission of data from one device to another within a network is established by a routing protocol. There are different routing protocols, such as Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Destination-Sequenced Distance-Vector (DSDV), have been designed to tackle the diverse challenges encountered in WLAN design. Nevertheless, determining the most suitable routing protocol for a specific scenario is problematic due to the dynamic nature of WLANs. On the other hand network metrics, are used to evaluate the performance of routing protocols and the most commonly used metrics in WLANs include hop count, throughput, end-to-end delay, network congestion, packet delivery ratio, delay (latency) and packet loss rate. This research presents the design and implement a routing mechanism in computer network (wireless local area network) to achieve scalability, packet passing continuity and significant bandwidth processing capability. The essence is that clearly understanding the behavior the dynamics of routing in WLAN design will help to contribute to network designers in designing an efficient and reliable routing protocols. This can better enhance network performance n terms of data transfer speed, reduced latency, and improved network reliability. Network designers can determine suitable paths for transmitting data in order to reduce network congestion and maximize the use of network resources. The capability to swiftly identify and resolve routing challenges can help to minimize network downtime, which will otherwise lead to significant operational disruption and financial consequences in businesses and organizations. The behavior of routing in WLAN design can influence network security. Relatedly, having an understanding of the threats and weaknesses in routing protocols enables network designers to create networks that are more resilient to cyber-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1262

attack and security breaches. The study will be centered on investigating the routing behavior in wireless local area network (WLAN) design techniques and to evaluate the performance impact of different routing protocols and metrics in optimizing network efficiency.

➢ *Statement of the Problem*

In wireless local area networks (WLANs), the effectiveness of data transmission and overall network performance depend heavily on the routing protocol's ability to adapt to dynamic conditions. However, existing routing protocols often struggle with scalability issues, resulting in reduced efficiency as the network grows and accommodates more devices. Furthermore, common challenges such as routing loops, slow convergence time, and network overhead degrade network performance and reliability, especially in high-mobility WLAN environments. Routing loops can cause packets to circulate indefinitely, consuming valuable bandwidth and leading to data loss, while slow convergence times hinder the network's ability to quickly adapt to changes, resulting in delayed or dropped transmissions. Additionally, network overhead generated by frequent route updates burdens WLAN resources, further impacting performance. This project intend to address these limitations by designing and simulating a robust, dynamic routing mechanism that enhances scalability, minimize routing loops, reduce convergence time, and lowers network overhead, thereby optimizing WLAN performance in diverse and demanding environments.

II. LITERATURE REVIEW

Routing dynamics describe the techniques and algorithms employed in identifying the most efficient and optimal paths for reliable data packets transmission through a network from source to destination node. The essence of routing behavior determination is to maximize the efficiency, reliability, and speed of data transmission in a network (Alizadeh *et al.*, 2012). Several routing algorithm such as distance vector, link-state, and path vector are common implementation in computer networks. They highly depend on metrics like hop count, delay, bandwidth, and cost to find the most suitable and applicable route for data transmission. Alqahtani and Zhang (2020) highlights that distance vector routing is a simple and straightforward algorithm that functions through the exchange of routing data between neighboring nodes to determine the shortest path to a destination. This algorithm is prone to routing loops and slow convergence, which can lead to network congestion and packet loss. Arora and Gupta (2019) explain, that link-state routing uses a more complex algorithm that involves each node in the network broadcasting its link state information to all other nodes.

This information is used to build a complete topology map of the network, which is then used to calculate the shortest path to a destination. Link-state routing is more reliable and faster than distance vector routing, but it requires more memory and processing power (Bhargavi.*et al*., 2021; Wang et al., 2018; Hoque et al., 2013). Path vector routing is an extension of distance vector routing is utilized in expansive networks like the internet. Instead of simple hop counts, this method employs a path vector to determine the most efficient path to transmit data *Path vector routing is an extension of distance vector routing that is used in large-scale networks, such as the internet. This algorithm uses a path vector instead of a simple hop count to determine the best path for data transmission* (Alam et al., 2019). While path vector routing provides enhanced scalability and reliability compared to distance vector routing, though it is more complex and challenging yet demands high computational resources. Also, computer networks utilizes different routing protocols like Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP) to exchange routing information between nodes and maintain up to date routing tables in real time (Bhushan & Kumar, 2010; Benslimane et al., 2011; Pradittasnee et al., 2016). BGP serves as the main routing protocol on the internet which manages the exchange of routing information between varying autonomous systems (AS). OSPF on the other hand is used in enterprise networks for optimizing routing challenges with a single domain, while RIP is an older protocol that is largely outdated but remains maintained in certain legacy systems.

Comer (2012) emphasized that routing dynamics are essential for establishing efficient and reliable data transmission in computer networks. The choice of routing algorithm and protocol is determined based on the network specific requirements and available resources. By assessing the advantages and limitations of different routing techniques, network engineers can design and optimize networks to satisfy user requirements. Over the years several researchers have investigated routing behaviors in diverse networking settings (Feamster, 2014; Zhao et al., 2017; Liu et al., 2024; Selim et al., 2025; Hashim et al., 2024**)**. The study highlights key important research findings in this area. In a separate study on routing dynamics over the internet analyzed the behavior of routing using data collected from a large-scale experimental platform (Comer, 2012). The study analyzed what leads to routing instability, its effect, and the relationship between changes in routing and overall network performance. Comer (2012) routing dynamics in the presence of congestion examines the impact of network congestion on routing behaviors analyzing the interaction between routing protocols and congestion control techniques. The study examined how congestion can lead to routing instability and network oscillations thereby offering a comprehensive assessment of routing dynamics in packet switching networks. The authors explore the response of routing protocols to varying network vents and identified factors contributing to instability and oscillations. In addition, the research considered the behavior of routing protocols in large-scale networks comprising multiple Autonomous Systems (ASes), evaluating how protocol interactions and routing instability affects the overall network performance. (Comer, 2012). Feamster (2014) presents an overview of routing dynamics in wireless mesh networks discussing the distinctive features responsible in influencing routing dynamics, and in reviewing the different routing protocols proposed for these networks.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1262

III. APPROACH

Dynamic routing is a technique for exchanging routing information between routers to select the optimal path within network devices. To understand the movement of data packets in a network and the associated performance with respect to time. We set up the experiment by configuring different network topologies to understand the behavior and the performance of the data packets from one network device to the other. The network configurations used for the experimentation are a single star topology and a combination of two topologies. The idea is to illustrate and find out the relationship between performances with respect to time (t) alongside network communication events. We adopted ChatGPT and anaconda to generate the time and network communication event relationship in our time lag and network topology graph. The research adopt the CISCO Packet Tracer to carryout hop count activities while data packets travel from source to destination device and a receipt of acknowledgement back to the source device in a communication network. The hop counts are carried out in micro-seconds (us). This technique is useful in capturing and tracking communication progress from the start node through the different devices connected in the network, such as laptops, switches, hubs, and so on. For clarity and avoidance of result bias network communication over a couple of network topology combinations were carried out to sustain fairness in this research. The integration selected for this research are a single star topology, a combination of bus and ring, bus and star, and star and tree network topologies. Also. For unique identification, network interface location, network segmentation and organization, we applied the Internet Protocol Addressing (IP) system to ensure that data sent over the network enroutes to the destination in the correct order and device. IP address is a unique numerical identifier assigned to each device connected to a network, enabling data to be routed between them. The IPv4 was used in this research with class C IP addressing because Class C can easily be sub-netted to create multiple smaller networks. Class C networks are well-suited for small and medium-sized networks and offers a more efficient use of the IP address space. Given a Network ID 209.44.33.0/24 with a default subnet mask 255.255.255.0. The default number of host bits will be 8 bits (i.e. IP address = 209.44.33.0/24). For example, if the default subnet mask is equal to 255.255.255.0. Then one number of bit to borrow will be equal to 3. However, applying the 2^n principle in subnetting (where n is the number of host bits to borrow) we have the borrowed one bit to be n = 3. Therefore, we have $2^3 = 8$. But given that two number of host per subnet will be equal to 30. This means number of host bits available minus n will be equal to h1, where n represent the subnet bits and h1 the host bits. By this we have 8 - 3 = 5. This means h will be equal to 5. Also, $2^h – 2$ = (number of hosts per subnet) $2^5 = 32 -2 = 30$. This establishes an updated subnet mask and prefix for a default Class network. The default subnet mask = 255. 255. 255. 0. Corresponds to a Class c prefix = /24. The new subnet mask = 255.255.255.224 with a = /27 prefix. The value 224 in the last octet results from borrowing of 3 bits from the host bit i.e. 11100000 which was converted to decimal as follow;

$1^7\ 1^6\ 1^5\ 0^4\ 0^3\ 0^2\ 0^1\ 0^0$

$1x\ 2^7 + 1x2^6 + 1x2^5 + 0x2^4 + 0x2^3 + 0x2^2 + 0x2^1 + 0x2^0$

$2^7 + 2^6 + 2^5 + 0 + 0 + 0 + 0 + 0$. $128 + 64 + 32 + 0 + 0 + 0 + 0 + 0 = 224$

The value for the new prefix resulted from adding the 3 bits borrowed from the host portion to the original 24 bits of the default Class C subnet mask, which yielded the new prefix/27.

The technology used for developing the dynamics routing in the WLANs include Cisco Packet Tracer, Ad hoc routing, Mesh routing and Hybrid routing. Cisco Packet Tracer is a network simulation tool created by Cisco Systems. It enables users to design network topologies and mimic modern computer networks. The tool provides users the capability to simulate the configuration of Cisco routers and switches using a simulated command line interface. Ad hoc routing is used in networks where there is no central infrastructure. Nodes in the network communicate directly with each other, and routes are dynamically established and updated as nodes move around, mesh routing is similar to ad hoc routing, but it uses a more structured network topology. Nodes are organized into a mesh, and routes are established between nodes in the mesh while hybrid routing combines ad hoc routing and mesh routing nodes in the network to communicate directly with each other, or they can use a central infrastructure to establish routes.

IV. RESULTS AND DISCUSSION

To understand the movement of data packets in a network and the associated performance with respect to time, we implemented star topology and a combination of two topologies together. The essence of implementing the star topology is its widespread use and configuration efficiency as well as its robust network performance.

- *Communication in Single Star Topology*

Here, we first carried out an experiment with a configured star topology (see Figure 1 for Star Topology and experimental result in table 1). The essence is that star network topology is a type of network configuration in which each device on the network is connected to a central hub or switch. This central node acts as a conduit to transmit data between the various devices (nodes) in the network. Star network topology is a widely used and efficient network configuration that offers ease of management and robust performance. Its main drawback is the reliance on a central hub, of which if it fails, it can bring down the entire network. However, for many applications, especially those requiring centralized control and easy troubleshooting, the star topology remains a popular choice.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1262

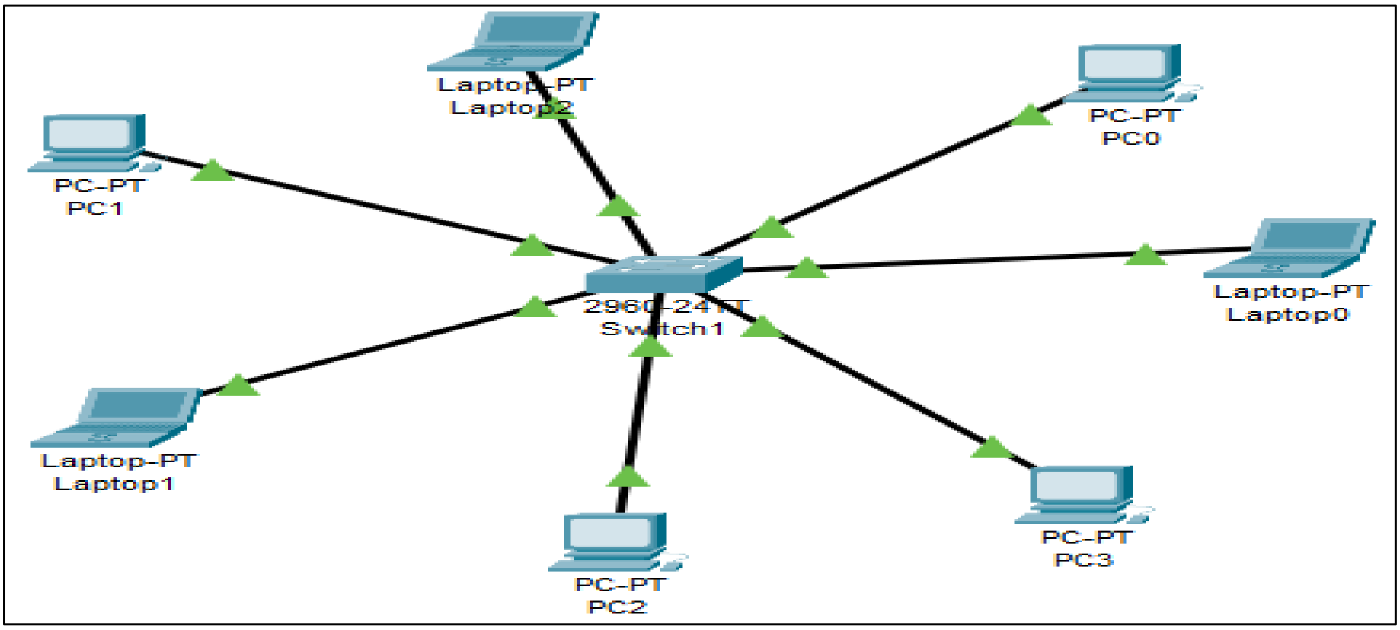

Fig 1 Wired Star Topology

In Table 1, at 0.000 seconds, the process begins from an unspecified source and reaches Laptop2 using internet control message protocol (ICMP). At 0.001 seconds, the signal moves from Laptop2 to Switch 1 via ICMP. At 0.002 seconds, the signal travels from Switch 1 to PC2 through ICMP. At 0.003 seconds, the signal returns from PC2 to Switch 1 using ICMP. At 0.004 seconds, the signal goes from Switch 1 back to Laptop2 through ICMP. At 0.029 seconds, no specific device is mentioned.

Table 1 Results from Communication Event Between Devices

Time(sec)	Last Device	At Device	Type
0.000	_	Laptop2	ICMP
0.001	Laptop2	Switch 1	ICMP
0.002	Switch1	PC2	ICMP
0.003	PC2	Switch 1	ICMP
0.004	Switch 1	Laptop2	ICMP
0.029			

The graph of network communication over time illustrates the time taken for network communication events. It tracks the progression of communication from the start point through the various stages involving laptops and switches, up to the final event. The time is measured in seconds (See Figure 2; Network Communication graph).

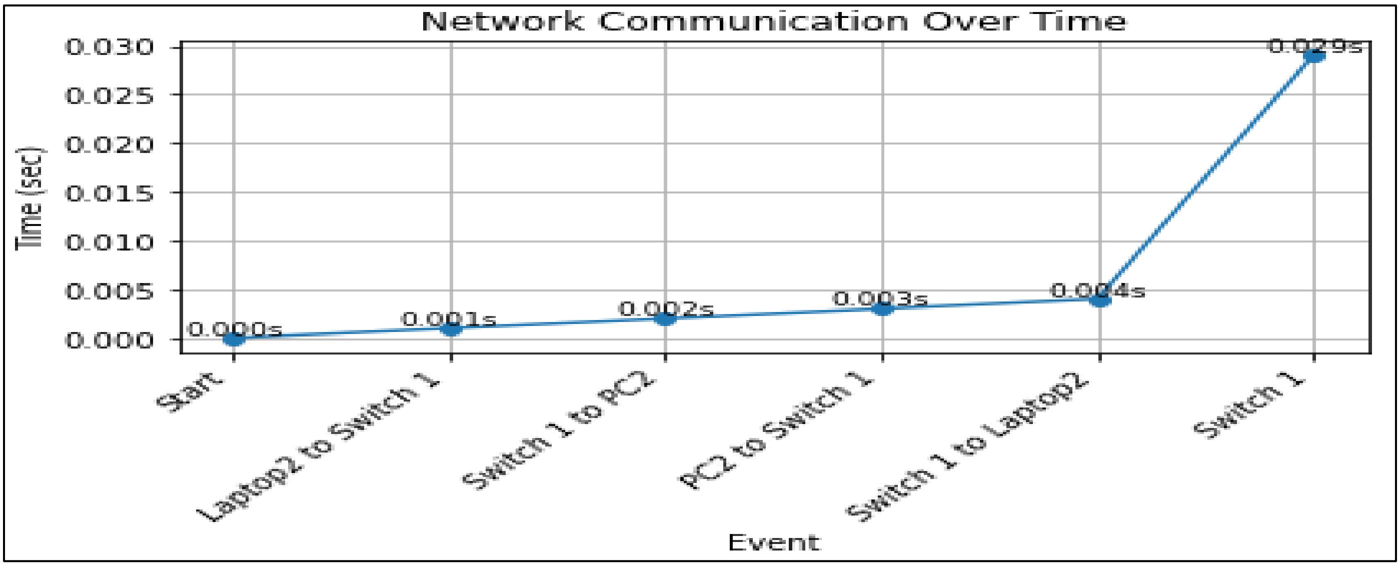

Fig 2 Graph of Network Communication Over Time

Volume 10, Issue 12, December – 2025 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1262

➢ *Combination of Bus and Ring Network Topology*

The integration of bus and ring network topologies alongside with the associated time lag in transmitting data packets from source to destination device. It is referred to as hybrid network topology. It combines characteristic features from both the bus and ring network topologies to design a uniquely tailored network structure. The integration in hybrid network created a balance between scalability, redundancy, fault tolerance, and performance. This makes it flexible and adaptable for different applications where these characteristic features are essential. Combining bus and ring network topologies can suit different enterprise settings with specific network demands. Choosing the appropriate network topology should consider the requirements of the organization budget, reliability and scalability (see figure 3 for the combination of bus and ring network topology)

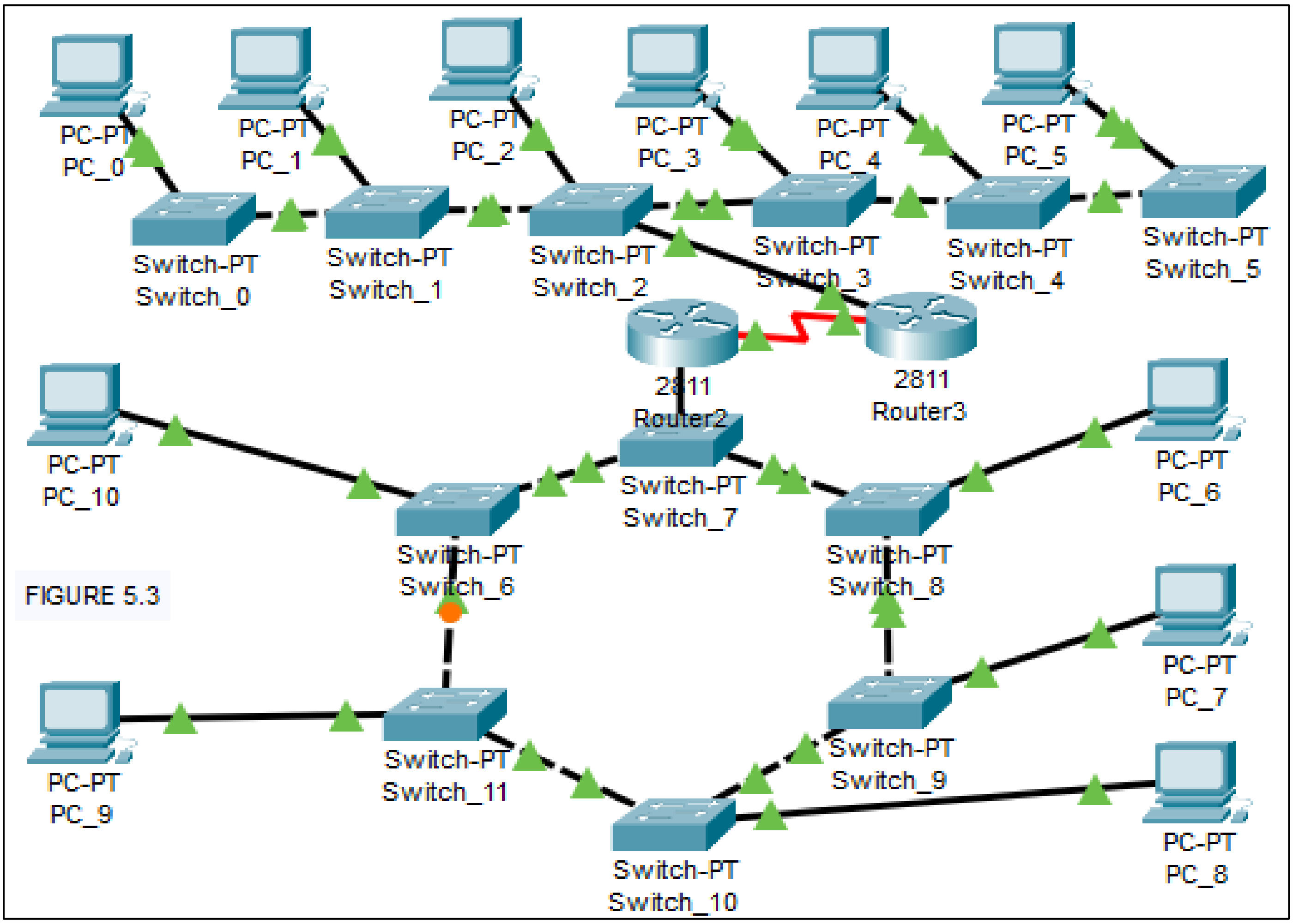

Fig 3 Combination of Bus and Ring Network Topology

The communication sequence between devices in the network, detailing the times, devices involved, and communication types. At 0.000 seconds, PC 6 initiates an ICMP communication. At 0.001 seconds, the ICMP packet moves from PC 6 to Switch 0. at 0.002 seconds, the packet is forwarded from Switch 0 to Switch 1. At 0.003 seconds, the packet travels from Switch 1 to Switch 2 and so on, lastly, at 0.269 seconds, a Spanning Tree Protocol (STP) event occurs at Switch 16. (See result of the device in table 2)

Table 2 Results from Communication Event Between Devices

Time (sec)	**Last Device**	**At Device**	**Type**
0.000	_	PC 6	ICMP
0.001	PC 6	Switch 0	ICMP
0.002	Switch 0	Switch 1	ICMP
0.003	Switch 1	Switch 2	ICMP
0.004	Switch 2	Router 2	ICMP
0.005	Router 2	Router 1	ICMP
0.006	Router 1	Switch 12	ICMP
0.007	Switch 12	Switch 10	ICMP
0.008	Switch 10	Switch 11	ICMP

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1262

0.009	Switch 11	PC 12	ICMP
0.010	PC 12	Switch 11	ICMP
0.011	Switch 11	Switch 10	ICMP
0.012	Switch 10	Switch 12	ICMP
0.013	Switch 12	Router 1	ICMP
0.014	Router 1	Router 2	ICMP
0.015	Router 2	Switch 2	ICMP
0.016	Switch 2	Switch 1	ICMP
0.017	Switch 1	Switch 0	ICMP
0.018	Switch 0	PC 6	ICMP
0.019	Switch 2	Switch 1	ICMP
0.020	Switch 1	Switch 1	ICMP
0.021	Router 1	PC 6	ICMP
0.022	Router 2	Switch 1	ICMP
0.269	_	Switch 16	**STP**

The graph in Figure 4 illustrates the relationship between network topology and time lag. The x-axis represents different points in the network topology, while the y-axis indicates the time lag in seconds.

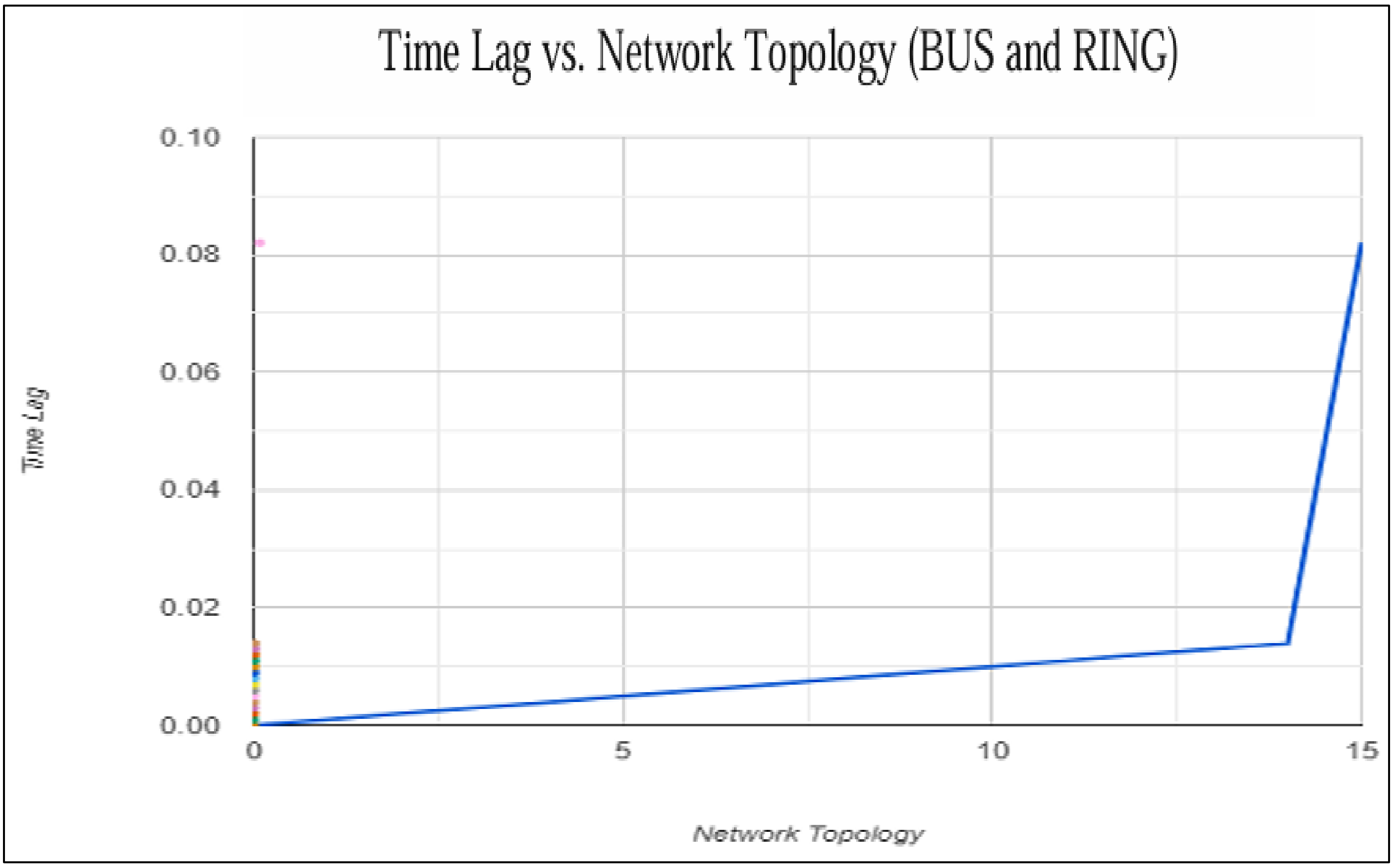

Fig 4 Time Lags vs Network Topology (Bus and Ring)

➢ *Combination of Bus and Star Network Topology*

The integration of bus and star network topologies and their time lag in routing of packet from source device to destination device (See Figure 5 Bus and Star network topologies combination). Their integration forms a hybrid network that combines the characteristic attributes and functionalities of both network topologies. The precise design and setup of an integrated bus-star network can vary based on the intended application and the network device to be used. The hybrid approach usually utilized in large enterprise networks to connect multiple smaller local area networks. The bus topology stands as the main backbone connecting the local area networks while the star topology guarantees and facilitates efficient connectivity with each local area network.

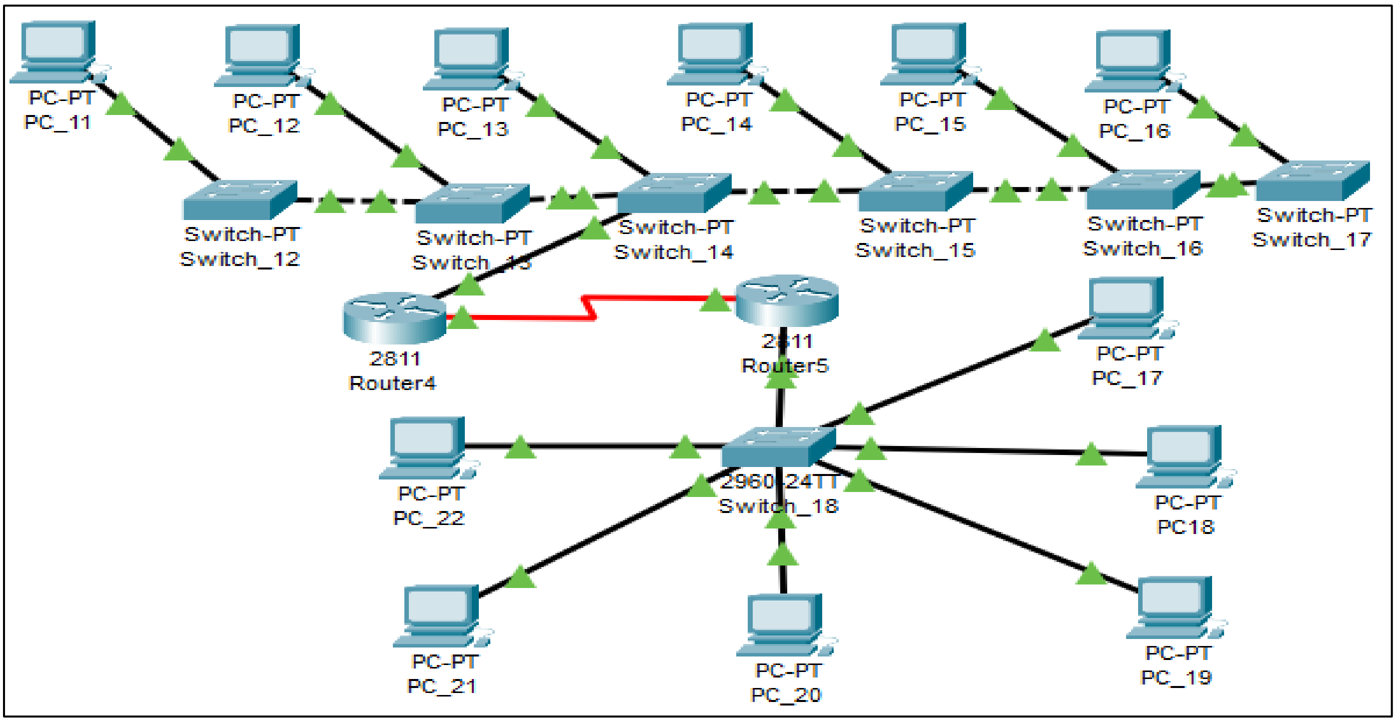

Fig 5 Combination of Bus and Star Network Topologies

The communication scenario where devices exchange ICMP (Internet Control Message Protocol) packets and a Spanning Tree Protocol (STP) message (Table 3 Device Communication). At time 0.000 seconds, the communication starts with an unspecified device attempting to reach a destination, indicated by "_", but the specific target is not mentioned. At 0.001 seconds, PC 6 sends an ICMP packet to Switch 0, indicating a network request from PC 6 to communicate with another device. At 0.002 seconds, Switch 0 forwards the ICMP packet to Switch 1, suggesting that Switch 0 is acting as an intermediary or forwarding device in the network. At 0.003 seconds, Switch 1 forwards the ICMP packet to Switch 2, continuing the path towards the destination, and so on indicating a change in the network path towards the destination, possibly indicating a routing decision. At 0.005 seconds, Router 2 forwards the ICMP packet to Router 0, suggesting that the packet is now moving towards another network or subnet. At 0.006 seconds, Router 0 forwards the ICMP packet to Switch 16, possibly indicating a change in network direction or path towards the final destination. At 0.007 seconds.

Table 3 Results from Communication Event Between Devices

Time(sec)	**Last Device**	**At Device**	**Type**
0.000	_	PC 6	ICMP
0.001	PC 6	Switch 0	ICMP
0.002	Switch 0	Switch 1	ICMP
0.003	Switch 1	Switch 2	ICMP
0.004	Switch 2	Router 2	ICMP
0.005	Router 2	Router 0	ICMP
0.006	Router 0	Switch 16	ICMP
0.007	Switch 16	PC 3	ICMP
0.008	PC 3	Switch 16	ICMP
0.009	Switch 16	Router 0	ICMP
0.010	Router 0	Router 2	ICMP
0.011	Router 2	Switch 2	ICMP
0.012	Switch 2	Switch 1	ICMP
0.013	Switch 1	Switch 0	ICMP
0.014	Switch 0	PC 6	ICMP
0.082	_	Switch 16	**STP**

Additionally, at 0.082 seconds, an unspecified device sends an STP message to Switch 16, indicating a network maintenance or management activity related to the Spanning Tree Protocol. The Time Lag vs. Network Topology (BUS and STAR) graph in Figure 6 depicts the relationship between network topology and time lag. The x-axis represents different points in the network topology, while the y-axis indicates the time lag in seconds.

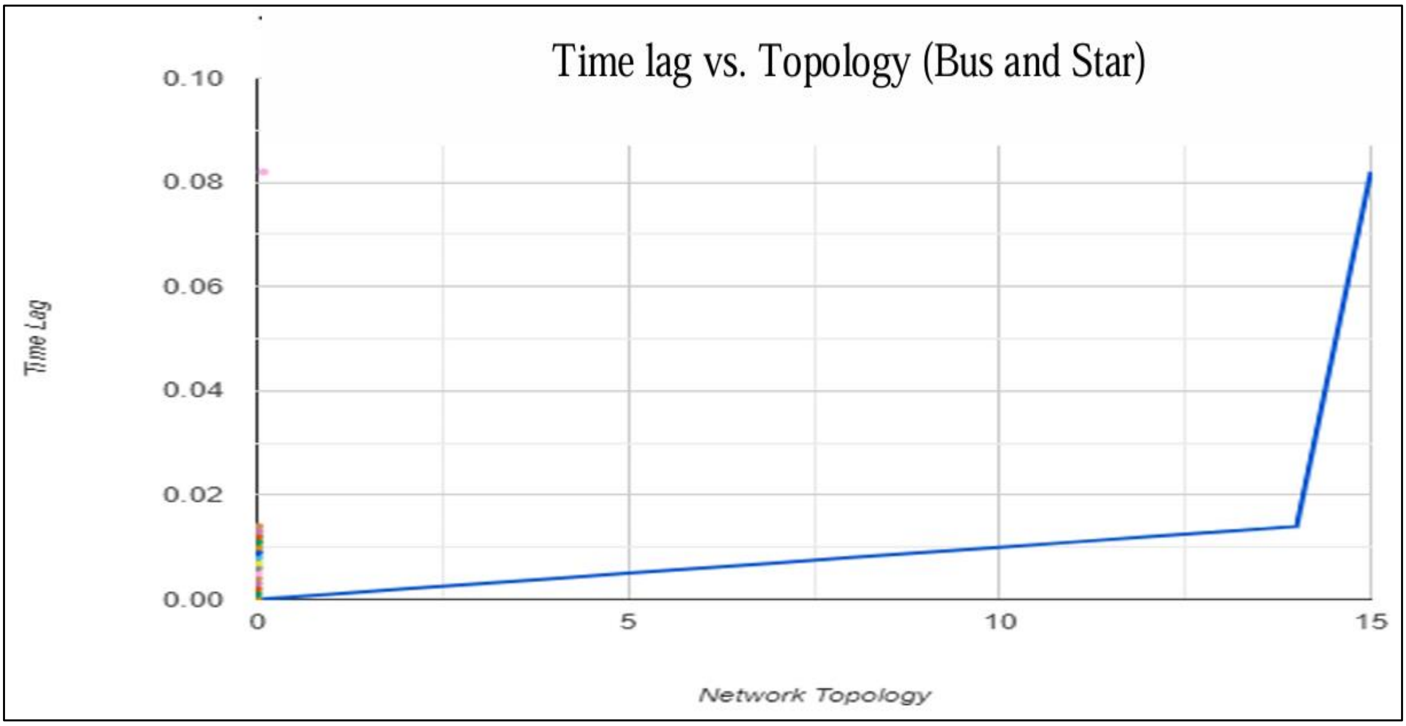

Fig 6 Time Lag vs. Network Topology (BUS and STAR)

➢ *Combination of Star and Tree Network Topology*

The hybridization of Star and Tree network topologies and the resulting time lag in routing a packet from source to destination device (See Figure 7 Combination of Star and Tree Network Topologies). This approach is commonly known as a hybrid network topology. It combines the features and functionalities of both star and tree topologies. This flexibility provides a scalable solution for various network sizes. The utilization of the hybrid topology is operationally effective for small to medium-sized in which scalability and flexibility required such as office environments or small campuses. These networks require a centralized structure with the ability to expand and accommodate additional nodes. Such environments require strong fault tolerance and effective data transmission especially in critical operations or high demanded applications.

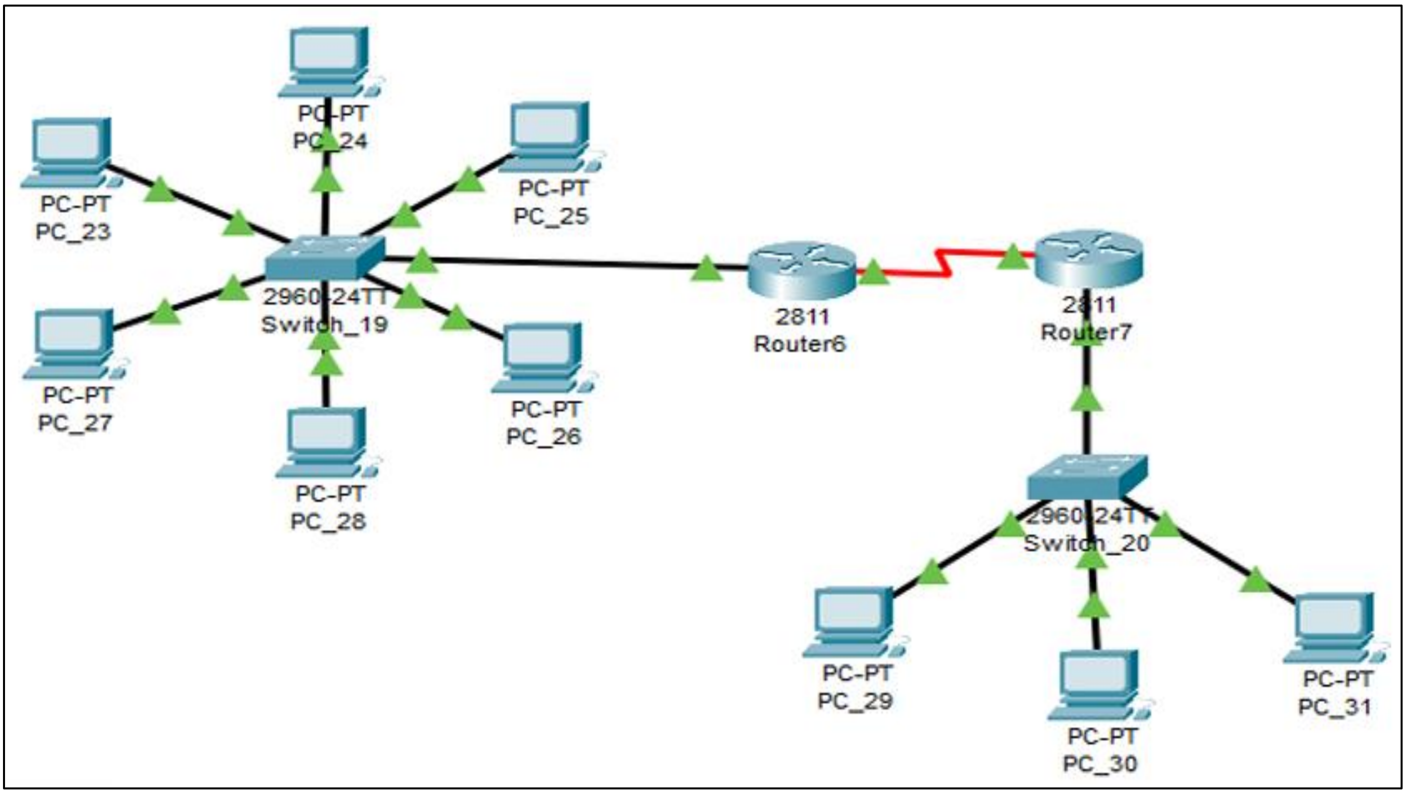

Fig 7 Combination of Star and Tree Network Topologies

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1262

The communication sequence between various network devices primarily involves an ICMP (Internet Control Message Protocol) exchange and an STP (Spanning Tree Protocol) message. Below is a comprehensive statement detailing the communication process (see table 5.4): At time 0.000 seconds, the ICMP message originates from PC1 Transmission Path: At 0.001 seconds, the ICMP message travels from PC 1 to Switch 16, and so on at 0.049 seconds, an STP (Spanning Tree Protocol) message is recorded, originating from an unspecified source and received by Switch 7. STP messages are used for managing and preventing loops in Ethernet networks by creating a loop-free logical topology.

Table 4 Communication Event Between Devices

Time (sec)	Last Device	At Device	Type
0.000	_	PC 1	ICMP
0.001	PC 1	Switch 16	ICMP
0.002	Switch 16	Router 0	ICMP
0.003	Router 0	Router 1	ICMP
0.004	Router 1	Switch 14	ICMP
0.005	Switch 14	PC 18	ICMP
0.006	PC 18	Switch 14	ICMP
0.007	Switch 14	Router 1	ICMP
0.008	Router 1	Router 0	ICMP
0.009	Router 0	Switch 16	ICMP
0.010	Switch 16	PC 1	ICMP
0.049	_	Switch 7	**STP**

The graph titled "Time Lag vs. Network Topology (STAR and TREE)" illustrates the relationship between network topology and the corresponding time lag in figure 8. The x-axis represents the network topology, with numerical values indicating different configurations or levels of complexity within the STAR and TREE topologies. The y-axis represents the time lag, measured in seconds, which indicates the delay in data transmission across the network.

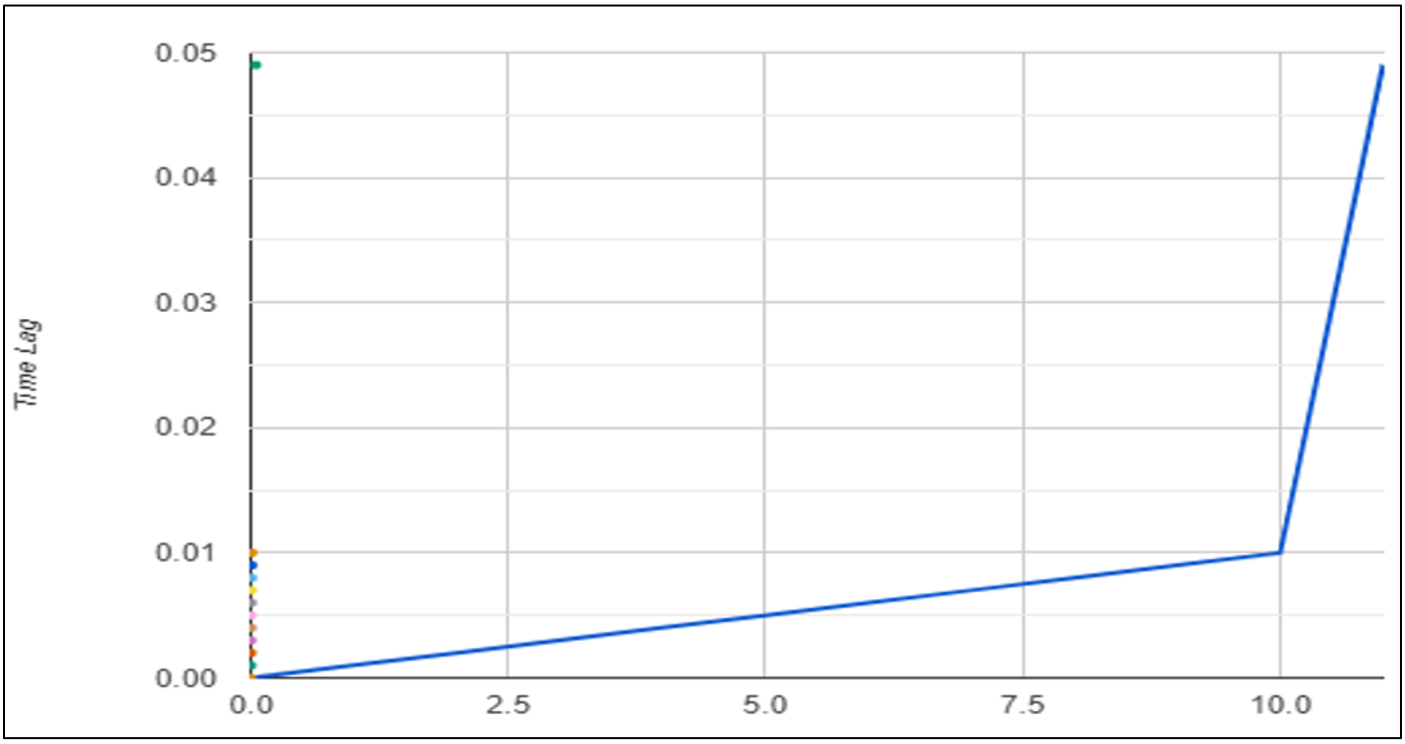

Fig 8 Illustrates the Relationship Between Network Topology

The research findings show that the single topology such as a star topology, provides faster data packet transmission rate compared to hybridized topologies. In star topology, the movement of data packets from source to destination device was observed to be using minimized latency thereby enhancing speed. On the other hand the hybrid topologies which are a combination two basic topologies (e.g., star and ring) introduces a variable time lag. This means they are slightly slower compared to the star topology. While the star portion of a hybrid topology benefits from direct switch connections, the ring portion can introduce delays due to the nature of ring-based data travel.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1262

V. CONCLUSION

The research investigates routing behavior in wireless local area network (WLAN) design techniques and found them to be critical factors influencing WLAN performance reliability and efficiency. The study explore and analyzed various routing protocols and techniques in WLANs, their characteristic impact on network dynamics and proposes guidelines for optimal WLAN creation and implementation. The research employed the Cisco packet tracer simulation tool and implemented a real world case scenario to evaluate the performance of the various routing techniques. Packet delivery ratio, end=to-end delay and throughput were used to evaluate the effectiveness and efficiency of the various mechanism under different conditions. With respect to the findings from the experiment, it was observed that the routing protocol selection in WLAN design greatly influenced network dynamics. For instance, reactive routing protocols such as AODV and DSR showed strong performance in mobile ad hoc networks with frequently changing topologies whereas proactive protocols like DLSR performed better in relatively stable network environments. Hybrid protocols comprises BATMAN balanced reactive and proactive approaches, making them effective in networks with moderate mobility.

REFERENCES

[1]. Alizadeh, M., & Mozaffari-Kermani, M. (2012). A survey of QoS routing protocols in wireless sensor networks. *Journal of Network and Computer Applications*, *35*(2), 625–651

[2]. Alqahtani, S., & Zhang, Y. (2020). Wireless Local Area Network (WLAN): A review of the history, standards, and evolution. *Journal of King Saud University-Computer and Information Sciences*, *32*(3), 224–237.

[3]. Bhargavi, G., Kumar, S., Prasad, N. V., & Reddy, K. K. (2021). Application of Routing Dynamics to Wireless Local Area Network Design Mechanism. *Journal of Network and Systems Management*, *29*(1), 108–126.

[4]. Bhushan, N., & Kumar, S. (2010). A survey on network simulators for wireless networks. *International Journal of Computer Applications*, *1*(6), 12–18.

[5]. Comer, D. (2012). Computer networks and internets. Pearson Education India.

[6]. Feamster, N. (2014). Software-defined networking. Morgan & Claypool Publishers.

[7]. Wang, L., Lehman, V., Hoque, A. M., Zhang, B., Yu, Y., & Zhang, L. (2018). A secure link state routing protocol for NDN. *IEEE Access*, *6*, 10470-10482.

[8]. Hoque, A. M., Amin, S. O., Alyyan, A., Zhang, B., Zhang, L., & Wang, L. (2013, August). NLSR: Named-data link state routing protocol. In *Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking* (pp. 15-20).

[9]. Alam, M. Z., Adhicandra, I., & Jamalipour, A. (2019). Optimal best path selection algorithm for cluster-based multi-hop MIMO cooperative transmission for vehicular communications. IEEE Transactions on Vehicular Technology, 68(9), 8314-8321.

[10]. Benslimane, A., Barghi, S., & Assi, C. (2011). An efficient routing protocol for connecting vehicular networks to the Internet. Pervasive and Mobile Computing, 7(1), 98-113.

[11]. Pradittasnee, L., Camtepe, S., & Tian, Y. C. (2016). Efficient route update and maintenance for reliable routing in large-scale sensor networks. IEEE Transactions on Industrial Informatics, 13(1), 144-156.

[12]. Zhao, X., Wan, C., Sun, H., Xie, D., & Gao, Z. (2017). Dynamic rerouting behavior and its impact on dynamic traffic patterns. IEEE Transactions on Intelligent Transportation Systems, 18(10), 2763-2779.

[13]. Liu, G., He, J., Luo, Z., Yao, X., & Fan, Q. (2024). Understanding route choice behaviors' impact on traffic throughput in a dynamic transportation network. Chaos, Solitons & Fractals, 181, 114605.

[14]. Selim, I. M., Abdelrehem, N. S., Alayed, W. M., Elbadawy, H. M., & Sadek, R. A. (2025). MANET Routing Protocols' Performance Assessment Under Dynamic Network Conditions. Applied Sciences, 15(6), 2891.

[15]. Hashim, S. A., Hamza, E. K., & Kamal, N. N. (2024). Analyzing Dynamic Source Routing Protocol Behavior in MANETs. Ingenierie des Systemes d'Information, 29(6), 2357.