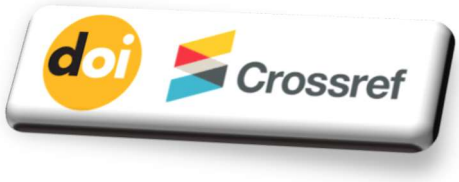
Journal, Advances in Mathematical & Computational Sciences
Vol. 11 No. 4, 2023 Series
www.isteams.net/mathematics-computationaljournal



Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA

Available online at https://www.isteams.net/ mathematics-computationaljournal.info
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

Survey of the Influence of Routing Protocols to Network Performance Enhancement

[1]Juliana I. Consul & [2]Bunakiye R. Japheth
[1]Department of Mathematics
[2]Department of Computer Science
Faculty of Science
Niger Delta University
Wilberforce Island, Nigeria.
E-mails: ji.consul@ndu.edu.ng; bunakiye.japheth@ndu.edu.ng

ABSTRACT

Routing protocols play a crucial role in the operation of computer networks by determining the optimal paths for data transmission. The selection of an appropriate routing protocol can significantly impact network performance, including factors such as latency, throughput, reliability, and scalability. This survey aims to provide a comprehensive analysis of the influence of various routing protocols on network performance enhancement. The survey begins by presenting an overview of common routing protocols with their key characteristics. Subsequently, it explores the impact of these protocols on network performance metrics, focusing on their ability to adapt to changing network conditions, mitigate congestion, and ensure efficient resource utilization. Through a systematic review of literature, empirical studies, and real-world implementations, this survey aims to provide network administrators, researchers, and practitioners with valuable insights into selecting and optimizing routing protocols for specific network environments. Additionally, it identifies areas for further research and development to continue advancing the field of routing protocols and network performance enhancement.

Keywords: Optimizing Routing Protocols, Performance Metrics, Reliability and Scalability, Resource Utilization, Wireless Local Area Networks, Accurate Routing Tables

Juliana I. Consul & Bunakiye R. Japheth (2023): Survey of the Influence of Routing Protocols to Network Performance Enhancement. Journal of Advances in Mathematical & Computational Science. Vol. 11, No. 4. Pp 13-28
Available online at www.isteams.net/mathematics-computationaljournal. dx.doi.org/10.22624/AIMS/MATHS/V11N4P2

1. INTRODUCTION

Wireless local area networks (WLANs) have become an integral part of modern communication systems. WLANs provide wireless connectivity to devices within a specified geographical area, making them ideal for use in homes, offices, and public places. However, designing WLANs that can efficiently transmit data in a dynamic and complex environment is challenging. The design of a WLAN system involves selecting appropriate routing protocols and metrics to optimize network performance. Routing protocols determine how data is transmitted from one device to another within the network. Different routing protocols, such as Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Destination-Sequenced Distance-Vector (DSDV), have been developed to address the various challenges in WLAN design. However, selecting the most suitable routing protocol for a given scenario is challenging due to the dynamic nature of WLANs.

Metrics, on the other hand, are used to evaluate the performance of routing protocols. The most commonly used metrics in WLANs include hop count, delay, and throughput. These metrics enable the evaluation of the effectiveness of different routing protocols in selecting the most appropriate path for data transmission. Research in this area has shown that the choice of routing protocol and metric has a significant impact on the performance of WLANs. Therefore, there is a need to investigate the dynamics of routing in WLAN design mechanisms and identify the most suitable routing protocols and metrics for different scenarios. This study aims to build on this research by investigating the dynamics of routing in WLAN design mechanisms and evaluating the effectiveness of different routing protocols and metrics in optimizing network performance. The findings of this study will provide insights into the selection of appropriate routing protocols and metrics for designing efficient and robust WLAN systems. Wireless networks are inherently dynamic, as nodes can move around and the signal strength between nodes can vary.

This makes it difficult to maintain accurate routing tables, which can lead to routing problems such as packet loss and increased latency. Limited bandwidth: Wireless networks typically have limited bandwidth, which can also lead to routing problems. If too much traffic is trying to use the same route, it can cause congestion and packet loss. Wireless networks are more vulnerable to security attacks than wired networks. This is because wireless signals can be easily intercepted by unauthorized parties. Routing problems can be exploited by attackers to disrupt network traffic or gain unauthorized access to the network.

Understanding the dynamics of routing in WLAN design can help network designers develop more efficient and effective routing protocols. This can result in improved network performance, such as faster data transfer rates, reduced latency, and improved network reliability. Network designers can determine the optimal routes for data transmission, which can help reduce network congestion and optimize network resource utilization. The ability to quickly identify and respond to routing issues can help reduce network downtime, which can have significant financial and operational consequences for businesses and organizations. The dynamics of routing in WLAN design can also impact network security. By understanding the potential vulnerabilities and threats associated with different routing protocols, network designers can develop more secure networks that are less susceptible to cyber-attacks and other security breaches.

2. ROUTING DYNAMICS

Routing dynamics refer to the processes and algorithms used to determine the optimal path for data packets to traverse through a network from a source node to a destination node. The goal of routing dynamics is to maximize the efficiency, reliability, and speed of data transmission in a network (Reddy et al., 2021). There are several routing algorithms used in computer networks, such as distance vector routing, link-state routing, and path vector routing. These algorithms are based on different metrics, such as hop count, delay, bandwidth, and cost, to determine the best path for data transmission. Kurose and Ross (2012) Distance vector routing is a simple algorithm that works by exchanging routing information 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.

2.1 Complex Algorithm Utilization

Garcia-Luna (2015) Link-state routing, on the other hand, 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 (Peterson & Davie, 2012). 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.

Path vector routing is more scalable and robust than distance vector routing, but it is also more complex and requires more computational resources. In addition to these routing algorithms, there are also several routing protocols used in computer networks, such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP). These protocols are used to exchange routing information between nodes and to ensure that routing tables are updated in real-time (Peterson & Davie, 2012). BGP is the primary routing protocol used in the internet and is responsible for exchanging routing information between different autonomous systems (AS). OSPF is used in enterprise networks and is designed to optimize intra-domain routing. RIP is an older routing protocol that is no longer widely used, but it is still supported by some legacy systems.

2.2 Reliable Transmission of Data

Kurose et al. (2021) Routing dynamics play a critical role in the efficient and reliable transmission of data in computer networks. The choice of routing algorithm and protocol depends on the specific requirements of the network and the available resources. By understanding the strengths and weaknesses of different routing algorithms and protocols, network engineers can design and optimize networks to meet the needs of their users. (Tanenbaum et al., 2011). Zhang (2010) over the years, numerous research studies have been conducted to investigate the behavior of routing dynamics in various network environments. In this response, an overview of some of the key research works in this area was provided. A Study of Routing Dynamics in the Internet" Ratul Mahajan et al. (2002) presents an analysis of the dynamics of routing in the Internet using measurements from a large-scale experimental platform. The authors investigate the causes and effects of routing instability, as well as the relationship between routing changes and network performance.

Routing Dynamics in the Presence of Congestion" Lixin Gao et al., (2000), focused on the effects of network congestion on routing dynamics. The authors analyze the interactions between routing protocols and congestion control mechanisms, and examine how congestion can cause routing instability and network oscillations. Providing a comprehensive analysis of the dynamics of routing in packet-switched networks. The authors study the behavior of routing protocols in response to various network events, and investigate the factors that contribute to routing instability and oscillations (Jennifer Rexford et al., 1996). Christophe Diot et al. (1997) examines the behavior of routing protocols in large-scale networks consisting of multiple Autonomous Systems (ASes). The authors investigate the effects of routing protocol interactions and the impact of routing instability on network performance. R. M. Chandrasekaran et al. (2015); provides an overview of the research on routing dynamics in wireless mesh networks. The authors discuss the unique characteristics of these networks that affect routing dynamics, and review the various routing protocols that have been proposed for these networks.

3. PERFORMANCE EVALUATION ON ROUTING DYNAMICS

The performance evaluation of routing algorithms is typically evaluated based on several metrics such as throughput, latency, and packet loss. One of the most common methods for evaluating the performance of routing algorithms is through simulation using tools such as Network Simulator (NS) or OPNET. Several studies have been conducted to evaluate the performance of different routing algorithms. For example, a study by Wu et al. (2014), compared the performance of OSPF and RIP in a wireless mesh network. The results showed that OSPF had lower latency, higher throughput, and lower packet loss compared to RIP. Another study by Jeong et al. (2015) evaluated the performance of several routing algorithms in a software-defined network (SDN). The results showed that the OSPF and Border Gateway Protocol (BGP) algorithms had the highest throughput and lowest latency. The methodology adopted in this research is based on Mobile Ad hoc Networks (MANETs).

MANETs are infrastructure less networks which consist of wireless mobile devices. Mubashir Husain Rehmani (2010) Since these mobile devices can join and leave the network freely, the network topology can change very frequently. Ad-hoc network consists of mobile stand which are free to communicate without any infrastructure and central control unit. .This can operate in an isolated manner or with fixed networks through gateways. Mahesh Motwani et al.(2012). The Ad hoc Networks is an independent system of nodes, which has numerous significant characteristics, namely, dynamic topologies, limited physical security, bandwidth and energy constrained operations. Unlike from wired networks,

Due to the lack of infrastructure, devices in such networks need to cooperate with each other and work in a self-organized manner through wireless channels. Therefore, developing proper routing protocols for MANETs is a challenging task. Piysh Shukla et al.(2012). New routing protocols designed for MANETs are supposed to work in a self- organized manner and provide low packet delay, high packet delivery rate and effective adaptation (praveen Lalwani et al.,2012).

3.1 Adaptive Technology

Mahesh Motwani et al. (2012). The proposed technique, which is Ad hoc On-Demand Distance Vector (AODV) allows dynamic, self-starting, multi hoop routing between contributing mobile nodes craving to set up and sustain an ad hoc network. Mubashir Husani Rehmani (2010) AODV routing and is a type of reactive protocol. Its procedure is hop-to-hop routing. The node creates the Route Request (RREQ) if it requires understanding the route to a specific destination. Praveen Lalwani et al. (2012). AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. Mubashir Husani Rehmani (2010). AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner.

The operation of AODV is loop- free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network), the typical algorithm to this counts is depicted in figure 1. When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. Every node seeks to preserve an efficient sight of its instantaneous neighbors at any time, in order to detect link failures rapidly, before they can lead to packet losses. The existence of a neighbor node can be confirmed when a message is received, or after any other successful interception or exchange of signals.Piysh Shukla et al. (2012). The disappearance of a neighbour is implicit when such an event has not taken place for a certain amount of time or when a unicast transmission to this neighbour fails (Mubashir Husani Rehmani 2010). The routing messages do not contain information about the whole route path, but only about the source and the destination. Mahesh Motwani et al.(2012). Therefore, routing messages do not have an increasing size. It uses destination sequence numbers to specify how fresh a route is (in relation to another), which is used to grant loop freedom as shown in figure 3.2 (Mubashir Husani Rehmani 2010).

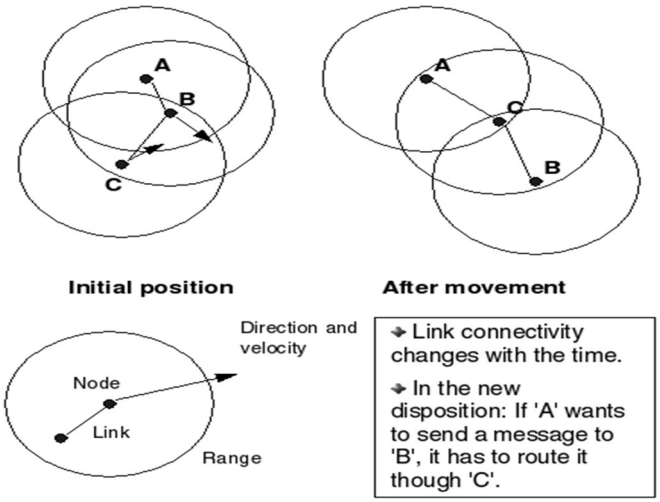


Figure 1 Mobility in Routing

Whenever a node needs to send a packet to a destination for which it has no 'fresh enough' route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in any RREQ that the node has received for that destination) it broadcasts a route request (RREQ) message to its neighbors. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ, unless it has a 'fresher' one (Praveen Lalwani et al.,2012)

3.2 Survey of Address Allocation and Assignment

IP addresses can be assigned to devices in different ways: Static Addressing: In static addressing, an IP address is manually configured and assigned to a device. Piysh Shukal et al. (2012) It remains fixed unless changed manually. Static addressing is commonly used for devices that require a permanent, unchanging address, such as servers or network infrastructure devices. Dynamic Addressing: Dynamic addressing involves the automatic assignment of IP addresses to devices using protocols like Dynamic Host Configuration Protocol (DHCP). DHCP servers dynamically allocate IP addresses to devices within a network, making it more efficient for managing and reusing addresses in dynamic network environments. Mubashir Husain Rehmani (2010).

Private and Public IP Addresses: IP addresses can be classified as private or public: Private IP Addresses: Private IP addresses are reserved for use within private networks and are not routable over the internet.Praveen Lalwani et al. (2012). They are primarily used for local addressing and allow multiple devices to share a single public IP address. Private IP address ranges include: IPv4: 10.0.0.0 to 10.255.255.255 172.16.0.0 to 172.31.255.255 192.168.0.0 to 192.168.255.255 IPv6: fc00::/7 (ULAs - Unique Local Addresses) Public IP Addresses: Public IP addresses are globally routable addresses assigned to devices that are directly connected to the internet. They are unique and allow devices to communicate with each other across different networks. Public IP addresses are obtained from Internet Service Providers (ISPs) or regional internet registries (Chen Y.& Li W. 2016).

3.3 IP Addressing Classes

IP addressing classes were used in the early days of the internet to categorize IP addresses based on their network size and structure. The IP addressing classes, namely Class A, Class B, Class C, Class D, and Class E, determined the default network and host portions of the IP address. Class A addresses have the first bit set to 0, indicating the network portion, and the next 7 bits representing the network identifier. Garcia Saavedra et al. (2012) the remaining 24 bits are used for host addressing. Class A addresses were designed for large networks, with the potential for up to 126 networks (2^7 - 2) and a maximum of 16,777,214 (2^24 - 2) host addresses per network. Example: 10.0.0.0 to 10.255.255.255 (Li.H & Li. L, 2015).

Class B addresses have the first two bits set to 10, indicating the network portion, and the next 14 bits representing the network identifier. Jain, S. et al.(2015). The remaining 16 bits are used for host addressing. Class B addresses were intended for medium-sized networks, with the potential for up to 16,382 networks (2^14 - 2) and a maximum of 65,534 (2^16 - 2) host addresses per network. Example: 172.16.0.0 to 172.31.255.255. Class C addresses have the first three bits set to 110, indicating the network portion, and the next 21 bits representing the network identifier. The remaining 8 bits are used for host addressing. Class C addresses were designed for small networks, with the potential for up to 2,097,150 networks (2^21 - 2) and a maximum of 254 (2^8 - 2) host addresses per network. Example: 192.0.0.0 to 223.255.255.255

Class D addresses have the first four bits set to 1110, indicating a multicast address used for group communication rather than individual hosts. Class D addresses are reserved for multicast addressing, where data is sent to a specific group of devices that have joined a multicast group. Example: 224.0.0.0 to 239.255.255.255. Class E addresses have the first four bits set to 1111, reserved for future use or experimental purposes. Class E addresses are not intended for general use and have not been allocated for specific applications. Example: 240.0.0.0 to 255.255.255.255 (Karami A. & Aslani F, 2017). Given a Network ID of 209.44.33.0/24 with a default subnet mask 255.255.255.0. The default number of host bits = 8 i.e. IP address = 209.44.33.0/24. The default subnet mask =255.255.255.0 (Perkins c.e & Bhagwat .P, 1994).

1 Number of bit to borrow = 3. 2^n (where n is the number of host bits to borrow) n = 3 ($2^3 = 8$).
2 Number of host per subnet =30. (Number of host bits available) – n = h. 8 - 3 = 5 h = 5

2^h – 2 = (number of hosts per subnet) 2^5 = 32 -3 = 30. 3 New subnet mask and prefix default class c. Subnet mask = 255. 255. 255. 0. Default class c prefix = /24. Das B. and Misshra S.K (2014). New subnet mask = 255.255.255.224 new prefix = /27. The 224 which is the last octet of the subnet mask was as a result of 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 Wang et al.(2020)

The value for the new prefix as demonstrated in table 1 was as a result of adding the 3 bits borrowed from the host bit to the Alan Thomas (2014). Previous 24 bits of the default subnet mask of class c. Hence, the new prefix/27 (Cisco Systems inc, 2021).

Table 1 Description of IP Address at Its Various Level

Network Address (In Binary)	11010001	00101100	00100001	00000000
Subnet Mask (In Binary)	11111111	11111111	11111111	11100000
Network/Host	NNNNNNNN	NNNNNNNN	NNNNNNNN	NNNHHHHH
Network Address (In Decimal)	209	44	33	0
Subnet Mask (In Decimal)	255	255	255	244

Subnet	Usable Range / Host Address	Broadcast
209.44.33.0	209.44.33.1- 209.44.33.30	209.44.33.31
209.44.33.32	209.44.33.33 - 209.44.33.62	209.44.33.63
209.44.33.64	209.44.33.65 - 209.44.33.94	209.44.33.95
209.44.33.96	209.44.33.97 - 209.44.33.126	209.44.33.127
209.44.33.128	209.44.33.129 - 209.44.33.158	209.44.33.159
209.44.33.160	209.44.33.161 - 209.44.33.190	209.44.33.191
209.44.33.192	209.44.33.193 - 209.44.33.222	209.44.33.223
209.44.33.224	209.44.33.225 - 209.44.33.254	209.44.33.255

S/N	Description	Binary Description/Representation	Decimal Description
1	Network Address	11010001.00101100.00100001.00000000	209.44.33.0
	First IPV4Address	11010001.00101100.00100001.00000001	209.44.33.1
	LastIPV4Address	11010001.00101100.00100001.00011110	209.44.33.30
	Broadcast Address	11010001.00101100.00100001.00011111	209.44.33.31
2	Network Address	11010001.00101100.00100001.00100001	209.44.33.32
	First IPV4 Address	11010001.00101100.00100001.00100001	209.44.33.33
	LastIPV4Address	11010001.00101100.00100001.00111110	209.44.33.62
	Broadcast Address	11010001.00101100.00100001.00111111	209.44.33.63

S/N	Description	Binary Description/Representation	Decimal Description
3	Network Address	11010001.00101100.00100001.01000000	209.44.33.64
	FirstIPV4 Address	11010001.00101100.00100001.01000001	209.44.33.65
	LastIPV4 Address	11010001.00101100.00100001.01011110	209.44.33.94
	Broadcast Address	11010001.00101100.00100001.01100000	209.44.33.95
4	Network Address	11010001.00101100.00100001.01100000	209.44.33.96
	First IPV4 Address	11010001.00101100.00100001.01100001	209.44.33.97
	LastIPV4 Address	11010001.00101100.00100001.01111110	209.44.33.126
	Broadcast Address	11010001.00101100.00100001.01111111	209.44.33.127
5	Network Address	11010001.00101100.00100001.10000000	209.44.33.128
	First IPV4 Address	11010001.00101100.00100001.10000001	209.44.33.129
	LastIPV4 Address	11010001.00101100.00100001.10011110	209.44.33.158
	Broadcast Address	11010001.00101100.00100001.10011111	209.44.33.159
6	Network Address	11010001.00101100.00100001.10100000	209.44.33.160
	FirstIPV4 Address	11010001.00101100.00100001.10100001	209.44.33.161
	LastIPV4 Address	11010001.00101100.00100001.10111110	209.44.33.190
	Broadcast Address	11010001.00101100.00100001.10111111	209.44.33.191

Journal, Advances in Mathematical & Computational Sciences
Vol. 11 No. 4, 2023 Series
www.isteams.net/mathematics-computationaljournal

S/N	Description	Binary Description/Representation	Decimal Description
7	Network Address	11010001.00101100.00100001.11000000	209.44.33.192
	FirstIPV4 Address	11010001.00101100.00100001.11000001	209.44.33.193
	LastIPV4 Address	11010001.00101100.00100001.11011110	209.44.33.222
	Broadcast Address	11010001.00101100.00100001.11011111	209.44.33.223
8	Network Address	11010001.00101100.00100001.11100000	209.44.33.224
	FirstIPV4 Address	11010001.00101100.00100001.11100001	209.44.33.225
	LastIPV4 Address	11010001.00101100.00100001.11111110	209.44.33.254
	Broadcast Address	11010001.00101100.00100001.11111111	209.44.33.255

The table above shows the detail description of IP address at its various level both in decimal and in binary representation. Figure 2 depict the combination of bus and ring network topologies and it is known as a hybrid network topology. It incorporates features from both the bus and ring topologies to create a unique network structure. The combination in a hybrid network offers a balance between scalability, redundancy, fault tolerance, and performance, making it suitable for various applications where these features are important.

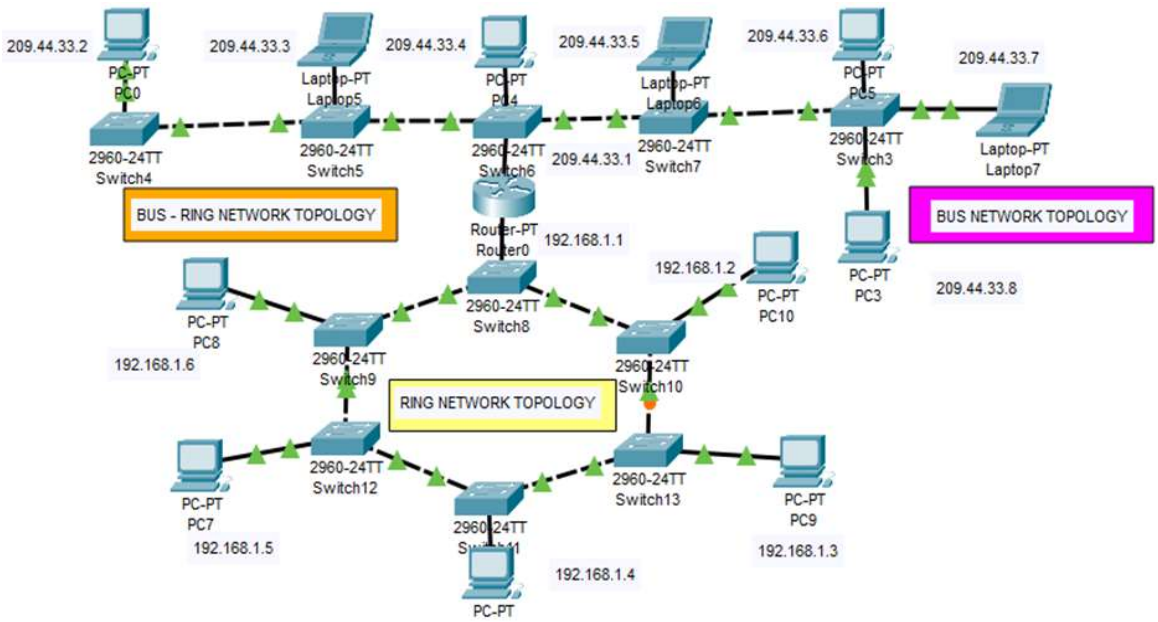


Figure 2: Combination of Bus and Ring Network Topologies

A combination of bus and ring network topologies can be used in various enterprise environments where specific requirements and network design considerations exist, it is important to note that the selection of network topologies depends on the specific requirements, budget, scalability, and reliability needs of each enterprise. Figure 3 depict the combination of the bus and star network topologies which create a hybrid network structure that incorporates the features, capabilities, and functions of both. It's important to note that the specific implementation and configuration of a combined bus and star network topology may vary depending on the intended use case and the network equipment being used.

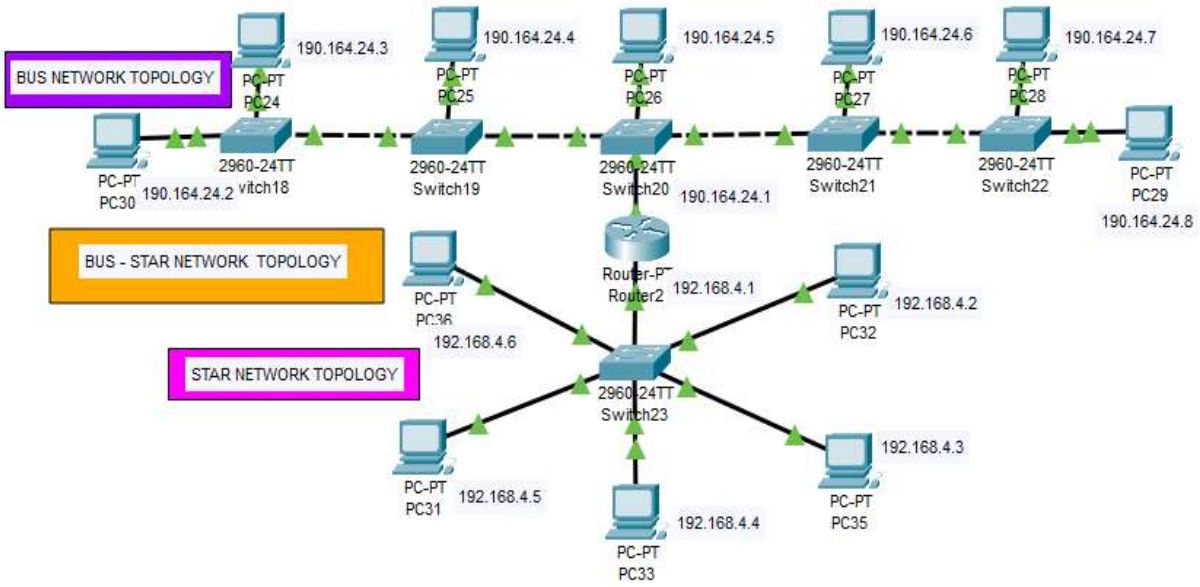


Figure 3: Combination of Bus and Star Network Topologies

This hybrid topology is commonly used in larger enterprise networks where multiple smaller local area networks (LANs) need to be interconnected. The bus network provides a central backbone for communication between different LANs, while the star networks allow for efficient connectivity within individual LANs. Figure 4 depict the combination of bus and tree network topologies is commonly referred to as a hybrid network topology. It incorporates features and capabilities of both bus and tree topologies, offering a flexible and scalable solution for various network setups. The usage scenarios for the hybrid topology are: small to medium-sized networks that require scalability and flexibility, such as office environments or small campuses.

Journal, Advances in Mathematical & Computational Sciences
Vol. 11 No. 4, 2023 Series
www.isteams.net/mathematics-computationaljournal

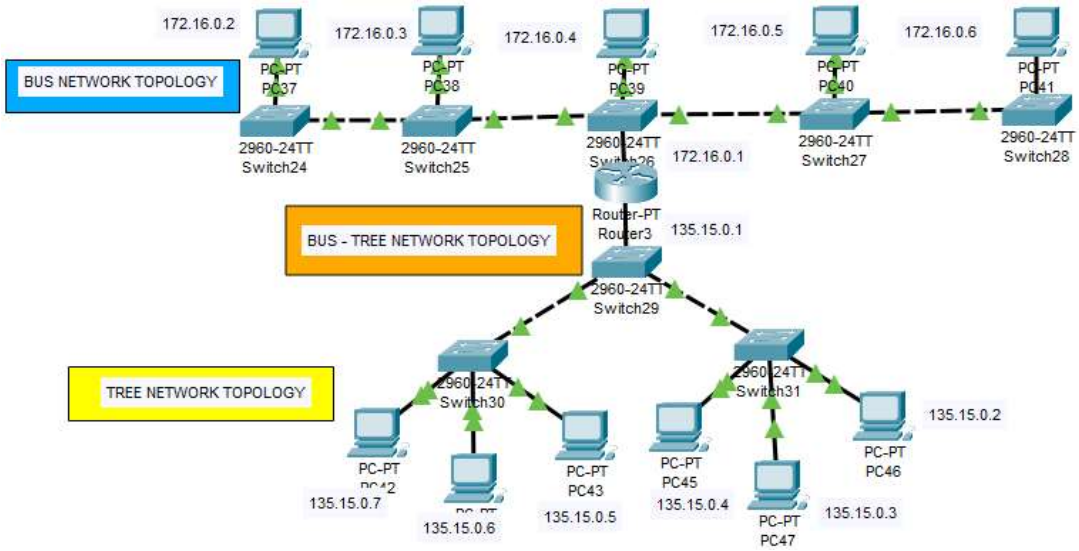


Figure 4 Combination of Bus and Tree Network Topology

Networks that require a centralized structure with the ability to expand and accommodate additional nodes. Environments where fault tolerance and efficient data transfer are important, such as critical systems or high-demand applications. Figure 5 depict the combination of star and tree network topologies is commonly known as a hybrid network. It incorporates the features and functions of both network topologies to provide a flexible and scalable solution for various applications.

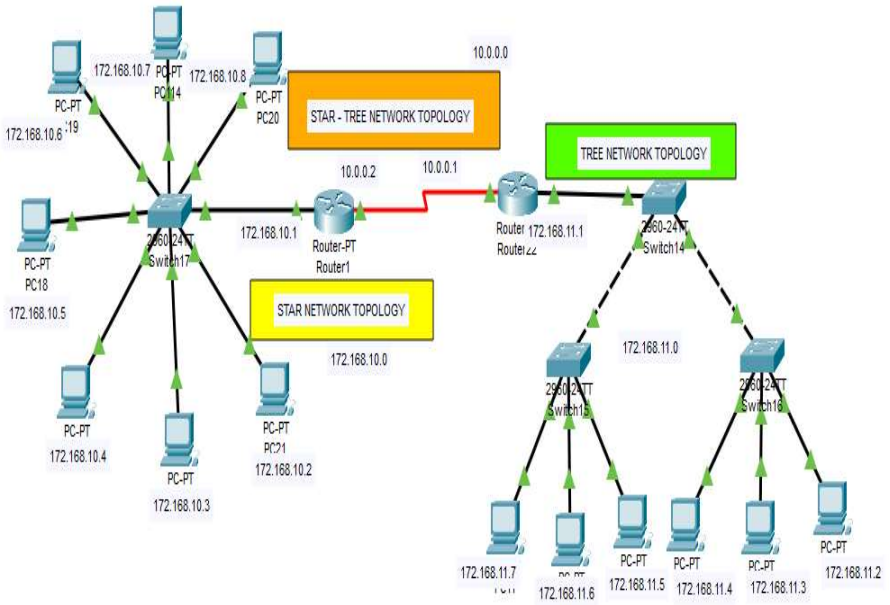


Figure 5 Combination of Star and Tree Network Topologies

The combination of star and tree network topology provides a flexible, scalable, and reliable solution for a wide range of applications, including corporate networks, smart home automation, industrial control systems, campus networks, and IoT deployments.

4. SUCCESSFUL PDU IN NETWORK SIMULATION

The sender transmits a protocol data unit (PDU) by clicking the send button, the receiver receives the PDU and checks for errors. If the PDU is received correctly, the receiver sends an acknowledgement (ACK) to the sender with the word **SUCCESSFUL** as an acknowledgement as shown in figure 6. The sender receives the ACK and knows that the PDU was received correctly. If the PDU is not received correctly, the receiver discards the PDU and does not send an ACK. The sender retransmits the PDU after a timeout period.

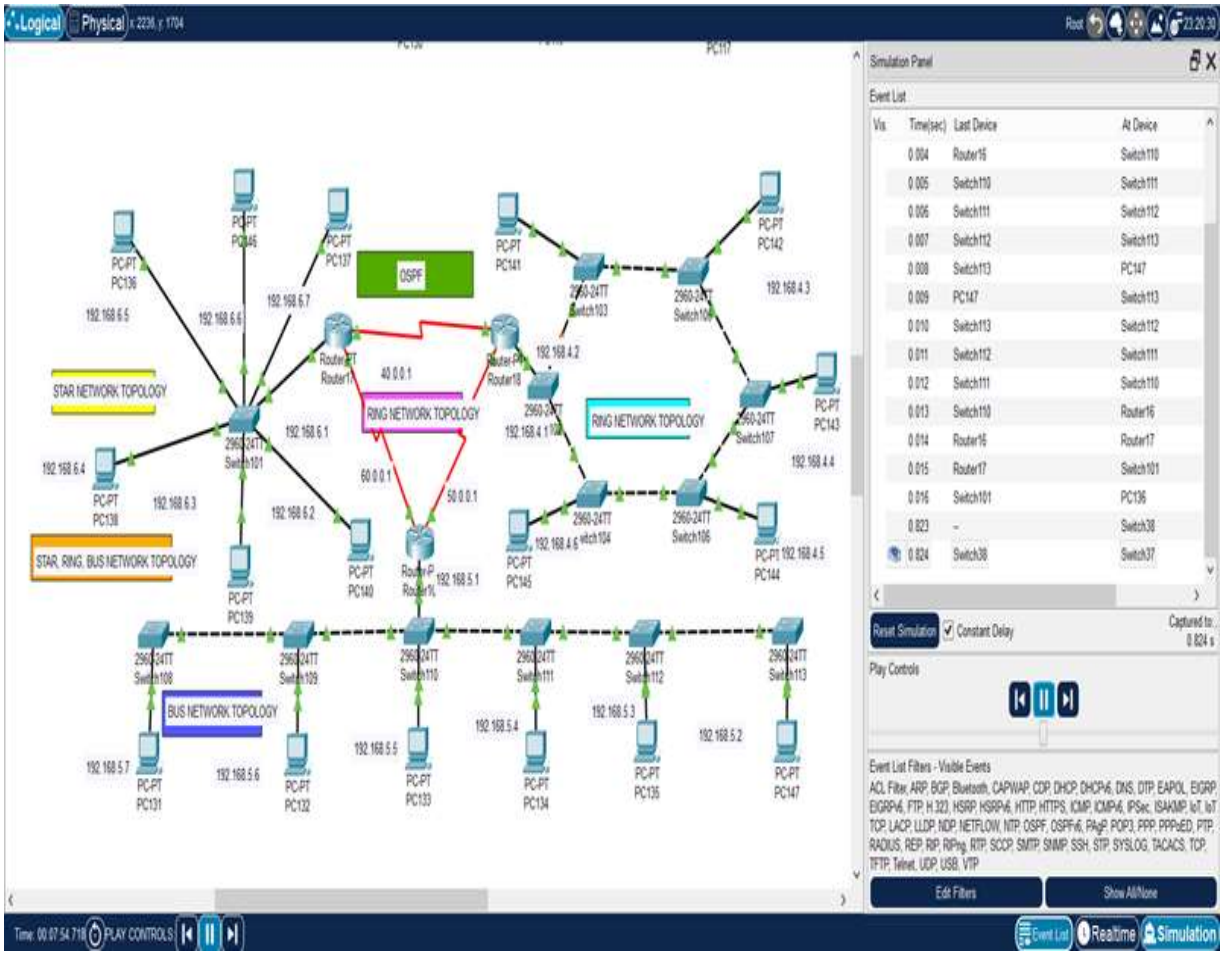


Figure 6: Star, Ring and Bus Network Topology Successful Simulation

The three basic topologies that were combined were the star, ring, and bus topologies. The simulation was successful in that it was able to create a network that exhibited the advantages of all the three topologies. For example, the network was able to provide centralized management and control: The star topology was used to provide centralized management and control of the network. This was done by connecting all of the devices in the network to a central hub. The ring topology was used to provide fault tolerance in the network.

This was done by connecting the devices in the network in a circular fashion. If one device in the ring fails, the data can still be transmitted through the other devices in the ring. The bus topology was used to provide scalability in the network. This was done by connecting all of the devices in the network to a single cable. As the network grows, new devices can be easily added to the bus without disrupting the existing network.The simulation was successful in demonstrating the benefits of hybrid network topologies. Hybrid network topologies can provide the advantages of multiple basic network topologies, which can make them a good choice for many different networking applications.

5. CONCLUSION

The dynamics of routing in wireless local area network (WLAN) design mechanisms play a crucial role in determining the performance, reliability, and efficiency of WLANs. This project aimed to explore and analyze various routing protocols and mechanisms used in WLANs, their impact on network dynamics, and provide recommendations for effective WLAN design. The survey involved the use of simulation tools and real-world case studies to evaluate the performance of different routing mechanisms. Metrics such as packet delivery ratio, end-to-end delay, throughput, and energy consumption were considered to assess the effectiveness and efficiency of each mechanism under varying conditions. Based on the findings, it was observed that the choice of routing protocol in WLAN design greatly influenced network dynamics.

Before implementing any routing protocol, it is crucial to assess the specific needs and characteristics of the WLAN, including network size, mobility patterns, traffic load, and application requirements. This analysis will help in selecting the most suitable routing mechanism. Consider the trade-off between reactivity and proactivity: WLAN designers should carefully evaluate the trade-off between reactive and proactive routing protocols. Reactive protocols are well-suited for dynamic networks, whereas proactive protocols offer better performance in stable environments. Hybrid protocols may be considered for scenarios with moderate mobility. Stay updated with advancements in routing protocols: WLAN designers should stay updated with the latest developments and advancements in routing protocols. New protocols and enhancements are regularly introduced, which may offer improved performance, scalability, and reliability.

REFERENCES

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.

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.

Arora, A., & Gupta, R. (2019). Application of routing dynamics to wireless local area network design mechanism. *International Journal of Advanced Science and Technology*, *28*(17), 308–318.

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.

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

Cisco (2022). *Wireless Access Point Placement: Best Practices*. https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/71967-wlan-ap-placement.html

Cisco Systems, Inc. (2021). *Wireless LAN Controller Configuration Guide, Release 8.10*. https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/wireless_lan_controller_configuration_guide_810_chapter_01100.html

Comer, D. (2012). Computer networks and internets. *Pearson Education India*.

Comer, D. E. (2015). *Computer networks and internets*. Pearson.

Feamster, N. (2014). Software-defined networking. *Morgan & Claypool Publishers*.

Forouzan, B. A. (2013). Data communications and networking. *McGraw-Hill Education*.

Gairola, K., Carrasco, R. A., & Jue, J. P. (2010). Routing Dynamics in Computer Networks: A Survey. *IEEE Communications Surveys & Tutorials*, *12*(4), 453–469.

Garcia-Luna-Aceves, J. J. (2015). Routing protocols for wireless sensor networks. *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*.

Hassan, W. A., & Ali, M. F. (2017). Performance evaluation of AODV and DSR routing protocols in wireless mesh networks. *Journal of King Saud University-Computer and Information Sciences*, *29*(4), 507–517.

IEEE 802.1 Wireless LANs. (2016). https://standards.ieee.org/standard/802_11.html

Jeong, J., Lee, S., Lee, H., & Yoon, Y. (2015). Performance evaluation of routing algorithms in Software-defined networks. *Journal of Network and Computer Applications*, *52*, 26–34.

Kaur, P., & Singh, K. (2020). A review of routing protocols for wireless local area networks. *International Journal of Computer Networks and Applications*, *7*(1), 1–10.

Kurose, J. F., & Ross, K. W. (2012). Computer networking: A top-down approach. *Pearson*.

Kurose, J. F., & Ross, K. W. (2013). Computer networking: A top-down approach. *Pearson*.

Kurose, J. F., & Ross, K. W. (2017). *Computer networking: A top-down approach*. Pearson.

Li, X., Li, J., Wei, Y., & Cai, Z. (2020). A Multi-Radio Power Level-Based Routing Mechanism for WLAN. *IEEE Access*, *8*, 223577–223585.

Lifewire. (2022). *Wi-Fi 6 vs. Wi-Fi 5 vs. Wi-Fi 4: What's the Difference?* https://www.lifewire.com/wifi-6-vs-wifi-5-vs-wifi-4-4172665

Liu, K., & Wu, J. (2018). Wireless network design: Optimization models and solution procedures. *IEEE Communications Magazine*, *56*(10), 182–188.

Networks, F. (2022). *Best Practices for Wireless Site Surveys*. https://www.flukenetworks.com/blog/cabling-chronicles/best-practices-wireless

Perlman, R. (1985). An algorithm for distributed computation of a spanning tree in an extended LAN. *ACM SIGCOMM Computer Communication Review*, *15*(4), 44–53.

Peterson, L. L., & Davie, B. S. (2012). *Computer networks: A systems approach*. Morgan Kaufmann.

Qu, X., Zhao, Z., Tang, Y., & Chen, Y. (2021). A Decision Tree-Based Routing Algorithm for Wireless Local Area Networks. *Journal of Communications*, *16*(1), 17–25.

Rashidi, A., & Al-Ani, A. (2019). WLAN Design and Optimization for High-Density Environments. *IEEE Communications Magazine*, *57*(10), 26–33.

Stallings, W. (2017). *Data and computer communications*. Pearson.

Tanenbaum, A. S., & Wetherall, D. (2011). *Computer networks*. Pearson.

Tang, L., Zhang, J., & Wang, C. (2018). Dynamic routing mechanism for wireless sensor networks. *Journal of Network and Computer Applications*, *117*, 75–82.

Wang, S., Chen, H., & Shen, X. (2019). A dynamic routing protocol based on traffic load balancing for wireless sensor networks. *Wireless Personal Communications*, *107*(3), 1909–1923.

Wang, Y., Zhou, Q., & Lin, K. (2019). Hybrid routing mechanism based on AODV and OLSR in wireless mesh networks. *Journal of Ambient Intelligence and Humanized Computing*, *10*(4), 1427–1438.

Wu, J., & Xu, K. (2011). A comprehensive survey of wireless mesh network routing protocols. *Journal of Network and Computer Applications*, *34*(2), 529–543.

Yin, Y., Liu, X., & Zhang, H. (2021). Dynamic routing based on node information prediction in wireless networks. *IEEE Access*, *9*, 41603–41615.

Zhan, J., Gu, Y., & Xu, S. (2016). Routing dynamics in wireless mesh networks: A survey. *IEEE Communications Surveys and Tutorials*, *18*(1), 657–678.

Zhang, W., Zhang, S., & Zhang, Y. (2019). A dynamic channel selection routing algorithm for improving throughput in WLANs. *Wireless Networks*, *25*(5), 2335–2346.

Zhang, Y., Liu, J., Liu, Z., & Yang, J. (2019). Multi-channel Wireless Routing Protocol Based on Improved Distance Vector Algorithm for WLAN. *Journal of Physics: Conference Series*, *1236*(1), 012073.

Zhang, Y., & Liu, Z. (2010). Dynamic behavior of the Internet. *Springer*.

Zhao, F., & Wang, L. (2014). A Survey of Wireless Local Area Networks (WLANs) Technology. *Journal of Communications*, *9*(11), 929–937.