Comparative Analysis of DMVPN Phase 3 Performance Across Dynamic Routing Protocols

Buthaina Mohamed[1], Rafe Alasem[2], Mahmud Mansour[1], Najia Ben Saud[1]

[1]Faculty of Information Technology, University of Tripoli, Tripoli, Libya
[2]School of Engineering, Architecture and Interior Design, Amity University Dubai
Dubai International Academic City, Dubai, UAE
bensaoud.najia@gmail.com

Abstract. Dynamic Multipoint Virtual Private Network (DMVPN) by Cisco, was developed to overcome the limitations of traditional VPNs by improving their scalability, which had been a drawback. DMVPN achieves this by utilizing technologies like Multipoint Generic Routing Encapsulation (mGRE), Next Hop Resolution Protocol (NHRP), and various routing protocols. Additionally, the inclusion of IPsec is mandatory to ensure robust security measures.

In our research challenge, we sought to implement DMVPN Phase Three within a network configuration comprising one hub, two spokes, and three LANs. To execute this, we employed the GNS3 emulator, facilitating the deployment of different routing protocols such as RIPv2, EIGRP, OSPF, and BGP. The objective of this implementation was to assess and make comparisons based on performance metrics including latency, jitter, TCP/UDP throughput, and round-trip time (RTT). Our evaluation of DMVPN Phase 3 performance across various routing protocols showed significant variations. RIPv2 offered the lowest latency, while BGP achieved the highest TCP throughput. EIGRP demonstrated the least jitter and shared the highest UDP throughput with OSPF. This comprehensive evaluation helps in determining which routing protocol best suits the specific network's needs and goals, shedding light on their respective advantages and limitations within the DMVPN framework.

Keywords: DMVPN, NHRP, mGRE, IPsec, RIPv2, EIGRP, OSPF, BGP.

1 Introduction

A common method for creating remote connections over the internet is to utilize a Virtual Private Network (VPN) with an IPsec profile between various places and can be set up to guarantee confidentiality, integrity, and availability. Branch offices can access the company's resources by connecting to the hub router through spoke routers that are located at the branches. Due to static configuration, the traditional VPN system has the drawbacks of increasing implementation time and latency as more locations are required to connect to the main site as network topologies change. To get over this limitation and offer a more scalable option, Cisco developed the Dynamic Multipoint Virtual Private Network (DMVPN), which applies routing algorithms to build a partial mesh network topology between at least two spokes and the hub. As a result, traffic can pass directly between spokes instead of travelling through the hub. A central router, often located at the headquarters, serves as the hub while the other routers, which are found at the branch offices, serve as spokes. The branch offices can access the company's resources according to the spokes' connection to the hub router.

DMVPN has three different phases, Phase 1 supports Spoke to Hub communication, and it is a classic approach in which traffic between any spokes must pass via the primary hub with no direct connection between spokes. Phase 2 allows Spoke to Spoke direct connection, in each spoke node, mGRE tunneling is employed to assure all traffic in this model is routed through a direct connection between all spokes. thus, reduces latency and bandwidth consumption, however all the spokes must have entire routing data with the next-hop preserved, as a result scalability may be limited especially in large networks. Phase 3 also allows Spoke to Spoke direct connection and improves the scalability of phase 2, Phase 3 includes new NHRP redirect and shortcut functions to enhance updates to the routing [1].

A dynamic routing protocol is necessary to set up a DMVPN connection and control routing updates among spokes and hub to link DMVPN network components. DMVPN supports a number of routing protocols, including Routing Information Protocol (RIP), Open Short Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System to Intermediate System (IS-IS), and Border Gateway Protocol (BGP). Each routing protocol offers unique path calculation metrics that highlight the benefits and downsides of that protocol.

To create a secured DMVPN network, IPsec encapsulation protocol is used to encrypt data sent between two remote sites, each node must have a minimal configuration of IPsec in order to provide a foundational degree of confidentiality and integrity. In order to establish a secure DMVPN network, the utilization of the IPsec (Internet Protocol Security) encapsulation protocol is essential. IPsec plays a critical role in enhancing the security of data transmitted between two remote sites within the DMVPN framework. To ensure a baseline level of confidentiality and integrity for the data being exchanged, each node within the network must be configured with IPsec.

IPsec is a suite of protocols that delivers strong security features for network communications. It provides authentication, data reliability, and encryption, all crucial aspects for safeguarding sensitive information during transit over potentially insecure networks, such as the internet or other public networks.

By implementing IPsec at each node within the DMVPN network, data is not only encrypted but also subjected to verification processes that confirm its authenticity and integrity. This ensures that the information remains confidential and tamper-proof as it traverses the network, mitigating the risk of eavesdropping, data alteration, or unauthorized access.

In summary, IPsec is an indispensable component within DMVPN networks, as it establishes a foundational layer of security, guaranteeing the confidentiality and integrity of data exchanged between remote sites, thereby providing a secure and private communication channel within the DMVPN infrastructure.

This paper delves into the performance evaluation of DMVPN Phase 3 across various routing protocols. We begin by introducing the concept of virtual private networks and their limitations in a traditional setting. This is followed by an in-depth exploration of Dynamic Multipoint VPN, its different phases (Phase 1, Phase 2, and Phase 3), and the crucial role of the IPsec protocol in securing the network. Section 2 then delves into existing research on DMVPN performance and the influence of routing protocols. Section 3 details the simulation tools employed, and the designed network topology used for the evaluation. Section 4 presents the findings obtained from the performance evaluation. Section 5 analyzes these results, comparing the performance of different routing protocols within DMVPN Phase 3. Finally, Section 6 summarizes the key findings and highlights the impact of routing protocol selection on DMVPN performance. It also outlines potential areas for future research.

1.1 DMVPN Overview

The main goal of DMVPN is to achieve better flexibility and scalability in corporate networks. This solution uses a combination of several standard technologies working together to build DMVPN network, below we will discuss main DMVPN components, namely: mGRE, NHRP, IPsec, and Routing Protocols. Followed by DMVPN phases of operation that will be discussed in the following sub-section [2][3].

mGRE. In Dynamic Multipoint Virtual Private Networks, Multipoint Generic Routing Encapsulation (mGRE) plays a pivotal role in establishing dynamic tunnels. mGRE allows for the on-the-fly creation of these tunnels, which is especially useful when multiple remote sites need to connect to a central hub. What makes mGRE particularly valuable is its ability to encapsulate multicast and broadcast packets into unicast GRE packets by appending a GRE header. However, to ensure the security of data transmitted within these GRE packets, IPsec (Internet Protocol Security) is employed. IPsec complements mGRE by encrypting all the data contained in the GRE packets, utilizing an IPsec header. In essence, mGRE handles the efficient transportation of data, while IPsec steps in to provide robust encryption, collectively enabling the secure transport and encryption of multicast packets within the DMVPN framework [4].

NHRP. Maps between Underlay (public or WAN side IP) and Overlay (GRE tunnel private IP), all configured spokes' underlay IP addresses are stored in a specific NHRP database kept by the Hub. All spokes register its underlay IP address with the hub and search the underlay IP address of the destination spoke it wants to establish a VPN tunnel with in the NHRP database [5].

IPsec. Although using IPsec with DMVPN is optional, GRE tunnels are not at all safe, hence IPsec is crucial to ensuring security. While optional in the context of DMVPN (Dynamic Multipoint Virtual Private Network), plays a critical role in enhancing the security of network communications. Without IPsec, GRE (Generic Routing Encapsulation) tunnels, which DMVPN relies on for dynamic and efficient connections, lack robust security features. In many scenarios, particularly when sensitive data or confidential information is being transmitted, relying solely on GRE tunnels can leave the network vulnerable to various security threats. Therefore, the integration of

IPsec is highly recommended and often considered essential. IPsec adds layers of security by providing authentication, data integrity, and encryption for network packets, ensuring that data remains confidential and tamper-proof during transit. In essence, while DMVPN establishes the connectivity framework, IPsec is the cornerstone for safeguarding the integrity and confidentiality of the data being transmitted, making it a crucial component for secure network communications [6].

Routing protocols. In addition to the previously listed technologies, For DMVPN, a dynamic routing protocol is required. Because they guarantee the efficient formation of tunnels and have a substantial impact on network behavior, routing protocols are a crucial part of the DMVPN system. As a result, numerous studies have been done to evaluate the network performance and choose the most practical routing protocol for DMVPN [4].

Following brief about routing protocols applied in this paper:

- Enhanced Interior Gateway Routing Protocol (EIGRP), a distance-vector routing protocol is one of the routing protocols used for DMVPN. A router can use EIGRP to exchange routes with other nodes within a single AS.
- Routing Information Protocol (RIP), hop count is used as a routing matrix in this distance-vector routing protocol. To stop the spread of false routing information, RIP uses the split horizon, route poisoning, and hold-down methods.
- Open Shortest Path First (OSPF) is an IP-based routing protocol that belongs to the class of interior gateway protocols that operate within a single autonomous system. It uses a link state routing algorithm [7].
- A standardized exterior gateway protocol called Border Gateway Protocol (BGP) is used on the Internet to send routing data between different Autonomous Systems (AS). The protocol is sometimes categorized as a distance-vector routing protocol; however, it is commonly categorized as a path vector protocol.

1.2 DMVPN Phases

Phase One. The primary objective is to establish basic connectivity and secure communication between remote sites, or "spokes," and a central hub. In this configuration, each spoke is manually configured with the IP address of the hub, designating the hub as the network server. Consequently, every spoke establishes a static tunnel with a destination IP address that matches the physical address of the hub.

The consequence of this setup is that communication between spokes is funneled through the central hub. In other words, spokes can only communicate with each other by routing their traffic through the hub. While this arrangement simplifies the configuration of the hub, it introduces limitations, especially when it comes to the efficiency and scalability of the network.

One of the notable advantages of DMVPN Phase 1 is its simplified hub configuration. The hub's responsibility is reduced to advertising a default route to the spokes, making the setup relatively straightforward. Furthermore, Phase 1 is flexible when it comes to the choice of routing protocols. Nearly any dynamic routing system can be employed to ensure reachability between the spokes, simplifying the configuration process further.

However, a significant drawback of DMVPN Phase 1 is the lack of direct communication between spokes. Since all traffic must pass through the hub, this can lead to increased latency, decreased network efficiency, and potentially overload the hub in scenarios with heavy inter-spoke traffic.

To overcome this limitation and enable direct communication between spokes, DMVPN Phase 2 introduces the Next Hop Resolution Protocol (NHRP), allowing spokes to dynamically establish tunnels with each other. This enhancement not only improves overall network efficiency but also enhances scalability by reducing the dependency on the central hub for inter-spoke traffic.

Phase Two. Introduces the NHRP, allowing spokes to establish direct communication with each other without relying solely on the central hub. However, this phase has certain limitations. For Phase Two to work effectively, all spokes must maintain full routing information and store the next hop for each destination. This requirement ensures that spokes can efficiently route traffic directly to their intended destinations without going through the hub.

While Phase Two significantly improves network efficiency by enabling spoke-to-spoke communication and reducing the load on the central hub, it introduces scalability challenges. In large networks with a substantial number of spokes, maintaining full routing information for each spoke can become impractical. For instance, in a network with 1000 spokes, each spoke's routing table would contain an excessive number of entries, many of which may not be necessary for its operation. Managing such large routing tables can strain router resources and potentially lead to performance issues.

To address this limitation, network administrators need to carefully consider the design and size of their DMVPN Phase Two deployments, especially in scenarios with a large number of spokes. It may be necessary to implement strategies like route summarization and selective routing to optimize network performance and scalability while still benefiting from the advantages of direct spoke-to-spoke communication provided by DMVPN Phase Two.

Phase Three. DMVPN Phase Three builds upon the foundation laid by Phase Two and is designed to achieve similar goals while addressing some of its limitations. The key improvement in Phase Three lies in its approach to scalability.

In Phase Three, each spoke maintains visibility of all the necessary routes from the central hub. Instead of requiring each spoke to maintain a full routing table with information about every other spoke, the hub is used to summarize the network's routes. This design significantly enhances scalability. Spokes can efficiently access routing information without the burden of storing and processing excessive route entries.

The result is a more hierarchical and scalable architecture compared to Phase Two. This makes DMVPN Phase Three particularly well-suited for large-scale deployments where a substantial number of remote spokes are needed to communicate securely and efficiently. In such scenarios, Phase Three optimizes network performance and resource utilization by minimizing the routing table size at the spokes while still facilitating direct spoke-to-spoke communication when needed.

Overall, DMVPN Phase Three refines the DMVPN architecture, making it more adaptable and scalable, especially in situations where large networks with numerous spokes require secure and optimized communication.

2 Related Work

An earlier study conducted by Said, M. A., & Jadied, E. M. in 2022, that delved into the performance characteristics of Dynamic Multipoint Virtual Private Network (DMVPN) in different configurations. Their research specifically examined DMVPN with and without the inclusion of IPsec, a popular security protocol, and utilized the BGP (Border Gateway Protocol) routing protocol. The study assessed key performance metrics including latency, throughput, jitter, and packet loss, crucial factors for evaluating network efficiency and reliability [8].

One noteworthy finding from this study was that the presence of IPsec within the DMVPN architecture had a discernible impact on the transport of UDP (User Datagram Protocol) packets. UDP is known for its low-latency characteristics and is often used for real-time applications. The study's results indicate that the additional security measures introduced by IPsec may introduce some trade-offs in terms of UDP packet transport performance. This insight underscores the importance of carefully considering the balance between network security and performance requirements when implementing DMVPN with IPsec, as different applications and use cases may have varying sensitivities to latency and packet loss [8].

In a study conducted by Hasan Mohamed et al (2021) [9], the influence of IPsec and routing protocols on DMVPN was examined. Their research revealed that DMVPN Phase 2 exhibited superior performance compared to Phase 1. Furthermore, the study highlighted that using the OSPF routing protocol without additional security measures resulted in the best network performance, characterized by higher throughput, minimal jitter, and lower latency. These findings underscore the importance of selecting the appropriate DMVPN phase and routing protocols based on specific performance and security requirements, with Phase 2 and OSPF emerging as strong choices for optimized network performance when security considerations permit.

In another study done by Ummi Masruroh et al (2018) [10], the performance of DMVPN was assessed across three distinct routing protocols: RIP, OSPF, and EIGRP. The study primarily focused on three key performance metrics: throughput, jitter, and packet loss. Notably, the findings indicated that DMVPN Phase 2 with RIP exhibited the highest throughput among the configurations studied. Conversely, DMVPN Phase 2 with EIGRP demonstrated the lowest jitter, signifying minimal variations in packet delivery times. However, the study also revealed that DMVPN Phase 3 with RIP had the highest packet loss rate, highlighting the trade-offs and performance nuances associated with different DMVPN configurations and routing protocol choices.

In addition, N. Angelescu and colleagues in (2017) were focusing on the creation and implementation of a DMVPN Phase 2 network, specifically emphasizing the establishment of spoke-to-spoke tunnels [11]. The study compared this approach to conventional VPN solutions, exploring the operational aspects and benefits of DMVPN

Phase 2 in facilitating direct communication between remote sites. This research sheds light on the advantages and operational differences between DMVPN Phase 2 networks and traditional VPN setups, underlining the importance of dynamic multipoint virtual private networks in modern networking scenarios that require efficient and secure communication between dispersed locations.

In research conducted by Gebere and colleagues (2017) [12], a comprehensive analysis and evaluation of different routing techniques in the context of DMVPN were performed. The study's findings indicated that for the establishment of a secure enterprise network utilizing the Dual Hub Dual DMVPN hub-to-spoke topology, OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) emerged as the most suitable routing protocols. These results highlight the importance of selecting the appropriate routing mechanisms when implementing DMVPN in complex enterprise environments, emphasizing OSPF and EIGRP as optimal choices for achieving secure and efficient communication in such configurations.

Fenny and et al (2018) [13], they performed research focused on comparing various encryption methods within the context of Dynamic Multipoint Virtual Private Network (DMVPN). The study assessed the performance of these encryption methods by considering key metrics such as throughput, jitter, and packet loss. These metrics were used to evaluate the effectiveness of different encryption techniques when it comes to data transfer and video streaming within a DMVPN environment. This research underscores the significance of encryption in DMVPN deployments, as it directly impacts the network's ability to handle data transfer and multimedia streaming tasks efficiently while maintaining security. The findings of this study contribute valuable insights into selecting appropriate encryption methods to optimize DMVPN performance for specific applications and use cases.

3 Design and Simulation

This paper delves into the realm of DMVPN Phase 3 and conducts a comparative analysis of network performance, emphasizing the influence of the underlying routing protocol. The study commences by outlining a Hub and Spoke mesh topology designed specifically for our DMVPN network, accommodating multiple sites dispersed across various geographical locations. Through the utilization of a public WAN or Internet connection, these branch locations are able to establish communication channels, facilitating the sharing of shared resources among them. Notably, each site, irrespective of its physical location, has the capability to communicate directly with every other site, eliminating the necessity of routing all traffic through the central hub. To comprehensively evaluate the efficacy of different routing protocols in our network, we will implement four distinct scenarios, involving EIGRP, RIPv2, OSPF, and BGP. The objective is to ascertain the most suitable routing protocol for our specific network requirements.

3.1 Simulation Tools

GNS3. short for "Graphical Network Simulator 3" is a free and open-source software application designed to mimic the intricacies of real-world networks. This powerful tool eliminates the need for physical network hardware such as switches and routers, allowing users to create and configure virtual networks effectively. GNS3 offers a user-friendly graphical interface that simplifies the process of building and customizing these virtual networks. It is compatible with standard PC hardware and can be run on various operating systems, including OSX, Linux, and Windows. GNS3 is a valuable resource for network professionals and enthusiasts, enabling them to experiment, test, and simulate network configurations and scenarios without the need for costly physical equipment.

iPerf3. It is a an open-source measurement and optimization tool for networks. Iperf3 includes both client and server capabilities, and it can generate a data stream to measure the transfer rate in either one or both ways between the two endpoints.

Ipterm. It is a Debian-based networking toolkit that provides various essential networking utilities. It incorporates tools like Net-tools, iproute2, ping, traceroute, iperf3, an SSH client, tcpdump, and multicast testing tools. These utilities assist in network diagnostics, performance measurement, and network management tasks. Ipterm is a valuable resource for network administrators and professionals, offering a comprehensive suite of tools for various networking needs.

Wireshark. is a widely used, free, and open-source network packet analyzer. It allows users to capture and inspect data packets on a network in real-time. Wireshark is a powerful tool for network administrators, security professionals, and developers, as it enables the examination of network traffic, troubleshooting network issues, and analyzing network protocols for various purposes, including debugging, security audits, and performance optimization. Its user-friendly interface and extensive protocol support make it a valuable resource for anyone working with computer networks.

3.2 Network Design

The Topology consists of one main site in which the central Hub router is installed, 2 branch sites with Spoke routers, 3 LANs one per site, and WAN connection between the 3 sites, as shown in Figure. 1.

For the same network topology phase 3 DMVPN is configured with a different routing protocol in each scenario, in order to evaluate the performance.

In Figure 1, the topology shows three ipterm terminals running the Ubuntu operating system with a built-in software tool. The end device "ipterm2-2" was set as a server and "ipterm2-3" as a client. The ipterm tool is connected as an end device to each LAN and runs the iPerf software to send input and measure output data. Following details about test data and performance parameters:

Input data. Using the iPef3 tool to generate traffic, TCP and UDP packets were sent 10 times every 10 seconds from source to destination with a TCP window size of 8000 KB and UDP bandwidth of 1 Mbits/sec.

10 ICMP packets were forwarded from the source to the destination using the ping command.

Output data. Is measured in terms of throughput, Jitter, and Latency.

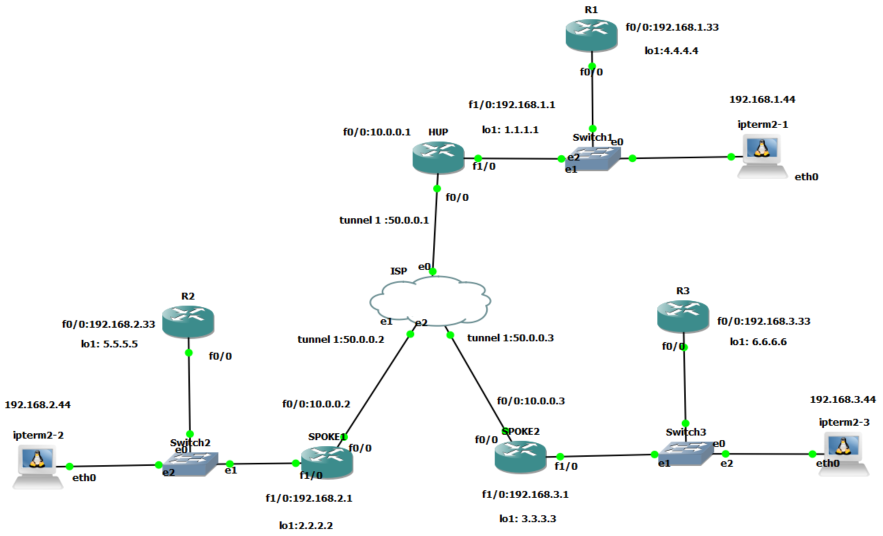

Fig. 1. Network Topology.

4 Results

In this section, we present the outcomes for each routing protocol in four different scenarios, encompassing latency, jitter, and TCP/UDP throughput as the key performance metrics. We initiate the analysis with EIGRP, followed by an examination of RIPv2, subsequently delving into OSPF, and culminating with an assessment of BGP. This structured presentation enables a comprehensive evaluation of how each routing protocol performs in diverse network settings, facilitating a clear understanding of their strengths and weaknesses across the specified performance criteria.

4.1 EIGRP

The measurements provided in Figure 2, with a jitter measurement of 338.651 milliseconds and a latency of 167.6 milliseconds for an EIGRP (Enhanced Interior Gateway Routing Protocol) network, reveal some notable characteristics about the network's performance. Let's discuss the implications of these measurements:

- Jitter (338.651 milliseconds):

- Excessive Jitter: A jitter measurement of 338.651 milliseconds is exceptionally high. Jitter represents variations in the arrival time of data packets, and such a high value suggests significant and unpredictable delays in packet delivery.
- Impact on Real-time Applications: High jitter is problematic for real-time applications such as VoIP (Voice over Internet Protocol) and video conferencing. It can lead to distorted audio, video freezes, and interruptions in communication. These applications require low and consistent jitter to provide a seamless user experience.
- Causes of Jitter: Addressing high jitter often involves optimizing network traffic prioritization, implementing Quality of Service (QoS) policies, and ensuring network equipment is functioning correctly. Identifying and rectifying the root causes of jitter is essential for improving network performance.

— Latency (167.6 milliseconds):

- High Latency: A latency measurement of 167.6 milliseconds is considered high, however it may be acceptable for many non-real-time applications, such as general web browsing and file transfers.
- Real-time Application Considerations: However, for real-time applications, this level of latency can still be problematic. While it may not be as severe as very high latency values, it can introduce noticeable delays in communication.
- Reducing Latency: Reducing latency may involve optimizing network routing, minimizing the number of hops, and improving network infrastructure to reduce transmission delays.

In summary, the measurements in Figure 2 indicate that the EIGRP network suffers from high jitter, which is a significant concern for real-time applications. While the latency value is moderate and may be acceptable for some applications, it can still affect real-time communication. To improve network performance, it is essential to address the root causes of jitter, which may require network optimization, QoS implementation, and equipment evaluation. Additionally, considering the specific requirements of real-time applications when designing and managing the network is crucial for delivering a better user experience.

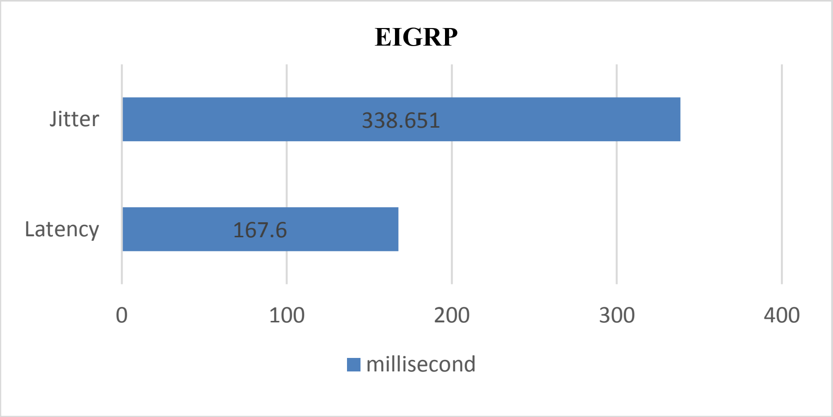

Fig. 2. EIGRP- Latency and Jitter.

Figure 3 presents the outcomes of our throughput tests, both for TCP and UDP, conducted within a network employing the EGRP protocol. These tests utilized a network monitor to gauge throughput, with results expressed in kilobits. For TCP, the measured throughput yielded a value of 503 kilobits, signifying the data transfer rate achievable under these network conditions. In contrast, the throughput assessment for UDP displayed a different performance, registering a value of 1040 kilobits. These results shed light on the data transfer capabilities within the network when utilizing the EGRP protocol, highlighting distinctions between the performance of TCP, which prioritizes reliability and error correction, and UDP, known for its low-latency characteristics and suitability for real-time applications. This insight aids in assessing the network's suitability for various types of data traffic and applications.

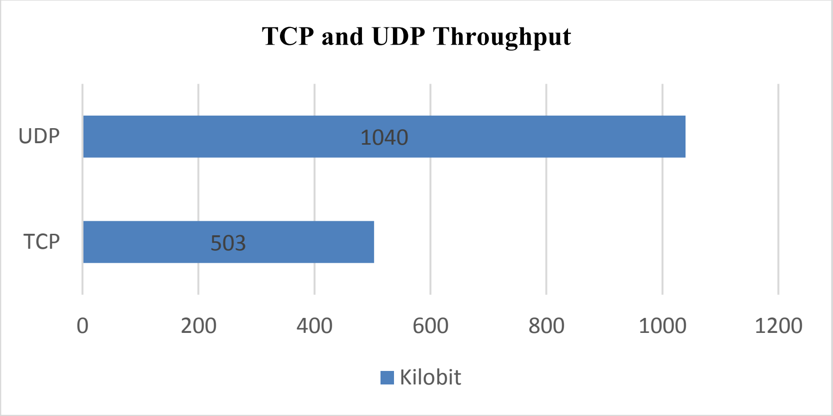

Fig. 3. EIGRP- TCP and UDP Throughput.

4.2 RIPv2

The latency measurement of 48.953 milliseconds and the jitter measurement of 833.101 milliseconds, as shown in Figure 4 for a network using the RIPv2 (Routing Information Protocol version 2) protocol, raise significant concerns about the network's performance, particularly for real-time applications. Let's discuss the implications of these measurements:

— Latency (48.953 milliseconds):

- Latency Tolerance: A latency of 48.953 milliseconds can be considered as Moderate latency, however for many types of network traffic, especially for applications that require low latency, it is relatively high. For comparison, most internet users are accustomed to latencies in the range of tens of milliseconds or less for streaming applications.

- Application Impact: Moderate latency can negatively impact various applications. For instance, in online gaming, even moderate latency can result in lag and unresponsive gameplay. In video conferencing or VoIP calls, it can lead to delays in communication and a poor user experience.
- Root Causes: To address latency, it's essential to identify its root causes. Common factors contributing to latency include network congestion, inefficient routing, long physical distances, and network equipment performance issues.

— Jitter (833.101 milliseconds):

- Excessive Jitter: A jitter measurement of 833.101 milliseconds is extremely high and concerning. Jitter represents variations in latency, and such a high jitter value indicates significant and unpredictable delays in the arrival of packets at their destination.
- Real-time Applications: High jitter is particularly problematic for real-time applications like VoIP and video conferencing, as it can result in distorted audio, video freezing, or dropped calls. These applications require consistent and low jitter for smooth communication.
- Causes of Jitter: Addressing high jitter often involves optimizing network traffic prioritization, implementing Quality of Service (QoS) policies, and ensuring network equipment is functioning correctly.

In summary, the latency and jitter measurements provided in Figure 4 suggest that the network may be experiencing performance issues, especially for real-time applications. Improving network performance will likely require a thorough analysis of network components, configuration, and traffic patterns to identify and address the specific causes of these latency and jitter problems. Additionally, it's crucial to consider the network's intended use and application requirements when setting latency and jitter targets to ensure a satisfactory user experience.

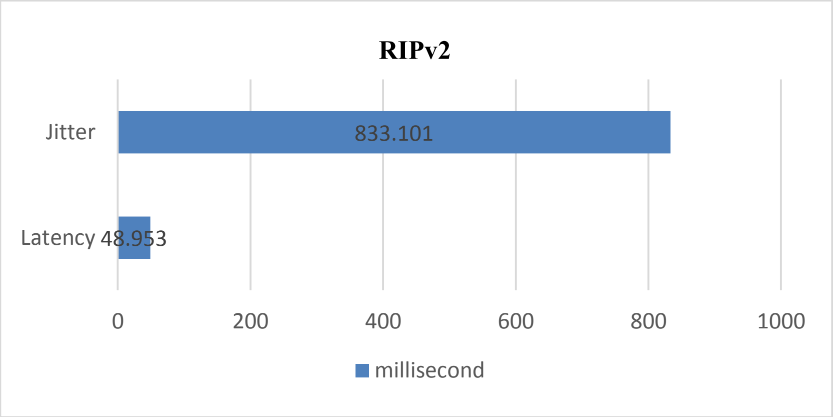

Fig. 4. RIPv2- Latency and Jitter.

Figure 5 presents the throughput results for TCP and UDP within the DMVPN network utilizing the RIPv2 protocol. Notably, the throughput values for both TCP and UDP are closely aligned, showcasing a marginal difference. Specifically, the throughput for TCP recorded a rate of 566 kilobits, while UDP demonstrated a slightly higher throughput of 567 kilobits. These findings indicate that under the network conditions governed by the RIPv2 protocol, both TCP and UDP exhibit comparable data transfer rates, with UDP showing only a slight advantage. This insight provides valuable information regarding the network's performance when employing the RIPv2 protocol and its suitability for various data traffic types and applications.

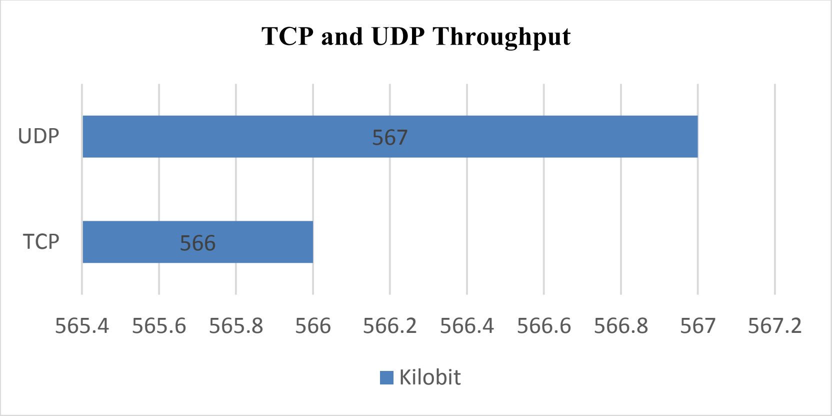

Fig. 5. RIPv2- TCP and UDP Throughput.

4.3 OSPF

The graph in Figure 6 shows the latency and Jitter of the DMVPN network using the OSPF protocol, with a jitter value of 441.668 milliseconds and a latency value of 81.97 milliseconds. The graph indicates a jitter value of 441.668 milliseconds and a latency value of 81.97 milliseconds.

Latency and jitter are important metrics in network performance monitoring:

Latency: Latency refers to the delay in data transmission through a network. In your case, the latency value of 81.97 milliseconds indicates the time it takes for data packets to travel from the source to the destination in the DMVPN network. Lower latency is generally desirable, especially for real-time applications like video conferencing and online gaming, where high latency can lead to noticeable delays.

Jitter: Jitter represents the variation in latency or the inconsistency in the arrival time of data packets at their destination. A jitter value of 441.668 milliseconds suggests that the latency measurements for packets in your network vary considerably, potentially causing disruptions in real-time communication. Minimizing jitter is essential for ensuring a smooth and reliable network performance, particularly for voice and video traffic.

To optimize network performance, it's crucial to analyze and address the causes of high jitter and latency. This might involve optimizing network configuration, adjusting

Quality of Service (QoS) settings, or addressing network congestion issues. Additionally, monitoring these metrics over time can help you identify trends and make necessary adjustments to maintain a stable and responsive network.

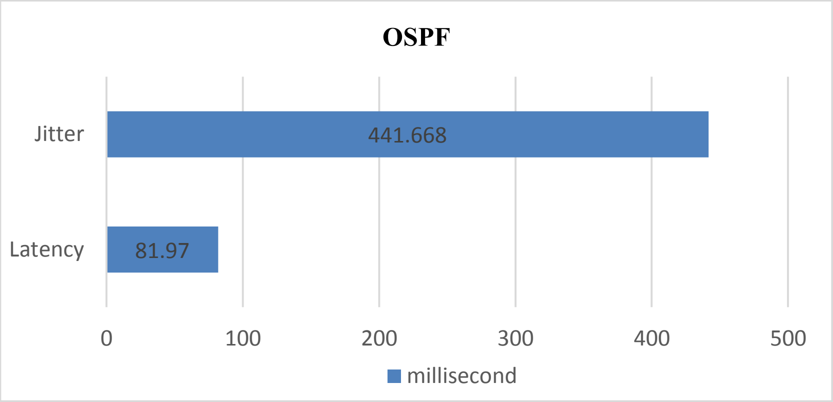

Fig. 6. OSPF- Latency and Jitter.

The graph in Figure 7 illustrates OSPF throughput results for both TCP and UDP connections.

TCP Throughput: The graph shows a TCP throughput value of 452 kilobytes. This value represents the data transfer rate achieved using the TCP (Transmission Control Protocol) communication protocol. TCP is known for its reliability and error-checking mechanisms but may have slightly lower throughput compared to UDP due to its additional control overhead.

UDP Throughput: The graph indicates a UDP throughput value of 1040 kilobits. This value represents the data transfer rate achieved using the UDP communication protocol. UDP is often used for applications that require low latency and can tolerate some packet loss, such as real-time video streaming or online gaming. It typically has higher throughput compared to TCP due to its minimal overhead.

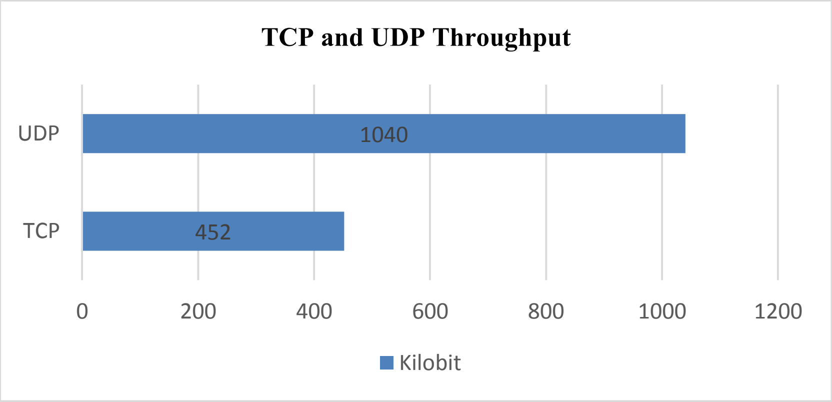

Fig. 7. OSPF- TCP and UDP Throughput.

4.4 BGP

As shown in the graph in Figure 8 graph the latency and jitter values in the DMVPN for the BGP protocol are 200.5 and 534.807 milliseconds respectively.

Latency: The graph shows a latency value of 200.5 milliseconds. Latency represents the time it takes for data packets to travel from the source to the destination in the network. A latency of 200.5 milliseconds indicates a delay in data transmission, which can impact the responsiveness of network applications. Lower latency is generally preferred, especially for applications that require real-time communication.

Jitter: The graph indicates a jitter value of 534.807 milliseconds. Jitter represents the variation in latency or the inconsistency in the arrival time of data packets at their destination. A high jitter value like 534.807 milliseconds suggests that the latency measurements for packets in your network vary considerably, which can lead to disruptions in real-time communication.

Having high latency and jitter values can affect the performance of applications running on the network, particularly those sensitive to delays, such as VoIP (Voice over IP) or video conferencing. Addressing the causes of high latency and jitter may involve optimizing network configurations, addressing network congestion, or implementing Quality of Service (QoS) policies to prioritize traffic.

It's essential to monitor and analyze latency and jitter values regularly to ensure the network meets the performance requirements of your applications and users.

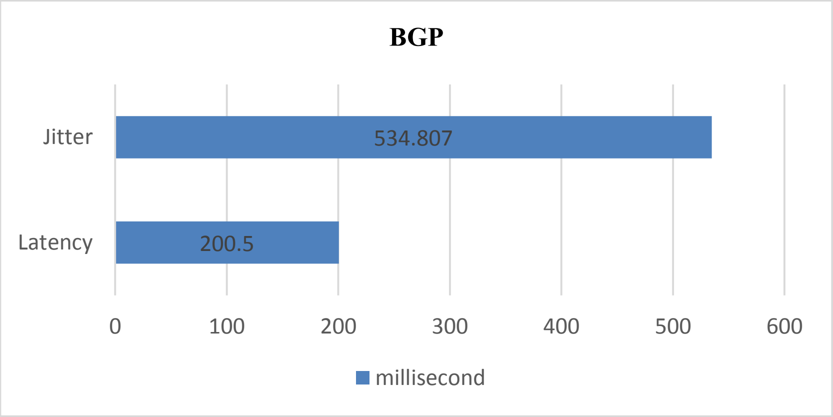

Fig. 8. BGP- Latency and Jitter.

In Figure 9, representing the performance of a DMVPN network using the BGP protocol, the graph displays significant throughput values for both TCP and UDP. The TCP throughput measures at 627 kilobytes, showcasing the data transfer rate achieved with the reliable but somewhat overhead-intensive Transmission Control Protocol. On the other hand, UDP demonstrates a higher throughput of 857 kilobytes, emphasizing its suitability for applications that prioritize low latency and can tolerate some packet loss due to its minimal overhead. These throughput values are essential metrics for evaluating network efficiency and aligning the protocol choice with the specific requirements of the applications running over the network.

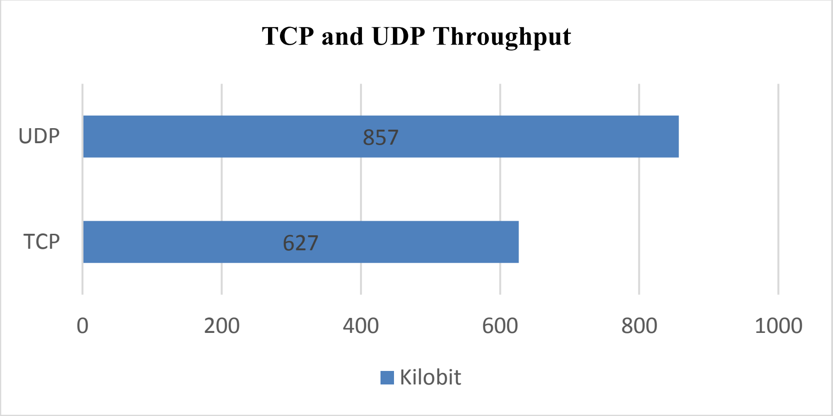

Fig. 9. BGP- TCP and UDP Throughput.

5 Comparison and Evaluation

It appears that different routing protocols exhibit varying performance characteristics in terms of latency and jitter:

- RIPv2: RIPv2 (Routing Information Protocol version 2) performs well in terms of latency, particularly in small networks, where it quickly selects paths with fewer hops, resulting in lower latency. However, it suffers from high jitter, which indicates inconsistent packet arrival times, possibly due to less robust mechanisms for handling variations in network conditions.
- EIGRP: EIGRP (Enhanced Interior Gateway Routing Protocol) demonstrates the best jitter results, likely due to its metric calculation, which takes into account factors like bandwidth, load, and delay to determine the most efficient network path. This leads to smoother and more predictable packet delivery. It's also worth noting that EIGRP usually offers low latency, although this aspect is not explicitly mentioned.
- OSPF: OSPF (Open Shortest Path First) ranks second in both latency and jitter. OSPF calculates efficient network paths, with a focus on minimum traffic and bandwidth-based link cost. While it may not have the lowest latency or jitter, it strikes a balance between performance and network optimization.
- BGP: BGP (Border Gateway Protocol) appears to have the longest latency and high jitter values. BGP is designed for interdomain routing on the Internet and prioritizes factors like path attributes and policies over speed, leading to comparatively higher latency and jitter.

Routing protocol selection should consider the specific network requirements and priorities. Low latency and low jitter are essential for real-time applications like VoIP and video conferencing, while other networks may prioritize factors like path stability and convergence speed. Figure 10 displays latency and jitter results for EIGRP, RIPv2, OSPF and BGP. Although RIPv2 achieved the best latency result, it ranks the worse when it comes to jitter, which make it unsittable selection for most of applications.

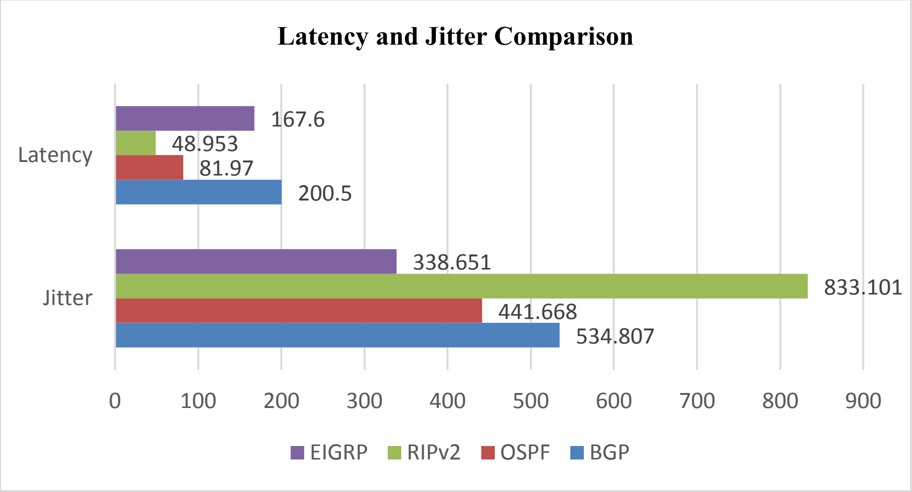

Fig. 10. Latency and Jitter Comparison.

In the Figure 11, it is notable that both EIGRP and OSPF achieve the highest throughput values for UDP. This outcome is attributed to the fact that both EIGRP and OSPF, despite being different routing protocols, consider bandwidth as a significant metric in their path selection algorithms. Consequently, they tend to choose paths that have higher available bandwidth, which is advantageous for UDP traffic, leading to similar high throughput results.

TCP Throughput: BGP stands out with the highest throughput for the TCP protocol. This is likely due to the fact that BGP operates as its own application layer protocol running over TCP. It uses TCP for reliable communication between routers, which can result in efficient and high-throughput data transfer when compared to other routing protocols that may use their own methods of communication.

The importance of considering the characteristics and requirements of specific applications when selecting a routing protocol. UDP-focused applications, such as real-time streaming or VoIP, benefit from protocols that prioritize high bandwidth paths, while the choice of routing protocol can also affect TCP-based applications based on their interaction with the protocol itself.

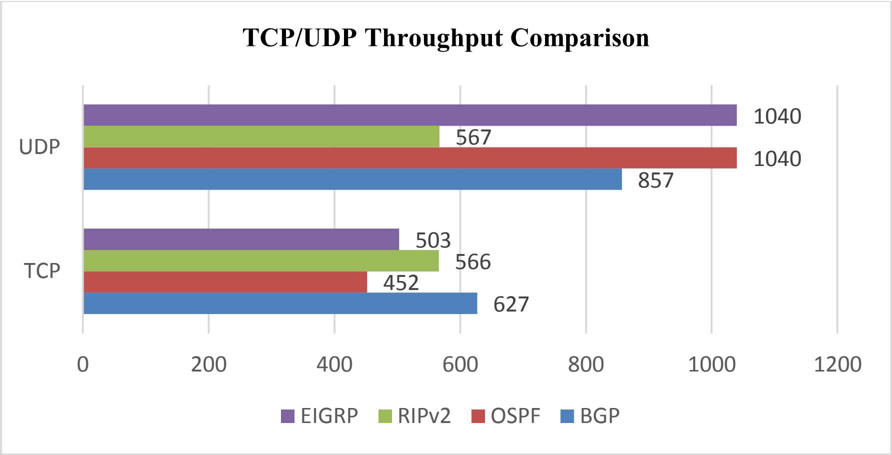

Fig. 11. TCP/UDP Throughput Comparison.

6 Conclusion

This paper evaluated the performance of various routing protocols for deploying a Dynamic Multipoint Virtual Private Network (DMVPN) network. We compared EIGRP, RIPv2, OSPF, and BGP based on key metrics including latency, jitter, and throughput for both TCP and UDP connections.

The analysis revealed that EIGRP performed the best results terms of latency and jitter. This makes EIGRP a strong choice for applications requiring real-time responsiveness within a DMVPN environment. EIGRP offers several advantages for DMVPN deployments, primarily because it is not constrained by the topological limitations often associated with link-state protocols. EIGRP, classified as a distance-vector protocol, possesses extensive capabilities that make it well-suited for DMVPN networks. It can summarize routing information dynamically, adjust metrics on the fly, and doesn't rely on the concept of areas. These characteristics simplify the deployment and scalability of EIGRP within a DMVPN topology, making it a practical choice for such environments.

OSPF also exhibited relatively good performance. While OSPF's throughput might be comparable to EIGRP in some scenarios, its higher latency and jitter could impact certain applications.

BGP, while renowned for its scalability, demonstrated higher latency and jitter when compared to EIGRP and OSPF protocols. This suggests that BGP might not be the most suitable option for latency-sensitive applications in a DMVPN setup. However, BGP remains a compelling choice for extremely large and complex DMVPN networks as BGP is renowned for its ability to scale gracefully to accommodate a large number of peers, making it a viable choice for networks with substantial complexities and routing requirements.

It's important to note that RIPv2's extremely high jitter makes it a less suitable choice for most DMVPN deployments due to its potential impact on real-time communication.

In conclusion, after this evaluation, EIGRP emerges as the most suitable choice for DMVPN deployments demanding low latency and jitter due to its superior performance in these metrics. BGP remains a strong contender for complex networks requiring exceptional scalability and advanced routing policies, while also offering overall good performance.

7 References

1. Cisco Systems, Configuring Dynamic Multipoint VPN with On-demand Routing, https://networkdirection.net/articles/routingandswitching/dmvpn/dmvpn-and-dynamic-routing, November 7, 2021.
2. Understanding Cisco Dynamic Multipoint VPN - DMVPN, MGRE, NHRP. (2022), www.Firewall.Cx. Retrieved November 5, 2021, visited April,2023
3. Polezhaev, P., Shukhman, A., & Ushakov, Y. (2015, October). Implementation of dynamically autoconfigured multiservice multipoint VPN. In 2015 9th International Conference on Application of Information and Communication Technologies (AICT) (pp. 211-215). IEEE.
4. Thorenoor, S. G. (2010, April). Dynamic routing protocol implementation decision between EIGRP, OSPF and RIP based on technical background using OPNET modeler. In 2010 Second International Conference on Computer and Network Technology (pp. 191-195). IEEE.
5. Jankuniene, R., & Jankunaite, I. (2009, June). Route creation influence on DMVPN QoS. In Proceedings of the ITI 2009 31st International Conference on Information Technology Interfaces (pp. 609-614). IEEE.
6. Chen, H. (2011, May). Design and implementation of secure enterprise network based on DMVPN. In 2011 international conference on business management and electronic information (Vol. 1, pp. 506-511). IEEE.
7. Guo, L., Liu, Y., & Liu, H. (2022, September). Research on Types of LSA in OSPF Multi-area Network Based on ENSP. In *2022 8th Annual International Conference on Network and Information Systems for Computers (ICNISC)* (pp. 55-59). IEEE.
8. Said, M. A., & Jadied, E. M. (2022). Analysis of IPSec Implementation on Dynamic Multipoint VPN Protocol Using Routing Border Gateway Protocol. *Building of Informatics, Technology and Science (BITS)*, *4*(2), 595-605.
9. Marah, H. M., Khalil, J. R., Elarabi, A., & Ilyas, M. (2021, June). DMVPN Network Performance Based on Dynamic Routing Protocols and Basic IPsec Encryption. In *2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)* (pp. 1-5). IEEE.
10. Masruroh, S. U., Widya, K. H. P., Fiade, A., & Julia, I. R. (2018, August). Performance evaluation dmvpn using routing protocol rip, ospf, and eigrp. In *2018 6th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-6). IEEE.
11. Angelescu, N., Puchianu, D. C., Predusca, G., Circiumarescu, L. D., & Movila, G. (2017, June). DMVPN simulation in GNS3 network simulation software. In *2017 9th international conference on electronics, computers and artificial intelligence (ecai)* (pp. 1-4). IEEE.
12. Tizazu, G. A., Kim, K. H., & Berhe, A. B. (2017, July). Dynamic routing influence on secure enterprise network based on DMVPN. In *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 756-759). IEEE.
13. Daud, F. A., Ab Rahman, R., Kassim, M., & Idris, A. (2018, October). Performance of encryption techniques using dynamic virtual protocol network technology. In *2018 IEEE 8th International Conference on System Engineering and Technology (ICSET)* (pp. 29-34). IEEE.