REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

DEVELOPMENT OF VIRTUAL PRIVATE NETWORK SYSTEM BASED ON PERFORMANCE COMPUTER NETWORK USING VARIOUS T RAFFIC SOURCES

Khidhab Ali Hammood AL-KRAINI

Master`s Thesis

Supervisor

Asst. Prof. Dr. Sefer KURNAZ

İstanbul, 2024

DEVELOPMENT OF VIRTUAL PRIVATE NETWORK SYSTEM BASED ON PERFORMANCE COMPUTER NETWORK USING VARIOUS TRAFFIC SOURCES

Khidhab Ali Hammood AL-KRAINI

Electrical and Computer Engineering

Master of Thesis

ALTINBAŞ UNIVERSITY

2024

The thesis DEVELOPMENT OF VIRTUAL PRIVATE NETWORK SYSTEM BASED ON PERFORMANCE COMPUTER NETWORK USING VARIOUS TRAFFIC SOURCES prepared by Khidhab Ali HAMMOOD and submitted on 00/00/2023 has been **accepted unanimously** for the degree of Master in Electrical and Computer Engineering.

Asst. Prof. Dr. Sefer KURNAZ

Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Sefer KURNAZ	Department of Electrical-Electronics Engineering, Altinbaş University	
Asst. Prof. Dr.	Department of Computer Engineering, Altinbaş University	
Asst. Prof. Dr.	Department of Computer Engineering, İstanbul Topkapi University	

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis.

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Khidhab Ali Hammood AL-KRAINI

Signature

DEDICATION

To My wonderful parents, who never stop in giving themselves in countless ways.

To the sources of hope, who stand by me in everything and lead me through the valley of darkness with light of hope and support… (My brothers, sisters, and all my family members)

To all the people in my life who touch my heart.

ACKNOWLEDGEMENTS

I owe everything to ALMIGHTY ALLAH, who is gracious, kind, and supreme. Whose grace and glory have provided me with brilliant instructors, loving parents, and supportive siblings. With quivering lips and tearful eyes, we give thanks to the HOLY PROPHET MUHAMMAD (P.B.U.H.) for awakening in us the core of faith in ALLAH and focusing ALLAH's mercy and compassion on him.

Asst. Prof. Dr. Sefer KURNAZ empathetic demeanor, friendly demeanor, animated directives, observant pursuit, scholarly critique, encouraging perspective, and enlightened helped me complete the work described in this book. Not only did his in-depth analysis and critical feedback enhance this dissertation, but they also helped me gain a deeper grasp of Agricultural Extension. I owe a great debt of gratitude to his unflagging support, enthusiastic curiosity, insightful criticism, and helpful advice throughout my education.

I'd want to take this opportunity to thank Prof. Dr. Mesut EVK, head of the Electrical and Computer Engineering department, for allowing me to finish my degree despite the many challenges I encountered. The members of my Dissertation Committee provided me with valuable feedback, for which I am really appreciative. While the committee's support and insight have undoubtedly made this study stronger and helped me avoid several mistakes, I bear full responsibility for any shortcomings that remain. The present distinction would have been nothing more than a pipe dream if it weren't for the spiritual and material support of my family, especially my late father, mother, brothers, and sisters, who I loved dearly. They were a beacon of hope for me in the stormy seas of my life's journey. It is because of the encouragement and inspiration I receive from my coworkers and friends that I am able to consistently deliver my best work. At last, I pray that ALLAH ALMIGHTY grants each of these individuals a life filled with joy and contentment (Ameen).

ABSTRACT

DEVELOPMENT OF VIRTUAL PRIVATE NETWORK SYSTEM BASED ON PERFORMANCE COMPUTER NETWORK USING VARIOUS TRAFFIC SOURCES

AL-KRAINI , Khidhab Ali Hammood

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Sefer KURNAZ

Date: 07 / 2024

Pages: 74

This study investigates the effects of implementing a Virtual Private Network (VPN on network performance, with a specific emphasis on throughput and time delay. The study entails the manipulation of connection types within three separate protocols, namely HTTP, FTP, and CBR, in order to examine the fluctuations in network performance metrics. The findings suggest that the integration of VPN has a minimal impact on the throughput of the Constant Bit Rate (CBR) protocol, whereas the File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP) protocols exhibit a decrease in throughput. Furthermore, the implementation of the VPN network results in a notable augmentation in the average time delay experienced across all protocols. The aforementioned findings provide significant contributions to the understanding of the intricate correlation between the implementation of VPNs and the performance of computer networks. These insights illuminate the complexities involved in ensuring security while simultaneously considering the potential compromises in network dynamics.

Keywords: VPN, FTP, HTTP, CBR, Delay, Throughput, Manhattan Grid.

ÖZET

ÇEŞİTLİ TRAFİK KAYNAKLARINI KULLANARAK PERFORMANS BİLGİSAYAR AĞINA DAYALI SANAL ÖZEL AĞ SİSTEMİNİN GELİŞTİRİLMESİ

AL-KRAINI, Khidhab Ali Hammood

Yüksek Lisans, Elektrik ve Bilgisayar Mühendisliği, Altınbaş Üniversitesi,

Danışman: Dr. Öğr. Üyesi Sefer KURNAZ

Tarih: 07/2024

Sayfa: 74

Bu çalışma, bir Sanal Özel Ağ (VPN) uygulamasının ağ performansı üzerindeki etkilerini, özellikle verim ve zaman gecikmesine vurgu yaparak araştırmaktadır. Çalışma, bağlantı türlerinin, HTTP, FTP ve CBR olmak üzere üç ayrı protokol dahilinde, sırayla değiştirilmesini içermektedir. ağ performansı ölçümlerindeki dalgalanmaları incelemek için bulgular, VPN entegrasyonunun Sabit Bit Hızı (CBR) protokolünün verimi üzerinde minimum etkiye sahip olduğunu, oysa Dosya Aktarım Protokolü (FTP) ve Köprü Metni Aktarım Protokolü (HTTP) protokollerinin olduğunu göstermektedir. Ayrıca, VPN ağının uygulanması, tüm protokollerde yaşanan ortalama zaman gecikmesinde dikkate değer bir artışa neden olmaktadır. Yukarıda belirtilen bulgular, VPN'lerin uygulanması ile performans arasındaki karmaşık ilişkinin anlaşılmasına önemli katkılar sağlamaktadır. Bu içgörüler, güvenliğin sağlanmasıyla ilgili karmaşıklıkları aydınlatırken aynı zamanda ağ dinamiklerindeki olası riskleri de göz önünde bulunduruyor.

Anahtar Kelimeler: VPN, FTP, HTTP, CBR, Gecikme, Verim, Manhattan Grid.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

CBR : Constant Bit rate

FTP : File Transfer Protocol

HTTP : Hypertext Transfer Protocol

IP : Internet Protocol

ISPs : Internet Service Providers

LAN : Local Area Network

NS2 : Network Simulator version 2

PEAP : Protected Extensible Authentication Protocol

PPTP : Point-to-Point Tunneling Protocol

SSTP : Secure Socket Tunneling Protocol

VLAN : Virtual Local Area Network

VPN : Virtual Private Network

WAN : Wide Area Network

1. INTRODUCTION

1.1 BACKGROUND

The growth and advancement of security systems have been propelled by the escalating demand for safeguarding privacy and ensuring the security of confidential information. In the contemporary era characterized by widespread digitalization, wherein communication and the exchange of data are pervasive, the imperative for robust firewalls to safeguard against theft or unauthorized intrusion has assumed paramount importance. In light of these challenges, VPN have emerged as a resilient solution for ensuring security across data networks. The noteworthy efficacy of VPN in mitigating privacy risks has garnered considerable attention from technology vendors [1,2].

The exponential expansion of internet and mobile communication has effectively enabled the transfer of extensive quantities of personal and commercial information across public networks. The sensitivity of this data has elicited concerns regarding privacy and the safeguarding of data. VPNs were initially developed with the purpose of establishing secure channels, commonly known as "tunnels," between designated nodes [3-4]. The quantity of nodes within the VPN may exhibit variability and can be expanded in accordance with networking necessities. The tunnels facilitate communication between predetermined nodes, thereby establishing a VPN.

The term "virtual" in the context of a VPN denotes the notion of hypothetical or conceptual connections within the extensive array of connections existing in a tangible network. VPNs are utilized in order to uphold privacy within computer networks [5]. These entities have the capability to encapsulate and safeguard distinct connections, providing different levels of confidentiality for diverse objectives. In contrast to conventional networks, VPNs operate through software rather than relying on dedicated hardware. Therefore, it can be argued that VPN protocols have a significant impact on the overall performance and efficacy of network security measures.

In order to assess the effectiveness of security measures, a range of established standards and metrics are utilized to measure the ability of VPNs to withstand network attacks [6,7].

The examination of the VPN's reaction to various network attacks allows for the observation of the system's capacity to uphold privacy and defend against potential risks.

The demand for privacy and secure data transmission has been a driving force behind the advancement of security systems, with VPNs emerging as a dependable solution. The inherent virtual characteristics of VPNs enable the establishment of secure channels for communication, eliminating the need for specialized hardware. This versatility and effectiveness of VPNs make them valuable tools in the implementation of network security measures. The ongoing advancement of technology necessitates the continued importance of VPNs in preserving the security of confidential data and upholding privacy within computer networks.

1.2 VIRTUAL PRIVATE NETWORK SYSTEM

A VPN system refers to a technological solution that facilitates the establishment of secure and confidential communication channels across public or untrusted networks, such as the internet [8]. A virtual encrypted tunnel is established between the user's device and a remote server or network, facilitating a secure pathway for the transmission of data and enabling access to resources.

The primary objective of a VPN system is to guarantee the preservation of data confidentiality, integrity, and authentication. When a user establishes a connection to a VPN, their data undergoes encryption prior to transmission across the internet [9]. The encryption employed in this context obfuscates the data in a manner that exclusively permits decryption and comprehension by the designated recipient, namely the VPN server. This procedure effectively mitigates the risk of unauthorized entities, such as hackers and individuals engaged in covert surveillance, from intercepting and decrypting the data being transmitted.

The fundamental elements and principles of a Virtual Private Network (VPN) system [10]:

a. Encryption: In VPN systems, data is encrypted at the sender's end and decrypted at the receiver's end using cryptographic algorithms, ensuring that only authorized parties can access the information.

b. Tunneling: VPNs use the concept of tunneling, where data packets are encapsulated within VPN-specific packets, enabling them to traverse public networks securely.

c. Protocols: VPNs utilize various protocols like OpenVPN, IPSec, L2TP, and PPTP to establish, manage, and secure the communication tunnel.

d. Authentication: VPN systems require users to authenticate themselves before gaining access, which can involve username and password authentication or the use of digital certificates for enhanced security.

e. Remote Access: VPNs enable secure remote access to resources within a private network, allowing remote users to access files, applications, and services as if they were physically present on the network.

f. Geolocation Spoofing: VPNs can hide a user's real IP address and assign them an IP address from a different location, enabling access to region-restricted content and bypassing censorship.

g. Business Applications: VPNs are widely used in corporate settings to facilitate secure communication between remote employees, branch offices, and the main office network, enhancing collaboration and enabling secure remote work.

The advantages of implementing a Virtual Private Network (VPN) system are manifold, as shows in the Figure 1.1.

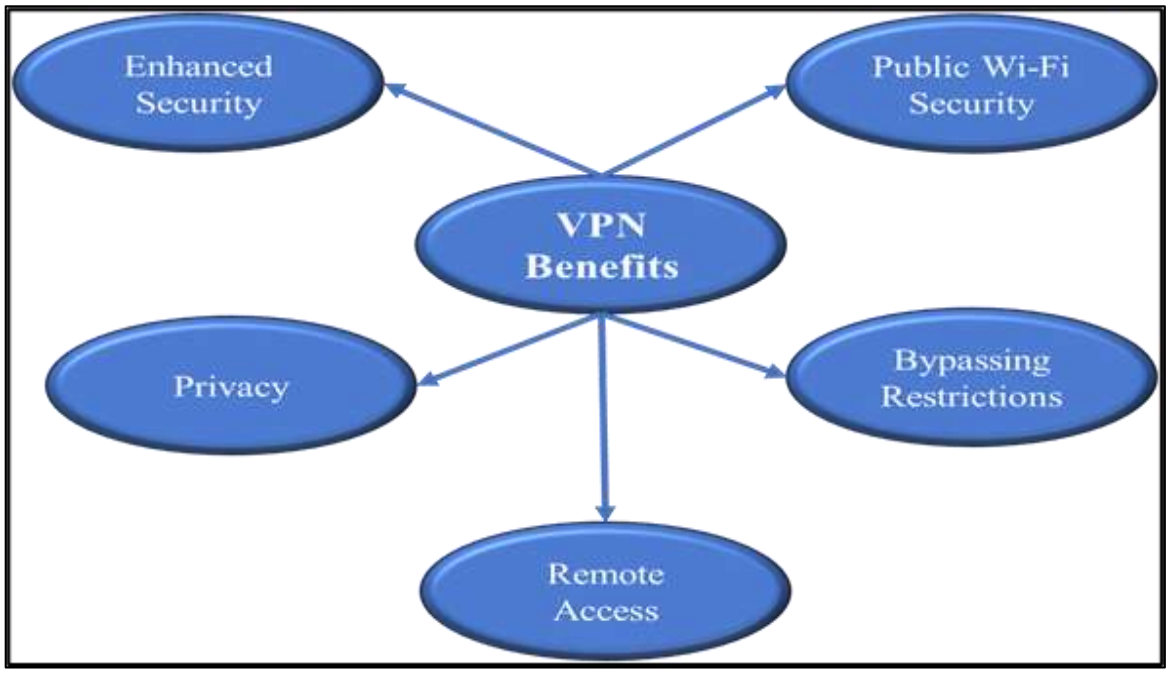

Figure 1.1: The Advantages of VPN.

Therefore, the utilization of a VPN system is an essential mechanism for guaranteeing the confidentiality and integrity of communication conducted over public networks. VPNs offer a robust solution for safeguarding sensitive information and facilitating secure remote access to resources through the implementation of data encryption, secure tunnel establishment, and authentication mechanisms [11]. Figure 1.2 shows (VPN) structure.

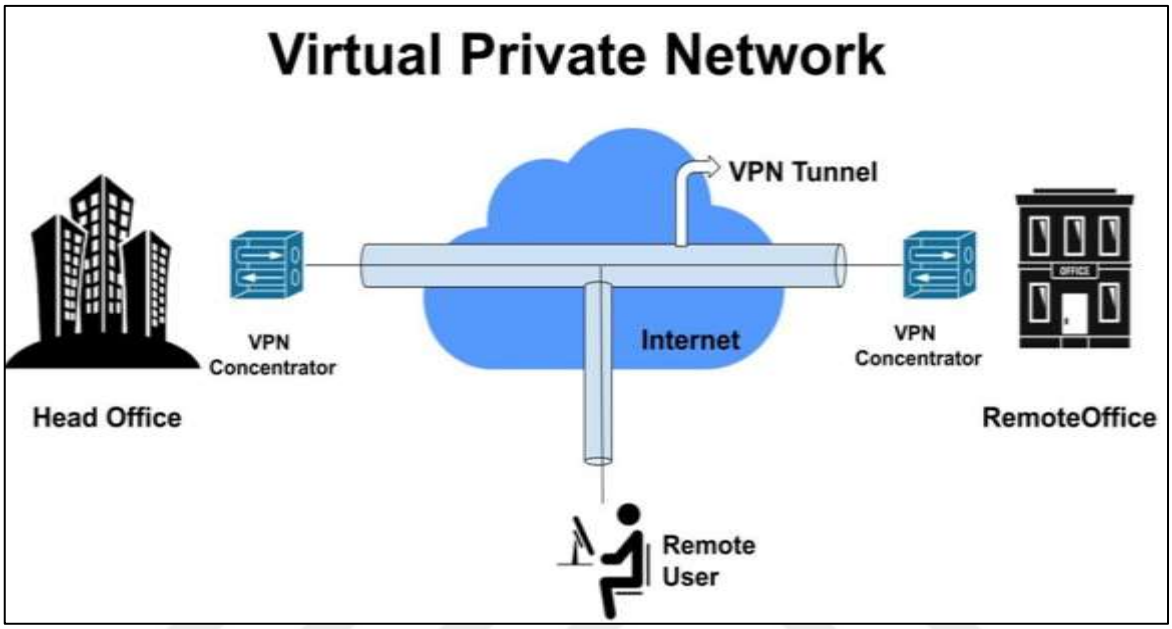

Figure 1.2 : VPN Structure.

1.3 PERFORMANCE OF NETWORKS

With the large amount of existing digital pornographic material, enabling the separation of pedophilia content from another is currently an arduous and complex Even trained experts need to carry out a thorough analysis of the seized material to obtain evidence against criminals in this analysis process, it is necessary to check all digital files (images and videos), demanding a lot of time and resources for this task. Because it is a repetitive process, the human factor can fail because of mental exhaustion.

The evaluation of computer networks pertains to the network's efficacy in terms of speed, efficiency, reliability, and overall effectiveness in facilitating data transmission and facilitating communication among devices or nodes. The performance of network design and management is a crucial factor that directly influences user experience, productivity, and the network's capacity to support diverse applications and services [12].

Several crucial factors that have an impact on the performance of networks are [13]:

a. Bandwidth: Represents the network's capacity to transmit data, higher bandwidth allows faster data transfer and reduced delays.
b. Latency: Refers to the time taken for data packets to travel from source to destination, lower latency is important for real-time applications.
c. Throughput: Measures the network's efficiency in data transfer over a given time period, influenced by bandwidth, latency, and congestion.
d. Reliability: Ensures consistent and error-free data delivery, minimizing packet loss and data corruption.
e. Packet Loss: Occurs when data packets fail to reach their destination due to congestion or errors, affecting data integrity and communication efficiency.
f. Scalability: The network's ability to handle increasing demands and growth without sacrificing performance.

Quality of Service (QoS): Prioritizes critical traffic to ensure better performance for time-sensitive applications.

1.4 TYPES OF ROUTING

The process of routing plays a pivotal role in the field of computer networking as it entails the determination of the most efficient path for data packets to traverse from their point of origin to their intended destination within a network. Various routing protocols and algorithms are employed in order to attain optimal and dependable data transmission [14]. Figure 1.3 shows three classifications of routing.

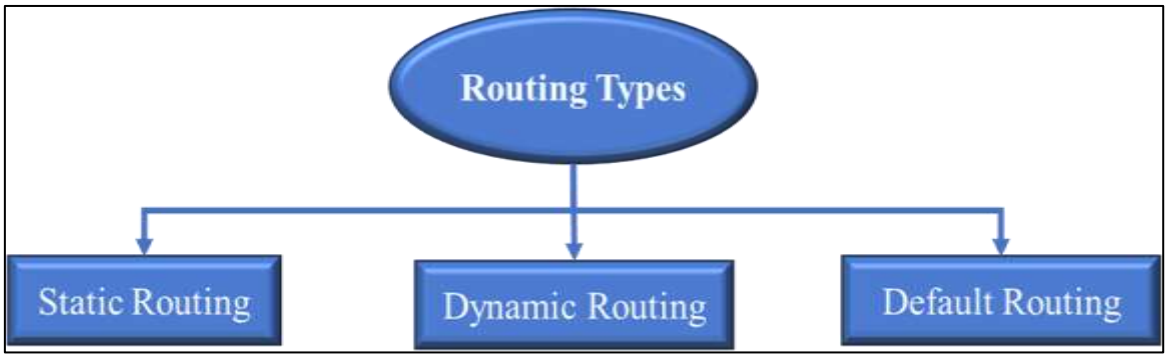

Figure 1.3: Types of Routing.

a. Static Routing: The process of static routing entails the manual configuration of the routing table on every network device. The network administrator establishes the routing paths for data packets by utilizing a pre-established collection of routes. Static routes remain unchanged unless they are explicitly modified by the administrator. Although the configuration process for static routing is straightforward, it lacks scalability and may not effectively accommodate dynamic network changes. Figure 1.4 explain this type of routing.

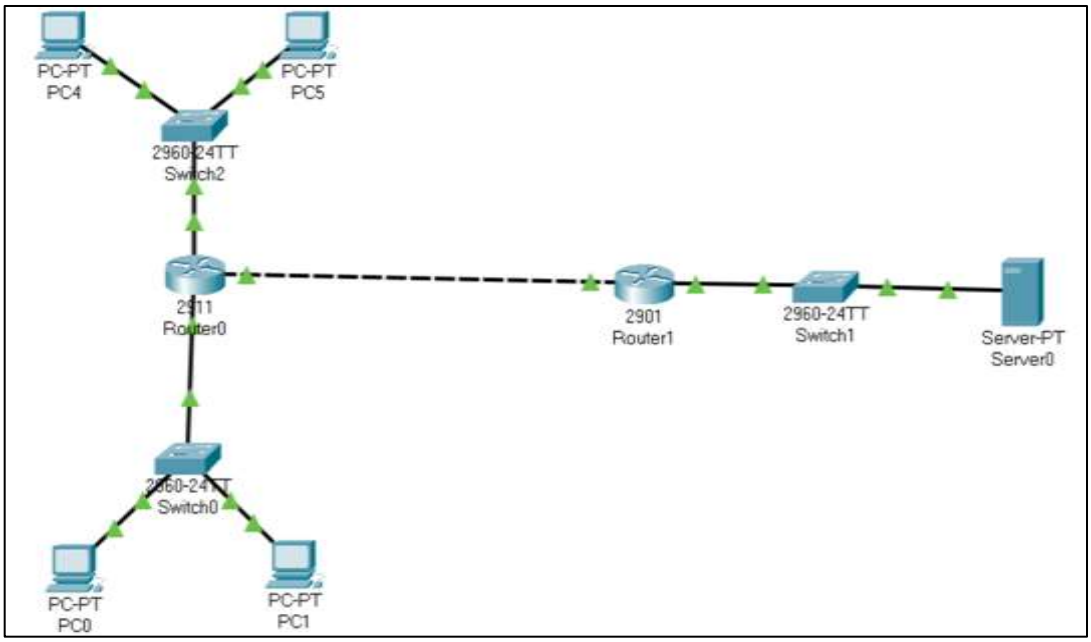

Figure 1.4: Explain Static Type of Routing.

b. Dynamic routing: protocols facilitate the automation of routing table updates and management. These protocols facilitate inter-router communication and the exchange of information pertaining to network topology and reachability. The routers utilize the dynamic information in order to ascertain the optimal route for data packets, taking into account the prevailing network conditions. Dynamic routing is considered to be a more adaptable and scalable approach compared to static routing, rendering it well-suited for larger networks that undergo frequent modifications. Figure 1.5 explain this type of routing.

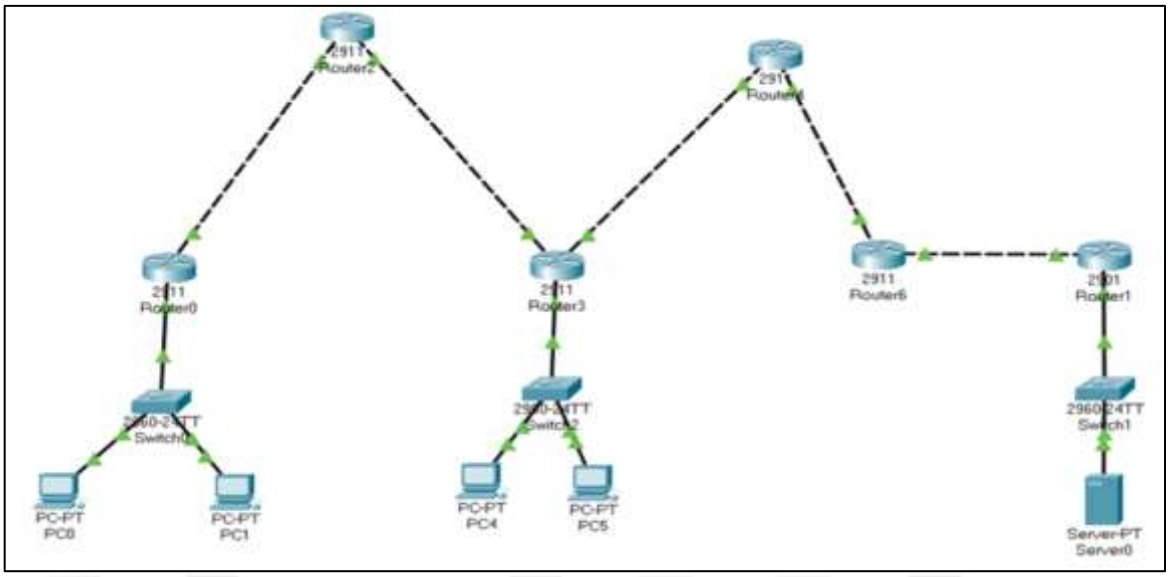

Figure 1.5: Explain Dynamic Type of Routing.

c. Default Routing: Default routing is a distinct form of routing in which a router directs packets to a default gateway in the event that it lacks an entry in its routing table for the intended network destination. Default routes are employed in situations where a specific route is not accessible, serving as a final option for directing traffic towards a default exit point. Figure 1.6 explain this type of routing.

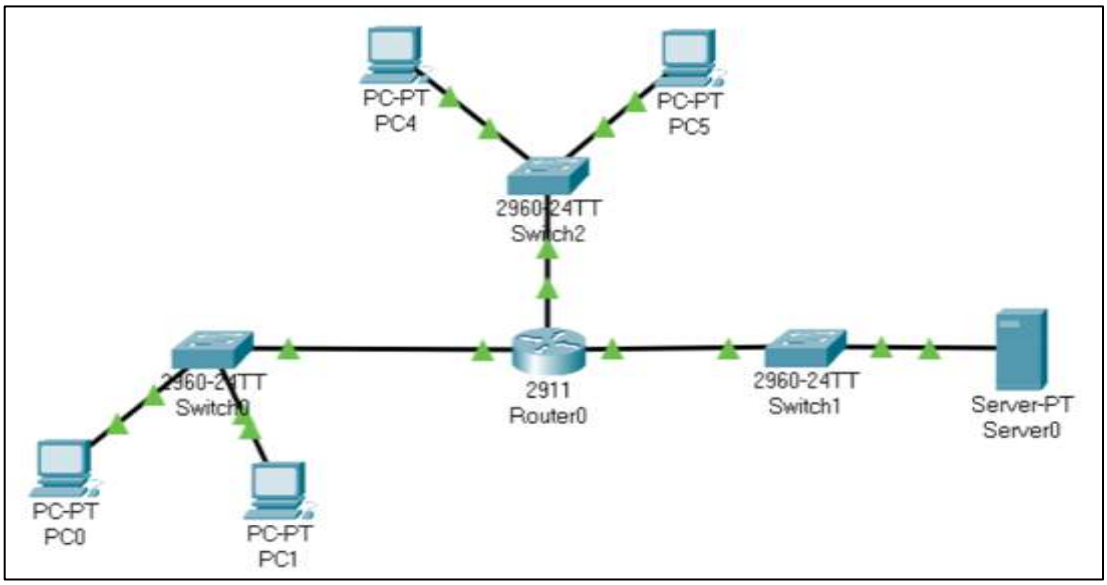

Figure 1.6: Explain Default Type of Routing.

Different types of routing possess distinct advantages and are applicable in various scenarios, depending on factors such as the scale, intricacy, and specific needs of the network. In order to optimize their network environment, network administrators must carefully choose the most suitable routing strategy.

1.5 PROBLEM STATEMENT AND SOLUTION

In today's interconnected world, the importance of secure and efficient communication over computer networks in the contemporary interconnected global landscape cannot be overemphasized. Virtual Private Network (VPN) systems have become a vital solution for establishing secure as well as private transmission channels over public networks, like internet. These networks have a crucial role in protecting sensitive data, guaranteeing data privacy, and facilitating uninterrupted access to resources from distant locations. In order for a VPN system to achieve optimal efficacy, it is imperative that it is constructed upon a resilient and high-capacity computer network infrastructure.

The problem statement in the work is to assess the influence of VPN implementation on a performance of computer networks under various traffic sources. The main challenge is to determine how the VPN system influences performance of network, particularly in statuses of throughput, latency, packet loss, as well as jitter when compared to the non-VPN scenario.

The solution involves developing a network simulation using the network simulation tool NS2 to create a representative network topology and generate traffic sources for the specified protocols. By implementing both VPN and non-VPN scenarios and measuring performance metrics, the study aims to provide insights into the efficiency of the VPN system in enhancing performance of network. Therefore, this project aims to contribute valuable insights into the design and implementation of Virtual Private Network systems for enhancing the performance of computer networks in real-world scenarios by conducting the simulation and analyzing the impact of VPN on network performance with different protocols.

1.6 AIM OF STUDY

The objective of this project is to create and assess a Virtual Private Network System that exhibits superior performance by utilizing diverse traffic sources. The primary focus will be on evaluating its efficiency, security, and overall network performance. We will explain these objective in the below:

a. Development of VPN: The objective of this research is to design and implement a VPN system utilizing a computer network architecture with superior performance capabilities. The system is designed to cater to the growing need for secure remote access, data encryption, and uninterrupted connectivity among businesses, organizations, and individual users.
b. Evaluation of VPN Performance: By simulating real-world traffic scenarios, this study aims to assess how the VPN system performs under different workloads. The evaluation will include measuring data transmission rates, latency, jitter, and overall system throughput to ensure that the VPN system meets the required performance metrics.
c. Understanding the Capabilities and Limitations of VPN: The examination of the VPN system's evolution and its assessment through diverse traffic sources will yield significant insights regarding its functionalities and constraints. The primary aim of work is to improve the protection of data privacy, facilitate remote access, and promote uninterrupted connectivity in the era of digitalization, thereby making a valuable contribution to the realm of secure and efficient communication.
d. Comparison of VPN and Non-VPN Configurations: this work is to conduct a comparative analysis of network performance across various traffic sources, specifically (CBR, FTP, HTTP). The study will encompass both VPN and non-VPN configurations. The objective of this work is to analyze how the VPN system influences network performance and potential trade-offs, considering various data loads and communication patterns.

1.7 THESIS ORGANIZATION

a. Chapter Tow: The second chapter will explain the literature related to the work and focus on the goals, solutions and problems encountered by the studies reviewed through the literature survey.
b. Chapter Three: The third chapter will introduce the methodology that was used to implement.
c. Chapter Four: The fourth chapter discusses the results obtained through the implementation of the proposed method.
d. Chapter Five : In this chapter, we will discuss the results with other studies, analyze them, and provide a comprehensive comparison between them and other studies
e. Chapter six : in this chapter, we will present the conclusions obtained from the methodology and the results obtained, which were compared with other result; as well as we present the future work.

Figure 1.7 shows the scheme through which this thesis is implemented.

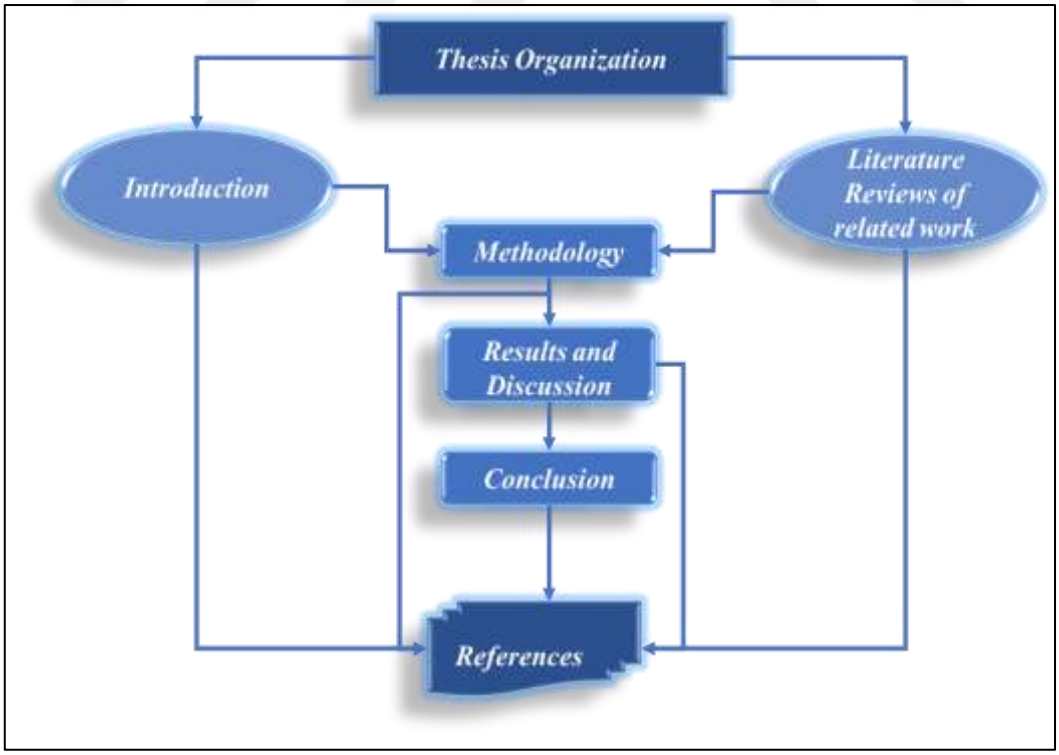

Figure 1.7 : The Scheme of Thesis Implementation.

2. LITERATURE REVIEW

Internet communication has become an essential component of contemporary infrastructure, facilitating the efficient operation of various applications and services [14, 15]. VPN systems are widely acknowledged as highly effective solutions for providing shared services over public network infrastructures. VPNs provide a cost-effective and efficient means of utilizing bandwidth, while also offering scalable, flexible, and secure remote connections. VPNs enable the secure transmission of network traffic by establishing a virtual secure line connecting two network sites. The performance and functionality of VPN networks are subject to the influence of multiple factors, such as the operating system, hardware devices, interoperability, and applied algorithms [16-18].

At present, VPNs have gained significant popularity as a prevalent approach for remote connectivity. In the present era, corporations are presented with the prospect of broadening their business activities by establishing offices in diverse geographical locations, spanning across multiple nations [19, 20]. VPNs offer a means of ensuring the secure transmission of various forms of data, such as file sharing and video conferencing, across the Internet. This enables individuals in both close proximity and distant locations from office branches and business associates to connect to an expanded corporate network [21, 22].

One of the primary advantages of VPNs lies in their inherent scalability, which facilitates seamless adjustment to accommodate diverse demands. This particular capability is particularly advantageous when establishing connections between the main office and newly established branch buildings, as it obviates the necessity of constructing new connections from the beginning. In contrast, VPNs make use of the pre-existing infrastructure provided by Internet Service Providers (ISPs), thereby conserving significant time and resources. The flexibility provided by this feature also allows for the smooth incorporation or adjustment of interconnected users, enabling companies to increase their capabilities without the need to expand their infrastructure [23].

Network-level VPNs are created using Layer 3 tunneling and encryption methods. One common approach involves using the IPsec tunneling and encryption protocol. Additionally, technologies like the Generic Routing Encapsulation (GRE) and Wire Guard protocols have also been utilized for this purpose [24, 25].

2.1 VPN IN STATIC AND DYNAMIC NETWORKS

This section offers a comprehensive summary of the main contributions related to applications and protocols within the scope of both dynamic and static networks.

2.1.1 Traditional Virtual Private Network (VPN) Solutions for Fixed Networks

There are several protocols available for the creation of secure Virtual Private Networks (VPNs). It is imperative to acknowledge that the mere implementation of a Virtual Private Network (VPN) does not provide any form of encryption or confidentiality to the data that passes over it.

A widely used VPN solution is the Layer 2 Tunneling Protocol (L2TP)/IPsec [26], which is known for its compatibility with modern operating systems and devices equipped for VPN capabilities. The L2TP protocol makes use of User Datagram Protocol (UDP) port 1701, along with Internet Protocol Security (IPsec) ports 500 and 4500, specifically for Network Address Translation (NAT) functionality. In contrast to SSL, L2TP necessitates intricate configuration, specifically port forwarding, when employing a firewall. SSL, on the other hand, has the capability to imitate regular HTTPS traffic by utilizing TCP port 443. In contrast, IPsec encryption is widely regarded as highly secure due to its utilization of robust algorithms such as AES, which has been widely recognized as a "de facto" standard. However, it is worth noting that IPsec employs a double encapsulation process, leading to a marginally reduced performance when compared to SSL.

OpenVPN, an open-source technology, employs the Open Secure Sockets Layer (OpenSSL) [27] and SSLv3/TLSv1 [28] library protocols (TLS for Transport Layer Security). This technology is developed by the OpenVPN company, headquartered in Pleasanton, CA, USA [Address: 6200 Stoneridge Mall Road, Pleasanton, CA 94588]. The discussed technology provides a robust and dependable VPN solution, known for its extensive customization options and the ability to function on any port, notably TCP 443.

By default, the OpenVPN protocol utilizes the User Datagram Protocol (UDP) on port 1194 for transportation. It's important to note that OpenVPN effectively evades attempts at blocking due to its use of TCP port 443, which allows its traffic to mimic HTTPS, posing a significant challenge for blocking measures. Additionally, OpenVPN utilizes the OpenSSL library, which offers a variety of encryption algorithms such as AES, Blowfish, 3DES, CAST-128, and others [29]. The speed of an OpenVPN connection depends on the chosen encryption level, though it generally demonstrates superior performance compared to IPsec in terms of speed.

The SSTP was advanced by SP1 [30]. Despite its recent availability for Linux platforms, the software continues to be predominantly associated with the Windows operating system. The Secure Socket Tunneling Protocol (SSTP) utilizes the SSL v3 protocol and functions in a manner comparable to OpenVPN. One notable benefit of SSTP is its ability to circumvent NAT firewall complications by utilizing TCP port 443. The incorporation of this software into the Windows operating system enhances its user-friendliness and dependability, thereby contributing to its perceived level of ease of use and stability.

PPTP, an networking protocol developed by Microsoft, finds widespread use for establishing VPN connections over dial-up networks. Historically, it has been the primary choice for private corporate networks. The protocol offers a variety of authentication methods, including Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) v2, ensuring security. To enhance security, PPTP can also be configured with Protected Extensible Authentication Protocol (PEAP). Nevertheless, for heightened security, it's advisable to explore alternatives like L2TP/IPsec [31] or Secure Socket Tunneling Protocol (SSTP) [30]. The Point-to-Point Tunneling Protocol (PPTP) provides a unified client compatible with various operating systems, including smartphones, and demands minimal computational resources. Its straightforward configuration allows for efficient data management.

2.1.2 Potential Strategies for Addressing Mobility in Virtual Private Networks (VPNs)

Extensive research within the academic literature has been dedicated to the topic of mobility within VPNs. Sustaining tunneling during mobile sessions requires consistent provision of session information via the VPN client. Proposed caching mechanisms [18)]aim to reduce the need for frequent data exchanges between clients and servers. These mechanisms work to mask disconnections and reconnections of VPN tunnels at the application layer, ensuring a smooth user experience.

A specific approach detailed in the mentioned study [19] involves modifying the OpenVPN protocol to address the issue of frequent client disconnections. This method incorporates packet caching to effectively minimize the risk of data loss, service degradation, and TCP retransmission-related actions like slow start, which can negatively impact overall throughput.

Figure 2.1 depicts a direct connection between the mobile application and the application server, while the linkage to the VPN client remains exclusive. The VPN session between the mobile client and the server is established through the utilization of the Wireless Transport Layer Security (WTLS) protocol [32].

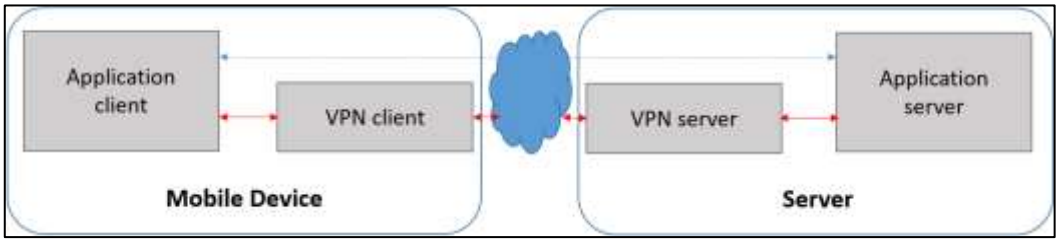

Figure 2.1: Split VPN Connection (Solid Lines) And Transparent VPN Connection (Dotted Lines) Shown as An Example.

The authors introduce a novel approach in their study [33] that facilitates the establishment of mobile OpenVPN sessions for users who are transitioning between WiFi cells. The primary concept pertains to the automatic reconfiguration of the OpenVPN tunnel in a prompt manner subsequent to handover events involving mobile users. The process involves informing the VPN server regarding the modified VPN tunnel context subsequent to the mobile user's acquisition of the new address. In contrast to caching techniques, this approach

prioritizes the reduction of packet loss rather than complete elimination. There exists a direct correlation between the quantity of lost packets and the duration of the handover operation executed by mobile users.

In [34], the authors introduce an extension to Secure SHell (SSH) designed to enable applications to maintain their sessions even during brief and temporary physical network disconnections. The core concept revolves around the ability to reinstate a previously established connection, albeit requiring the setup of new TCP connections upon reconnection. To achieve this, a buffer is employed to store data received from the previous socket. This data is then duplicated and retransmitted after establishing the new connection. However, this specific approach introduces a notable additional computational load, particularly during the process of renegotiating new session keys.

In [35], the authors build upon the work of the IETF Network Mobility working group [36] to present their Secure Network Mobility (SeNEMO) scheme. Extending the Mobile VPN described in reference [34], this scheme incorporates the Session Initiation Protocol (SIP) and integrates a dedicated framework for real-time applications within the VPN context. The effectiveness of the SeNEMO concept is established through rigorous analytical models and simulations.

Table 2.1 provides a concise overview of the primary advantages offered by VPNs within high-performance computer networks. VPNs offer a means of ensuring secure transmission of data, optimizing network performance, and facilitating remote access, all while effectively protecting sensitive information against potential cyber threats. They play a crucial role in safeguarding the privacy of users and facilitating uninterrupted connectivity in a worldwide, interconnected setting.

Table 2.1 : Summarizes the Main Benefits of Vpns in High-Performance Computer Networks.

Points	Explanation
VPNs operate across different network layers, offering versatile deployment.	VPNs function at various layers of the network stack for adaptable implementation.
VPNs create secure subsets within larger networks, enhancing security.	They establish isolated portions within big networks, boosting security.
VPNs enable secure communication between entities, ensuring encrypted data transmission.	They provide a safe channel for encrypted data exchange between separate parties.
VPNs establish encrypted virtual tunnels for secure data transmission over the Internet.	They create encrypted virtual pathways to securely transmit data over the Internet.
VPNs use encryption for data protection and provide IP address anonymization.	Employing encryption, they safeguard data and mask users' IP addresses.
VPNs improve efficiency and collaboration in geographically dispersed networks.	They enhance network efficiency and collaboration across diverse locations.
VPNs are designed for unsecured online environments to maintain data security.	Specifically designed for unsecured online spaces, they uphold data security.
VPNs ensure secure transmission of sensitive data, maintaining confidentiality.	They guarantee secure transmission of sensitive data, preserving confidentiality.
VPNs enable secure communication between partners, protecting data transmission.	They facilitate secure partner communication, safeguarding data in transit.
VPNs protect against unauthorized access and cyber threats, ensuring security.	They guard against unauthorized access

2.2 VPN APPLICATIONS FOR HANDLING MOBILITY

Wire-Guard is a newly developed open-source software that has been specifically designed for the purpose of creating highly efficient VPNs within the information technology (IT) industry. The system provides a secure means of regulating access to network resources and effectively segregates the flow of user data from external entities. WireGuard, a software known as the "Next Generation Kernel Network Tunnel," has been seamlessly incorporated into the Linux kernel, thereby enabling its utilization across various interconnected devices. WireGuard distinguishes itself through its comparatively lightweight nature and minimal hardware prerequisites. Its streamlined codebase contributes to heightened levels of security and improved performance. The system utilizes Cryptokey Routing, a method in which IP addresses are allocated in a one-to-one correspondence with peer public keys, thereby guaranteeing the secure decryption of packets. The primary advantage of WireGuard is its compact codebase, which ensures enhanced security and reduced energy consumption. The security features of the software have undergone thorough analysis, encompassing aspects such as confidentiality, authentication, and resilience against malicious attacks.

WireGuard demonstrates a wide range of applicability in the realm of mobile and Internet of Things (IoT) technologies, providing seamless connectivity while transitioning between Wi-Fi and mobile networks. The efficacy of this technology has been substantiated through a range of studies, including a study conducted at African universities, which effectively highlighted its robust data security features in authentic VPN situations. Furthermore, the importance of WireGuard in the context of 5G network slicing becomes apparent, as it offers tangible benefits through the deployment of virtualized network functions. The extensive utilization of the software is apparent, as it has been incorporated into a diverse range of devices, encompassing unmanned aerial vehicles (UAVs), RaspberryPi, and sophisticated Internet of Things (IoT) sensor systems. Users have the opportunity to enhance the security of their network by integrating firmware solutions like OpenWRT and employing MQTT as a reliable intermediary for transmitting data securely. In the contemporary IT environment, WireGuard has established itself as a highly effective and secure VPN solution, owing to its strong capabilities and seamless integration.

Figure 2.2 depicts a prevalent situation wherein a VPN, potentially implemented via WireGuard, is employed to establish a connection between an Unmanned Aerial Vehicle (UAV) equipped with either an LTE or 5G connection, as well as the corresponding GCS, which may likewise possess an LTE or/and 5G connection.

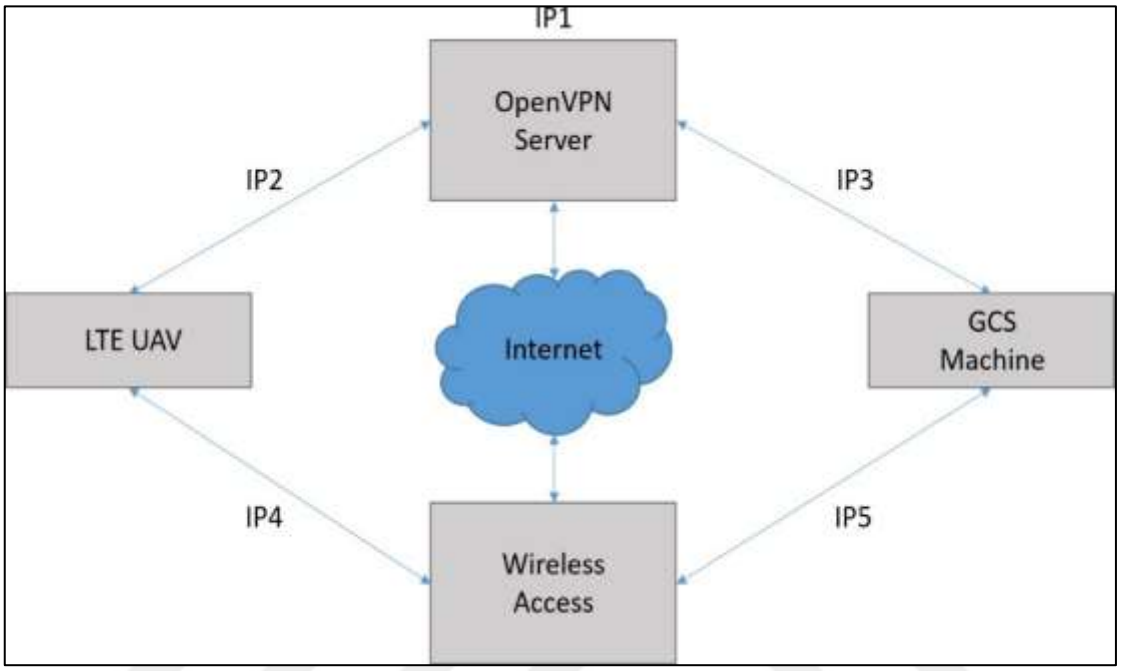

Figure 2.2: VPN Management for an LTE-UAV And GCS Device.

In this scenario, both the UAV and the GCS have IP addresses that were assigned by their respective service providers. Consequently, direct communication between these entities is rendered impossible. Figure 4 depicts the use of a VPN by organizations in order to establish effective management and assure secure communication. The OpenVPN service is hosted on a server with a fixed IP address (IP1), whereas the UAV (IP4) and GCS (IP5) obtain their IP addresses from the LTE Wireless Network. On the (UAV and GCS) devices, OpenVPN clients are executed, permitting them to obtain VPN addresses. IP2 is allocated to the UAV, while IP3 is assigned to the GCS. The use of VPN addresses establishes a shared virtual network for the (UAV and GCS), allowing for direct and seamless communication between the two entities. The VPN is an efficient means of establishing a connection between the UAV and GCS, allowing for the transmission of data in a secure and uninterrupted manner.

As depicted in Figure 2.3, the authors of [37] present a secure interconnection framework for Unmanned Aerial Vehicles (UAVs and GCS) using VPN technology. The study provides

evidence of the viability of implementing a 4G connection to establish a direct connection between a drone and a data server, as indicated by the green dashed line. This connectivity enables the storage of data of interest, such as audio, video, and telemetry, for subsequent processing and analysis. In addition, a secondary VPN connection, denoted by the red long dashed line, is established between the UAV and GCS to enable FPV operations in both Line of Sight (LOS) and Beyond Line of Sight (BVLOS) scenarios.

The efficacy of the proposed VPN-based method in establishing a robust and efficient connection over long distances with a substantial data transmission capacity is supported by the findings of their empirical investigations, which involved the streaming of video and audio content [38]. The architecture enables the secure transmission of data by establishing a VPN tunnel between the public Internet as well as the GCS. This ensures a seamless and protected UAV scenarios [39], this study emphasizes the importance of employing VPN technology to improve the communication and data transfer between (UAVs and GCSs) in a dependable and secure manner.

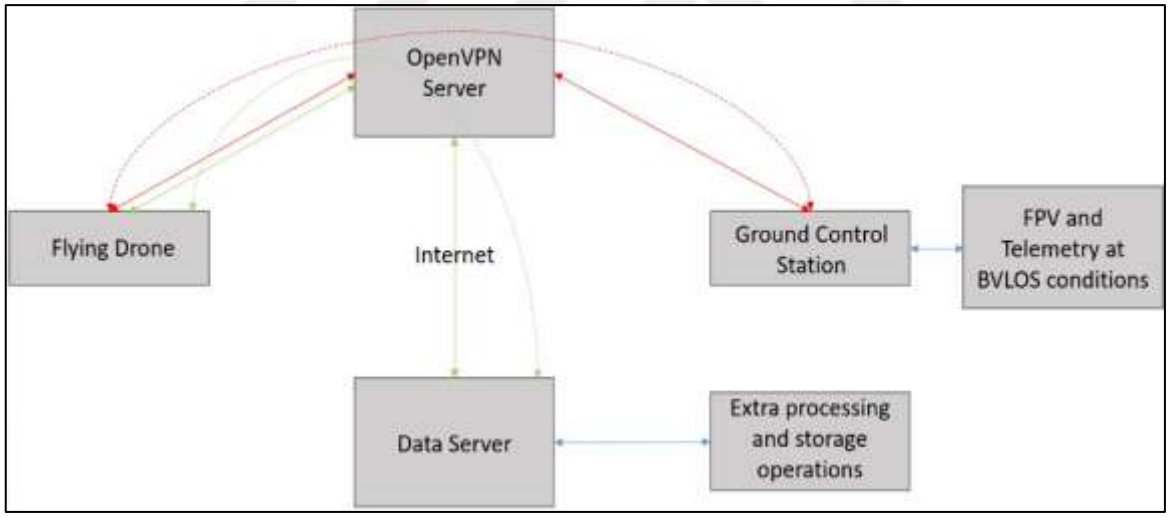

Figure 2.3: A Schematic of The VPN Setup Discussed In.[40]

2.3 VIRTUAL PRIVATE NETWORKS: SECURITY CONCERNS AND SOLUTIONS

In today's network infrastructures, VPN functionalities have become widely embraced as integral components across diverse network devices. The inclusion of a firewall stands out as a pivotal factor in upholding network security within the framework of VPN safeguarding.

To enhance the efficacy of VPN security measures, contemporary security solutions propose the incorporation of firewalls alongside advanced Intrusion Detection Systems (IDSs) [41] or Intrusion Prevention Systems (IPSs) [33,42]. These amalgamated systems offer comprehensive capabilities for identifying and mitigating potential risks within the VPN environment. In the forthcoming sections, a succinct overview of Intrusion Detection Systems (IDSs) will be presented, followed by an exploration of their seamless integration with VPNs to bolster the overall security of computer networks.

2.3.1 IDSs, IPSs, and IDPSs are Varieties of Intrusion Detection and Prevention Systems.

An Intrusion Detection System (IDS) encompasses both software components and hardware devices equipped with specialized embedded software. Its primary purpose is to examine the incoming and outgoing network traffic of a specific network. The primary function of an IDS within a network, typically a Local Area Network (LAN), is to consistently monitor network traffic for indications of potentially harmful or unauthorized activity targeting any host, be it a client or server within the network. When the IDS detects potential threats or anomalies, it has the capability to generate alerts and log files, which can offer valuable insights to network administrators. In addition, IDS have the capability to retrieve and store pertinent data from relational databases pertaining to network traffic that is deemed noteworthy in terms of security. These capabilities enable network administrators to adopt a vigilant and proactive stance in protecting the network against potential security breaches.

An Intrusion Prevention System (IPS) refers to a software or hardware component that is seamlessly incorporated into a network infrastructure, aiming primarily to impede and counteract any attempted attacks directed towards the network. The IPS implements a range of proactive measures, such as the termination of packets or sessions, the initiation of session resets, and the inclusion of the offending host in a blacklist. The IPS effectively enhances the network's security and aids in the mitigation of potential risks and vulnerabilities by promptly addressing potential threats.

In the domain of network security, (IDS and IPS) are two interconnected technologies that can effectively work together to augment the overall level of protection. These entities operate by utilizing predetermined algorithms established by the network, allowing them to

activate notifications or implement precautionary actions upon identification of particular patterns within the network's traffic. The establishment of a robust hybrid system, referred to as (IDS and IDPS), is achieved by integrating the functionalities of both (IDS and IPS). The provided solution offers a comprehensive and robust defense mechanism by efficiently detecting potential threats through intrusion detection and promptly implementing preventive measures to counteract any malicious activities. The incorporation of IDS and IPS) within an IDPS facilitates a proactive strategy in protecting the network against diverse security threats and potential unauthorized access attempts.

2.3.2 Combining VPNs with IDSs and IPSs

A considerable body of scholarly research has been dedicated to investigating the augmentation of VPN security by incorporating (IDSs and IPSs). As an example, the study conducted by [41] addressed the issue of TCP SYN-based Denial-of-Service attacks targeting HTTP servers. The researchers proposed the implementation of IDS to promptly identify such attacks, along with the utilization of ACL to effectively prevent them. The incorporation of a VPN with an IPS facilitates the automated prevention of such attacks. The primary objective of the study conducted in reference [33] was to deploy an IPS within wireless networks by utilizing WBVPN. This implementation aimed to establish a singular pathway for the analysis of network traffic and the prevention of unauthorized activities. The efficacy of the proposed scheme was demonstrated by the authors through the utilization of real-case scenarios. A different study introduced a novel framework [42] that aims to optimize the synchronization of security services and minimize the associated overhead traffic. This framework specifically focuses on addressing security concerns within networks that rely on VPN technology. These endeavors aid in strengthening VPNs against possible risks and guaranteeing a more secure and resilient network environment.

3. MATERIALS AND METHODS

3.1 INTRODUCTION

In this chapter centers on the exposition of methodology and model that we have developed. This particular model functions in conjunction with three distinct protocols, specifically (CBR, FTP, and HTTP). The aforementioned protocols serve a crucial function in coordinating and overseeing the transmission of data within networks. In order to thoroughly assess the effectiveness of our model, we have chosen to employ a network configuration that exhibits a Manhattan topology. This decision enables the establishment of a systematic and regulated setting for our assessments. The study presented in this paper encompasses two separate scenarios, each of which provides unique and valuable insights.

The initial scenario has been formulated to incorporate the utilization of a VPN. The inclusion of this integral component serves to augment the security and isolation measures within our network, thereby bolstering data privacy and facilitating controlled access. On the contrary, the second scenario depicts a network devoid of a VPN. The utilization of the "non-VPN" configuration permits us to establish a direct juxtaposition with the VPN-enabled situation, thereby elucidating the ramifications of VPN integration on network efficacy.

The subsequent sections will provide a more comprehensive analysis of the intricate composition of each phase within our proposed framework. Our objective is to present a thorough and enlightening explanation of our methodology and its subsequent application in these two separate scenarios, with the intention of providing a comprehensive understanding.

3.2 VIRTUAL PRIVATE NETWORK (VPN)

VPN is designed for enhancement of security over the networks using software only. Deployment of VPN technology implies implementation of software based network between two parties (or more) over the bigger physical network. VPN technology can be realized in many applications such as internet (i.e. web applications), intranet (local/private network made between particular candidates for preforming a specific task where this network is separated from the public internet network).

The development of internet and computer technologies have motivated the security engineers to design virtual network that can be operated over any physical network and can be used by any number of subscribers to protect the connection privacy [43]. As an example of VPN are the banking applications. Since all the banking activates (at least those related to the bank clients) are made over the internet and folded under the so-called internet banking. The internet banking is susceptible for malicious activities since it is operating over a public network like internet. Banks have tried many (methods) to protect the online transactions. Those methods are categorized into several groups and can be generalized according to their existence. Therefore, there are some that security and precautions implemented at the end users handset to ensure [44].

That only the authorized person can access to the account, this implemented security features on the banking applications such as face recognition, finger impression, eye recognition, etc. As well as the network can be upgraded to accommodate a safe connection between the user (client) and the bank server. The network upgrading is the most important step to ensure safety of connection and prevent malicious activities. Banks are adopting a virtual network that encapsulate the active transaction between the client and banks servers, this virtual encapsulation is termed as VPN. The VPN creates a private and secure connection, known as tunnels, through systems that use the data communication capability of an unsecured and public network like the Internet. VPNs employ robust protocols to establish confidential communication channels across the Internet. Virtual connections are established through the utilization of the Internet, facilitating the linkage of private corporate networks with remote business sites or employees working from home offices. When making a decision on a secure communication method, organizations frequently weigh the merits of two commonly employed protocols, namely IPsec and SSL, as illustrated in Figure 3.1. Every protocol exhibits its own set of advantages and disadvantages, with the final decision depending on various factors such as the infrastructure of the corporate network, specific security requirements, cost considerations, and reliability demands.

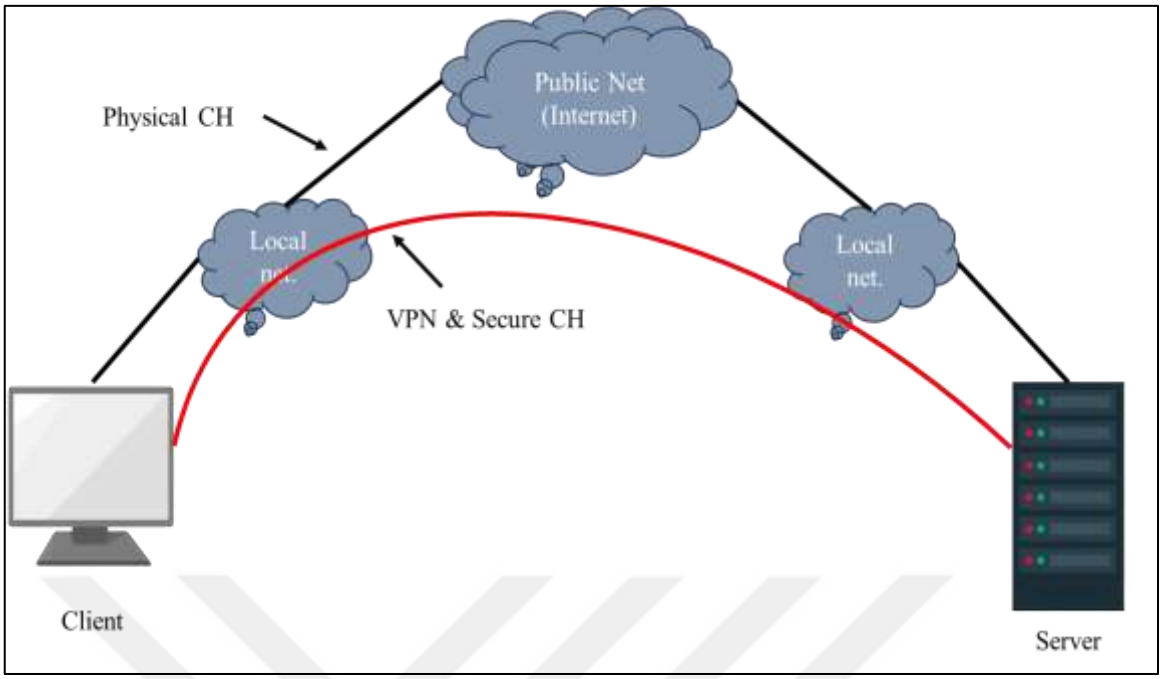

Figure 3.1: An Overview of the VPN Network's Foundational Architecture.

Many enterprises choose to implement IPsec VPNs over the internet as a cost-effective alternative to private WAN connections, leased lines, and long-distance phone charges, which can be prohibitively expensive. Businesses and enterprises can achieve significant cost savings by opting for IPsec VPNs. Additionally, these VPNs contribute to increased productivity through the facilitation of smooth business-to-business interactions, the augmentation of sales efforts, and the optimization of customer service management processes. IPsec provides an additional advantage by facilitating secure and convenient access to an organization's network resources for remote employees, including those operating from home offices or remote locations, via remote internet connections.

3.3 PROPOSED MODELS

A Virtual Private Network (VPN) is established with the purpose of establishing secure tunnels for connections over public networks, thereby guaranteeing that only authorized participants within the VPN are able to engage in these connections. The aforementioned method of safeguarding has exhibited efficacy in maintaining connectivity within vast networks, such as the internet. Networks consist of a wide range of activities, each of which may have unique requirements in terms of bandwidth and routing.

Various applications may necessitate different levels of throughput, whereas certain applications function in real-time situations where minimizing packet transmission delay is of utmost importance. The seamless incorporation of VPN technology necessitates meticulous coordination with other network configurations, particularly those that prioritize critical factors such as time delay and throughput. Network planners must prioritize both network security and performance equally. Hence, it is imperative to conduct a thorough investigation into the effects of VPN on various network performance metrics in order to establish a robust network. In order to examine the impact of VPNs on network performance, two models were constructed utilizing Network Simulator (Version 2).

In the second scenario, a network consisting of ten nodes is implemented and distributed in the form of a Manhattan grid, as depicted in Figure 3.2. The Manhattan model employs a grid road topology. It functions most effectively in areas where streets are arranged in an organized manner. The model involves the distribution of mobile nodes in either a horizontal or vertical direction on an urban map.

In each of the models mentioned below, network is examined by realizing performance metrics throughput and time delay, ultimately results from both proposed models are compared.

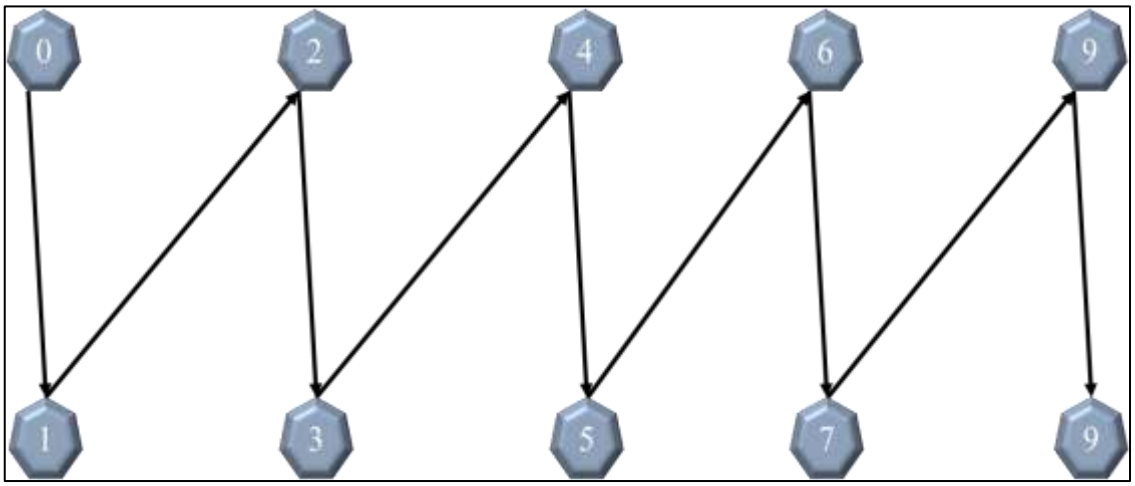

Figure 3.2: Nodes Connected in Manhattan Grid Topology Without VPN.

3.3.1 Manhattan Topology Model

The Manhattan topology, also known as a grid or lattice topology, is a network architecture that bears resemblance to the structured and perpendicular grid-like street layout commonly observed in urban areas such as Manhattan. Within the domain of computer networks, the Manhattan topology replicates the grid-like structure by organizing network nodes and connections in a comparable manner.

In a Manhattan topology, the network nodes are arranged in a grid-like structure resembling the layout of streets in Manhattan, with horizontal and vertical connections between adjacent nodes. Several crucial guidelines must be followed when constructing this network.

a. Node Placement: In the architecture of a network, the placement of network nodes, which encompass computers, routers, and devices, is akin to the arrangement of intersections formed by horizontal and vertical lines, resembling the grid-like structure of streets within a city. Every individual node within the system is intricately linked to its adjacent nodes, resulting in the formation of a highly organized and coherent pattern.
b. Connections: Network links or connections are established in a manner that mirrors the layout of streets in a city grid, with horizontal and vertical lines serving as the primary means of connectivity. This guarantees that every node is directly linked to its adjacent nodes.
c. Predictable Paths: The predictability and determinability of data transmission paths are notably high. The transmission of data occurs along predetermined pathways, typically adhering to a linear trajectory along the grid lines.
d. Scalability: The process of incorporating additional nodes into the network is relatively uncomplicated, as they can be seamlessly integrated into the preexisting grid structure.
e. Controlled Layout: The implementation of an organized layout offers several advantages in the realm of network management, troubleshooting, and maintenance. This is primarily due to the regular and systematic structure that it provides.
f. Limited Redundancy: Although the Manhattan topology presents a clear and regulated design, it may exhibit restricted redundancy. The occurrence of a solitary link failure has the potential to result in the isolation of a network segment.

The utilization of Manhattan topologies is prevalent in situations that prioritize predictability and simplicity, such as sensor networks, wireless mesh networks, and specific variations of

ad-hoc networks. These protocols offer a clearly defined framework for the transmission of data and can prove to be highly advantageous in the realms of research and experimentation. Additionally, they serve as valuable tools for examining network dynamics within controlled environments. Within the framework of our research, the utilization of a Manhattan topology facilitates the establishment of a regulated setting for the assessment of the efficacy of a VPN system across diverse traffic origins. As shown in Figure 3.2.

3.3.2 First Scenario without VPN

The wireless network is comprised of ten immobile nodes that are organized in a Manhattan grid topology. This implies that the placement of these nodes occurs at the points where horizontal and vertical lines intersect, thereby replicating the arrangement of streets in a city grid. Every individual node possesses wireless communication capabilities, enabling the seamless exchange of data without the necessity of physical connections.

At the outset, the network is established in the absence of any VPN configuration. This scenario represents the fundamental state in which data is transferred directly between nodes without any supplementary encryption or tunneling facilitated by a VPN.

The term "throughput" pertains to the velocity at which data is effectively conveyed between interconnected nodes within a network. In the present investigation, the objective is to assess and juxtapose the mean throughput throughout the entirety of the network, with regards to various protocols namely (CBR, HTTP, and FTP). This task encompasses the transmission of data packets utilizing specified protocols and the computation of the mean rate at which these packets are successfully received at their designated endpoints. The metric of throughput offers valuable insights into the network's ability to efficiently manage data transmission across various protocols.

Time delay, also referred to as latency, denotes the temporal duration required for a data packet to traverse from the originating node to the receiving node. The desirability of lower latency stems from its correlation with faster data transmission. The objective of this study is to assess and contrast the mean time delay associated with data transmission across the network for three distinct protocols, namely (CBR, HTTP, and FTP). The task at hand entails the computation of the mean latency for data packets that are transmitted utilizing each respective protocol.

The task at hand entails conducting a comparative analysis of three distinct protocols, namely (CBR , HTTP ,and FTP), within the given scenario. Each of these protocols fulfills a distinct purpose. The utilization of CBR is frequently observed in real-time applications that necessitate a steady and uninterrupted flow of data. HTTP, on the other hand, is predominantly employed for web browsing purposes, while FTP finds its primary application in facilitating file transfers.

By conducting a comparative analysis of the average throughput and time delay of these three protocols, valuable insights can be obtained regarding the performance of each protocol within the wireless network. This comparative analysis facilitates comprehension of the respective merits and demerits of each protocol with regard to the efficiency and speed of data transmission.

The initial comparison is conducted in the absence of VPN, serving as a baseline for assessing the effects of implementing a VPN in the subsequent phases of the second scenario. A VPN enhances the level of security and privacy in the transmission of data, potentially impacting variables such as throughput and latency.

Hence, the present scenario pertains to the assessment of the operational efficiency of a wireless network comprising ten immobile nodes organized in a Manhattan grid configuration. This study aims to analyze and compare the average throughput and time delay of various data transmission protocols (CBR, HTTP, and FTP) within the given network. This comparative analysis will provide a basis for conducting further research on the implementation of VPN, wherein the impact of VPN on network performance metrics will be investigated within the context of identical protocols. Figure 3.3 shows the flowchart to explain the first scenario.

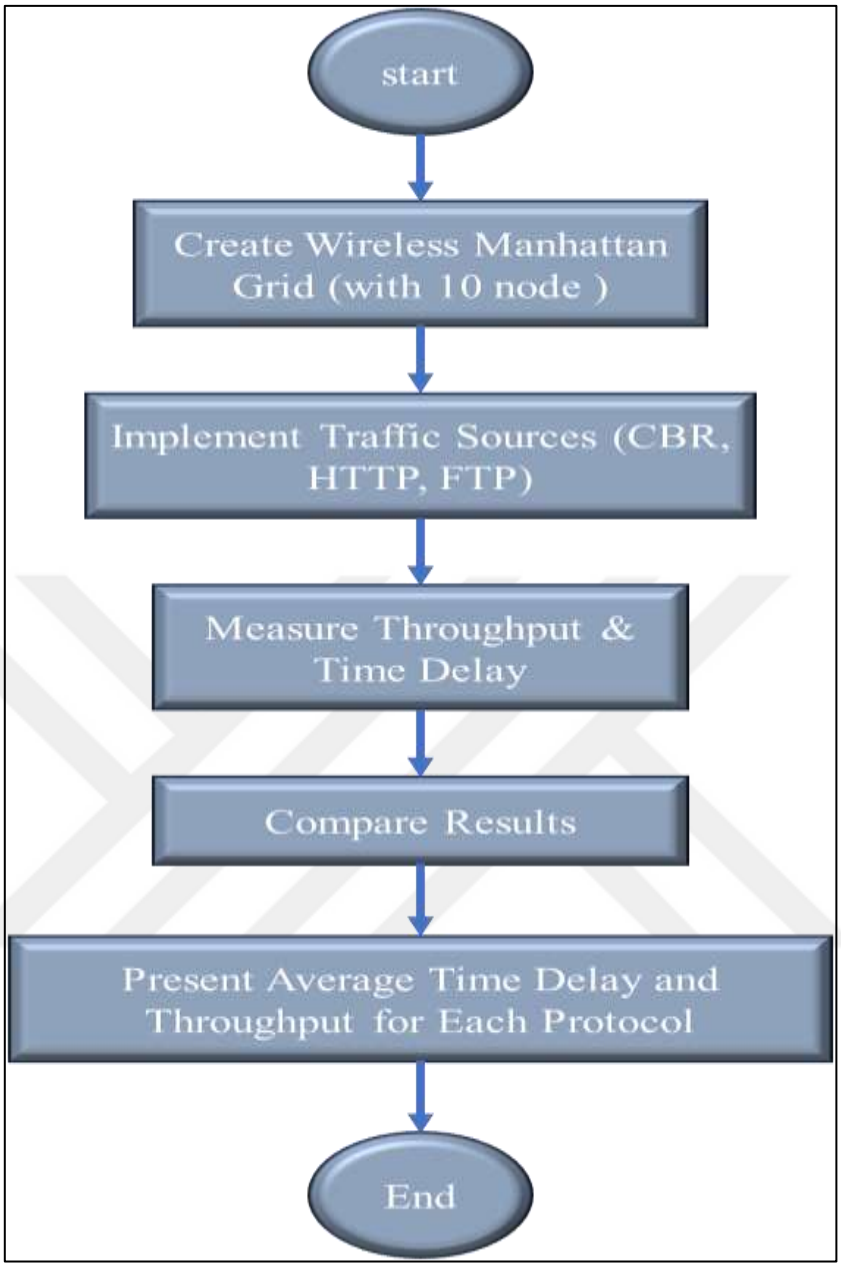

Figure 3.3: Diagram to Illustrate the First Scenario.

3.3.3 Second Scenario With VPN

In the new scenario, an additional layer of VPN is introduced to the existing network topology. The VPN is specifically deployed between two designated nodes, namely node 2 and node 3. Consequently, the transmission of data traffic between node 2 and node 3 will be facilitated via the VPN tunnel. As show in the figure 3.4.

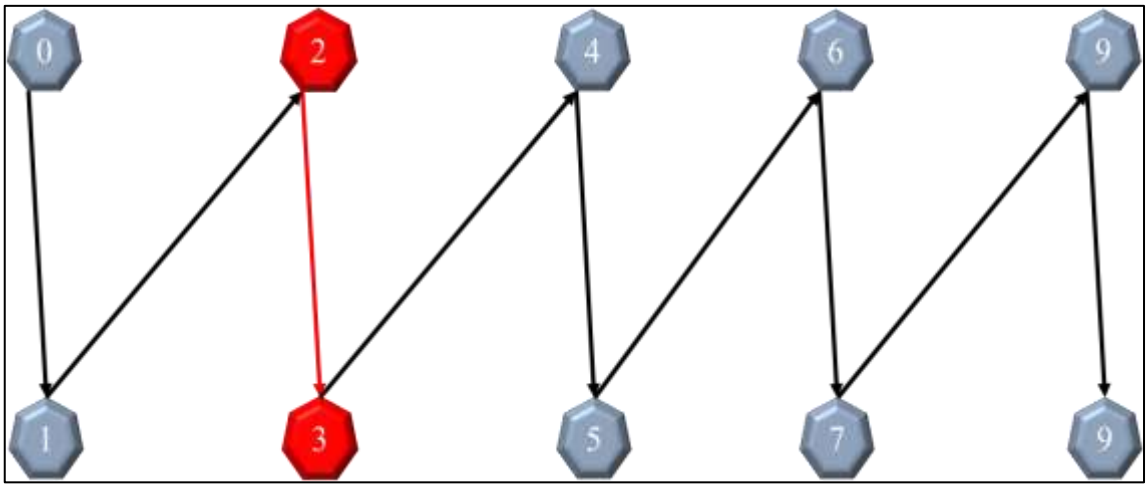

Figure 3.4: Depict of Second Scenario That Demonstrates the VPN Connection.

The followings steps explain the phases of new scenario:

a. With the same wireless network that consists of ten non-mobile nodes arranged in a Manhattan grid. In this new model, we apply a VPN connection between node 2 and node 3. This connection creates a secure and private tunnel between these two nodes, ensuring that the data transmitted between them is encrypted and protected.
b. Then we proceed to test three different protocols - CBR, HTTP, and FTP - within the network. These protocols represent different types of network traffic. The focus is on evaluating the impact of the introduced VPN on network performance metrics, specifically throughput and time delay.
c. The throughput, which refers to the amount of data that can be transmitted over the network, is measured and compared for the protocols (CBR, HTTP, FTP) in the presence of the VPN connection between node 2 and node 3. The time delay, also known as latency, is measured and compared for the same protocols under the influence of the VPN connection.
d. By comparing the throughput and time delay results of the protocols (CBR, HTTP, FTP) with the VPN connection between node 2 and node 3, you can assess the impact of the VPN on the specific connection.
e. The final step involves comparing the entire network's performance in two modes: one with the introduced VPN (specifically affecting the connection between node 2 and node 3) and the other without any VPN.

Overall, the goal of this new model is to analyze how the addition of a VPN connection between two nodes (node 2 and node 3) within the network affects the network's performance metrics, and subsequently, how it impacts the overall network performance when compared to the scenario without any VPN. Figure 3.5. shows the flowchart to explain the second scenario with apply VPN.

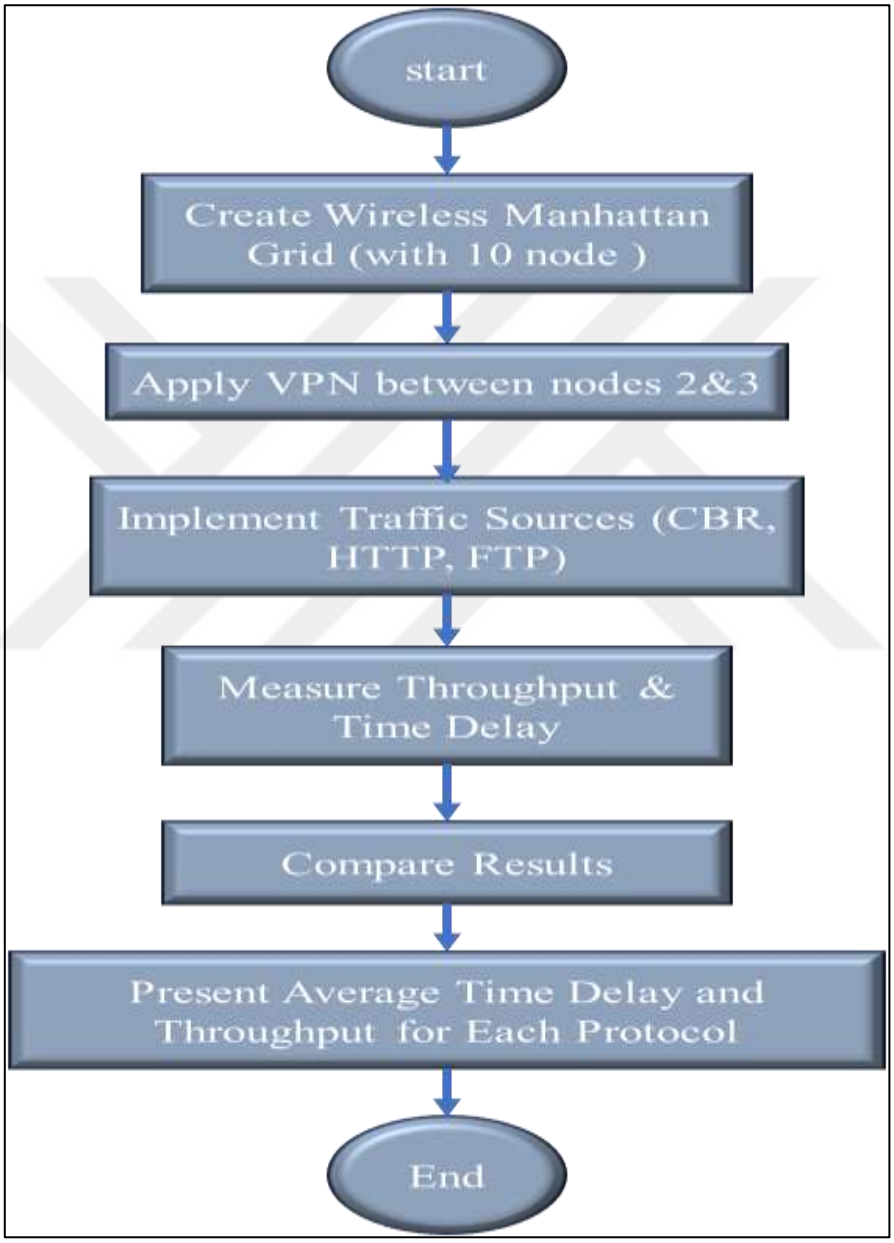

Figure 3.5: Flowchart to Explain the Second Scenario with Apply VPN.

3.4 GENERATORS OF TRAFFIC SOURCES

3.4.1 HTTP Traffic Source Generator

HTTP has the potential to function as a substantial generator of network traffic in both simulated environments and real-world situations [45]. Simulation and analysis of network behavior, performance, and efficiency are of utmost importance in the field. HTTP serves as the fundamental framework for facilitating the exchange of data on the global network known as the World Wide Web. When an individual interacts with a website, their web browser initiates (http) requests to a server, soliciting a diverse range of resources including HTML documents, images, videos, stylesheets, scripts, and additional elements [45,46]. Each of these resources is individually retrieved from the server. HTTP, as a means of traffic generation, produces traffic through the emulation of web page loading. Every component present on a webpage, including but not limited to images, videos, and scripts, necessitates a distinct HTTP request in order to be retrieved from the server. The cumulative impact of numerous requests and corresponding responses plays a significant role in the generation of network traffic.

HTTP adheres to a client-server paradigm, wherein the client, typically a web browser, initiates requests to the server, and the server reciprocates by providing the requested resources in its response [47]. The reciprocal exchange of information between the client and the server results in the generation of network traffic, thereby emulating interactions that occur in real-world scenarios.

Web applications frequently depend on the HTTP as the primary means of facilitating data exchange between the client and the server. This encompasses the transmission and reception of data for the purpose of processing form submissions, verifying user identities, and facilitating various other types of interactions. Every transaction encompasses HTTP requests and responses, thereby contributing to network traffic. HTTP communication is characterized by the exchange of discrete messages, namely requests and responses, as opposed to a continuous flow of data. The inherent characteristic of HTTP being message-based facilitates the generation of distinct packets of traffic, thereby enabling the possibility of analysis and measurement.

The utilization of HTTP traffic simulation in network models facilitates the assessment of network performance, capacity, and latency. This enables the examination of the influence of diverse variables, such as network congestion, on the dissemination of web-based information. Various web pages and applications exhibit diverse traffic patterns. An instance can be observed in which a webpage containing abundant media elements leads to an increased number of HTTP requests and consequently contributes to heightened network utilization.

In essence, HTTP functions as a multifaceted and practical generator of traffic sources in both network simulations and real-life situations. The utilization of this technology in retrieving online resources, emulating user actions, and enabling data transmission between clients and servers is of utmost importance in the examination of network efficiency and the enhancement of network architecture. Figure 3.7. shows the transfer of information from one server to another using the HTTP protocol.

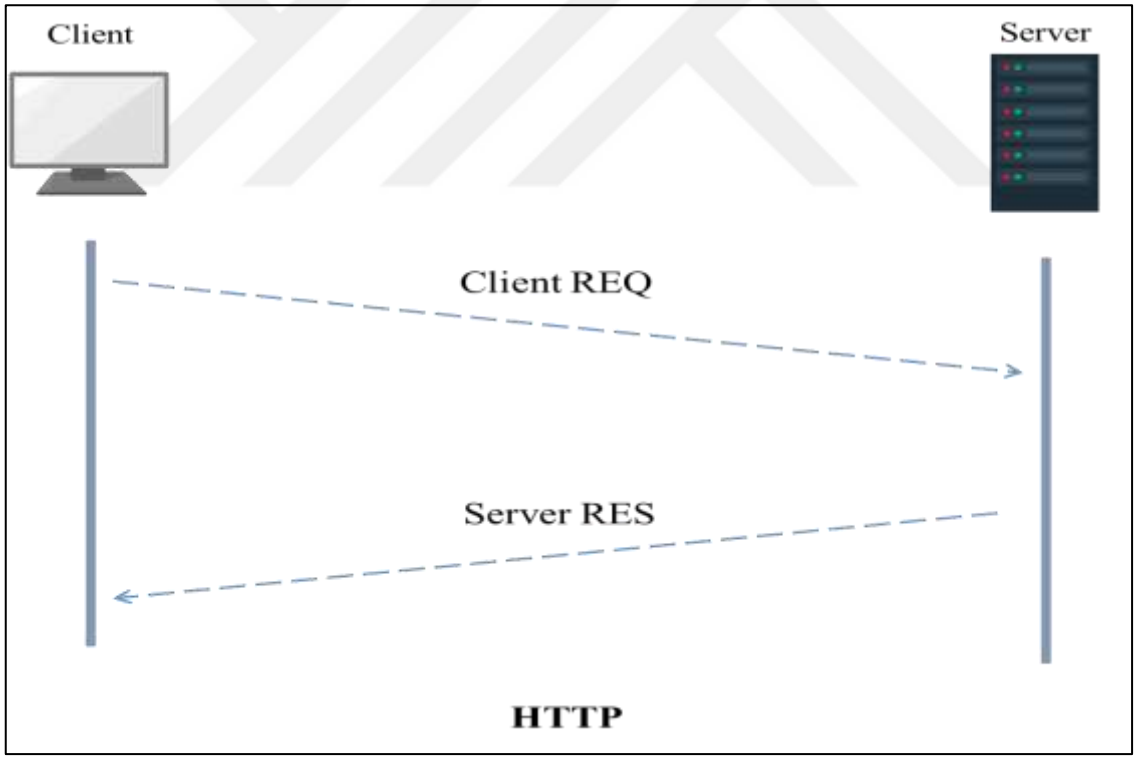

Figure 3.6: The Transfer of Information from One Server to Another Using the HTTP Protocol.

3.4.2 FTP Traffic Source Generator

FTP, also known as File Transfer Protocol, is a dedicated protocol that has been specifically developed to facilitate the seamless transfer of files between a client and a server across a network [48]. The utilization of this tool has the potential to function as a substantial generator of traffic sources in both network simulations and real-world situations, particularly when assessing the efficiency of data transfer and network performance. The primary objective of the FTP is to facilitate the seamless transfer of files between a client and a server [49]. In its capacity as a traffic source, this system emulates the motion of files across a network by producing data packets that replicate the characteristics of genuine file transfers observed in real-world scenarios.

FTP encompasses two primary operations, namely uploading, which entails the transmission of files from a client to a server, and downloading, which involves the retrieval of files from a server to a client. Both operations result in the transmission of network traffic as data packets are exchanged between the client and server. FTP is capable of effectively managing and transferring substantial files, rendering it a suitable choice for situations that involve the transfer of substantial volumes of data. The transmission of sizable data files results in continuous and significant network congestion.

FTP functions in a sequential manner, facilitating the transfer of files or file segments in a consecutive fashion [50]. The exchange of sequential data plays a significant role in the generation of structured traffic patterns that can be subjected to analysis and measurement. Just like HTTP, FTP also adheres to a client-server architecture. The client is responsible for establishing connections and transmitting requests to the server in order to facilitate the transfer of files. The server provides the requested files, resulting in bidirectional traffic.

The (FTP) employs distinct connections for the transmission of data, which encompasses the actual content of files, and for the management of control, which involves the exchange of commands and responses. The inherent duality of this connection nature gives rise to numerous concurrent streams of traffic, thereby contributing to the intricacy of network interactions. The presence of diverse file formats and sizes can result in heterogeneous traffic patterns. As an example, the act of transferring a video file of substantial size results in a greater amount of network traffic in comparison to the transfer of a small text document.

In the context of network simulations, FTP can be employed to replicate real-world scenarios wherein users are required to transfer files to or from remote servers. This facilitates the assessment of network performance, including metrics such as throughput and latency. FTP is commonly employed for the objectives of data backup and synchronization. The simulation of these activities results in the generation of traffic that accurately represents the common backup and synchronization operations.

In essence, FTP functions as a multifaceted facilitator of traffic origins, particularly in the context of evaluating data transmission and network efficiency. The tool possesses significant value in the analysis of network behavior and the optimization of network design due to its capabilities in file transfer, simulation of client-server interactions, and generation of diverse traffic patterns. Figure 3.8 shows the model for sharing files via the FTTP protocol.

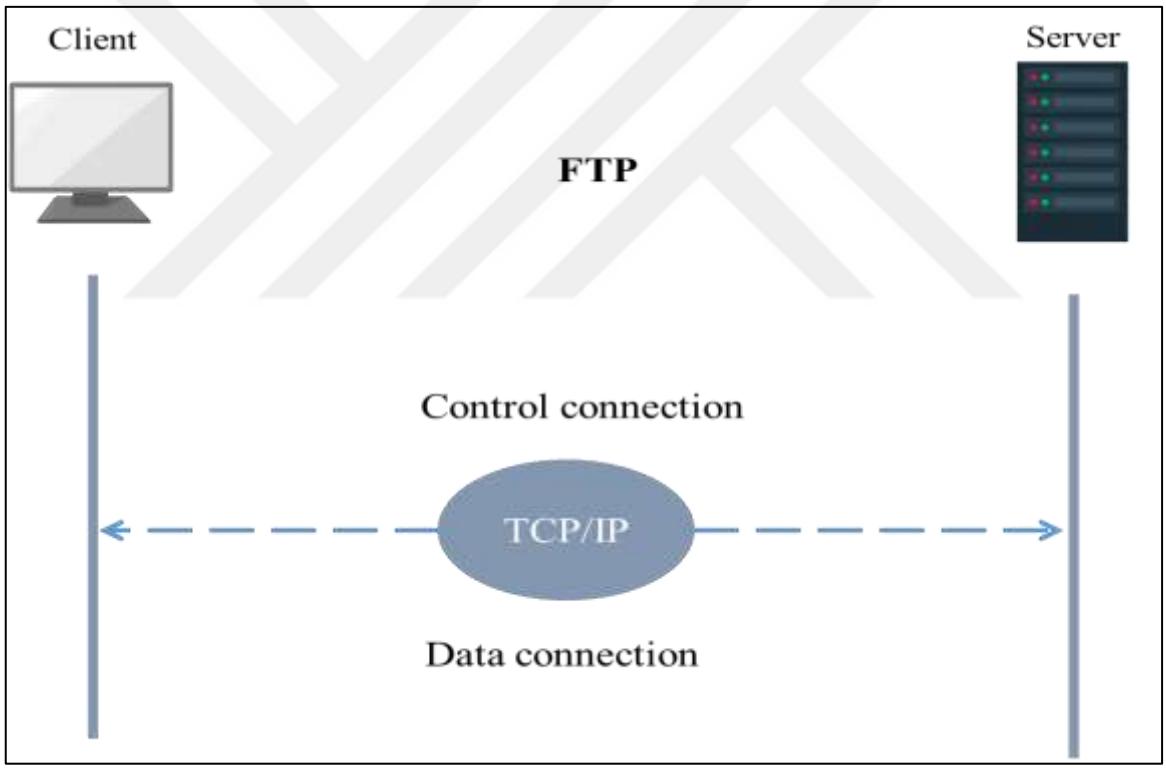

Figure 3.7: Model for Sharing Files Via the FTTP Protocol.

3.4.3 CBR Traffic Source Generator

Constant Bit Rate (CBR) is a widely utilized form of traffic source in network simulations and performance assessments [51]. The process produces a continuous and uniform flow of data packets at a predetermined rate, rendering it advantageous for examining the

performance of networks when subjected to consistent and foreseeable traffic loads. The process of constant bit rate (CBR) involves the generation of a consistent stream of data packets without interruption. This phenomenon establishes a uniform and foreseeable flow of traffic, enabling researchers to conduct an analysis of network performance, capacity, and potential points of congestion.

CBR traffic exhibits a constant and unvarying rate of data transmission, thereby emulating applications or services that necessitate a predetermined and uniform allocation of network bandwidth [52]. This encompasses the utilization of real-time multimedia streaming, voice calls, or any situation in which a consistent bit rate is imperative. The utilization of CBR (Constant Bit Rate) can effectively facilitate the regulation and management of data transmission quantities within a network. Researchers have the ability to analyze the network's reaction to a consistent data load by establishing a predetermined bit rate.

The utilization of CBR can facilitate the assessment of a network's ability to manage congestion in the presence of a persistent data flow [53]. This enables the evaluation of variables such as packet loss, latency, and throughput within a controlled environment. The utilization of CBR proves to be an appropriate approach for the simulation of real-time applications that necessitate a continuous and uninterrupted flow of data, such as video conferencing or online gaming. This aids in the evaluation of the network's capacity to support these applications without any disruptions.

The utilization of traffic generated by CBR plays a crucial role in the assessment of significant performance indicators such as throughput, latency, and jitter. These metrics offer valuable insights into the responsiveness and efficiency of the network [54].

The utilization of CBR is employed in the development of traffic models that aim to simulate the precise behaviors exhibited by various applications. The bit rate can be manipulated by researchers in order to replicate various scenarios and examine their effects on network performance. The utilization of CBR facilitates the examination of network components and infrastructure through load testing. This process aids in the identification of potential vulnerabilities and challenges related to scalability. The utilization of CBR facilitates the establishment of a consistent and controlled testing environment, thereby enhancing the comparability of outcomes across diverse experiments and network configurations.

The utilization of CBR-generated traffic facilitates the examination of the conduct exhibited by diverse network protocols in circumstances characterized by stability. This analytical approach empowers researchers to meticulously adjust protocol parameters for optimal performance.In essence, it can be concluded that (CBR) plays a significant role as a valuable catalyst for the generation of traffic sources in the context of network simulations and performance evaluations. The consistent and predictable data stream it offers renders it a valuable instrument for examining network behavior, evaluating real-time applications, and quantifying crucial performance metrics within controlled settings. Figure 3.9 shows data sent by CBR.

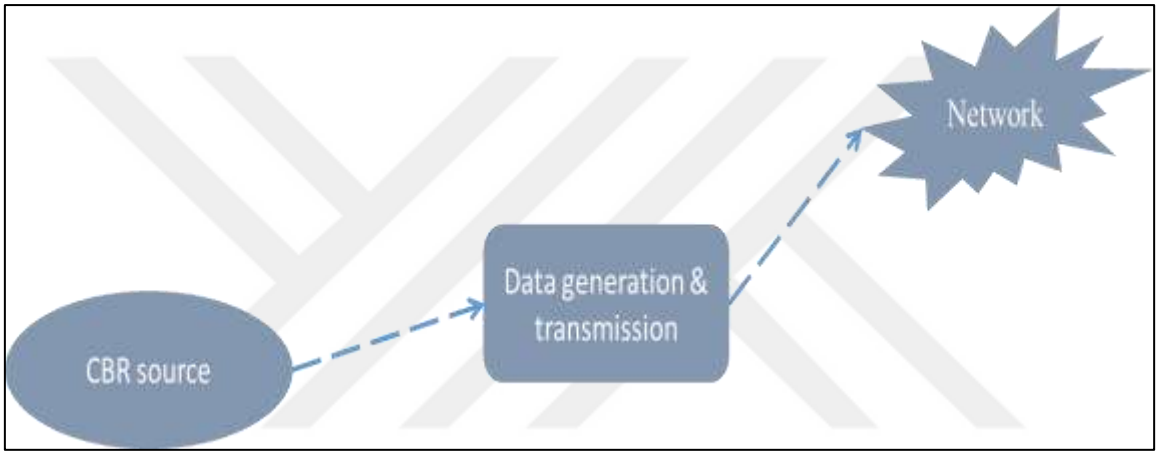

Figure 3.8: Transmission Data by Using CBR.

4. IMPLEMENTATION AND RESULTS

4.1 INTRODUCTION

This chapter focuses on the elucidation of the implementation of two scenarios and the outcomes that have been devised, with three traffic protocols (CBR, FTP, and HTTP). The first scenario implemented with non-VPN. The second scenario implemented with VPN.

Two primary performance metrics are utilized to assess the influence of VPN on the network, specifically: latency and throughput. The initial metric, denoted as "time," quantifies the duration expressed in seconds, during which the packets transmitted by multiple nodes are required to remain in a queue until the receiving node confirms their successful delivery. Furthermore, the throughput can be defined as the quantity of packets that are successfully delivered within a given transmission episode, which is measured in terms of simulation time. The first scenario involves utilizing first baseline technology to enable transmission without the need for a VPN. In contrast, the second scenario involves performing the same transmission task while utilizing a VPN. The performance evaluation entails the utilization of throughput and time delay measurements conducted on a set of ten nodes, each employing distinct traffic generators (CBR, HTTP, and FTP).

The execution of the scenarios involves conducting simulations using NS2 for a predetermined duration. The experiments encompass various configurations, including the manipulation of VPN settings, network topologies, and traffic loads. Subsequently, an assessment will be conducted to analyze the impact of these modifications on the performance of the (VPN) as well as the broader network infrastructure. Table 4.1 presents the simulated network models' configurations in NS2.

Throughput can be described in the Equation below (4.1):

$$Throughput = NoDT\ (bit/sec.) \tag{4.1}$$

Where NoD stands for number of delivered packets from the source to the destination. And T is the time taken for performing the transmission operations.

Table 4.1: Presents the Simulated Network Models' Configurations in Ns2.

Subjects	Inside Information
Dimensions of Topology	300 X 300 meter square
Time of Simulation	30 S (seconds)
Nodes No.	Ten Nodes (10)
Types of Traffic	CBR & HTTP & FTP
Type of Topology	Manhattan grid

4.2 RESULT OF (CBR, FTP, AND HTTP) WITH ABSENCE OF VPN

4.2.1 CBR with absence of VPN

Table 4.2 presents a comprehensive analysis of the delay and throughput attributes pertaining to (CBR) traffic, considering various packet sizes. This analysis specifically focuses on scenarios where a (VPN) is not present. The table has been structured with three distinct columns, wherein each column corresponds to a particular packet size measured in bytes: 512, 1024, and 2048.

The second column, denoted as "CBR (milliseconds)," presents the recorded latency encountered by (CBR) traffic for each corresponding packet size. The data suggests that as the size of the packet increases, there is a marginal rise in latency. As an example, when considering a packet size of 512 bytes, the corresponding delay measures at 0.017 milliseconds. Similarly, for a packet size of 1024 bytes, the delay increases to 0.02 milliseconds. Finally, when dealing with a packet size of 2048 bytes, the delay further extends to 0.023 milliseconds.

The third column, denoted as "Throughput (Mbit/second)," showcases the attained throughput of the (CBR) traffic in relation to the packet sizes. As the size of the packet increases, there is a corresponding increase in the throughput. In particular, the measured

throughput for packet sizes of 512 bytes, 1024 bytes, and 2048 bytes are 0.006 Mbit/second, 0.014 Mbit/second, and 0.029 Mbit/second, respectively.

Table 4.2: Delay and Throughput of CBR With Different Packet Size Absence Of VPN.

Packet size (bytes)	Delay (milliseconds)	Throughput (Mbit/second)
512	0.017	0.006
1024	0.02	0.014
2048	0.023	0.029

4.2.2 FTP with absence of VPN

The evaluation of delay and throughput pertaining to (FTP) traffic in a network configuration without (VPN) is illustrated in Table 4.3. The table exhibits a structured arrangement comprising of three essential parameters, namely "packet size (bytes)," "Delay (milliseconds)," and "Throughput (Mbit/second)." The column labeled "packet size (bytes)" provides an overview of the different packet sizes employed in the transmission of FTP data, spanning from 512 to 2048 bytes. Within this particular context, the term "Delay" pertains to the temporal duration, quantified in milliseconds, required for FTP packets of varying sizes to traverse the network and successfully arrive at their designated endpoint. Significantly, the delay exhibits a consistent value of 0.03 milliseconds regardless of the packet sizes, suggesting a uniform transmission time for FTP packets.

The column labeled "Throughput" denotes the rate at which data is transmitted by the FTP traffic for each respective packet size. It is worth noting that the throughput values exhibit variation depending on the size of the packets. As an illustration, when employing a packet size of 512 bytes, the resulting throughput amounts to 0.45 megabits per second. In a similar vein, it can be observed that increased packet sizes are positively correlated with enhanced throughputs. Specifically, when employing a packet size of 1024 bytes, the resulting throughput amounts to 3 Mbit/second. Conversely, utilizing a larger packet size of 2048 bytes yields the highest achievable throughput of 7.4 Mbit/second.

Table 4.3: Delay and Throughput of FTP with Different Packet size Absence of VPN.

packet size (bytes)	Delay (milliseconds)	Throughput (Mbit/second)
512	0.03	0.45
1024	0.03	3
2048	0.03	7.4

4.2.3 HTTP with absence of VPN

Table 4.4 presents a comprehensive examination of the delay and throughput pertaining to (HTTP) traffic. This analysis takes into account various connection rates within a network configuration that does not incorporate (VPN). The table has been structured according to three primary parameters, namely "Number of connection rate," "Delay in milliseconds," and "Throughput in Mbit/second."

The column labeled "No. of connection rate" represents the quantity of concurrent connections established for HTTP traffic. In this instance, the table presents three distinct connection rates, namely 5, 10, and 15. The connection rates mentioned here pertain to the simultaneous interactions between clients, typically web browsers, and a web server. During these interactions, multiple clients make requests to the server and receive resources from it concurrently.

The column labeled "Delay" denotes the duration of time, quantified in milliseconds, required for HTTP requests and responses to traverse the network at the given connection rates. It is worth mentioning that the delay remains consistently at 0.03 milliseconds across all connection rates, suggesting a uniform transmission time for HTTP traffic irrespective of the quantity of concurrent connections.

The column labeled "Throughput" demonstrates the rate at which data is transmitted by the HTTP traffic for each connection rate. It is noteworthy that the throughput values exhibit consistency across various connection rates, as evidenced by each scenario attaining a throughput of 18 Mbit/second. This observation implies that the network configuration, in

the absence of (VPN), is capable of effectively managing HTTP traffic with a consistent and elevated data transmission rate, regardless of the quantity of concurrent connections.

Table 4.4: Delay and Throughput of HTTP With No. of Connection Rate Absence of VPN.

No. of connection rate	Delay (milliseconds)	Throughput (Mbit/second)
5	0.03	18
10	0.03	18
15	0.03	18

In In brief, the provided table 4.2 presents significant findings regarding the correlation between packet size, delay, and throughput for (CBR) traffic within the examined network conditions. It highlights the notable influence of packet size on both delay and throughput measurements within a network that does not employ (VPN). As well as the presented data in Table 4.3 provides an illustration of the influence of different packet sizes on the delay and throughput of (FTP) traffic in a network setup that does not employ (VPN). In spite of persistent latency, the efficiency of (FTP) traffic exhibits a positive correlation with packet size, thereby suggesting a direct association between the size of packets and the rate at which data is transmitted. In addition, the findings presented in Table 4.4 illustrate that manipulating the quantity of simultaneous connections in the absence of (VPN) does not have a substantial impact on the latency or data transfer rate of (HTTP) traffic. The network's ability to effectively handle HTTP requests and responses, irrespective of the quantity of active connections, is demonstrated by its stable delay and consistent high throughput.

4.3 RESULT OF (CBR, FTP, AND HTTP) WITH VPN

4.3.1 CBR with VPN

The delay and throughput characteristics of (CBR) traffic in (VPN) are analyzed in Table 4.4. The examination considers different packet sizes. The table exhibits a structured format comprising of three essential parameters, namely "Packet size (bytes)," "Delay (milliseconds)," and "Throughput (Mbit/second)."

The column labeled "Packet size (bytes)" denotes the byte size of data packets involved in the transmission of (CBR) traffic. The study examines three discrete packet sizes, namely 512 bytes, 1024 bytes, and 2048 bytes. The varying packet sizes observed in this context serve as a reflection of the quantity of data encompassed within each individual transmission.

The column labeled "Delay" denotes the duration of time delay encountered during the transmission of (CBR) traffic, quantified in milliseconds. Significantly, the latency consistently maintains a minimal value of 0.01 milliseconds for all packet sizes. This finding suggests that the configuration of the VPN has a negligible effect on the latency encountered by (CBR) traffic, irrespective of the packet size.

The column labeled "Throughput" provides information on the achieved data transmission rate of (CBR) traffic for each packet size, measured in megabits per second (Mbit/s). The throughput values are indicative of the efficacy of data transmission. It is noteworthy that the throughput values exhibit a consistent pattern regardless of the packet size. The network demonstrates throughputs of 0.006, 0.014, and 0.029 Mbit/second for packet sizes of 512 bytes, 1024 bytes, and 2048 bytes, correspondingly.

Table 4.5: Delay and Throughput of CBR With Different Packet Size and VPN.

Packet size (bytes)	Delay (milliseconds)	Throughput (Mbit/second)
512	0.01	0.006
1024	0.01	0.014
2048	0.01	0.029

4.3.2 FTP with VPN

The analysis of delay and throughput related to (FTP) traffic, taking into account various packet sizes, is presented in Table 4.5. This analysis is conducted within a network configuration that incorporates (VPN). The table comprises three primary parameters, namely "Packet size (bytes)," "Delay (milliseconds)," and "Throughput (Mbit/second)."

The column labeled "Packet size (bytes)" denotes the size of the data packets employed in the (FTP) communication, quantified in bytes. The study investigates three unique packet sizes, namely 512 bytes, 1024 bytes, and 2048 bytes. Increasing the size of packets has the potential to enhance the efficiency of data transfer by mitigating the overhead linked to packet headers.

The column labeled "Delay" denotes the duration of time delay encountered by (FTP) network traffic, quantified in milliseconds, for each packet size within (VPN) configuration. Significantly, the delay exhibits a consistent and minimal value of 0.01 milliseconds for all three packet sizes. This observation suggests that (VPN) possesses the capability to sustain a rapid data transmission procedure, thereby leading to negligible latency for (FTP) communication.

The column labeled "Throughput" presents the achieved data transmission rate of FTP traffic for each packet size, denoted in megabits per second (Mbit/s). As the size of the packet increases, there is a corresponding increase in the throughput. In the context of packet transmission, it is observed that the throughput varies depending on the size of the packets. For instance, when the packet size is set at 512 bytes, the throughput is measured to be 1.5 Mbit/second. Similarly, when the packet size is increased to 1024 bytes, the throughput significantly improves to 9.4 Mbit/second. Furthermore, when the packet size is further increased to 2048 bytes, the throughput reaches its peak at 19.3 Mbit/second. This observation suggests that the utilization of larger packet sizes positively impacts the rate of data transmission, thereby facilitating the transfer of a greater volume of data within a given time frame.

Table 4.6: Delay and Throughput of FTP with Different Packet Size and VPN.

Packet size (bytes)	Delay (milliseconds)	Throughput (Mbit/second)
512	0.01	1.5
1024	0.01	9.4
2048	0.01	19.3

4.3.3 HTTP with VPN

The analysis of delay and throughput related to (HTTP) traffic, taking into account various connection rates in the presence of (VPN), is presented in Table 4.6. The table has been structured according to three primary variables: "Number of connection rate," "Delay in milliseconds," and "Throughput in Mbit/second."

The column labeled "Number of connection rate" provides information regarding the quantity of concurrent connections established specifically for HTTP traffic. Within the present framework, the table takes into account three discrete connection rates, specifically 5, 10, and 15. The connection rates depicted herein pertain to the simultaneous interactions between clients, typically in the form of web browsers, and a web server, while making use of (VPN).

The column labeled "Delay" denotes the temporal interval, quantified in milliseconds, during which HTTP requests and responses encounter latency while traversing the network under the designated connection rates and in the presence of an active VPN. It is worth noting that the delay consistently maintains a constant and minimal value of 0.01 milliseconds regardless of the connection rates. This implies that the utilization of (VPN) has effectively mitigated latency, resulting in enhanced transmission speed for HTTP data.

The column labeled "Throughput" presents the achieved data transmission rate of the HTTP traffic for each connection rate, taking into account the presence of a VPN. The throughput values exhibit minor fluctuations depending on the quantity of simultaneous connections. At a connection rate of 5, the measured throughput is 49.9 Mbit/second. However, when the connection rates increase to 10 and 15, the throughput experiences a slight reduction to 40 Mbit/second and 42 Mbit/second, respectively. This observation suggests that the network, when utilizing the VPN, is capable of consistently sustaining a substantial data transmission rate for HTTP traffic, even when faced with different levels of concurrent connections.

Table 4.7: Delay and Throughput of HTTP with No. of connection rate and VPN.

No. of connection rate	Delay (milliseconds)	Throughput (Mbit/second)
5	0.01	49.9
10	0.01	40
15	0.01	42

In brief, the findings presented in Table 4.4 demonstrate that the implementation of (VPN) does not have a substantial impact on the latency encountered by (CBR) traffic, irrespective of the size of the packets. Moreover, the observed uniformity in throughput measurements for different packet sizes indicates that (VPN) is capable of sustaining a consistent rate of data transmission for (CBR) traffic. The aforementioned data highlights the efficacy of (VPN) in maintaining the prompt and efficient transfer of (CBR) data across various packet sizes. As well as the findings presented in Table 4.5 indicate that in the specific setting of a network equipped with (VPN), the delay experienced by FTP traffic remains consistently low while the throughput increases as the packet size is enlarged. This implies that the VPN configuration demonstrates effective support for efficient and expedient FTP data transfer, wherein larger packet sizes yield enhanced throughput performance. In addition the findings presented in Table 4.6 illustrate that the inclusion of (VPN) does not significantly impact network latency and ensures a consistently robust data transfer rate for HTTP traffic. The observed low delay values indicate a high level of efficiency in transmitting data, while the consistent throughput values highlight the network's capacity to effectively manage HTTP requests and responses. This holds true even when employing (VPN) and across various connection rates.

4.4 VISUALIZING NS2 SIMULATIONS AND VPN IMPACT ON NETWORK PERFORMANCE

The preceding sections have provided the outcomes obtained by employing the Network Simulator 2 (NS2), a widely used and robust tool for conducting network simulations. The experimental configuration and simulation results are depicted using a sequence of graphical

representations, facilitating a comprehensive comprehension of the observed network dynamics.

The architecture of the Network Simulator 2 project is illustrated in Figure 4.1. The provided figure offers a comprehensive depiction of the structural organization of the simulation environment, highlighting the various components that are integral to the simulation process. The provided information functions as a guide for comprehending the subsequent illustrations and their contextual significance within the simulation framework.

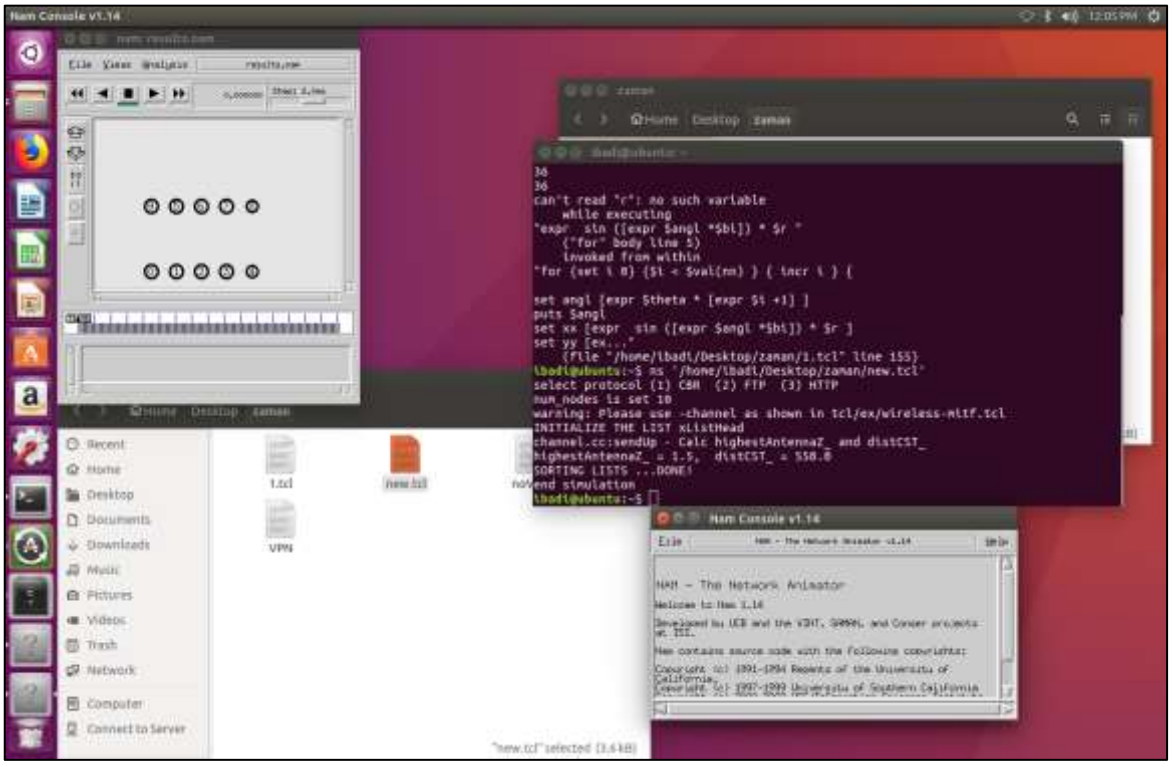

Figure 4.1 : Network Simulator 2 Project Overview.

The distribution of network nodes in a Manhattan grid topology is depicted in Figure 4.2. The Manhattan grid is a spatial arrangement in which nodes are systematically positioned in a structured grid pattern, thereby emulating a real-world scenario. The presented diagram illustrates the configuration of nodes and their interconnections, which significantly impact the behavior and efficiency of the network.

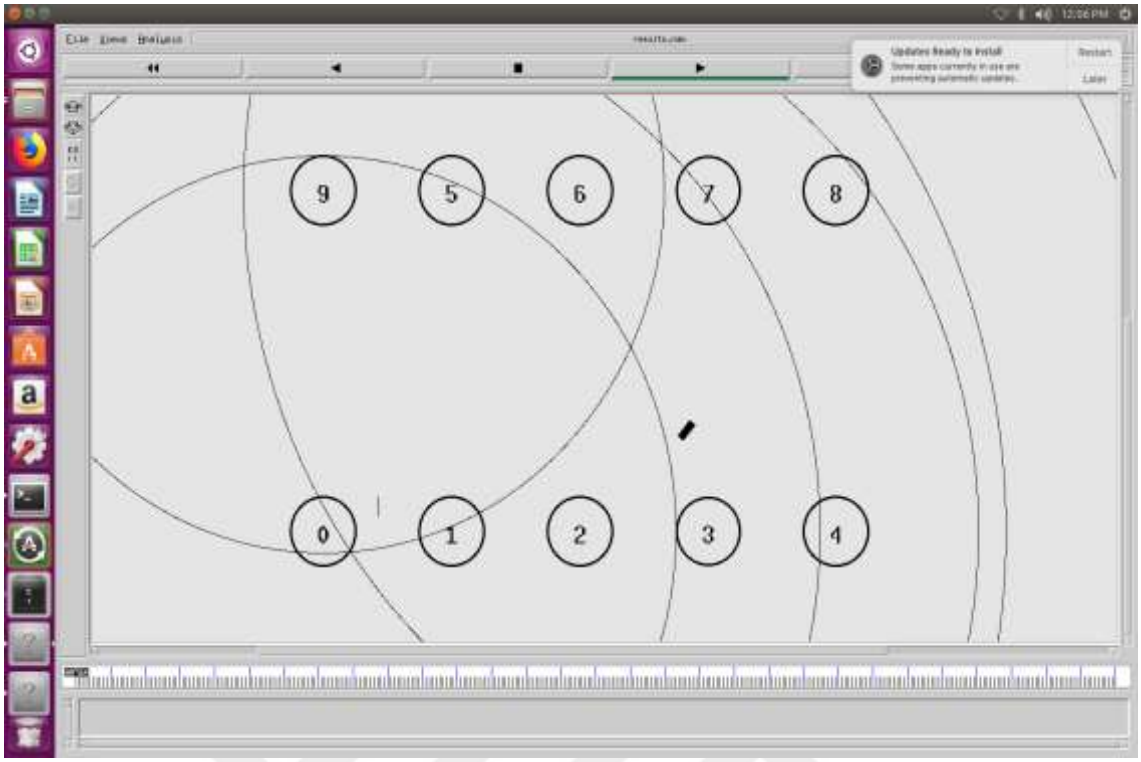

Figure 4.2: Network Simulator 2 Nodes Distribution in Manhattan Grid Topology.

The results of the network incorporating VPN integration are depicted in Figure 4.3. The presented diagram illustrates the precise performance metrics, including delay and throughput, that are observed upon the deployment of VPN technology within the network. Through the process of comparing these metrics in the presence and absence of a VPN, significant knowledge can be obtained pertaining to the influence of VPN on network performance across varying circumstances.

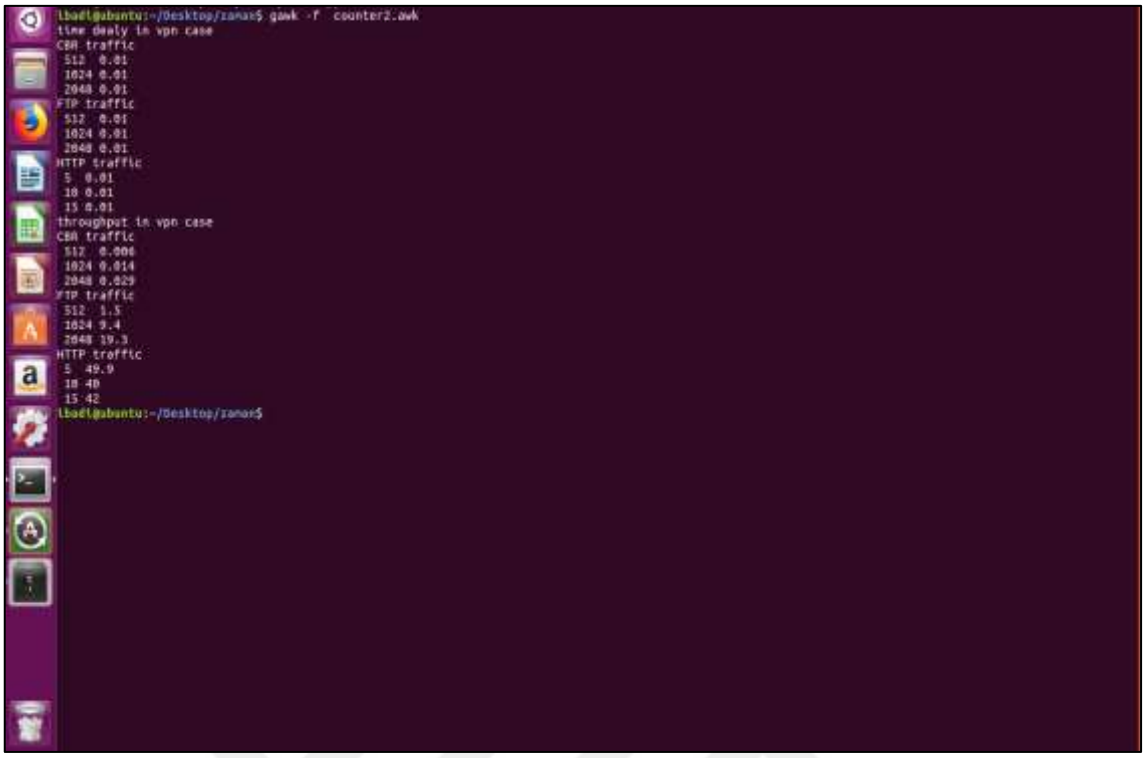

Figure 4.3: The Outcomes of the VPN-Integrated Network.

In a similar vein, the outcomes of a network that does not employ a VPN are depicted in Figure 4.4. This figure provides a direct comparison to the scenario with integrated VPN as illustrated in Figure 4.4. By juxtaposing these results, it becomes feasible to evaluate the benefits or potential compromises linked to the implementation of VPNs on network performance, taking into account variables such as latency and data transfer rate.

In essence, the aforementioned sequence of visual depictions (Figure 4.1 to Figure 4.4) offers a graphical portrayal of the experimental configuration, network simulation, and resultant findings. The aforementioned data collectively contribute to a comprehensive comprehension of the study's findings and illuminate the implications of integrating Virtual Private Networks within the simulated network environment.

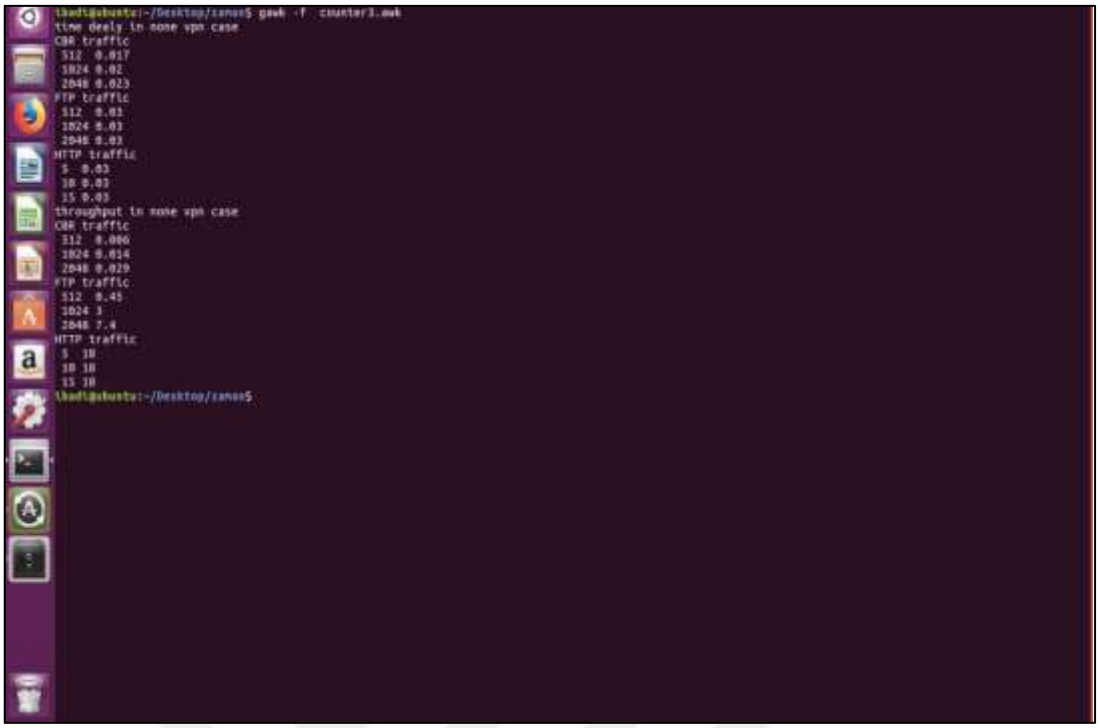

Figure 4.4: Depicts the Outcomes of An Integrated Network That Does Not Utilize A VPN.

5. RESULTS AND DISCUSSION

5.1 INTRODUCTION

This chapter provides an in-depth examination of traffic sources in relation to both VPNs and non-VPN situations. The analysis commences with a thorough examination of the delay characteristics shown by various traffic sources. In this study, we aim to examine the effects of VPN and non-VPN configurations on the latency performance of (CBR), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP) traffic sources.

Following this, our attention is redirected onto the assessment of throughput, which is another crucial element of network performance. This study employs a systematic methodology to investigate the impact of VPN presence or absence on the throughput of CBR, FTP, and HTTP traffic sources. The objective is to get insights into the efficiency and effectiveness of these sources across different scenarios.

In order to enhance our comprehension, we utilize comparative analyses with other pertinent research, so offering a more comprehensive framework for the results. Through an in-depth exploration of these comparisons, we acquire significant insights on the distinctive contributions of our research and its congruence with the current body of knowledge in the respective subject. This study endeavors to offer a complete analysis in order to present a holistic viewpoint on the intricate relationship between traffic sources, VPNs, and network performance.

5.2 TRAFFIC SOURCE COMPARISON OF THE DELAY

5.2.1 Comparison of CBR Traffic Source with VPN and non-VPN

The figure 5.1presents a comparison of the delay experienced in scenarios involving both VPN and non-VPN setups, specifically for the (CBR) traffic source. The delay values are presented for several packet sizes, specifically 512, 1024, and 2048 bytes, under both situations. When employing a VPN, the measured latencies for all sizes of data packets consistently exhibit a lower value of 0.01 milliseconds, in contrast to the absence of a VPN where latencies vary between 0.017 and 0.023 milliseconds. The results indicate that the integration of a VPN has led to a decrease in latency for (CBR) traffic. This underscores the

capability of VPNs to improve network performance by mitigating delays specifically for this type of traffic.

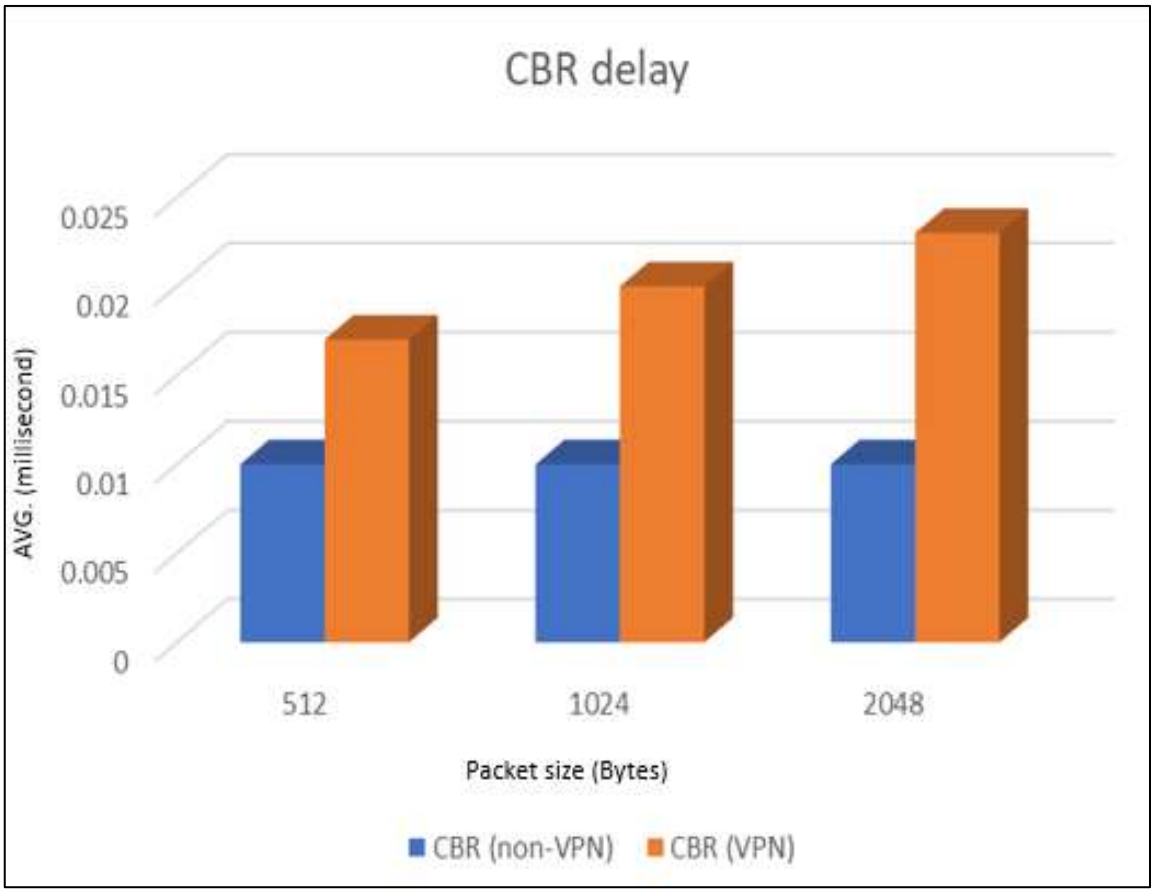

Figure 5.1: Comparing VPN vs. non-VPN Delays with CBR Traffic.

5.2.2 Comparison of FTP Traffic Source with VPN and non-VPN

Figure 5.2 shown analysis of the delay experienced by the FTP traffic source in two separate network environments: one involving the utilization of a VPN, and the other without the implementation of a VPN (non-VPN). The comparison is conducted using different packet sizes, specifically 512, 1024, and 2048 bytes. In the context of a VPN, it is observed that the latency for (FTP) traffic remains continuously low, with a constant value of 0.01 milliseconds, regardless of the size of the packets. On the other hand, the scenario without a VPN demonstrates a latency of 0.03 milliseconds per packet size. The results of this study suggest that the utilization of a VPN has led to a significant decrease in latency, thereby highlighting its effectiveness in improving the efficiency of (FTP) data transmission. The

persistent low delay exhibited by the VPN underscores its capacity to enhance network performance and provide seamless data transmission. The aforementioned comparison highlights the notable benefits associated with the utilization of a VPN for (FTP) traffic, emphasizing its capacity to reduce latency and enhance network performance as a whole.

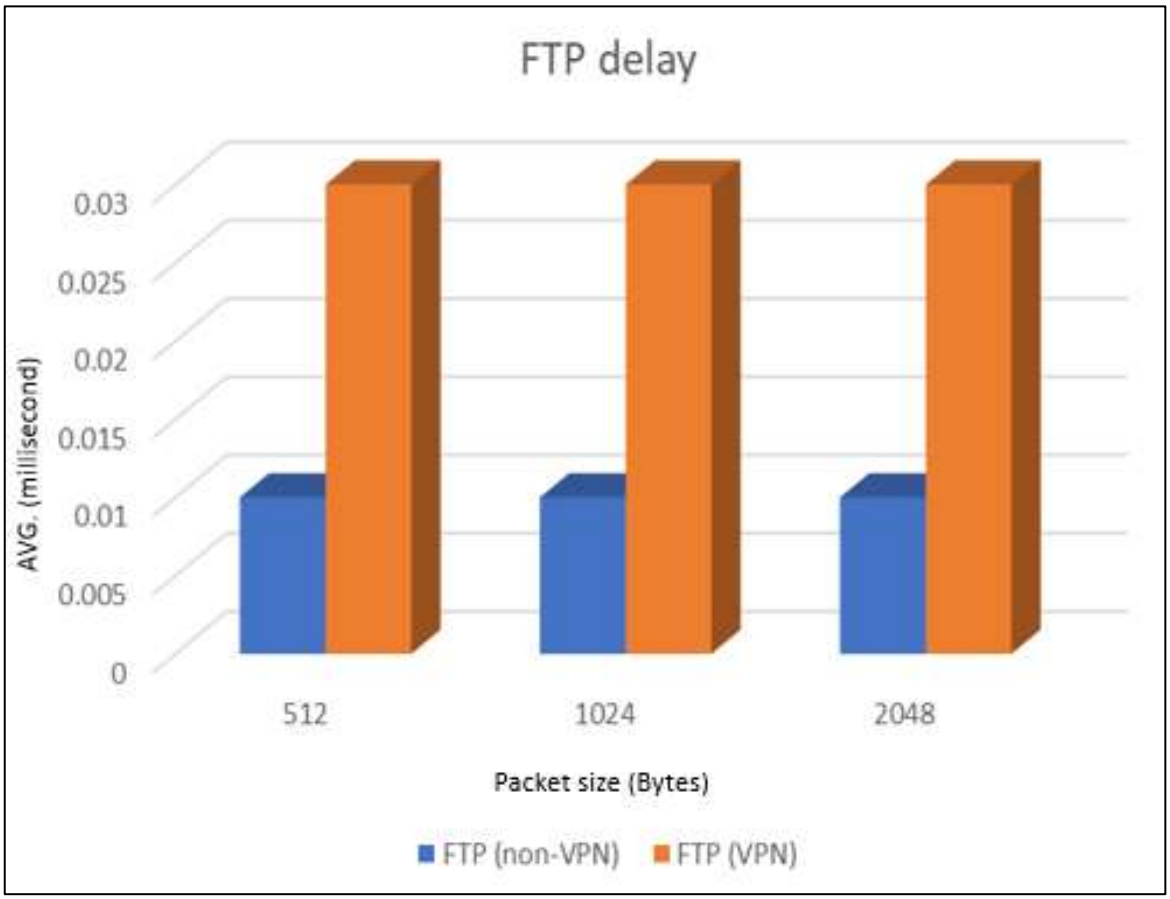

Figure 5.2: Comparing VPN vs. non-VPN Delays with FTP Traffic.

5.2.3 Comparison of HTTP Traffic Source with VPN and non-VPN

To compare the delay between scenarios including the use of a VPN and situations without a VPN, specifically focusing on the "HTTP" traffic source. The objective was to evaluate the effect of using a VPN on transmission latency. In the context of the VPN scenario, the delay observed for the transmission of "HTTP" traffic consistently maintained a low value throughout various intervals. Specifically, a delay of 0.01 milliseconds was reported. In contrast, in the absence of a VPN, the transmission of "HTTP" traffic demonstrated a marginal increase in delay, with a recorded average of 0.03 milliseconds each transmission

interval. This discovery highlights the possible advantages of employing a VPN in mitigating transmission latency for the "HTTP" traffic source. The results indicate that the utilization of VPN technology enhances network efficiency and facilitates efficient data transfer, especially in situations when minimizing latency is of utmost importance, as shown in figure 5.3.

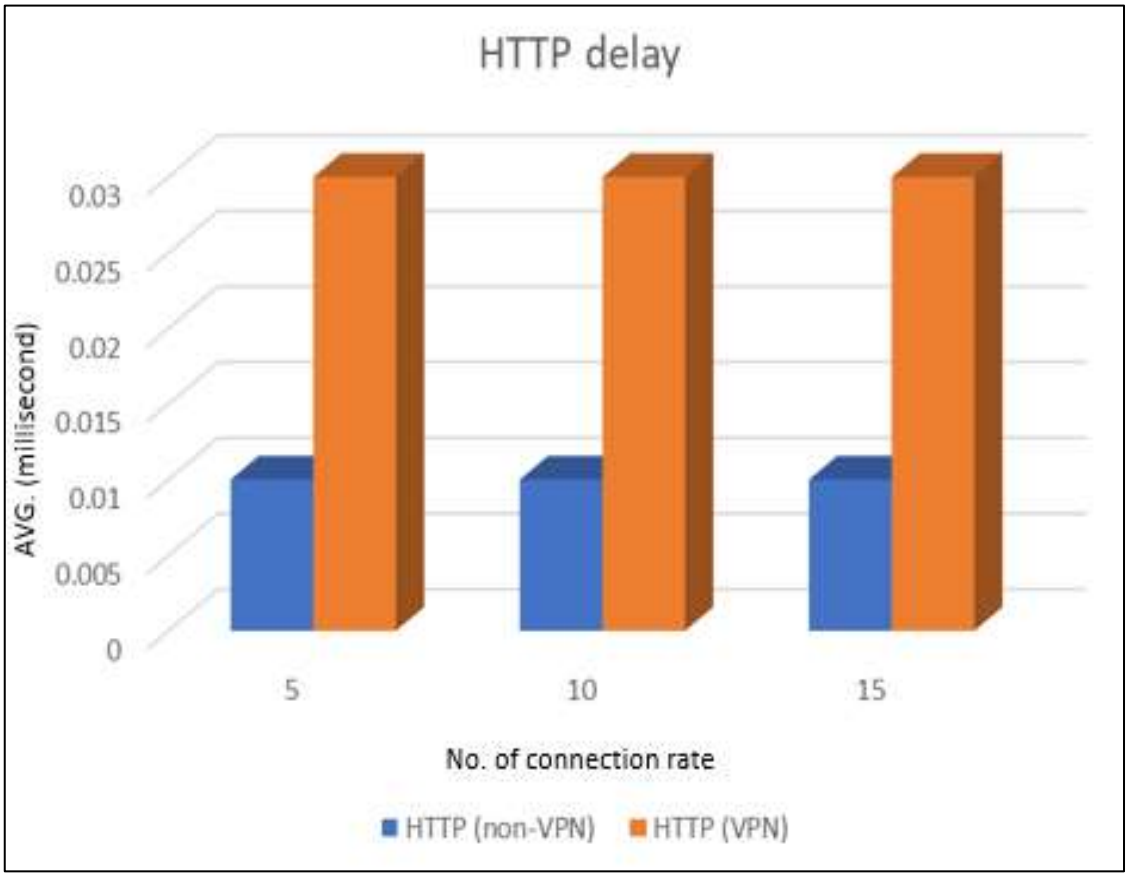

Figure 5.3: Comparing VPN vs. non-VPN Delays with HTTP Traffic.

5.3 TRAFFIC SOURCE COMPARISON OF THE THROUGHPUT

5.3.1 Comparison of CBR Traffic Source with VPN and non-VPN

To compare the throughput of data transmission between scenarios with VPN and situations without VPN. The focus of the study was to examine the effects of implementing a VPN on data transfer rates, specifically for the "CBR" traffic source. Consistent throughput numbers were observed for "CBR" traffic across various packet sizes in both the VPN and non-VPN scenarios. The observed throughput for both circumstances was 0.006 Mbit/second, with a

packet size of 512 bytes. In a comparable manner, it was observed that the throughput values for packet sizes of 1024 and 2048 bytes remained constant at 0.014 and 0.029 Mbit/second, correspondingly, irrespective of the existence of a VPN. The findings suggest that the introduction of a Virtual Private Network had no substantial impact on the throughput of the "CBR" traffic source. The results indicate that the throughput of "CBR" traffic is resistant to modifications in VPN configurations and maintains a generally stable performance across various packet sizes. This underscores the consistency of data transfer rates in both VPN and non-VPN situations. As shown in figure 5.4.

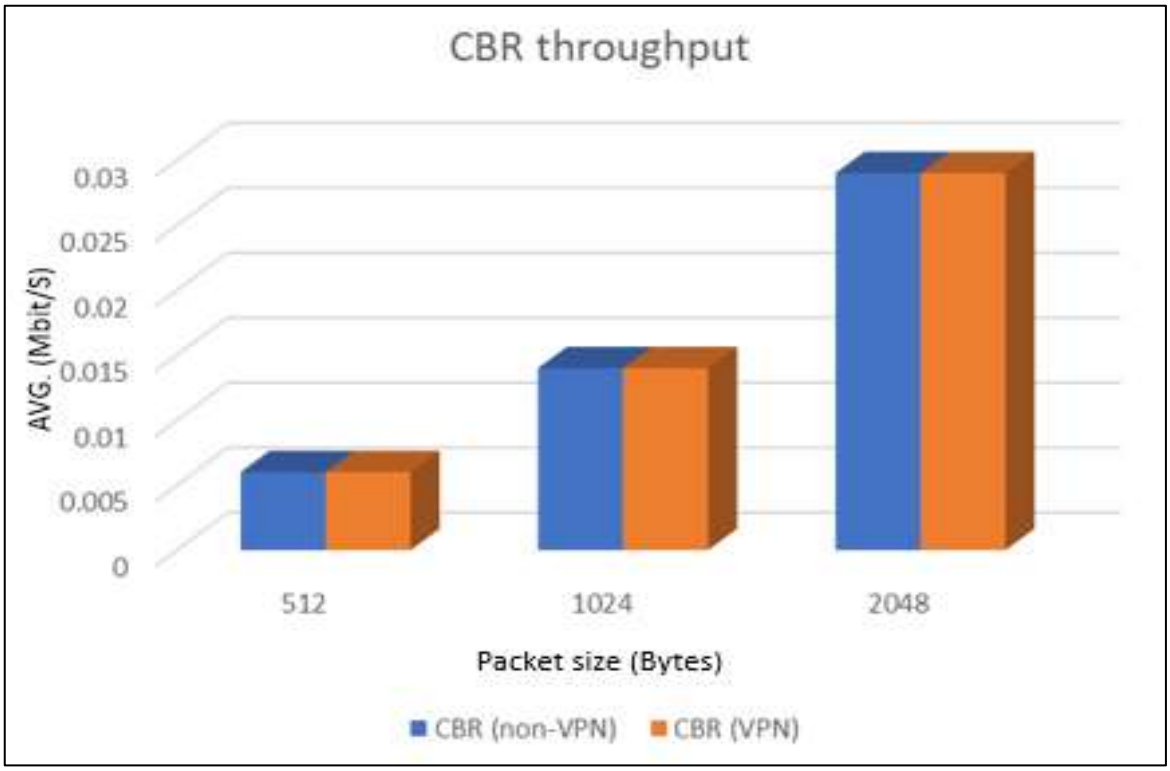

Figure 5.4: CBR Performance Under VPN Versus non-VPN Conditions.

5.3.2 Comparison of FTP Traffic Source with VPN and non-VPN

The investigate the disparity in throughput between situations with VPN and those without VPN, specifically for the "FTP" traffic source. The primary objective was to gain insights into the influence of a Virtual Private Network on the rates of data transfer. In the given context of "FTP" traffic, there were significant variations seen in the throughput figures

between the two situations. In the context of the VPN scenario, the measurement of throughput was conducted for packet sizes of 512, 1024, and 2048 bytes, resulting in respective values of 1.5, 9.4, and 19.3 Mbit/second. On the other hand, the scenario without a VPN exhibited varying throughput numbers, specifically 0.45, 3, and 7.4 Mbit/second for the respective packet sizes. The findings suggest that the introduction of a VPN had a noticeable effect on the data transfer rate of the "FTP" traffic origin. The results indicate that the throughput of "FTP" traffic showed notable enhancements when employing a VPN, particularly when dealing with higher packet sizes. This highlights the potential advantages of utilizing a VPN to improve the efficiency of data transfer speeds for (FTP) traffic across different packet sizes. As shown in figure 5.5.

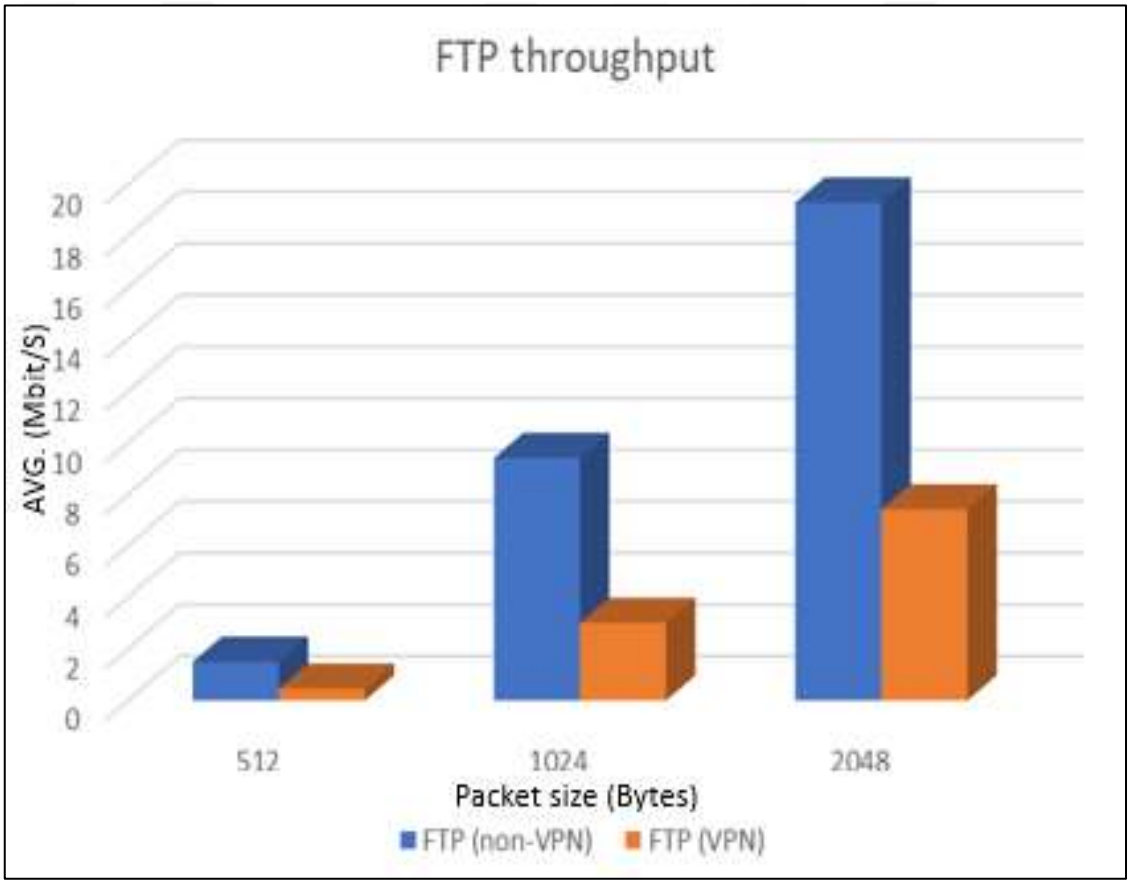

Figure 5.5: FTP Performance Under VPN Versus non-VPN Conditions.

5.3.3 Comparison of HTTP Traffic Source with VPN and non-VPN

The examines the impact of a VPN on data transfer rates by comparing the throughput of "HTTP" traffic in both VPN and non-VPN scenarios. The objective is to gain insights into the influence of VPNs on the efficiency of data transmission. The throughput numbers observed for "HTTP" traffic displayed notable variations between the two situations at varying connection rates. In the context of the VPN scenario, it was seen that the throughput exhibited a noticeable increase when connection rates of 5, 10, and 15 were employed, resulting in measured values of 49.9, 40, and 42 Mbit/second, respectively. On the other hand, the scenario without a VPN exhibited a consistent throughput of 18 Mbit/second for all three connection rates. The results of this study indicate that the introduction of a VPN has a notable influence on the throughput of "HTTP" traffic, leading to considerable enhancements in data transfer speeds, especially when dealing with different connection rates. This highlights the possible benefits of utilizing a VPN to optimize the speed of data transmission for "HTTP" traffic in various connection settings. As shown in figure 5.6.

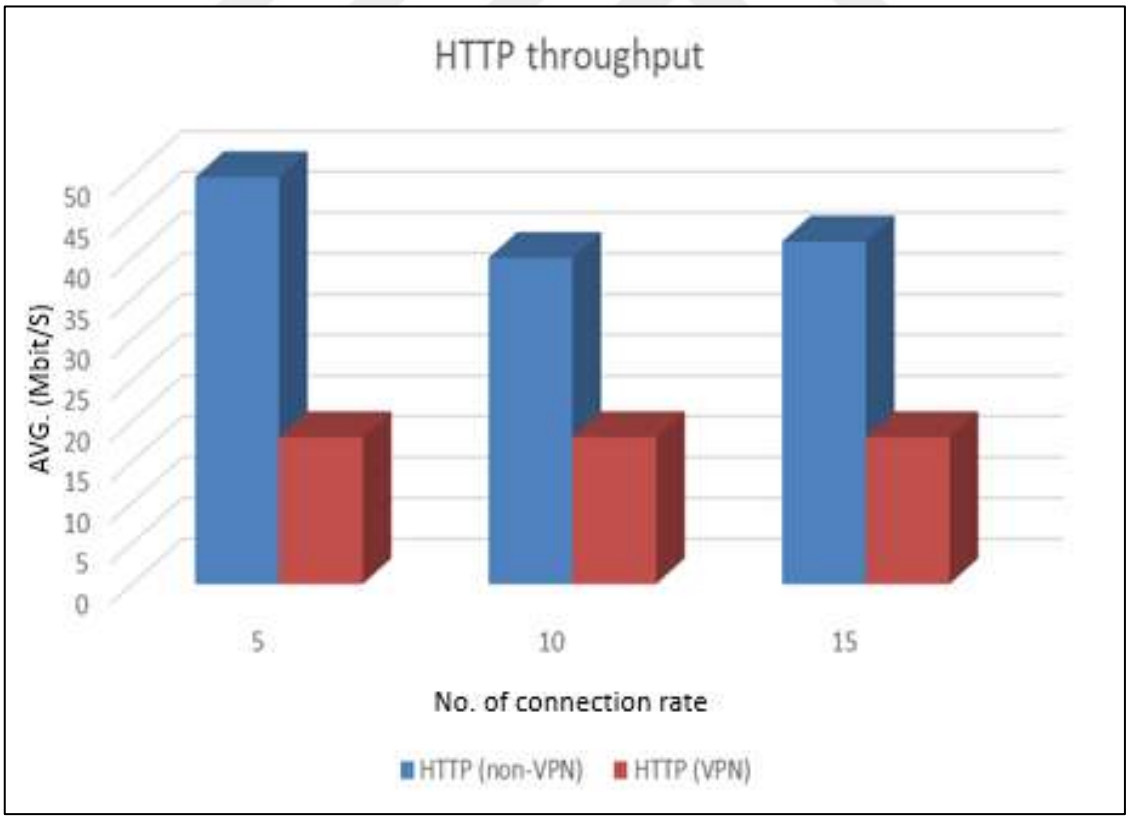

Figure 5.6: HTTP Performance Under VPN Versus non-VPN Conditions**.**

6. CONCLUSION

The research investigated the effects of VPN on network performance, with specific emphasis on throughput and latency. The investigation yielded several significant findings:

a. The research thoroughly investigated the modifications in connection types among three distinct protocols, namely HTTP, FTP, and CBR. The systematic methodology employed facilitated the observation and measurement of both throughput and time delay across diverse circumstances.
b. Prior to the implementation of a VPN, the throughput demonstrated a consistent performance across various protocols. Subsequent to the implementation of the VPN infrastructure, a noticeable reduction in data transfer rates was observed specifically for the (FTP) and (HTTP) protocols. It is noteworthy that the performance of the (CBR) protocol exhibited minimal impact from the VPN.
c. Significantly, the study revealed a remarkable pattern in the average duration of delay. The implementation of the VPN network led to a noticeable rise in the average latency experienced across the three protocols, namely (CBR), (HTTP), and (FTP).

The discoveries provide insight into the complex relationship between the deployment of VPNs and the performance of networks, revealing the subtle differences in data transfer rate and latency among various types of network traffic. The findings offer significant insights into the inherent trade-offs and considerations associated with utilizing VPN technology to bolster network security, while also impacting the dynamics of network performance.

In the future work, a multitude of captivating avenues arise from the findings of this study. Improving VPN configurations to mitigate the decrease in data transfer rate, conducting protocol-specific analyses to develop customized VPN strategies, and implementing hybrid VPN approaches may present more sophisticated resolutions. Additional investigation into network architecture, empirical evaluation, and the specific effects on applications may reveal valuable practical knowledge. Promising avenues include the exploration of dynamic VPN adaptation, comparative analyses involving various protocols, and the development of energy-efficient VPN implementations. Evaluating the user experience and the wider environmental implications of VPN deployment has the potential to offer a comprehensive viewpoint. By thoroughly examining these instructions, a deeper understanding of the impact

of VPN on network performance and security can be attained, facilitating the development of stronger and more flexible network solutions

REFERENCES

[1] Yin, C. (2021, May). Application of Virtual Private Network Technology in University Network Information Security. In Journal of Physics: Conference Series (Vol. 1915, No. 4, p. 042071). IOP Publishing.

[2] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177-183.

[3] Kepuska, V., & Bohouta, G. (2018, January). Next-generation of virtual personal assistants (microsoft cortana, apple siri, amazon alexa and google home). In 2018 IEEE 8th annual computing and communication workshop and conference (CCWC) (pp. 99-103). IEEE.

[4] Lopez, M. A., Baddeley, M., Lunardi, W. T., Pandey, A., & Giacalone, J. P. (2021, July). Towards secure wireless mesh networks for UAV swarm connectivity: Current threats, research, and opportunities. In 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS) (pp. 319-326). IEEE.

[5] Fang, C., Yao, H., Wang, Z., Wu, W., Jin, X., & Yu, F. R. (2018). A survey of mobile information-centric networking: Research issues and challenges. IEEE Communications Surveys & Tutorials, 20(3), 2353-2371.

[6] Ambika, N. (2019). Energy-perceptive authentication in virtual private networks using GPS data. Security, privacy and trust in the IoT environment, 25-38.

[7] Suo, S., Chen, L., Cheng, R., Kuang, X., & Zou, J. (2021, December). Design of Secure Access to Distributed Load Resources of Virtual Power Plant based on Virtual Communication Private Network. In 2021 IEEE Sustainable Power and Energy Conference (iSPEC) (pp. 4142-4149). IEEE.

[8] Ramesh, R., Vyas, A., & Ensafi, R. (2023, May). All of them claim to be the best": Multi-perspective study of VPN users and VPN providers. In 32nd USENIX Security Symposium (USENIX Security 23). USENIX Association.

[9] Wibisono, G., Nasution, A. S., Firmansyah, T., & Prabuwono, A. S. (2020). Hybrid Reversible Data Hiding in Encrypted Satellite Images Using Fluctuation

Modification Extraction and Reed-Solomon Code Embedding. IEEE Access, 8, 221367-221384.

[10] Lackorzynski, T., Köpsell, S., & Strufe, T. (2019, May). A comparative study on virtual private networks for future industrial communication systems. In 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS) (pp. 1-8). IEEE.

[11] Kaur, S., Kaur, G., & Shabaz, M. (2022). A secure two-factor authentication framework in cloud computing. Security and Communication Networks, 2022, 1-9.

[12] Qazi, A. S., & Ahmad, W. (2018). Performance estimation of real-time video conferencing in MPLS and non MPLS environment. International Journal of Networks and communications, 8(2), 34-36.

[13] Taneja, D., & Tyagi, S. S. (2019). Factors impacting the performance of data transferred via vpn. International Journal of Innovative Technology and Exploring Engineering, 8, 2962-2966.

[14] Kurniawan, D. E., Arif, H., Nelmiawati, N., Tohari, A. H., & Fani, M. (2019, March). Implementation and analysis ipsec-vpn on cisco asa firewall using gns3 network simulator. In Journal of Physics: Conference Series (Vol. 1175, No. 1, p. 012031). IOP Publishing.

[15] Bibraj, R., Chug, S., Nath, S. A. N. K. A. R., & Singh, S. L. (2018). Technical study of remote access VPN and its advantages over site to site VPN to analyze the possibility of hybrid setups at radar stations with evolving mobile communication technology. MAUSAM, 69(1), 97-102.

[16] Simatimbe, C. K., & Lubobya, S. C. (2020). Performance evaluation of an internet protocol security (IPSec) based multiprotocol label switching (MPLS) virtual private network. Journal of Computer and Communications, 8(9), 100-108.

[17] Habibovic, S. (2019). Virtual Private Networks: An Analysis of the Performance in State-of-the-Art Virtual Private Network solutions in Unreliable Network Conditions.

[18] Khan, M. T., DeBlasio, J., Voelker, G. M., Snoeren, A. C., Kanich, C., & Vallina-Rodriguez, N. (2018, October). An empirical analysis of the commercial vpn ecosystem. In Proceedings of the Internet Measurement Conference 2018 (pp. 443-456).

[19] Coonjah, I., Catherine, P. C., & Soyjaudah, K. M. S. (2018, October). Design and Implementation of UDP Tunneling-based on OpenSSH VPN. In 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (pp. 640-645). IEEE.

[20] Akter, H., Jahan, S., Saha, S., Faisal, R. H., & Islam, S. (2022, February). Evaluating performances of VPN tunneling protocols based on application service requirements. In Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering: TCCE 2021 (pp. 433-444). Singapore: Springer Nature Singapore.

[21] Zeebaree, D. Q., Haron, H., & Abdulazeez, A. M. (2018, October). Gene selection and classification of microarray data using convolutional neural network. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 145-150). IEEE.

[22] Zebari, R., Abdulazeez, A., Zeebaree, D., Zebari, D., & Saeed, J. (2020). A comprehensive review of dimensionality reduction techniques for feature selection and feature extraction. Journal of Applied Science and Technology Trends, 1(2), 56-70.

[23] Jyothi, K. K., & Reddy, B. I. (2018). Study on virtual private network (VPN), VPN's protocols and security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3(5), 919-932.

[24] Budiyanto, S., & Gunawan, D. (2023). Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice over Internet Protocol. IEEE Access.

[25] Tran, N. H., Phung, C. V., Nguyen, B. Q., & Bahri, L. (2018). An Effective Privacy-Preserving Data Coding in Peer-To-Peer Network. arXiv preprint arXiv:1806.05430.

[26] Randolph, M., & Diehl, W. (2020). Power side-channel attack analysis: A review of 20 years of study for the layman. Cryptography, 4(2), 15.

[27] Felgueiras, N., & Pinto, P. (2021). An Overview of the Status of DNS and HTTP Security Services in Higher Education Institutions in Portugal. International Summit Smart City 360°, 457-469.

[28] Tarkhani, Z., & Madhavapeddy, A. (2020). $\mu $ Tiles: Efficient Intra-Process Privilege Enforcement of Memory Regions. arXiv preprint arXiv:2004.04846.

[29] Semwal, P.; Sharma, M.K. Comparative study of different cryptographic algorithms for data security in cloud computing. In Proceedings of the 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA), Dehradun, India, 15–16 September 2017.

[30] Luo, J.; Ji, Q. Password Acquisition and Traffic Decryption Based on L2TP/IPSec. In Proceedings of the IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 28–31 October 2020.

[31] Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91-99.

[32] Gentile, A. F., Fazio, P., & Miceli, G. (2021, November). A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios. In Telecom (Vol. 2, No. 4, pp. 430-445). MDPI.

[33] Burkert, C., McDougall, J. A., Federrath, H., & Fischer, M. (2021, June). Analysing leakage during VPN establishment in public Wi-Fi networks. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.

[34] Ahmat, D., & Magoni, D. (2018). A Survey on Secure and Resilient Session Schemes: Technical Comparison and Assessment. ICST Transactions on Ubiquitous Environments, 4(13).

[35] Chen, T.-C.; Chen, J.C.; Liu, Z.H. Secure Network Mobility (SeNEMO) for Real-Time Applications. In Proceedings of the IEEE Transactions on Mobile Computing, Abu Dhabi, United Arab Emirates, 10 October 2011; Volume 10, pp. 1113–1130.

[36] Ernst, T.; Tj, K. Network Mobility Working Group, IETF. Available online: https://datatracker.ietf.org/wg/nemo/about/ (accessed on 18 May 2021).

[37] Guirado, R.; Padró, J.C.; Zoroa, A.; Olivert, J.; Bukva, A.; Cavestany, P. StratoTrans: Unmanned Aerial System (UAS) 4G Communication Framework Applied on the Monitoring of Road Traffic and Linear Infrastructure. Drones 2021, 5, 10. [CrossRef]

[38] Hu, Z., Yan, H., Yan, T., Geng, H., & Liu, G. (2020). Evaluating QoE in VoIP networks with QoS mapping and machine learning algorithms. Neurocomputing, 386, 63-83.

[39] Álvares, P.; Silva, L.; Magaia, N. Blockchain-Based Solutions for UAV-Assisted Connected Vehicle Networks in Smart Cities: A Review, Open Issues, and Future Perspectives. Telecom 2021, 2, 108–140. [CrossRef]

[40] Trevor Perrin, Noise Protocol Framework. Available online: http://www.noiseprotocol.org/ (accessed on 27 May 2021).

[41] Taib, A. M., Ishak, M. F. H., & Kamarudin, N. K. (2020). Securing network using raspberry Pi by implementing VPN, Pi-hole, and IPS (VPiSec). International Journal, 9(1.3).

[42] Gentile, A. F., Fazio, P., & Miceli, G. (2021, November). A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios. In Telecom (Vol. 2, No. 4, pp. 430-445). MDPI.

[43] P. Mishra, “Introduction to Cloud Computing,” Cloud Computing with AWS, pp. 1–34, 2023, doi: 10.1007/978-1-4842-9172-6_1.

[44] Mostafaei, H. (2018). Energy-efficient algorithm for reliable routing of wireless sensor networks. IEEE Transactions on Industrial Electronics, 66(7), 5567-5575.

[45] M. HOSAMO, “Source Traffic Modeling Using Pareto Traffic Generator,” Journal of Computer Networks, vol. 4, no. 1, pp. 11–19, Aug. 2017, doi: 10.12691/jcn-4-1-2.

[46] Kang, J., Xiong, Z., Niyato, D., Zou, Y., Zhang, Y., & Guizani, M. (2020). Reliable federated learning for mobile networks. IEEE Wireless Communications, 27(2), 72-80.

[47] Baratè, A., Haus, G., & Ludovico, L. A. (2019, January). State of the art and perspectives in multi-layer formats for music representation. In 2019 International Workshop on Multilayer Music Representation and Processing (MMRP) (pp. 27-34). IEEE.

[48] Rahim, R., Lubis, S., Wibowo, P., Siahaan, A. P. U., Hermansyah, H., & Djanggih, H. (2018). Prototype file transfer protocol application for LAN and Wi-Fi communication. Int. J. Eng. Technol, 7(2.13), 345-347.

[49] Ruwaida, D., & Kurnia, D. (2018). Rancang Bangun File Transfer Protocol (Ftp) Dengan Pengamanan Open Ssl Pada Jaringan Vpn Mikrotik Di Smk Dwiwarna. CESS (Journal of Computer Engineering, System and Science), 3(1), 45-49.

[50] "Professional Media Over Managed IP Networks: Constant Bit-Rate Compressed Video", doi: 10.5594/smpte.st2110-22.2019.

[51] Sun, W., He, X., Ren, C., Xiong, S., & Chen, H. (2022). A quality enhancement network with coding priors for constant bit rate video coding. Knowledge-Based Systems, 258, 110010.

[52] Salkute, R., & Vyawahare, D. G. Survey on Concurrent Multipath Scheduling for Real Time Video Streaming in Wireless Network.

[53] N. Singh, I. Elamvazuthi, P. Nallagownden, G. Ramasamy, and A. Jangra, "Routing Based Multi-Agent System for Network Reliability in the Smart Microgrid," Sensors, vol. 20, no. 10, p. 2992, May 2020, doi: 10.3390/s20102992.

[54] Panem, C., Rane, U. V., & Gad, R. S. (2022). Data of multilayer mesh NoC performance analysis for throughput and delay over FTP and CBR applications. Data in Brief, 42, 108196.