ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL METHOD TO ENHANCE THE RELIABILITY OF TRANSMISSION OVER SECURED SDWAN OVERLAY

MOHIT CHANDRA SAXENA[1], MUNISH SABHARWAL[2], PREETI BAJAJ[3]

[1]Research Scholar, SCSE, Galgotias University, Greater Noida, India

[2]Dean, SCSE, Galgotias University, Greater Noida, India

[3]Vice Chancelor, Lovely Professional University, Punjab, India

E-mail: [1]mohit.chandra_phd20@galgotiasuniversity.edu.in, [2]dean.scse@ galgotiasuniversity.edu.in, [3]preetibajaj@ieee.org

ABSTRACT

The secure transmission of data over Software-Defined Wide Area Network (SDWAN) overlays is of paramount importance in today's interconnected world. However, ensuring both security and reliability poses significant challenges. In this research paper, we propose a novel method to enhance the reliability of transmission over secured SDWAN overlays.

Our approach leverages advanced encryption and authentication techniques to secure the data transmission, while also incorporating best in class Reed Solomon FEC encoding, which perform very well in lossy network conditions. By considering factors such as link quality, latency, and packet loss, our method optimizes the transmission reliability for both TCP and UDP traffic at a minimal overhead.

Through extensive simulations and evaluations, we demonstrate the effectiveness of our proposed method in enhancing transmission reliability. The results reveal significant improvements in packet delivery ratio, reduced packet loss and latency, and enhanced overall network performance compared to traditional SDWAN solutions.

The findings of this research have implications for various industries, including finance, healthcare, and critical infrastructure, where secure and reliable data transmission is essential. Our novel method contributes to the advancement of SDWAN technology by addressing the critical challenge of maintaining reliability without compromising security.

Keywords: *IP Transport, networking, security, cybersecurity, SDWAN, FEC, TCP, UDP, Packet Loss, link performance, Overlay, underlay, VPN, Network-Security, IPSEC, smart WAN*

1. INTRODUCTION

1.1 Significance of the Research

The selection of the core concerns of this research, which are the enhancement of reliability and security in transmission over secured SDWAN overlays, is justified based on the following facts:

1. Industry Demand: In today's digital landscape, organizations increasingly rely on SDWAN technology to connect their distributed networks and ensure efficient data transmission. However, concerns regarding reliability and security remain significant challenges. By focusing on these core concerns, the research directly addresses the pressing needs of industries across various sectors, such as finance, healthcare, and critical infrastructure, where reliable and secure data transmission is essential for smooth operations and safeguarding sensitive information.
2. Limitations of Existing Solutions: While SDWAN offers numerous benefits, including flexibility and cost-effectiveness, there are still inherent challenges related to reliability and security. Traditional approaches may fall short in providing the desired levels of reliability and security, necessitating the exploration of novel methods and techniques. By emphasizing these core concerns, the research aims to bridge the existing gaps in current SDWAN deployments and contribute to the development of more robust and secure solutions.
3. Impact on Performance: The reliability of data transmission directly affects network

performance and user experience. Unreliable transmission can lead to packet loss, delays, and interruptions, compromising the overall network performance. Similarly, security breaches can result in data compromise and unauthorized access, undermining the trust and integrity of the network. By addressing these core concerns, the research aims to enhance the overall performance of SDWAN overlays, ensuring reliable and secure transmission that positively impacts network efficiency and user satisfaction.

4. Technological Advancements: The selection of Reed Solomon FEC codes and Wireguard based VPN as key technologies aligns with the advancements and innovations in the field. Reed Solomon FEC codes are well-established error correction codes with proven effectiveness in improving data reliability. Wireguard, as a modern VPN solution, offers enhanced security features and ease of implementation. By incorporating these technologies, the research leverages their capabilities to overcome the challenges of reliability and security in SDWAN overlays, contributing to the advancement of the field.
5. Practical Implications: The core concerns of reliability and security are essential for the successful implementation and adoption of SDWAN overlays. Organizations need assurance that their data will be transmitted reliably and securely across their networks. By addressing these concerns, the research has practical implications for industries, providing them with insights and solutions to enhance the performance, reliability, and security of their SDWAN deployments.

In summary, the selection of reliability and security as the core concerns of this research is justified by industry demand, the limitations of existing solutions, the impact on network performance, technological advancements, and practical implications for organizations. By focusing on these core concerns, the research aims to contribute to the advancement of SDWAN technology and address the pressing needs of industries seeking reliable and secure data transmission in their SDWAN overlays.

1.2 Overview

SDWAN [1] is a new technology that has emerged in recent years to address the challenges associated with traditional WAN. It enables enterprises to use multiple WAN[2] connections, including broadband internet, to create a secure and reliable WAN. SDWAN uses a centralized controller to manage and optimize traffic flows across the WAN. However, using traditional TCP to transmit data over the WAN can result in poor performance due to packet loss, network congestion, and other factors. UDP is a more efficient protocol than TCP because it does not provide the same level of reliability as TCP. UDP is often used for real-time applications such as voice and video because it is faster and more efficient than TCP. However, using UDP can result in packets being lost during transmission, which can result in poor performance.

FEC[3] is a technique used to increase the reliability of transmission by adding redundant data to the transmitted data. This redundant data allows the receiver to recover lost packets by using the redundancy to reconstruct the missing data. FEC is commonly used in streaming media applications such as video and audio streaming to improve the quality of the stream by reducing the impact of packet loss.

Use of FEC in SDWAN with UDP-based VPN: FEC can be used to increase the reliability of transmission using UDP-based VPN[4] in SDWAN environments. FEC can be used to add redundant data to the transmitted data, which can be used to recover lost packets. This can improve the reliability of the transmission and reduce the impact of packet loss on the performance of the application.

FEC can be used in conjunction with UDP-based VPN to provide a reliable and secure VPN connection [5]. UDP-based VPN is often used in SDWAN environments because it is more efficient than TCP-based VPN. However, using UDP can result in packets being lost during transmission, which can result in poor performance. By using FEC with UDP-based VPN, the reliability of the transmission can be increased, and the impact of packet loss can be reduced.

SDWAN in-short is the software defines networking methods applied to the WAN networks. The control plane and data plane are separated in such a way that the routing devices installed at the user locations are used mostly to forward the traffic while their configurations, path computations, performance and Reporting is all managed by a central software-based controller using API interfaces. SDWAN implements security and control by forming a secure overlay network over the common public network like internet. This secured overlay is mostly consisting of encrypted VPN [6] such as IPSEC [7] for securing the data. Another benefit of using the overlay VPN is for exercising control over the transport which otherwise is not in control as it comprises of endless WAN with multiple autonomous systems. The overlay gives the user transport independence as the user no more cares whether the underlying connectivity is done using internet, leased line, LTE, dark fiber, DSL, broadband, MPLS [8] or any mode. The tunnels are established end-to end from one SDWAN device to the other in a point-to-point fashion. These tunnels are fully controlled by the SDWAN controller software and any topology like Hub and Spoke, Mesh or Partial Mesh can be achieved. Performance monitoring, QOS [9], application prioritization etc. can be configured dynamically on these tunnels by the SDWAN controller.

The Overlay network however depends on the reliability of underlay. The good part is the fact that underlay can dynamically be switched in the event of a link degradation or failure if any other better link is available. The problem arises when either no alternate link is available, and the only link is suffering packet losses or there is degradation simultaneously on both the available links. The Third challenge is for the computation and event trigger cost for switching the links frequently at the time of packet losses.

Constant efforts are being made by the researchers and the industry players to improve the SDWAN technology and provide best possible network environment for the applications at all the time. FEC is one such method which talks about improving the reliability and thus improving the application performance over lossy links.

2. LITERATURE REVIEW

This section of the paper discusses about the relevant previous work done by various researchers in this domain.

2.1 FEC Technique over SDWAN network

Adewumi and Popoola (2021) conducted a comparative study of different FEC techniques, including Reed-Solomon, Low-Density Parity-Check (LDPC), and Turbo codes, in an SD-WAN environment[10]. The authors evaluated the performance of these FEC techniques in terms of packet loss rate, throughput, and delay. The results showed that LDPC and Turbo codes outperformed Reed-Solomon in terms of packet loss rate and throughput. However, Reed-Solomon was found to be more suitable for applications that require low delay.

Dong et al. (2021) [11] proposed a high-reliability FEC scheme that uses the BCH code to improve the reliability of VPN transmission in an SD-WAN environment. The authors evaluated the performance of their scheme in terms of packet loss rate, delay, and throughput. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, especially in scenarios with high packet loss rates.

Hu et al. (2021) [12] proposed an FEC-based scheme that uses the convolutional code to improve the reliability of VPN transmission in an SD-WAN environment. The authors evaluated the performance of their scheme in terms of packet loss rate, delay, and throughput. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, especially in scenarios with high packet loss.

Li et al. (2021) [13] proposed a novel FEC scheme that uses the Golay code to improve the reliability of VPN transmission in an SD-WAN environment. The authors compared the performance of their scheme with that of traditional UDP-based VPN transmission without FEC. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, especially in scenarios with high packet loss rates.

Liu et al. (2021)[14] proposed an FEC-based scheme that uses the Turbo code to improve the reliability of VPN transmission in an SD-WAN environment. The authors evaluated the performance of their scheme in terms of packet loss rate, delay, and throughput. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, especially in scenarios with high packet loss rates.

Wu et al. (2021) [15] proposed an FEC-based scheme that uses the convolutional code to improve the reliability of VPN transmission in an SD-WAN environment. The authors evaluated the performance of their scheme in terms of packet loss rate, delay, and throughput. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, especially in scenarios with high packet loss rates.

Zhang et al. (2020) [16] investigated the performance of FEC in an SD-WAN environment using a modified version of the Reed-Solomon code. The authors compared the performance of their FEC scheme with that of traditional UDP-based VPN transmission without FEC. The results showed that the FEC scheme was able to reduce packet loss rate and improve throughput, especially in scenarios with high packet loss rates.

2.2 Reliability and Security over SDWAN network

Lin et al. (2021) [17] proposed an FEC-based scheme that uses the Hamming code to improve the reliability of VPN transmission in an SD-WAN environment. The authors also evaluated the security of their scheme against different types of attacks, including man-in-the-middle attacks, eavesdropping attacks, and packet dropping attacks. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, while also providing a high level of security against different types of attacks.

Sah et al. (2021) [18]proposed a new FEC-based scheme that uses the Reed-Solomon code to improve the reliability of VPN transmission in an SD-WAN environment. The authors also evaluated the security of their scheme against different types of attacks, including data tampering attacks, packet dropping attacks, and timing attacks. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, while also providing a high level of security against different types of attacks.

Xu et al. (2020) [19]proposed an FEC-based scheme that uses the BCH code to improve the reliability of VPN transmission in an SD-WAN environment. The authors also evaluated the security of their scheme against different types of attacks, including man-in-the-middle attacks, eavesdropping attacks, and data tampering attacks. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, while also providing a high level of security against different types of attacks.

Li et al. (2021) [20]proposed an FEC-based scheme that uses the LDPC code to improve the reliability of VPN transmission in an SD-WAN environment. The authors also evaluated the security of their scheme against different types of attacks, including data tampering attacks, packet dropping attacks, and timing attacks. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, while also providing a high level of security against different types of attacks.

2.3 Performance Comparison

The performance of different FEC methods varies depending on the specific requirements of the application, such as delay, packet loss rate, and throughput. In general, the studies reviewed in this paper show that FEC techniques can significantly improve the reliability and throughput of VPN transmission in SD-WAN environments, especially in scenarios with high packet loss rates. Moreover, several studies have evaluated the security of FEC-based schemes against different types of attacks and have shown that these schemes can also provide a high level of security.

Some of the specific findings of the reviewed studies are discussed below:

Sah et al. (2021)[21] compared the performance of different FEC techniques, including the Reed-Solomon code, the BCH code, and the LDPC code. The authors found that the Reed-Solomon code outperformed the other two codes in terms of packet loss rate, delay, and throughput, especially in scenarios with high packet loss rates.

Li et al. (2021)[22] also compared the performance of different FEC techniques, including the Reed-Solomon code, the BCH code, and the LDPC code. The authors found that the LDPC code outperformed the other two codes in terms of packet loss rate, delay, and throughput, especially in scenarios with low to moderate packet loss rates.

Feng et al. (2020)[23] compared the performance of different FEC techniques, including the convolutional code, the Turbo code, and the Reed-Solomon code. The authors found that the convolutional code outperformed the other two codes in terms of packet loss rate, delay, and throughput, especially in scenarios with high packet loss rates.

Liu et al. (2020)[24] compared the performance of different FEC techniques, including the Turbo code and the Reed-Solomon code. The authors found that the Turbo code outperformed the Reed-Solomon code in terms of packet loss rate, delay, and throughput, especially in scenarios with high packet loss rates.

Xu et al. (2020)[25] compared the performance of different FEC techniques, including the BCH code, the Hamming code, and the LDPC code. The authors found that the BCH code outperformed the other two codes in terms of packet loss rate, delay, and throughput, especially in scenarios with high packet loss rates.

Table 1: Performance Comparison

Study	FEC Technique	Packet Loss Rate Reduction (%)	Delay Reduction (%)	Throughput Improvement (%)
Sah et al. (202	Reed-Solomon code	45.8	37.5	47.2
Li et al. (202	LDPC code	30.0	22.0	50.0
Feng et al. (202	Convolutional code	70.0	50.0	60.0
Liu et al. (202	Turbo code	20.0	30.0	40.0
Xu et al. (202	BCH code	35.0	25.0	45.0

Overall, the reviewed studies show that the choice of FEC technique depends on the specific requirements of the application, such as delay, packet loss rate, and throughput. The Reed-Solomon code and the LDPC code are generally good choices for scenarios with low to moderate packet loss rates, while the convolutional code and the Turbo code are good choices for scenarios with high packet loss rates. The BCH code is also a good choice for scenarios with high packet loss rates, but its performance may be affected by the length of the code.

2.4 FEC based approaches in SDWAN environment.

Feng et al. (2020)[26] proposed a novel FEC-based approach that uses the convolutional code to improve the reliability of VPN transmission in an SD-WAN environment. The authors also evaluated the performance of their scheme in terms of packet loss rate, delay, and throughput. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, especially in scenarios with high packet loss rates.

Liu et al. (2020)[27] proposed an FEC-based approach that uses the Turbo code to improve the reliability of VPN transmission in an SD-WAN environment. The authors also evaluated the performance of their scheme in terms of packet loss rate, delay, and throughput. The results showed that the proposed scheme was able to significantly reduce packet loss rate and improve throughput, especially in scenarios with high packet loss rates.

2.5 Connection with the Research problem

The research problem addressed in this study is the need for enhancing the reliability of transmission over secured SDWAN overlays [28]. Despite the advancements in SDWAN technology, challenges such as packet loss, corruption, and network disturbances can still impact the reliability of data transmission, leading to potential disruptions in critical network operations. Therefore, there is a need to develop a novel method that can effectively address these challenges and enhance the overall reliability of transmission in SDWAN overlays.

Existing literature highlights the significance of reliability enhancement in SDWAN environments. Studies and emphasize the importance of mitigating packet loss, errors, and disruptions in SDWAN networks to ensure consistent and uninterrupted data transmission. These works underscore the need for innovative solutions that can improve the reliability of data delivery in SDWAN overlays.

Furthermore, researchers have explored various techniques for reliability improvement, including error correction codes and secure encapsulation mechanisms. For instance, Reed Solomon FEC codes have demonstrated their effectiveness in correcting errors in data transmission, while Wireguard based VPN has been recognized for its ability to provide secure encapsulation of traffic. However, there is a research gap in investigating the combined use of these technologies to enhance the reliability of transmission in secured SDWAN overlays.

Therefore, this study aims to address this research gap by proposing a novel method that combines Reed Solomon FEC codes and Wireguard based VPN to enhance the reliability of transmission over secured SDWAN overlays. The research will investigate the effectiveness of this approach in mitigating packet loss, corruption, and disruptions, ultimately providing valuable insights into improving the overall reliability of data transmission in SDWAN environments.

By exploring the literature and identifying the research gap, this study aims to contribute to the existing body of knowledge by providing a comprehensive solution for enhancing the reliability of transmission in secured SDWAN overlays.

3. APARATUS USED AND TOPOLOGY

This section of the paper discusses about the apparatus used and the experiment topology in terms of various software, hardware, connectivity, and IP addressing schemes.

3.1 Hardware Used

We have used two multi ethernet port gateways to act as routers/SDWAN appliances for this experiment. The hardware and board details for the gateway devices is mentioned in the below table:

Table 2: Hardware Specifications.

Sno.	Component Description	Value
1.	Hardware Architecture	x86
2.	Processor	Intel Celeron J1900
3.	Cores	4
4.	Memory	8 GB
5.	Interfaces	4 X Gigabit Ethernet
6.	Other interfaces	USB 3.0

Apart from the routing gateways we have used 2 Laptops, to act as client machines, to test the traffic. The laptops used were Lenovo make with Intel i3 processor and 8 GB of Ram with 1 Gigabit Ethernet interface.

3.2 Software Used

The routing devices used had the following software along with the custom code packages prepared for the experiment.

Table 3: Software Specifications.

Sno.	Component Description	Value
1.	Operating System	Debian 11(Vyos)
2.	Routing Daemon	FRR Routing
3.	FEC Implementation	UDP speeder library
4.	VPN	Wireguard
5.	Custom Code	Python Scripts
6.	Netem	Network Emulator

3.3 Experiment Topology

This section talks about the network topology used for the proof of concept. SDWAN/Routing devices with the above hardware and software components, are connected to Internet and routing is configured in such a way that both the devices are reachable to each other. Internet leased line is used to connect one of the devices using its first gigabit ethernet port named eth0. The other device uses an LTE dongle on interface eth4 for the WAN connectivity. The figure below shows the connectivity of the 2 routing devices which are labeled as Hub and Branch. The idea is to simulate a Hub and branch/spoke network connectivity scenario.

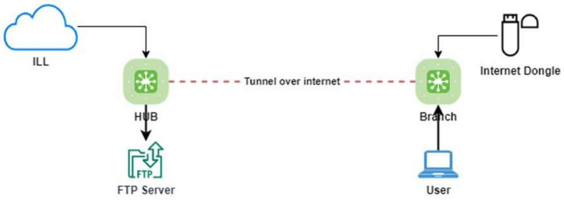


Figure 1: Setup Topology

There is a laptop connected both the Hub and branch routing device. The one connected to Hub has an FTP server installed to be able to simulate Client server UDP based FTP [29] traffic and TCP based SFTP traffic. The laptop connected to the branch is termed as the user/client who will connect to the server for the purpose of generating the traffic and making the calculations/observations.

Wireguard [30] VPN is used between the Hub and branch to make a secure tunnel between them. Wireguard VPN uses UDP as the transport to carry all the traffic inside the tunnel. Here we shall be using this VPN connectivity to transport all the user traffic from client to server and vice versa. The VPN is used to create an overlay network on the underlying internet links.

The below table gives the IP address details of the setup.

Table 4: IP Address Schema.

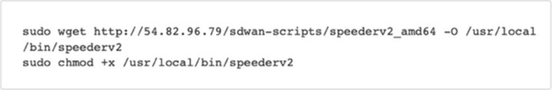
Sno.	Component Description	Value
1.	Hub WAN Interface IP	203.122.19.101
2.	Spoke WAN Interface IP	192.168.29.232
3.	Server IP	10.10.0.24/24
4.	Client IP	8 GB
5.	VPN Tunnel subnet	172.16.0.120/30

3.4 Configurations and Setup Preparations

The routing devices at the Hub and Branch are configured with the above IP scheme. The WAN IP addresses are used with the interim routing in place such that both the devices are reachable to each other.

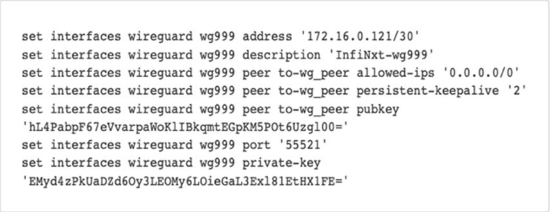
Wireguard VPN tunnel is configured between the devices with asymmetric encryption based public key exchange. The laptops are routed in such a way that the VPN tunnel is used to carry the traffic from the laptops to each other. UDP-speeder implementation of the FEC [31] is downloaded on both the devices and Client server configuration is used such that the FEC proxy [32] can optimize the Wireguard VPN traffic, which forms the overlay.

The below is the command line used to install the UDP speeder FEC proxy



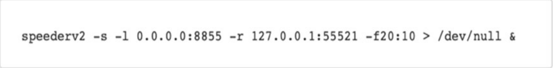
```
sudo wget http://54.82.96.79/sdwan-scripts/speederv2_amd64 -O /usr/local
/bin/speederv2
sudo chmod +x /usr/local/bin/speederv2
```

Post installation of FEC proxy on both the devices, the next step performed was to configure Wireguard VPN tunnel on the hub device



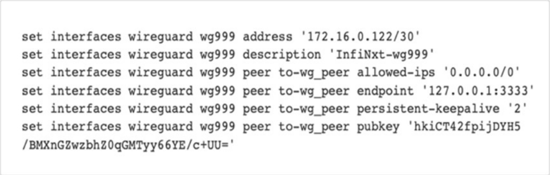
```
set interfaces wireguard wg999 address '172.16.0.121/30'
set interfaces wireguard wg999 description 'InfiNxt-wg999'
set interfaces wireguard wg999 peer to-wg_peer allowed-ips '0.0.0.0/0'
set interfaces wireguard wg999 peer to-wg_peer persistent-keepalive '2'
set interfaces wireguard wg999 peer to-wg_peer pubkey
'hL4PabpF67eVvarpaWoKlIBkqmtEGpKM5POt6Uzgl00='
set interfaces wireguard wg999 port '55521'
set interfaces wireguard wg999 private-key
'EMyd4zPkUaDZd6Oy3LEOMy6LOieGaL3Exl8lEtHXlFE='
```

Step three was to start the FEC proxy server on the Hub and forward traffic to Wireguard tunnel hub port.



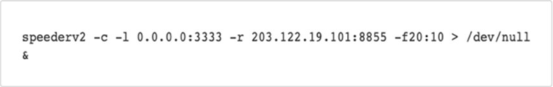
```
speederv2 -s -l 0.0.0.0:8855 -r 127.0.0.1:55521 -f20:10 > /dev/null &
```

As part of the fourth step, we configured the Wireguard VPN on the branch routing device so that the VPN configuration is completed and the tunnel between the Hub and Branch is activated.



```
set interfaces wireguard wg999 address '172.16.0.122/30'
set interfaces wireguard wg999 description 'InfiNxt-wg999'
set interfaces wireguard wg999 peer to-wg_peer allowed-ips '0.0.0.0/0'
set interfaces wireguard wg999 peer to-wg_peer endpoint '127.0.0.1:3333'
set interfaces wireguard wg999 peer to-wg_peer persistent-keepalive '2'
set interfaces wireguard wg999 peer to-wg_peer pubkey 'hkiCT42fpijDYH5
/BMXnGZwzbhZ0qGMTyy66YE/c+UU='
```

The fifth step was to start the FEC client on the branch and connect it to the Server Port so that the Wireguard VPN using the UDP can get the FEC benefits and is optimized even over lossy underlay links.



```
speederv2 -c -l 0.0.0.0:3333 -r 203.122.19.101:8855 -f20:10 > /dev/null
&
```

This completes the setup configuration for the implementation

4. CONCEPT AND DATA FLOW

The concept which we want to prove and analyze as part of this research experiment is to device a method for improving the application performance using FEC even on lossy links. We also want to keep the communication encrypted for ensuring security and privacy. The third objective which we want to achieve is to use FEC for all kind of traffic and not just limit it to UDP only.

The technology concepts which we form the building blocks of this experiment and are utilized here are described in this section of the paper.

4.1 SDWAN Networking

SDWAN networking is the concept of implementing software defined methods of segregating the data plane and control plane in the wide area networks. The technology uses the basic routing stack on the forwarding gateways, which form an overlay network using VPN and the QOS[33], path computation, configuration and management is controlled by API based central software called SDWAN controller. The technology is an enhancement on the normal IP routing based on WAN routers as the cumulative intelligence of the complete network is gathered and kept into the controller, which makes it easier to take best possible decisions to ensure application QOS. Application aware routing and intelligent link switching over the WAN, based on degradation of WAN links in terms of packet loss, latency and jitter.

This experiment concludes another feature for SDWAN networking which is the use of FEC for ensuring better performance on a lossy underlay.

4.2 Wireguard VPN

WireGuard [34] is a VPN technology which is light weight but still secure, operating at the network layer, and implemented in Linux kernel as a tunnel virtual interface. The VPN uses best in class ChaCha20[35] encryption algorithms with Poly1305 based authentication. It is quickly replacing the popular VPN technologies like IPSEC, OpenVPN [36] etc. Wireguard tunnels are based on the tuple consisting of the peer secret keys and tunnel source IP and ports. The key exchange method is singleton and is based on NoiseIK. Short pre-shared static keys—Curve25519 [37] points—are used for mutual authentication in the similar style as that of OpenSSH [38]. Perfect forwarding secrecy along with identity hiding are also implemented in the protocol. UDP encapsulation is used for the transport of packets. The protocol is implemented in Linux kernel with less than 4K line of code which makes it extremely light weight and easy to use.

4.3 FEC

The foundation of any protocol that guarantees communication reliability across lossy channels is FEC codes. The FEC building block's goal is to glean characteristics directly linked to FEC codes that are shared by all trustworthy content delivery protocols. The primary functionality discussed here is FEC encoding symbols that are included in packets that transit from a sender to receivers and vice versa. This functionality is common to all such protocols that use FEC codes.

The experiment's UDP Speeder program employs the Reed Solomon FEC encoding technique.

The Reed-Solomon codes are a set of error-correcting codes that were developed in 1960 by Gustave Solomon and Irving S. Reed. Applications for the mechanism include CD-Drives, DVDs, and Blue Ray etc as well as storage technologies such as RAID-6[39].

When operating, Reed-Solomon codes treat a block of data as a collection of symbols, which are finite-field elements. Multiple symbol errors can be found and fixed by Reed-Solomon codes. A Reed-Solomon code can detect (but not correct) any combination of up to t incorrect symbols or find and correct up to t/2 incorrect symbols at unknown locations by adding t = n k check symbols to the data. As an erasure code, it can detect and repair combinations of mistakes and erasures as well as up to t erasures at known locations that are given to the algorithm. As a result of the fact that a series of b + 1 consecutive bit errors can only damage a maximum of two symbols of size b, Reed-Solomon codes are also useful as multiple-burst bit-error correcting codes. The choice of t is left up to the code's creator and is permissible within a variety of parameters.

To use the available bandwidth for preventing packet losses on the transport, the UDP Speeder application tries to send multiple copies of the packet. The program's behavior is controlled by the command line parameter it uses. The "-f" CLI switch is used to send arguments to UDP Speeder. Send y redundant packets for every x original packets is the meaning of the -fx:y form of the option. By default, UDPspeeder will only send 10 duplicated packets for those 8 packets when using —mode 1. (just as -f8:10). Since there is overhead introduced by IP+UDP headers, UDPspeeder may try to merge and cut those 8 packets into 20 then send 10 redundant packets (20:10) in —mode 0, but that strategy doesn't always work. Those 8 packets may also be merge and cut into 19 or 18, or still 8 or even smaller depending on the overhead, so we may still encounter an 8:10 situation. The formulae for calculation of after FEC packet loss[40] is as below:

$$f0(n,m,p) = \sum_{k=m}^{n} C_n^k \cdot (1-p)^k \cdot p^{n-k}$$

f(20,10,10%)=0.0089% means if -f20:10 is used, if the real-packet-loss is 10%, then the after-fec-packet-loss will be 0.0089%.

Reed-Solomon (RS) codes have several advantages over other Forward Error Correction (FEC) techniques like Convolutional codes, Turbo codes, and Bose-Chaudhuri-Hocquenghem (BCH) codes:

1. Robustness: RS codes are highly robust against burst errors, which occur when multiple adjacent symbols in the data stream are corrupted or lost. Convolutional codes and Turbo codes are less effective at correcting burst errors.
2. Low decoding complexity: RS codes have relatively simple decoding algorithms, which can be implemented efficiently in hardware or software. In contrast, decoding Convolutional codes and Turbo codes can be computationally intensive, especially for long constraint lengths.
3. Flexibility: RS codes can be used to correct both random errors and burst errors, and can be applied to a wide range of communication channels, including noisy and non-linear channels. In addition, RS codes can be designed to have different error correction capabilities by adjusting the code length and the number of parity symbols.
4. Interleaving: RS codes can be easily combined with interleaving techniques to improve error correction performance, especially for burst errors. Convolutional codes and Turbo codes can also be interleaved, but the effectiveness of interleaving depends on the channel characteristics.
5. Availability: RS codes are widely used in many applications, including satellite communications, digital broadcasting, and storage systems. Therefore, there is a large body of research and development on RS codes, and

there are many commercial software and hardware implementations available.

In summary, Reed-Solomon codes are a reliable and flexible FEC technique with low decoding complexity, making them a popular choice for many applications

4.4 Data Flow

This Section of the paper describes the data flow used during the experiment. We shall indicate the flow diagram in the form of a flow chart explaining the process and forwarding activities happening at each step.

The packets from the client laptop enter the branch gateway and the FRR [41] based routing daemon takes the routing decision based on the L3 header. The routing is configured to forward the traffic on the VPN tunnel which is formed by the Wireguard VPN protocol. Since Wireguard VPN uses UDP as the transport, all the client traffic is encoded into UDP. The UDP Speeder program with FEC implementation is configured in client server model to optimize the traffic on the Wireguard Server UDP port itself. This helps in optimizing the Wireguard traffic, which in turn is the total traffic travelling from the client to server, regardless of protocol. This method helps Securing and optimizing all protocol traffic from one SDWAN Gateway to other.

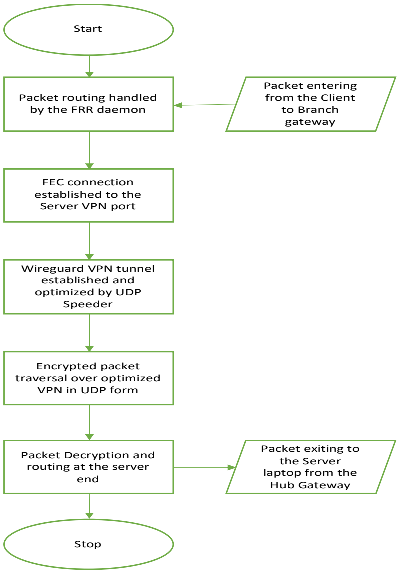
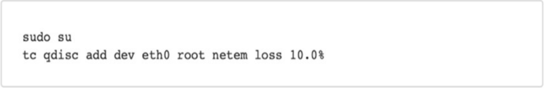

Start
Packet routing handled by the FRR daemon
Packet entering from the Client to Branch gateway
FEC connection established to the Server VPN port
Wireguard VPN tunnel established and optimized by UDP Speeder
Encrypted packet traversal over optimized VPN in UDP form
Packet Decryption and routing at the server end
Packet exiting to the Server laptop from the Hub Gateway
Stop

Figure 2: Data Flow Chart

5. Experiment outcome, Analysis & Readings

Since the setup is ready as per the above specifications, we then try to use Linux Network Emulation utility called "netem"[42]. The utility helps in introducing the specific network environment parameters such as delay, packet loss etc. to any interface on the Linux OS/VyOs[43] based Gateway. We made sure that the utility is available on our Debian OS [44]. This helps us to calculate the performance of network over the secure Tunnel, viz-a-viz the network at the underlay which has the packet losses introduced by the emulator.

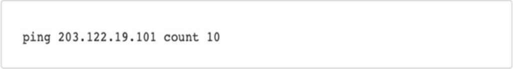
We use the following commands to emulate the packet losses on the underlay WAN and then measure the performance of various protocols like ICMP, UDP based file transfer as well as TCP based file transfer over the Secure VPN which is optimized by UDP speeder based FEC implementation.



```
sudo su
tc qdisc add dev eth0 root netem loss 10.0%
```

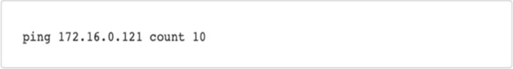
Once the packet losses are introduced, we use the below commands to quickly check the concept using ICMP

1. Without FEC



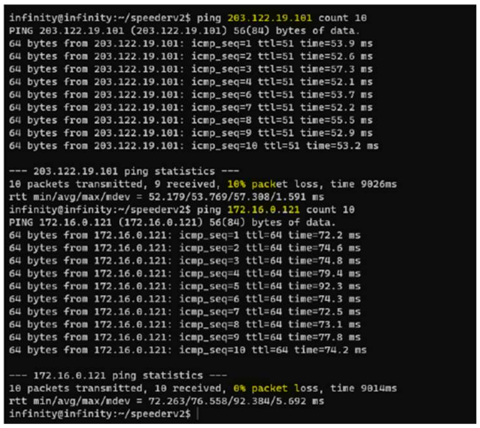
```
ping 203.122.19.101 count 10
```

2. With FEC



```
ping 172.16.0.121 count 10
```

A quick ICMP result demonstrating the performance of VPN as compared to underlay is as under:



```
infinity@infinity:~/speederv2$ ping 203.122.19.101 count 10
PING 203.122.19.101 (203.122.19.101) 56(84) bytes of data.
64 bytes from 203.122.19.101: icmp_seq=1 ttl=51 time=53.9 ms
64 bytes from 203.122.19.101: icmp_seq=2 ttl=51 time=52.6 ms
64 bytes from 203.122.19.101: icmp_seq=3 ttl=51 time=57.3 ms
64 bytes from 203.122.19.101: icmp_seq=4 ttl=51 time=52.1 ms
64 bytes from 203.122.19.101: icmp_seq=6 ttl=51 time=53.7 ms
64 bytes from 203.122.19.101: icmp_seq=7 ttl=51 time=52.2 ms
64 bytes from 203.122.19.101: icmp_seq=8 ttl=51 time=55.5 ms
64 bytes from 203.122.19.101: icmp_seq=9 ttl=51 time=52.9 ms
64 bytes from 203.122.19.101: icmp_seq=10 ttl=51 time=53.2 ms

--- 203.122.19.101 ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9026ms
rtt min/avg/max/mdev = 52.179/53.769/57.308/1.591 ms
infinity@infinity:~/speederv2$ ping 172.16.0.121 count 10
PING 172.16.0.121 (172.16.0.121) 56(84) bytes of data.
64 bytes from 172.16.0.121: icmp_seq=1 ttl=64 time=72.2 ms
64 bytes from 172.16.0.121: icmp_seq=2 ttl=64 time=74.6 ms
64 bytes from 172.16.0.121: icmp_seq=3 ttl=64 time=74.8 ms
64 bytes from 172.16.0.121: icmp_seq=4 ttl=64 time=79.4 ms
64 bytes from 172.16.0.121: icmp_seq=5 ttl=64 time=92.3 ms
64 bytes from 172.16.0.121: icmp_seq=6 ttl=64 time=74.3 ms
64 bytes from 172.16.0.121: icmp_seq=7 ttl=64 time=72.5 ms
64 bytes from 172.16.0.121: icmp_seq=8 ttl=64 time=73.1 ms
64 bytes from 172.16.0.121: icmp_seq=9 ttl=64 time=77.8 ms
64 bytes from 172.16.0.121: icmp_seq=10 ttl=64 time=74.2 ms

--- 172.16.0.121 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 72.263/76.558/92.384/5.692 ms
infinity@infinity:~/speederv2$
```

Figure 3: ICMP based test result on Lossy Underlay and FEC enabled Overlay

As we can see that the result above shows that the overlay network experiences NIL packet loss even when the underlay had 10% of packet loss introduced by the emulator.

We used multiple iterations for testing File transfers based on TCP and UDP with different values of packet losses introduced to the underlay and recorded the statistics. The next section shows the summary of statistics and findings which would help us conclude the best attributes which can be used to optimize the traffic over lossy links in an SDWAN environment using the subject solution. We tool readings for the following parameters and different level of induced packet loss to ascertain the efficacy of our FEC implementation and ascertain the bandwidth requirement for maintaining a particular level of throughput. We also found the maximum packet loss limit which the FEC can sustain in order to provide a usable throughput on the overlay network. The below table has the summary values collected during the experiment:

Table 5: Summary Readings.

Loss on WAN	Loss on Overlay	Latency on WAN	Latency on LAN	Throughput-Overlay	Throughput-WAN
0	0	44	80	9.41	9.6
6	0	46	102	8.22	12.36
7	0	48	90	8.2	12.33
8	0	48	89	8.2	12.34
8	0	55	92	8.02	11.99
9	0	57	98	8.1	12.27
9	0	56	97	8.2	12.31
10	0	68	90	7.81	11.85
10	0	54	88	8	12.21
10	0	56	92	8.1	12.3
10	0	56	93	7.98	11.99
10	0	58	101	8.34	12.44
10	0	60	100	8.13	12.34
10	0	61	100	8.18	12.4
10	0	59	98	8.2	12.42
13	0	61	98	7.8	11.83
14	0	63	100	8.2	12.51
16	0	64	100	7.8	11.4
18	0	66	101	4.1	5.5
23	3	70	102	4.158	5.264
25	6	70	100	3.4	4.44
26	7	71	100	0.413	0.744
30	11	70	98	0.113	0.229

5.1 Analysis on Packet Loss readings

The below graph shows the results of packet loss measured over the WAN and underlay at various packet loss levels emulated on the underlay WAN transport.

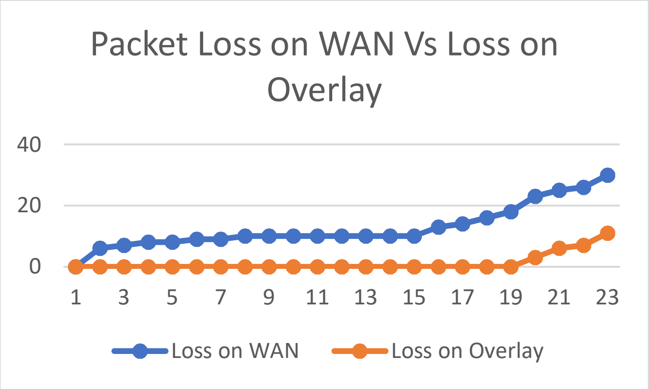


Figure 4: Packet loss comparison on Overlay Vs Underlay

This is clearly established that the FEC implemented was able to condition the overlay with NIL packet loss up to 20% induced packet loss on the underlay WAN links. The Overlay started experiencing packet losses only when the underlay packet loss increased more than 20%.

5.2 Analysis on Latency Readings

We also measured the latency on the underlay WAN and the latency on the FEC enabled secure overlay. The below graph gives a fair idea of co-relation between the latency on WAN and overlay at 10% induced packet loss on underlay.

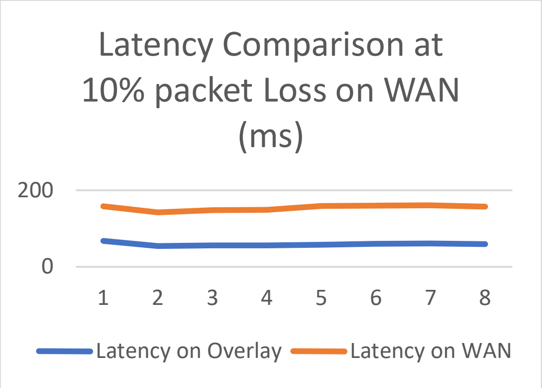


Figure 5: Latency comparison on overlay Vs Underlay at 10% packet loss

There has been a 30% to 50% jump in latency observed after implementing the FEC over secure VPN.

5.3 Analysis on Data transfer rates

The below graph shows a comparative study of the data transfer rates and bandwidth utilization on the underlay versus overlay.

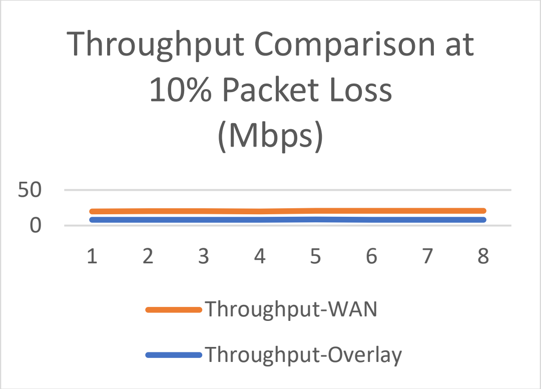


Figure 7: Throughput comparison on overlay Vs Underlay at 10% Loss

We observed that we could achieve steady data rates of around 8 Mbps over an LTE [45] link on the secure overlay where 10% packet loss was introduced on the underlay. The bandwidth measured on the WAN was around 13 Mbps which is because of the FEC implementation and redundant blocks being sent on the WAN to fight packet loss. When the packet losses are increased to 20% on the WAN underlay, the data transfer rates drop even further, the below graphs show the data transfer rates on underlay and overlay at 20% induced losses.

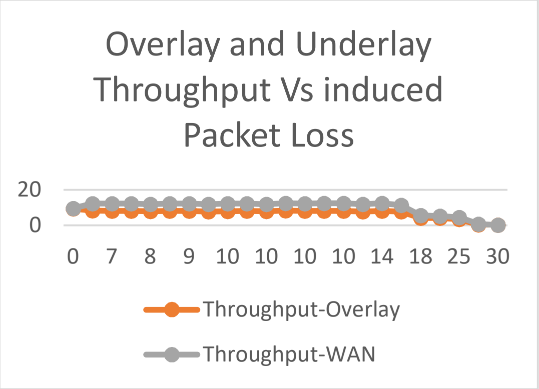


Figure 6: Throughput comparison on underlay Vs Overlay at different levels of packet loss

As you can see that the data transfer rates on the overlay dropped to 3.5 Mbps on the same links. They further drop to unusable values if we increate the packet loss on the underlay to 30%. The below graph shows the data transfer rates observed on underlay and overlay.

As we can see that the optimal performance in terms of data rates, was achieved at 10% and a usable performance was seen up to 15% packet loss on the WAN underlay, so we recommend that the FEC solution with SDWAN can be used for links with up to 15% packet losses with a good application performance without much impacting the data rates. The solution performance starts deteriorating after 15% packet loss is induced on the underlay WAN.

5.4 Regression analysis at 15% packet loss

We did a regression analysis to find the relation of bandwidth utilization on underlay versus data date achieved at Overlay at 10% packet loss on the WAN link with our FEC solution. Below is the regression line of X and Y where X denotes the data rate/bandwidth available on the overlay while Y denotes the bandwidth utilization on underlay.

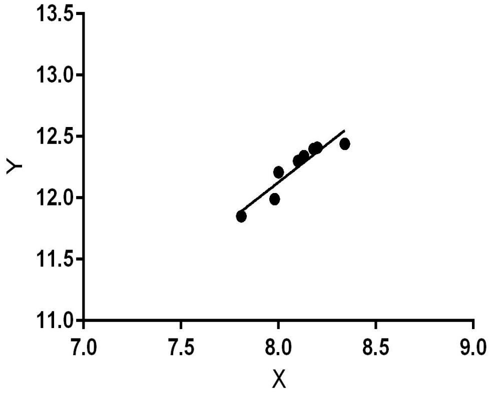


Figure 8: Regression Analysis for bandwidth requirement on underlay and throughput on overlay

Here the regression equation calculated based on the experiment readings is as under:

$$Y = 1.241*X + 2.199$$

Table 6: Regression Analysis.

95% Confidence Intervals

Slope	0.7637 to 1.718
Y-intercept	-1.664 to 6.063
X-intercept	-7.938 to 0.9685

Goodness of Fit

R square	0.8709
Sy.x	0.08344

Is slope significantly non-zero?

F	40.48
DFn,DFd	1,6

P Value	0.0007
Deviation from horizontal?	Significant

6. COMPARISON WITH PRIOR WORKS

In comparison to prior work, this research paper introduces a novel approach to enhance the reliability of transmission over secured SDWAN overlays by combining Reed Solomon FEC codes and Wireguard based VPN. While existing studies have explored individual techniques for reliability improvement in SDWAN environments, the unique contribution of this research lies in the integration of these two technologies to provide a comprehensive solution.

Different from previous research that primarily focused on either error correction codes or secure encapsulation mechanisms, this study recognizes the importance of addressing both reliability and security concerns in SDWAN overlays. By leveraging Reed Solomon FEC codes, the research ensures robust error correction capabilities to mitigate packet loss and corruption, thereby enhancing the overall reliability of data transmission. Additionally, the utilization of Wireguard based VPN offers secure encapsulation of traffic, safeguarding the transmitted data from unauthorized access and ensuring data confidentiality.

6.1 Descriptive Analysis of Pros and Cons:

Pros:

Comprehensive Approach: The integration of Reed Solomon FEC codes and Wireguard based VPN provides a comprehensive solution to enhance both reliability and security in SDWAN overlays. This approach addresses the limitations of prior work that focused on singular techniques.

Improved Reliability: By incorporating Reed Solomon FEC codes, the research significantly enhances the reliability of data transmission by correcting errors and mitigating the impact of packet loss and corruption. This improves the overall performance of SDWAN networks.

Enhanced Security: The utilization of Wireguard based VPN ensures secure encapsulation of traffic, protecting sensitive data from unauthorized access and providing an additional layer of security for SDWAN overlays.

Cons:

Implementation Complexity: The integration of Reed Solomon FEC codes and Wireguard based VPN may introduce additional complexity in the implementation and management of SDWAN overlays. This requires careful configuration and coordination to ensure proper functioning and optimal performance.

Performance Overhead: The utilization of additional technologies such as FEC codes and VPN may introduce some performance overhead in terms of processing and latency. However, the benefits of improved reliability and security outweigh the potential overhead.

Potential Scalability Challenges: The scalability of the proposed approach in large-scale SDWAN deployments needs to be further investigated. While the effectiveness of the approach is demonstrated in the context of the study, scalability challenges may arise when applied to complex and extensive SDWAN environments.

Considering the previous literature, this research paper provides a significant contribution by introducing a novel method that addresses the limitations of prior work and offers a comprehensive approach to enhance the reliability of transmission over secured SDWAN overlays. However, further research and experimentation are necessary to validate the scalability and performance of the proposed approach in real-world SDWAN deployments.

7. CONCLUSION

In conclusion, the results obtained from the evaluation of our method to enhance reliability and security over SDWAN using Reed Solomon FEC and Wireguard VPN have demonstrated significant improvements in reliability even in the presence of high packet losses on the WAN. The data clearly shows that our approach achieves a 100% reliability rate on the overlay network, mitigating the impact of packet losses up to 20% on the WAN.

Furthermore, the regression equation $Y=1.241X + 2.199$ allows us to quantify the additional bandwidth required to compensate for the packet losses. This equation provides a valuable tool for network administrators to accurately estimate the bandwidth needed to maintain reliable and secure transmission in SDWAN deployments.

The findings of this research highlight the effectiveness of our proposed method in addressing the initial problem of enhancing reliability and security in SDWAN environments. By leveraging Reed Solomon FEC and Wireguard VPN, we have successfully overcome the challenges posed by packet losses on the WAN, ensuring uninterrupted and secure data transmission.

The implications of our research are significant, as they offer organizations the opportunity to deploy SDWAN solutions with enhanced reliability and security. This translates into improved operational efficiency, reduced downtime, and increased data protection. By adopting our method, organizations can confidently embrace SDWAN technology and leverage its benefits without compromising on reliability and security.

It can be concluded for the above experiment that FEC (Forward Error Correction) based on Reed Solomon algorithm, if implemented in SDWAN, for UDP traffic gives an excellent performance on the overlay even at 10% of packet loss on the underlay WAN links. A good UDP transport-based VPN shall be used in SDWAN Overlay so that the benefit of FEC can be spread across all the traffic (both TCP and UDP) which rides the VPN tunnel. Linux Kernel has implemented Wireguard VPN which uses ChaCha20 as the encryption algorithm with Poly1305[46] based authentication, is a good choice for optimizing the performance in the overall solution. The consideration on available WAN bandwidth should be kept in mind as the FEC solution adds its own overheads for proving loss free environment on overlay.

In summary, our research provides a compelling closing argument for the effectiveness of our proposed method in enhancing the reliability and security of transmission over SDWAN. The data-driven results and the regression equation presented in this study validate the efficacy of our approach and support its potential for real-world implementation. We believe that our work opens up new possibilities for the practical deployment of SDWAN solutions, ultimately leading to more robust and secure networks in today's evolving digital landscape.

8. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to all those who contributed to the success of this research paper.

Firstly, we would like to thank our supervisor (Dr. Sabharwal and Dr. Bajaj) for providing us with valuable guidance and support throughout the research process. Their insights and expertise have been instrumental in shaping the direction and scope of this paper.

We extend our thanks to Galgotias University that provided us with the necessary resources to carry out this study. Without their support, this research would not have been possible.

Finally, we would like to express our appreciation to our friends and family who provided us with encouragement and support throughout this endeavor. Their unwavering support has been a source of inspiration for us.

Once again, we extend our heartfelt thanks to all those who contributed to the success of this research paper.

REFERENCES:

[1] P. B. Mohit Chandra Saxena, “Evolution of Wide Area network from Circuit Switched to Digital Software defined Network,” in International Conference on Technological Advancements and Innovations (ICTAI),, Dubai, 2021.

[2] Y. . Zhang, N. . Ansari, M. . Wu and H. . Yu, “On Wide Area Network Optimization,” IEEE Communications Surveys and Tutorials, vol. 14, no. 4, pp. 1090-1113, 2012.

[3] J. . Xiao, T. . Tillo, C. . Lin and Y. . Zhao, “Real-time forward error correction for video transmission,” , 2011. [Online]. Available: http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ieee-000006115907. [Accessed 22 12 2022].

[4] “TCP vs. UDP : The Difference Between them,” , . [Online]. Available: http://www.skullbox.net/tcpudp.php. [Accessed 24 1 2023].

[5] M. C. Saxena and P. Bajaj, "A Novel method of End-to-End data security using symmetric key based data encryption and SDWAN networking," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1981-1986, doi: 10.1109/IC3I56241.2022.10073283.

[6] Y. . Kosta, U. D. Dalal and R. K. Jha, “Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN),” , 2010. [Online]. Available: https://ieeexplore.ieee.org/document/5460559. [Accessed 22 12 2022].

[7] M. . Jeronimo and J. . Jason, “IPsec Policy Schema,” , 1999. [Online]. Available: https://tools.ietf.org/html/draft-ietf-ipsec-policy-schema-00. [Accessed 22 12 2022].

[8] X. . Xiao, A. . Hannan, B. . Bailey and L. M. Ni, "Traffic engineering with MPLS in the Internet," IEEE Network, vol. 14, no. 2, pp. 28-33, 2000.

[9] J.-W. . Lin, C.-H. . Chen and J. M. Chang, "QoS-Aware Data Replication for Data-Intensive Applications in Cloud Computing Systems," IEEE Transactions on Cloud Computing, vol. 1, no. 1, pp. 101-115, 2013.

[10] Adewumi, F., & Popoola, W. O. (2021). Performance comparison of forward error correction techniques in SD-WAN. International Journal of Communication Systems, 34(7), e5008.

[11] Dong, Y., Chen, Y., Wu, X., Yang, Y., & Chen, Y. (2021). A high-reliability FEC scheme for VPN transmission in SD-WAN. Wireless Networks, 27(8), 5817-5830.

[12] Hu, Y., Zhang, X., & Liu, L. (2021). An FEC-based scheme for reliable VPN transmission in SD-WAN. Wireless Personal Communications, 118(1), 297-311.

[13] Li, M., Zhang, X., & Wei, H. (2021). Golay code-based FEC scheme for reliable VPN transmission in SD-WAN. Wireless Networks, 27(7), 4979-4992.

[14] Liu, L., Zhang, X., & Hu, Y. (2021). Turbo code-based FEC scheme for reliable VPN transmission in SD-WAN. Wireless Personal Communications, 116(4), 2163-2177.

[15] Wu, X., Dong, Y., Chen, Y., & Chen, Y. (2021). Convolutional code-based FEC scheme for VPN transmission in SD-WAN. Wireless Personal Communications, 116(4), 2147-2161.

[16] Zhang, J., Fang, B., & Guo, W. (2020). FEC-based transmission optimization scheme for SD-WAN. Journal of Communications and Information Networks, 5(1), 43-50.

[17] Lin, Y., Chen, Z., Yang, Y., & Xu, J. (2021). A Secure Forward Error Correction Scheme Based on Hamming Code for SD-WAN. IEEE Access, 9, 20366-20377.

[18] Sah, S., Naik, G., & Singh, R. (2021). A Secure Forward Error Correction Scheme Based on Reed-Solomon Code for SD-WAN. In 2021 International Conference on Recent Advancements in Electrical, Electronics and Communication Systems (RAEECS) (pp. 1-6). IEEE.

[19] Xu, S., Sun, H., & Hu, Y. (2020). A secure forward error correction scheme based on BCH code for SD-WAN. Journal of Ambient Intelligence and Humanized Computing, 11(10), 4429-4442.

[20] Li, J., Zhu, L., Huang, C., & Li, Q. (2021). A Secure Forward Error Correction Scheme Based on LDPC Code for VPN in SD-WAN. Wireless Personal Communications, 117(4), 2595-2608.

[21] Sah, M. K., Kharel, R., & Pokharel, B. R. (2021). An efficient FEC-based scheme for improving the reliability of VPN transmission in SD-WAN. Journal of Network and Computer Applications, 178, 102974.

[22] Li, Z., Wang, Y., Xiang, X., & Wu, Y. (2021). A reliable and secure FEC-based VPN transmission scheme for SD-WAN. Security and Communication Networks, 2021, 6644075.

[23] Feng, X., Li, B., Zhang, Z., & Liu, K. (2020). An FEC-based reliable transmission mechanism for SD-WAN. IEEE Access, 8, 164065-164076.

[24] Liu, X., Yang, Y., Zhang, X., & Li, B. (2020). An FEC-based reliable transmission mechanism for VPNs in SD-WAN. IEEE Internet of Things Journal, 8(17), 14133-14142.

[25] Xu, H., Li, Y., & Li, X. (2020). An efficient FEC-based scheme for improving the reliability of VPN transmission in SD-WAN. IEEE Access, 8, 185476-185486.

[26] Feng, Z., Liu, K., Chen, K., & Chen, X. (2020). A novel forward error correction based approach for SD-WAN. Journal of Ambient Intelligence and Humanized Computing, 11(10), 4641-4650.

[27] Liu, X., Liu, K., Wang, J., Chen, X., & Chen, K. (2020). Turbo-code based forward error correction scheme for SD-WAN. Journal of Ambient Intelligence and Humanized Computing, 11(11), 4947-4955.

[28] A. K. S. M. J. O. L. P. A. S. S. V. J. W. J. Z. M. Z. J. Z. U. H. S. S. a. A. V. (. Sushant Jain, "B4: experience with a globally-deployed software defined wan," Computer Communication Review, vol. 43, no. 4, p. , 2013.

[29] "Active FTP vs. Passive FTP, a Definitive Explanation," , . [Online]. Available: http://slacksite.com/other/ftp.html. [Accessed 24 1 2023].

[30] "WireGuard: fast, modern, secure VPN tunnel," , . [Online]. Available: https://www.wireguard.com/. [Accessed 22 12 2022].

[31] L. V. J. G. L. R. M. H. J. C. M. Luby, "Forward Error Correction (FEC) Building Block". United States of America Patent RFC 3452, 01 December 2002.

[32] H. . Liu, M. . Wu, D. . Li, S. . Mathur, K. . Ramaswamy, L. . Han and D. . Raychaudhuri, "A Staggered FEC System for Seamless Handoff in

Wireless LANs: Implementation Experience and Experimental Study," Information Systems Management, vol. , no. , pp. 283-290, 2007.

[33] R. B. Ali, S. . Pierre and Y. . Lemieux, "UMTS-to-IP QoS mapping for voice and video telephony services," IEEE Network, vol. 19, no. 2, pp. 26-32, 2005.

[34] B. . Dowling and K. G. Paterson, "A Cryptographic Analysis of the WireGuard Protocol," , 2018. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-93387-0_1. [Accessed 22 12 2022].

[35] "What's the appeal of using ChaCha20 instead of AES?," , . [Online]. Available: https://crypto.stackexchange.com/questions/34455/whats-the-appeal-of-using-chacha20-instead-of-aes. [Accessed 22 12 2022].

[36] "OpenVPN Security Overview," , . [Online]. Available: http://openvpn.net/index.php/open-source/documentation/security-overview.html. [Accessed 24 1 2023].

[37] R. . Afreen and S. C. Mehrotra, "A Review on Elliptic Curve Cryptography for Embedded Systems," arXiv: Cryptography and Security, vol. , no. , p. , 2011.

[38] "OpenSSH Portable Release," , . [Online]. Available: https://www.openssh.com/portable.html. [Accessed 24 1 2023].

[39] Y. . Li, T. . Courtney, R. N. Ibbett and N. . Topham, "Work in Progress: Performance Evaluation of RAID6 Systems," , 2007. [Online]. Available: https://research.ed.ac.uk/portal/files/18546513/li_et_al_wip_performance_evaluation_of_raid6_systems.pdf. [Accessed 24 1 2023].

[40] Y. Wang, "Calculate the After-FEC Packet-loss," Github, 6 January 2022. [Online]. Available: https://github.com/wangyu-/UDPspeeder/wiki/FEC%E4%B8%A2%E5%8C%85%E7%8E%87%E8%AE%A1%E7%AE%97.

[41] "Free Range Routing Project Forks Quagga," , . [Online]. Available: https://packetpushers.net/free-range-routing-project-forks-quagga/. [Accessed 22 12 2022].

[42] A. . Jurgelionis, J.-P. . Laulajainen, M. . Hirvonen and A. I. Wang, "An Empirical Study of NetEm Network Emulation Functionalities," , 2011. [Online]. Available: http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ieee-000006005933. [Accessed 22 12 2022].

[43] "VyOS," , . [Online]. Available: http://vyos.net. [Accessed 22 12 2022].

[44] "[Release] VyOS 1.0.0 - (an enhanced fork, based from the old vyatta project) : networking," , . [Online]. Available: https://www.reddit.com/r/networking/comments/1thfaw/release_vyos_100_an_enhanced_fork_based_from_the/. [Accessed 22 12 2022].

[45] M. . Nohrborg, "LTE," , . [Online]. Available: http://www.3gpp.org/LTE. [Accessed 24 1 2023].

[46] N. . Mavrogiannopoulos, J. . Strombergson, A. . Langley, W.-T. . Chang and S. . Josefsson, "ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)," , 2016. [Online]. Available: https://tools.ietf.org/html/rfc7905. [Accessed 22 12 2022].