Ghanem, K., Ugwuanyi, S., Hansawangkit, J., McPherson, R., Khan, R., & Irvine, J. (2022).
Security vs bandwidth: performance analysis between IPsec and OpenVPN in smart grid.
In 2022 International Symposium on Networks,
Computers and Communications (ISNCC) IEEE. https://doi.org/10.1109/isncc55209.2022.9851717

Security vs Bandwidth: Performance Analysis Between IPsec and OpenVPN in Smart Grid

[1]Kinan Ghanem
Power Networks Demonstration Centre
University of Strathclyde
Glasgow, United Kingdom
kinan.ghanem@strath.ac.uk

[3]Jidapa Hansawangkit
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
jidapa.hansawangki@strath.ac.uk

[5]Rabia Khan
Power Networks Demonstration Centre
University of Strathclyde
Glasgow, United Kingdom
rabia.khan@strath.ac.uk

[2]Stephen Ugwuanyi
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
stephen.ugwuanyi@strath.ac.uk

[4]Ross McPherson
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
ross.mcpherson@strath.ac.uk

[6]James Irvine
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
j.m.irvine@strath.ac.uk

***Abstract*—Secure wireless communication is an essential element of smart grid systems. This enables distributed industrial Internet of Things (IoT) assets to be remotely controlled and monitored from the control centre. In this piece of work, we evaluate the impact of employing OpenVPN and IPsec on the bandwidth required for the operation of distribution assets in next-generation substations Remote Terminal Units (RTUs) over IEC 61850-5-104. This analysis showed that OpenVPN added an average of 42 bytes to each packet inside the VPN tunnel, while Internet Protocol Security (IPsec) contributed an average overhead of 64 bytes. This demonstrated that employing IPsec would require more bandwidth than OpenVPN. Discussions on the reliability of wireless communication media for smart grid is also presented.**

Keywords—Bandwidth, IEC 61850-5-104, IPsec, Encryption, OpenVPN, Remote Outstation, Security, Smart Grid.

I. INTRODUCTION

There is a crucial need for efficient and secure communication systems in smart grid networks. Smart grid networks require resilient, reliable, and secure communication systems to monitor and control network infrastructure safely and allow Engineers and Technicians to access these devices via remote access [1]. The large number of geographically diverse devices required for smart grid operation, make wireless communication networks an appropriate and cost-effective solution for connecting distributed assets in hard-to-reach areas [2]. The trade-off for this deployment simplification is the need to encrypt and secure these over-the-air connections. Employing such encryption and authentication algorithms presents an overhead for each message sent. This overhead will be amplified as the number of connected devices and the granularity of data increases.

Appropriately securing the massive number of future field devices is a considerable challenge [1]. Regulators have compulsory requirements and security standards, such as EU's Network and Information Security (NIS) directive, to ensure safe and reliable communication [2].

The large infrastructure costs of deploying dedicated wireless communication infrastructure, may lead utility operators to utilise existing communication infrastructure such as public 4G/5G mobile networks. Securing communication over such networks can be achieved by using a Virtual Private Network (VPN). These work by encapsulating, encrypting and signing the data packets which are then forwarded through public infrastructure to reach their destination, where they will be verified, decrypted and processed.

VPNs can be configured to use various encryption and authentication algorithms and different key lengths depending on the application. Two common VPN systems are OpenVPN and IPsec. Wireguard is an emerging open source secure and lightweight VPN solution which is gaining more interest in the industry [3]. However, IPsec and OpenVPN were selected to be analysed as these are existing common solutions within the OT and IT sector respectively. Each VPN solution creates an encrypted link over an insecure connection (public internet or third party network). To enable this connection third-party client software is required on each end of the connection.

This paper aims to help clarify the differences in the security bandwidth overhead needed for IPsec and OpenVPN based VPNs. An IPsec and an OpenVPN connection were set up and configured via a public LTE network using two industrial routers as endpoints, each with a public mobile networks SIM card. This study is mainly based on both DNP3 and the IEC 60870-5-104 protocols for Supervisory Control and Data Acquisition (SCADA) systems. This paper is organised as follows: Section II summarises the ongoing research activities work on IPsec and OpenVPN; The architecture setup will be explained in Section III; The bandwidth analysis of both IEC 60870-5-104 over OpenVPN and IPsec will be discussed in Section IV; and Section V will briefly conclude the paper.

II. RELATED WORK

Most existing smart grid communication technologies currently used in the power utilities are not supported with robust security systems which encrypt the data and mitigate new cybersecurity threat [2] - [4]. New digital distributed power assets such as charging stations, battery storage and smart transformers are predicted to consume more bandwidth than their previous counterparts [5]. Deploying new security techniques into existing connected industrial devices, while following the regulators' guidance and complying with the international standards, will potentially contribute additional security overhead. Studies have investigated the overhead caused by implementing security in various smart grid applications [6], [7], [8]. A few research studies have investigated the cost of security in smart grid applications [9], [10].

However, there are limited practical investigations on comparing the cost associated with the IPsec compared with the OpenVPN. Those few studies on OpenVPN and IPsec in a smart grid have focused on their requirements of reliability and security rather than bandwidth. Moreover, these two

techniques are able to provide security in communication by leveraging Internet Protocol (IP) technology.

Table 1. Summary of Related Literature and their Contributions

Authors	Year	Reviewed Area and Contribution
Neumann et al. [11]	2015	A parameterisation method of the IPsec protocol framework is proposed to secure data interoperability in smart grid networks with latency variation and throughput as the measured parameters benchmarked against the Smart Grid Interoperability Reference Model (SGIRM) recommendations.
Rosborough et al. [8]	2019	Survey on security protocols for Industrial Control Systems (ICS) focused on Internet Protocol Security (IPsec), Transport Layer Security and Distribution Network Operator v3-based Secure Authentication (DNP3-SA). Cryptography systems were considered essential for securing Operational Technology (OT) infrastructure in modern network integration.
Daniel et al. [12]	2018	Compared OpenVPN and OpenVPN-NL security capabilities based on state fuzzing at the state machine level. However, the approach could not infer certain superfluous states and data transitions of the state machine that may introduce security flaws into the network. It also demonstrates that the security of a network can be improved through state machine enhancement.
Pandurang et al. [13]	2015	OpenVPN is used in Wired Equivalent Privacy (WEP) and 802.11i (WPA2) on the wireless local area network to measure throughput, latency, and frame loss rate. OpenVPN with and without compression are also covered. WEP recorded higher data loss than WPA2 but with lower latency.
Coonjah et al. [14]	2015	The paper compared OpenVPN and OpenSSH performance over Wide Area Network (WAN) connections based on speed, latency and jitter. While OpenSSH outperformed OpenVPN with better link efficiency and faster data transfer time for remote access, it presents throughput limitations.
Aung et al. [15]	2020	Compared the performance measurement and analysed packets overheads of different Layer 2 VPN protocols for site-to-site connections. While each Layer 2 VPNs have higher overheads due to the associated Ethernet frames than Layer 3 VPN, the decision on the type of VPN for securing OT assets has to be a compromise between security and performance.
Ghanem et al. [5]	2020	The paper established the key communication network integration and security standard requirements for secondary substations. In a trial of a smart transformer, the data overhead due to IPsec and TLS over DNP3 and IEC-104 shows an increasing need for more bandwidth.

ARCHITECTURE TEST SETUP

In order to investigate the security overhead of RTUs in utility networks, our test network setup process followed the following approaches: The first step identified the data flow between connected RTUs, namely, the SCADA system polling of the RTU for measurements and the protocol used to link the RTU with the SCADA control centre. The RTU collects the measurement data from field devices and functions as a gateway between the field devices and the control centre. The measured field data used in this work are taken from existing configurations from one of the Distribution Networks Operators (DNOs) working with PNDC.

The second stage involved the protocols for linking the RTUs to the control centre. We applied DNP3 and IEC 60870-5-104 (IEC 104) in separate test scenarios in the bandwidth setup and calculations. In order to compare the bandwidth due to IPsec and OpenVPN implementations, a complete setup of an end-to-end secured IP-based smart grid network was installed at PNDC. The RTUs used for these implementations can support several power utilities' applications such as transmission and distribution automation with features enabled for different authentications and encryptions security approaches. The third step defined the main applications of RTUs for the DNOs in the remote outstation. This includes determining the number of analogue and digital measurements to be transmitted from the Master RTU to the control centre (i.e., configuring the Master SCADA server based on the established requirements). A representative setup for full IP RTU configuration to check the required security bandwidth is shown in Figure 1. It is assumed that the RTU transmits 18 analogue measurements every 10 minutes. This was selected as it was representative for DNOs. Additional network configurations used in this study are presented in Tables 2 and 3.

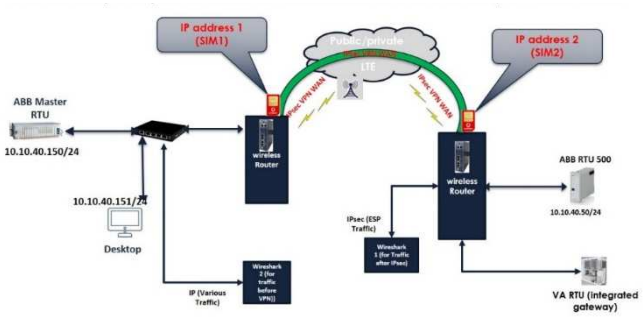

Fig. 1 IPsec Connectivity between an Industrial Router and an RTU End-Device

Due to the design of public mobile networks, direct device to device communication is not possible, therefore, both IPsec and OpenVPN configurations were set up to reach out to an intermediate server. A future area of research may be to investigate the overhead in a private LTE network which would allow direct connections between the industrial end devices and the control centre. Dedicated Machine-to-Machine (M2M) SIM Cards are also available which provide pseudo direct connectivity by presenting a unified network to the user but create an intermediary behind the scenes.

A. Bandwidth Test Setup

To determine the bandwidth requirements for the secondary substation, the following devices and tools have been used:

- An M2M wireless industrial router with dual SIMs and support capabilities for different SCADA applications and protocols.
- IEC 62351 compliant gateway that integrates security into the test setup, connectivity (M2M wireless router with 3 SIMs), RTU, HMI and SCADA protocols to enhance the business case for extending coverage.
- SCADA Traffic Generator, which can send both DNP3 or IEC 104 traffics.
- 2 SIMs to enable the connectivity through a public radio network.
- SCADA Concentrator is used to encrypt the IEC 104/DNP3 traffics and transfer the train traffic into a fully secured one. It is used to comply with the IEC 62351 standard for any transmitted IEC 60870-5-104 protocol (protection through TLS encryption).

With the specified RTU and routers configurations, end-to-end connectivity through a mobile radio network is established. The SCADA traffic generator sends the correct DNP3/IEC-104 commands. Several configurations have been investigated over many days to check the reliability of the connection and understand the bandwidth and security requirements for different scenarios. The tests ran over one level of security using two different security approaches over both DNP3 and IEC 104. A plain IEC 104 over OpenVPN and IPsec is used to understand the overhead caused by OpenVPN compared with IPsec. Reruning the tests with the same arrangements replacing IEC 104 with DNP3 is shown in Figure 2, we obtained similar results.

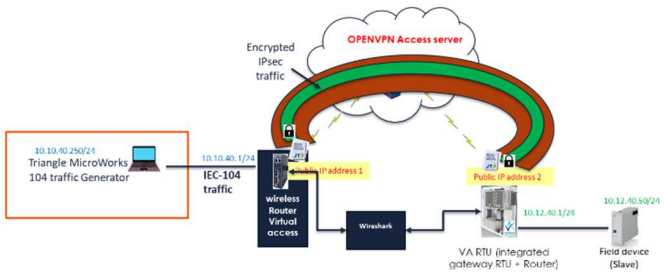

Fig. 2 Initial test of IEC 104 over OpenVPN/IPsec

B. *IEC 104 Main Configurations*

The protocol used to link the RTU with the SCADA control centre is the IEC 60870-5-104, generated by the Triangle MicroWorks traffic simulator. Two main configurations have been selected as more injected traffics along with fast frequent of polling aimed to better understand the effect of both the suitable configuration and any congestion or buffering issue on the packet loss and dropped packet rate. Table 2 shows the main IEC 104 commands configurations used for polling in a sequence of almost 15 seconds in addition to injecting more traffics aiming to create congestion somehow in a specific time slot (for example, when the time is 300 seconds, at least 5 commands arrived at the same time in addition to the injected background traffics).

Table 2 Configurations of IEC 104 Traffic Commands to Create Congestion

Command (IEC 104)	Polling Frequency in Seconds
General integration	60
Double point command	90
Floating measurement	180
Counter integration	120
Single point of measurement	30
Clock synchronisation	15

The configurations shown in Table 3 were chosen to avoid congestion (and queuing to the traffic entering the RTU) when possible, as no additional (extra) traffics have been injected in this test. The uncongested setup was used to check the effects of the command arrival time on the connection's performance and its reliability in terms of TCP retransmission and packet delivery ratio. We have not looked at the effects of the router's buffer size on the connection performance.

The tests were run over several days and in various durations during the day for four weeks. Each configuration has been repeated at least 3 times over that period, aiming to reflect and assess the real mobile network status (during the normal operation hours).

Table 3 Configurations of IEC 104 Traffic Commands to avoid Congestion

Command (IEC 104)	Polling Frequency in Seconds
General integration	15
Double point command	13
Floating measurement	31
Counter integration	31
Single point of measurement	23
Clock synchronisation	17

BANDWIDTH ANALYSIS OF IEC 104 OVER OPEN VPN VS IPSEC

This section compares the security overhead of IPsec vs OpenVPN for sending IEC 104 traffic from the SCADA Master to the RTUs. The router and RTU captured data analysis shows that the IPsec wraps each packet in a new and secure frame adding an average of 60-68 bytes for each frame, whereas OpenVPN adds only an average of 40-44 bytes for each frame. More specifically, the new payload is encapsulated by the IPsec headers, and then all packets inside the IP tunnel were in ESP format, while the OpenVPN was configured to use UDP. Figure 3 illustrates the new payload due to IPsec and OpenVPN.

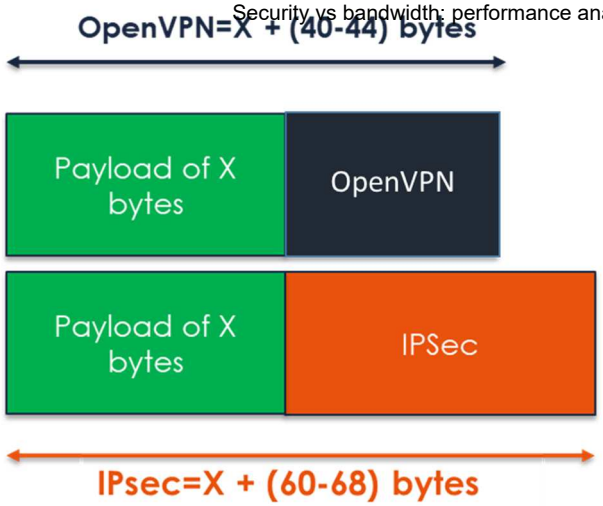

Fig. 3. The new Payload caused by the IPsec vs OpenVPN

Figure 4 shows the overhead for a number of different TCP packet sizes. IPsec will cost an average of 23% more bandwidth compared to OpenVPN (subject to average packet size). So far, we have investigated the cost of IPsec and OpenVPN due to IPsec and OpenVPN allowing direct communication between remote devices in industrial networks via mobile networks.

The National Cyber Security Centre (NCSC) stated that "from a security perspective, with all other things equal, there is very little difference in risk between using an IPsec and a TLS VPN" [3], However, IPsec IKEv2 remains the industry standard.

Most field devices that rely on VPN secure connections will become unusable if the VPN service itself has an outage, due to the communication dependency. Therefore, it is crucial to ensure the architecture is resilient and has backup options if components within the service fail, especially for highly critical applications. No specific reliability tests of either the LTE air interface or the VPN connection itself were conducted in this study. However, no notable issues of reliability were discovered.

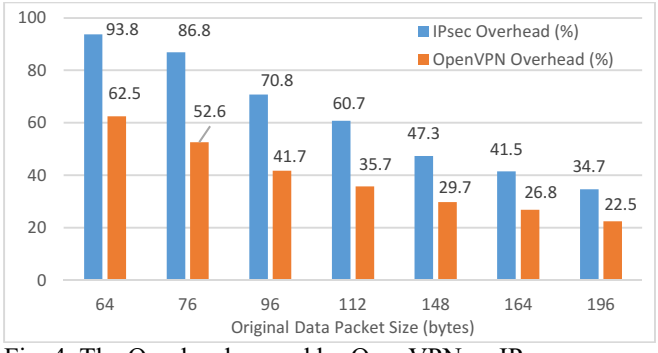

Fig. 4. The Overhead caused by OpenVPN vs IPsec

A. *Reliability of Communication Media*

The lack of interoperability and limited signal availability in rural areas are the main challenges facing any VPN approach in power networks. For public mobile networks, the reliability drawback caused by operation conditions affects the radio channel, degrades the VPN connection between the control centre and the RTU. Other problems such as network congestion, configuration error and lost packets could also lower the reliability of the connection. Latency issues due to limited number of mobile resource blocks can also cause the authentication process to timeout. The availability of the communication technology along with its cost, peak data rate and ability to accommodate any future development for the power network, will determine the most suitable wireless communication technology for the smart grid.

The test also shows that the quality of the communication medium affects the connection reliability in terms of dropped packets and retransmission rates. Based on the tests conducted at the PNDC, the secure tunnel shows high reliability in tested scenarios. It is found that using a multi-network SIM Card that can roam to the strongest signal strength, providing increased resilience and redundancy.

Several clarifications that might affect the reliability of the connection are listed below:

- Connection failure due to any power or radio signal loss will result in the loss of OpenVPN or IPsec tunnels providing secure data and command exchanging path for the field devices.
- Network congestion, configuration error and lost packets could affect the reliability, especially when a third-party service provider is involved.
- Synchronisation problems between the master clock and field devices could drop the reliability.
- Network delay can lead the authentication process to fail. This will not allow any commands to be transmitted from the master SCADA to the field device.
- Problems in the services of third-party service providers.

B. *Effect of Network Congestion*

High retransmission rates have been spotted due to congestion. Figure 5 shows that network congestion can increase the dropped packets rate, which could affect network performance. This could raise a question about the network performance during any black start scenario and very high demand during peak time. In such congested network scenarios, almost 1.3% of the packets were dropped and, this loss could create an issue with many real-time applications and also could increase the end-to-end delay.

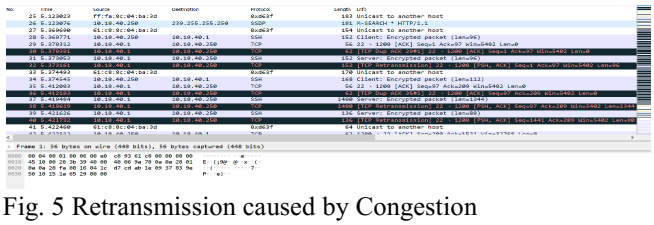

Fig. 5 Retransmission caused by Congestion

The analysis showed forced network congestion through issuing many simultaneous commands, resulted in dropped packets. This is partly due to the fact that all traffic was treated equally, and there is a finite amount of capacity on the network. Accordingly, this situation could be resolved through employing quality of service rules or employing dedicated infrastructure with sufficient resources even when the network is congested.

As public mobile networks inherently support bursty traffic, for non-real time traffic increasing the local buffer size could result in non-critical packets being stored until network congestion reduces.

C. Loss of Connection to Third-Party Cloud Servers

Third-party Machine-2-Machine (M2M) SIM cards enable device-to-device communication by placing devices on a pseudo LAN network by creating an internal VPN network between devices. This enables seamless communication but also creates a dependency on third-party servers, which must act as intermediaries to route traffic between devices. During testing such an issue was discovered where the providers cloud service went offline causing all device-to-device communication to fail, even though the underlying physical mobile infrastructure remained operational. This creates an additional consideration when using third-party M2M SIMs. Additional considerations include additional network latency due to all traffic having to go via an external service. This would further increase the overall bandwidth requirements, although the provider may consider this overhead part of the data package therefore not incur any additional financial cost. Finally, relying on third party infrastructure also brings policy and legal considerations, as data used within critical national infrastructure must be controlled and protected. For these reasons careful consideration should be employed when utilising third-party M2M SIM cards.

CONCLUSION

This paper discussed the difference in overhead between IPsec and OpenVPN over an LTE public network using 2 multi-network SIM Cards. The work built on established commercial deployments which employ IPSec and OpenVPN as a secure means of providing network connectivity between two RTUs. This work was expanded to investigate the overhead of employing end-to-end encryption and authentication. We found that OpenVPN added between 40-44 bytes for each packet inside the VPN tunnel, whereas IPsec contributed between 60-68 bytes, indicating a higher bandwidth cost. Moreover, a high TCP retransmissions rate is observed in different configurations, where polling with irregular times and the quality of the communication medium significantly affects the reliability in terms of packet loss and TCP retransmission rates. Public mobile networks showed high reliability in terms of packets loss and retransmission rate. The next stage of this research project will consider different protocols such as IEC 61850 conceptualising different smart grid applications with the cost of other encryption techniques for various data traffics.

High reliability for smart grid applications may require a dedicated private network with an appropriate spectrum, to avoid network congestion issues. Such private networks are needed to maintain communications reliability during extended power outages or when public communications networks are not available.

ACKNOWLEDGMENT

The authors acknowledge the contributions of PNDC Tier 1 members (Scottish Power Energy Networks, Scottish and Southern Electricity Networks, UK power networks, Vodafone, and Virtual Access) for funding and supporting this research project.

REFERENCES

[1] R. S. Geetha, S. Gowdhamkumar and S. Jambulingam, “Energy challenge, power electronics & systems (PEAS) technology and grid modernization,” *International Research Journal of Multidisciplinary Technovation,* vol. 1, no. 2, pp. 116-129, 2019.

[2] C. C. Sun, A. Hahn and C. C. Liu, “Cyber security of a power grid: State-of-the-art,” *International Journal of Electrical Power & Energy Systems,* vol. 99, pp. 45-56, 2018.

[3] NCSC, “NCSC CAF guidance,” National Cyber Security Centre (NCSC), 30 September 2019. [Online]. Available: https://www.ncsc.gov.uk/collection/caf. [Accessed 07 May 2021].

[4] M. I. Henderson, D. Novosel and L. M. Crow, “Electric power grid modernization trends, challenges, and opportunities.,” IEEE, 2017.

[5] K. Ghanem, I. Abdulhadi, A. Kazerooni and C. McGookin, “Communication requirements for future secondary substations to enable DSO functions,” in *CIRED Workshop 2020. 2020*, Berlin, 2020.

[6] J. Hiller, M. Henze, T. Zimmermann and O. Hohlfeld, “The Case for Session Sharing: Relieving Clients from TLS Handshake Overheads,” in *2019 IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium) (PP. 83-91).*, Osnabrueck, 2019.

[7] B. Pranali , M. Bharati and J. Debasish , “A Novel Smart Meter Authentication Scheme for Secure Smart Grid Communication,” in *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, Kochi, 2019.

[8] C. Rosborough, E. C. Gordon and B. Waldron, “All about eve: Comparing dnp3 secure authentication with standard security technologies for scada communications,” in *13th Australasian Information Security Conference*, 2019.

[9] K. Ghanem, R. Asif, S. Ugwuanyi and J. Irvine, “Bandwidth and Security Requirements for Smart Grid,” in *IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, The Hague, Netherlands, 2020.

[10] C. Rosborough, “All About Eve: Comparing DNP3 Secure Authentication With Standard Security Technologies for SCADA Communications,” Exelon and Schweitzer Engineering Laboratories, Inc., Washington , 2019.

[11] V. Neumann, C. L. Gomes, C. Unsihuay-Vila, K. V. Fonseca and P. R. Torres, “Parameterization of IPsec Framework for Security in the Smart Grid Interoperability Latency and Throughput IPsec Overhead,” in *IEEE PES Inoovation Smart Grid Technology Latin America (ISGT LATAM)*, Montevideo, Uruguay, 2015.

[12] L.-A. Daniel, E. Poll and J. d. Ruiter, “Inferring OpenVPN State Machines Using Protocol State Fuzzing,” in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, London, UK, 2018.

[13] R. M. Pandurang and D. C. Karia, “Performance measurement of WEP and WPA2 on WLAN using OpenVPN,” in *International Conference on Nascent Technologies in the Engineering Field (ICNTE)*, Navi Mumbai, India, 2015.

[14] I. Coonjah, P. C. Catherine and K. M. S. Soyjaudah, “Performance Evaluation and Analysis of Layer 3,” in *International Conference on Computing, Communication and Security (ICCCS)*, Pointe aux Piments, Mauritius, 2015.

[15] S. . T. Aung and T. Thein, “Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks,” in *IEEE Conference on Computer Applications(ICCA)*, Yangon, Myanmar, 2020.