Examination Of Triple Play Deployment In Wide Area Network

Seth Okyere-Dankwa[1], Mensah Sitti[2], Solomon Anab[3]

[1]Dean, School of Graduate Stadies, Koforidua Technical University,
Koforidua, Ghana PH +233208114115
Seth.okyere-dankwa@ktu.edu.gh

[2]Lecturer, Computer Science & Eng. Dept. University of Mines & Technology,
Tarkwa,Ghana PH +233208351347
msitti@umat.edu.gh

[3]Lecturer, Computer Science Department, Koforidua Technical University,
Koforidua, Ghana PH +233243158668
solomon.anab@ktu.edu.gh

Abstract: There has been a significant change in the communication industry for the past decade. Customers taste has changed and the deregulation in the industry brought about more competition. There is now much concern, talk and discussions on Triple Play that is video, voice and data services over an integrated network. Meanwhile most of the networks being used today are designed with data application in mind. Data being non-real time application is not affected by delay, drop and jitter as a result of congestion. The impact on delay, drop and jitter has negative effect on video and voice being transmitted over network. This Study discusses the characteristics of data, voice and video facilities and their network requirements. The Study also looks at the effective, efficient and more reliable network facilities that will support the convergence of voice, video and data. The Study will finally touch on the management and security issues of the network which support the convergence.

Keywords: PON, GPON, VOICE, VIDEO, DATA

1. Introduction

For data, voice and multimedia to be communicated from one location to another, they must be routed through a network. The transmission which is in a form of packets occur in physical media such as fibre optics, twisted pair or coaxial cable or even they could be broadcasted through the air. Decisions for routing are made on packets individually as to what routing path to take without recourse to the previous packets routing path. The routing independence in a specific media makes IP networks adjustable to diverse environment. Because packets can take different routing path to their destination, at times it is possible for voice and multimedia streams to be badly affected by jitter, latency and packet loss which in tend affect the dependability of the voice and the multimedia [19].

1.1 Objective

The main objective is to identify a solution to problems associated with the convergence of Triple Play in the integrated Network. This is achieved through the following specific objectives.

1. To examine the network requirements for Data, Voice and Video
2. To identify network resources that support voice, video and data convergence
3. To come out with management and security issues that support Triple Play convergence.

2. Related Works

2.1 Jitter

When packets within the same data stream arrive at their destination at different time, it causes jitter to occur. This is possible because packet transmission is independent of each other. Jitter occurs normally when the network is congested. Millisecond is the unit for measuring jitter. To minimise jitter, equipment like jitter buffer are set up. The jitter buffer reduces packets variation time in arriving at their destination [10].

2.2 Packet Loss

Pocket loss occurs when data packets are unable to reach their destination, misrouted, debarred from the medium stream or if the reception of the packet at the destination is out of order [6].

2.3 Voice

Voice traffic normally has an average packet size between 80bytes to 256bytes and bit rate traffic between 21Kbps to 320Kbps. Voice traffic has a low tolerance for packet loss, low tolerance for delay (latency) and even lower tolerance for jitter. These parameters control the features which decide the user experience for voice traffic. Latency occurs when the volume of traffic on the network is high and tends to put strain on the processing power. Then definitely some of the packets have to wait for their turn to be processed. This delay in processing causes the latency. Latency in voice normally creates so many problems. Conversation becomes uncomfortable when there is time lag between the speaker and the listener. Large latency cause disruption in the rhythm of conversation and create unwarranted disruptions and misapprehension. For example, latency above 200ms is noticeable and can affect quality of conversation. Another area of voice which is critical is voice clarity. The quality of voice signal is determined by voice clarity and this is affected by the packet loss and jitter. Jitter can completely damage voice quality [13].

2.4 Video
The frame size of streaming video is very high; it has a larger size than voice. An average packet size of video is between 65bytes to 1500bytes. Video also has a variable bit rate. It has a low tolerance for latency and low tolerance for packet loss. Compare to both data and voice, the requirement of bandwidth for streaming video application is very high and it runs into tens of Megabytes per second depending on the encoding and compression protocol employed [14].

2.5 Data
Data is affected by neither pocket loss nor jitter, data can handle delays. Data is also able to resend packets and handle in such a way that the user will not be aware of network impairment [15].

2.6 Bandwidth
High bandwidth is crucial to the effective and efficient running of Triple – play services. For example, the HDTV requires a bandwidth of 8-12Mbps depending on the encoding techniques used and the level of compression (MPEG-2 or MPEG-4). High Speed (Internet requires 3Mbps to 10Mbps and Voice/video telephony requires 64Kbps to 750Kbps [12].

3. Methodology
Here the study employed Descriptive research approach. The approach enables the study to accurately and systematically describe the situation and come out with a solution.

3.1 Ensured Service Quality
Introduction of voice, video and data (Triple Play) to the broadband network require a considerable increase in QoS. The network must ensure that the video and voice services match the quality of the distribution systems like the cables. The requirements in terms of bandwidth, compression and encoding techniques are taken into consideration. For example, the HDTV requires a bandwidth of 8-12Mbps depending on the encoding techniques used and the level of compression (MPEG-2 or MPEG-4) [3].

3.3 Security
The security here is a collection of services that work together to protect the network system from attack. The integrity of voice, data, and multimedia being transmitted should be guaranteed, this is done by putting in appropriate hardware and software requirements like VPN, antivirus, firewall, and access control. These are to ensure that there are no external interferences on subscribers' information [22].

3.4 Scalability
The network design should be flexible and allow for integration of new services. The network should also be able to meet the subscribers changing demands. Huge investment should be made in the bandwidth through scaling of Triple Play network, the demand for bandwidth from subscribers will grow and this will lead to increase in revenue per user [19].

4. Results

4.1 Network Requirements
From the above descriptions, the cabling of the network should be a combination of fibre and a minimum grade of category 5. This is to ensure that the needed bandwidth for effective and efficient transmission especially the multimedia is available. The network should not contain bridges and repeaters. This is to ensure that the copper cables will not be used for long distance transmission to avoid attenuation. The network should be a Passive Optical Network and run at a minimum of 100Mbps. The network should include features like tunneling, Virtual Private Network (VPN), Victual Local Area Network (VLAN), Firewall etc. for protection against intruders and also handle real time issues like latency, packet loss and jitter associated with voice and multimedia [23].

4.2 Selection of Appropriate Network Facilities
The communication industry is undergoing a revolution that is transforming the topography. The revolution is characterised by three factors. Firstly, more operators have joined the communication industry and are prepared to invest to develop innovative services based on customers' demand. Secondary the cost of fibre and Ethernet equipment have declined, making them appealing option for access network. Thirdly, the Internet has generated the need for broadband services which has brought about Internet protocol data traffic. The revolution has also brought about fibre expanding from backbone of a network to Wide Area Network and further to the local loop as well. Ethernet is also expanding from Local Area network to Wide Area Network. The unification of fibre and ethernet into the WAN is creating a concept of shift in communication industry. The shift combines the best of both fibre and Ethernet as a means of transmitting voice, video and data over a single platform. To select an appropriate network facility to support triple play, consideration should be given to the effect of the voice, video and the data on the bandwidth of the network. Since the capacity of the bandwidth determines the type of transmission media and also has a direct impact on the network. Video and voice signals are sensitive to both packet loss and jitter. The network should be able to deliver voice without any defect in quality. The network should also be able to supply IP multicast streaming for transmission of video and also provide huge data capacity at high data rate over cable or satellite [2].

6. Discussion
In addressing cost, response time, reliability and efficiency, the selected network facilities should be flexible, offer continuous service delivery and be able to meet customers demand.

6.1 Service flexibility.
The network design selected should be flexible and able to meet customers demand. It should be able to integrate new services without complete redesigned of the existing installation. This allows the network operator to decide where to extend money depending on the demand of subscribers, making the investment cost effective.

6.2 Reliability.
Audio and multimedia are very sensitive to traffic congestion which results in packet loss and jitter. These packet loss and jitter resulting from traffic congestion affect the quality of multimedia as well as the voice. The selected network facility should be able to handle traffic in such way that it will reduce to the barest minimum the incident of packet loss and jitter. This is achieved by eliminating congestion by ensuring continuous service delivery and scaling of bandwidth. The network facility should have enough security to protect the network from both internal and external attack to ensure continuous service delivery. The security provision should extend across the edge, aggregation and access end of the network. Security facilities include Ant-virus, firewall etc.

6.3 Performance
Interactivity is one of the advantages of Triple Play over the traditional broadcast of video network. This agility has led to variety of access technology. Broadband network operates under multiple access mode to reach subscribers. The various technology include central office based DSL, Fibre To The User (FTTU), Fibre To The Node (FTTN) and VDSL2.

6.4 PASSIVE OPTICAL NETWORK
Passive optical networks are frequently used in access networks, between end-users and the associated transport networks. Original metallic-based networks are nowadays being slowly substituted by optical or combined ones, which differ in how the optical distribution is terminated. Typical examples are fibre to the home (FTTH), fibre to the curb (FTTC), fibre to the building (FTTB), and fibre to the antenna (FTTA). The advantage of using passive optical networks is their operating and acquisition costs. They are composed of passive elements that do not require power because the signal is not amplified along the way. This method makes it possible to minimize and evenly distribute the costs among users [7].

A passive optical network creates a point-to-multipoint connection. The main idea of a passive optical network is to transmit the signal without further amplification, so that the network is composed only of the basic elements such as OLT, splitters, ONUs and optical network terminate (ONT), etc., see Figure 6.1

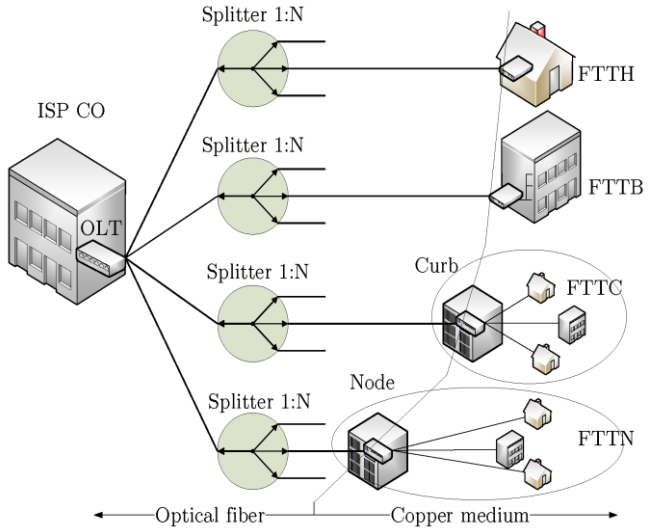

Figure 6.1 Passive Optical Network (PON) Topology

The Optical Link Terminal (OLT) device is the parent element of the passive optical network. The OLTs are located with the PON provider. Besides the conversion of the backbone and passive optical network protocols, the OLT also provides the supervision and management of Optical Network Units (ONUs) and Optical Network Terminals (ONTs), which determines the time for the transmission of single end units.

At the opposite end of the optical network (towards an end-user), the connection is terminated by ONTs or ONUs: optical network terminations for adapting protocols between the user and the optical network. The difference between the ONU and ONT is only given by how they are used in practice. Although these two units terminate the optical network on the user side, the ONU is positioned at an optical distribution point, and the signal is further propagated from that point by other technologies, for example by digital subscriber line (xDSL), or by wireless fidelity (Wi-Fi), etc.

Branching of the topology is ensured by using splitters. The transmitted signal is divided in a ratio of 1:N, where N can take values of 2, 4, 8, … 64, and 128. The cost of these elements depends on the number of ports used for branching. Since the splitters are passive components as well, they put in an additional attenuation in the signal paths and thus the parameters of the transmitted signal are deteriorated. With the increasing division ratio, total optical distribution network (ODN) attenuation increases as well [1]. Each element in the network is affecting the network. The number of network elements also limits the maximum distance that can be bridged. The parameters are specified by the gradually developed asynchronous transfer mode PON (APONs), broadband PON (BPON), GPON, etc. These are standards based on asynchronous transfer mode (ATM) technology, which allows the transmission of multiple data using time multiplexing

6.4.1 Gigabyte Passive Optical Network
GPON is the ITU-T G984.1 standard approved by the ITU in 2019. The use of the standard guarantees a sufficient capacity for today's commonly used services while providing an adequate margin for future services as well. The GPON standard is based on the previously released APON and BPON standards, but it uses a slightly modified layer model avoiding the backward compatibility. The frame processing is anchored on the time division. GPON frames are not fixed by bit size but with a time interval of 125 µs instead. The number of bits in a single frame depends on the network transmission rate. Two transmission rates of 1.244 and 2.488 Gb/s are defined in GPON [1]. The standard also defines bidirectional communication as full-duplex, but the way of upstream and downstream communication is different; however, individual data units are always transmitted in encapsulated GPON encapsulation method (GEM) frames.

6.4.2 GPON FTTH ACCESS NETWORK ARCHITECTURE
GPON's have a tree topology in order to maximize their coverage with minimum network splits, hence reducing optical power consumption. An FTTH access network comprises five areas, namely a core network area, a central

office area, a feeder area, a distribution area and a customer area as shown Figure 6.2

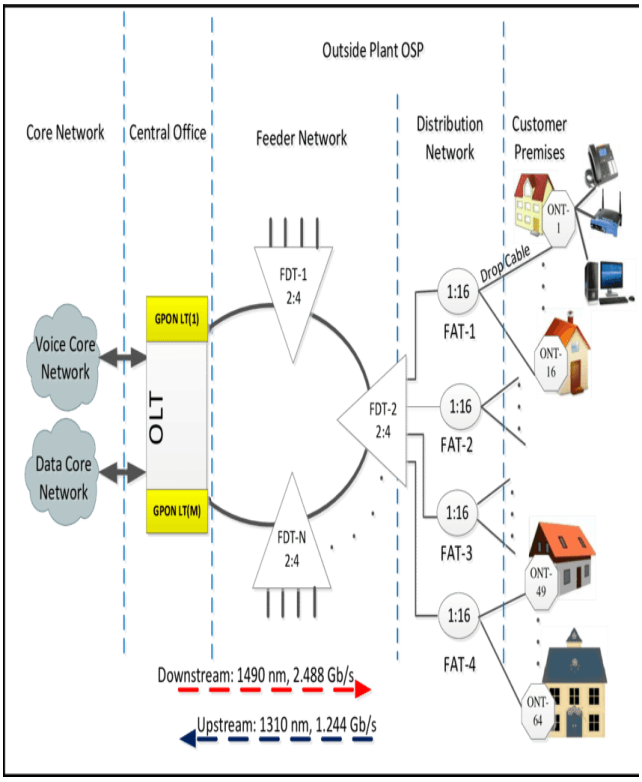

Figure 6.2: GPON FTTH Access Network Architecture

GPON is a leading standard of Passive Optical Network (PON) – a type of point-to-multipoint network technology that delivers broadband access to the end user via **fibre optic cable**. The term 'Gigabit' in GPON signifies the maximum speed it provides which is typically 2.488 Gbps downstream and 1.244 Gbps upstream. It should be noted that this bandwidth is shared amongst end users, which typically results in broadband access speeds starting at 10 Mbps. Conversely, 'Passive' denotes that the optical fibre network does not rely on any electrically-powered equipment in its path. Today, GPON technology has proven to be the most common **type of optical fibre** connection which is almost 95% more energy efficient than a standard copper cable network. Furthermore, GPON also has a 1:64 ratio on a single fibre. What this means is that one fibre cable in a GPON can deliver video, data and voice to up to 64 end users. This makes it the optical network standard of choice for achieving last-mile connectivity in an efficient and cost-effective manner, as a GPON reduces the number of fibre runs in a **fibre optic network**. There is one other GPON characteristic that out performs others. That is the use of Asynchronous Transfer Mode (ATM) encoding so as to integrate voice and data traffic on the same network. Finally, GPON is extremely useful today in delivering triple-play services (Data, IPTV, VoIP) at higher data rates, larger bandwidth and longer distances in a secure manner. GPON also supports all kinds of Ethernet protocols [18].

7. NETWORK SECURITY AND MANAGEMENT ISSUES

Network security measures are needed to protect data, voice and multimedia during their transmission and to guarantee that the information being transmitted is authentic. Computer and network security address three requirements. The requirements are Confidentiality, Integrity and Availability.

7.1 Confidentiality: This issue requires that data only be accessed for reading by the authorised parties. This type of access includes printing, displaying and other forms of disclosure.

7.2 Integrity: Requires that data can be modified only by authorised parties. Modification includes writing, changing status, deleting and creating.

7.3 Availability: This issue require that data is available to the authorised parties.

Attacks on network security are categorised into active and passive attacks. Passive attacks are in the nature of eavesdropping on or monitoring of data on transmission. The goal of the one prying is to obtain information. In this case sensitive information from an organisation could be read by these snoopers. Active attack involves some modification of data stream or creation of false stream. This can cause computers to behave abnormally. These attacks may have a specific target, an example is the disruption of an entire network, either by disabling it or overloading it with messages so as to degrade performance. To overcome these attacks a number of measures have to be taken by the customer to protect his network. These include introduction of firewalls, use of password, use of VPNs etc [22].

8. VIRTUAL PRIVATE NETWORK (VPN)

VPN is a simple means to use Internet instead of private leased lines or POTS dial-up lines to extend network connectivity. VPN ensures authentication, encryption and tunnelling ie an encapsulation of data from any source or protocol within a TCP/IP data stream. In line with this, an e-mail transaction, data transfer, or remote session is secured from prying eyes. Tunnelling is an important component that makes Internet based VPNs work. There are three widely used tunnelling protocols in VPN. They are Point-to-Point Tunnelling Protocol (PPTP), AltaVista Tunnel and L2F [5].

8.1 Microsoft PPTP

PPTP was designed to be an extension to the PPP protocol, the standard service used for remote access on Windows machines. PPTP is best suited for site-to-user implementation and work well in Windows NT platform. PPTP is built in to Remote Access Services (RAS) on Windows NT server. When the Windows server and client are configured VPN is enabled and both server and client are connected to the Internet. The connection is encrypted with 40-bit RC4 or DES in most implementations. Authentication is performed with Challenge Handshake Protocol (CHAP) or Password Authentication Protocol (PAP). PPTP allows for compatible third-party remote access servers integration like Ascend, Extended Systems and 3Com/U.S. Robotics. PPTP is an excellent and extremely cheap solution for offering secure remote access. The limitation of PPTP is that it is

Windows bias and does not support AppleTalk client, it rather supports only major client/server protocols of IP, IPX, and NetBEUI [16].

8.2 AltaVista Tunnel

AltaVista Tunnel runs on Windows NT, BSD UNIX, or Digital UNIX. It has a distinguish feature which uses a user-based authentication as opposed to IP-based authentication to initialise secure connections. Users can roam from location to location and IPS to IPS without changing their dial-up settings. AltaVista Tunnelling is used to establish site-to-site tunnels. Each server component can be used to connect to another sever component. AltaVista Tunnel uses 40 to 128-bit RC4 for encryption, and uses MD5 to hash data for verification that the data has not been corrupted or tampered with. AltaVista Tunnel is regarded as less secure than other VPN solutions because it uses use-based authentication to verify its connections [9].

8.3 FIREWALL

Firewall precludes hostile intruders from entering into a computer network. These intruders' actions normally compromise confidentiality, denial the network user some vital services or corrupt data. Firewall could be a programme (Software) or a hardware device. Firewalls normally have two interfaces, one interface is exposed to the external network and the other to the network that it is protecting.

Firewalls are configured to meet criteria, so firewall strains incoming and outgoing traffic. Firewall can also administer access to network resources like host applications. Packets can be strained by firewall based on their port numbers, destination addresses and source addresses. Users who use modem to dial into or out the network could not be prevented from firewall. Firewalls criteria differ from one firewall to another and it also depend on the layer of the OSI model it is operating. The lowest layer of OSI model that a firewall can operate is layer 3 (Network layer). There are four categories of firewalls namely: stateful multilayer inspection, application level gateways, circuit level gateways and packet filters firewall [11].

8.4 Packet filtering firewall

Packet filtering firewall operate at the Internet layer of the TCP/IP model and Network layer (layer 3) of the OSI model. Packet filtering firewalls are configured in the router, they compare packet one after the other against set of rules and forward it, send to the originator or drop it. Some of the criteria use here includes destination and source port numbers and IP address of destination and source packet. Packet filtering firewall is cheap and does not affect the performance of the network. The use of Packet filtering firewall gives some level of security at the lower level layer (Network) [4].

8.5 Application level gateways

Application layer gateway does filtering of packets at the layer seven (Application) of the OSI model. Access services are denied for inbound and outbound packets without proxy. An Application layer gateway firewall build up for web proxy will always reject traffic of telnet, gopher or ftp. Logins and log user activities use Application level gateway firewall for security. Application level gateway offer high security but reduce the speed of the network [17]

8.6 IPSec.

IPSec provides the capability to secure communications across a LAN, across private and public WANs and across the Internet. The main feature of IPSec that enable it to support these varied application is that it can encrypt and/ or authenticate all traffic at the IP level. IPSec can secure all distributed applications including remote logon, client/server, e-mail, file transfer, web access etc. IPSec offers three facilities namely: an authentication-only function referred to as Authentication Header (AH), a combined authentication/encryption function known as Encapsulating Security Payload (ESP) and a key exchange function [8].

8.7 Authentication Header

The authentication header offers support for data integrity and authentication of IP packets. The data integrity feature ensures that undetected modification to a packet's content in transit is not possible. The authentication feature enables network device to authenticate the user or application and filter traffic. It also prevents the address spoofing attacks observe on Internet. The Authentication Header also guards against the replay attack. Authentication is based on the use of a message authentication code (MAC).

The authentication header has the following fields [21].

- Next Header (8 bits): This identifies the immediate header following it.
- Security Parameters Index (32 bits): This field identifies security association.
- Authentication Data (variable): It contains an integrity check value for packets.

8.9 Encapsulating Security Payload

The encapsulating security payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality. The encapsulating security payload. The authentication feature enables network device to authenticate the user or application and filter traffic. Encapsulated Security Payload has the following format [20].

- Security Parameters Index (32 bits): Identifies a security association.
- Payload Data (variable): It is a transport level segment or IP packet that is protected by encryption.
- Padding (0 – 255 bytes): This is required when the encryption algorithm requires the plaintext to be a multiple of some number of octets.

9. CONCLUSION

The Study identified problems associated with voice and video when it comes to the convergence of these facilities over an integrated network. The Study also came out with Gigabyte Passive Optical Network as a solution to the problem. According the Study, this is possible because GPON uses fibre cable which has a high bandwidth. It also has other rich feature numerated in the Study which deals with issues like real-time, traffic management and effective management of network resources. Finally, the Study explore the security and management function of GPON and found to be very good especially the VPN and firewall. So it can be concluded that GPON is one of the best solutions to Triple Play technology.

REFERENCE:

[1] Abdellaoui, Z., Dieudonne, Y., & Aleya, A. (2021). Design, implementation and evaluation of a Fiber To The Home (FTTH) access network based on a Giga Passive Optical Network GPON. Array, 10, 100058.

[2] Aris, A. B., & Abd Rahman, M. K. (2019). A Novel Distributed Multi-access Platform for Broadband Triple-Play Service Delivery. In Advances in Information and Communication Networks: Proceedings of the 2018 Future of Information and Communication Conference (FICC), Vol. 1 (pp. 26-43). Springer International Publishing.

[3] Beshley, M., Romanchuk, V., Chervenets, V., & Masiuk, A. (2016, September). Ensuring the quality of service flows in multiservice infrastructure based on network node virtualization. In 2016 International Conference Radio Electronics & Info Communications (UkrMiCo) (pp. 1-3). IEEE.

[4] Durante, L., Seno, L., & Valenzano, A. (2021). A formal model and technique to redistribute the packet filtering load in multiple firewall networks. IEEE Transactions on Information Forensics and Security, 16, 2637-2651.

[5] Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damasevicius, R. (2022). Secured communication using virtual private network (VPN). Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021, 309-319.

[6] Frnda, J., Voznak, M., & Sevcik, L. (2016). Impact of packet loss and delay variation on the quality of real-time video streaming. Telecommunication Systems, 62(2), 265-275.

[7] Gupta, H., Gupta, P., Kumar, P., Gupta, A. K., & Mathur, P. K. (2018, October). Passive optical networks: Review and road ahead. In TENCON 2018-2018 IEEE Region 10 Conference (pp. 0919-0924). IEEE.

[8] Hauser, F., Häberle, M., Schmidt, M., & Menth, M. (2020). P4-ipsec: Site-to-site and host-to-site vpn with ipsec in p4-based sdn. IEEE Access, 8, 139567-139586.

[9] Koczka, F. (2020). Opportunities of Darknet Operations in Cyber Warfare: Examining its Functions and Presence in the University Environment. Academic and Applied Research in Military and Public Management Science, 19(1), 65-81.

[10] Latal, J., Kralik, M., Wilcek, Z., Kolar, J., & Vojtech, J. (2017). Deployment and measurement of quality of service parameters for triple play services in optical access networks. Communications-Scientific letters of the University of Zilina, 19(3), 34-45.

[11] Li, B. Q., & Ma, Y. L. (2023). A 'firewall'effect during the rogue wave and breather interactions to the Manakov system. Nonlinear Dynamics, 111(2), 1565-1575.

[12] Liem, A. T., Sandag, G. A., Hwang, I. S., & Nikoukar, A. (2017, August). Delay analysis of dynamic bandwidth allocation for triple-play-services in EPON. In 2017 5th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-6). IEEE.

[13] Mallick, K., Atta, R., Sarkar, N., Dutta, B., Kuiri, B., Mandal, P., & Patra, A. S. (2022). Performance evaluation of free space optics communication system in the scenario of triple play service using probabilistic shaping scheme. Optics Communications, 522, 128699.

[14] Mandal, G. C., Mukherjee, R., Das, B., & Patra, A. S. (2018). Next-generation bidirectional triple-play services using RSOA based WDM radio on free-space optics PON. Optics Communications, 411, 138-142.

[15] Mat, N. R. N., Rashidi, C. B. M., Aljunid, S. A., Endut, R., & Ali, N. (2020, January). Enrichment of wireless data transmission based on visible light communication for triple play service application. In AIP Conference Proceedings (Vol. 2203, No. 1, p. 020066). AIP Publishing LLC.

[16] Qin, R. (2022, May). Analysis and implementation of man-in-the-middle attack on Microsoft's PPTP. In International Conference on Cryptography, Network Security, and Communication Technology (CNSCT 2022) (Vol. 12245, pp. 32-38). SPIE.

[17] Ramana, S., Ramu, S. C., Bhaskar, N., Murthy, M. R., & Reddy, C. R. K. (2022, May). A Three-Level Gateway protocol for secure M-Commerce Transactions using Encrypted OTP. In 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1408-1416). IEEE.

[18] Singh, A., & Bhogal, R. K. (2022, August). Performance Investigation of Back-Compatible Integrated TWDM/GPON System Using MDM And Pulse Shapes. In Journal of Physics: Conference Series (Vol. 2327, No. 1, p. 012036). IOP Publishing.

[19] Singh, M. K., Singh, A. K., & Singh, N. (2019). Multimedia analysis for disguised voice and classification efficiency. Multimedia Tools and Applications, 78(20), 29395-29411.

[20] Smyslov, V. (2022). RFC 9227 Using GOST Ciphers in the Encapsulating Security Payload (ESP) and Internet Key Exchange Version 2 (IKEv2) Protocols.

[21] Taranov, K., Rothenberger, B., Perrig, A., & Hoefler, T. (2020, July). sRDMA: efficient NIC-based authentication and encryption for remote direct memory access. In Proceedings of the 2020 USENIX Conference on Usenix Annual Technical Conference (pp. 691-704).

[22] Zaripova, D. A. (2021). Network security issues and effective protection against network attacks. International Journal on Integrated Education, 4(2), 79-85.

[23] Zhao, Q., & Ding, G. Z. (2016, June). The Design and Analysis of Campus Network under the Background of Triple Play. In 2016 International Conference on Information System and Artificial Intelligence (ISAI) (pp. 100-103). IEEE.