Performance Evaluation of Multimedia over MPLS VPN and IPSec Networks

Azeddien M. Sllame
Tripoli University
Faculty of Information Technology
Tripoli, Libya
Aziz239@yahoo.com

Abstract— **In this paper multimedia streaming applications is performance is evaluated over MPLS network using two VPN techniques MPLS VPN and IPSec using OPNET simulation tool. However, to make the analysis study more realistic HTTP and FTP traffics are also injected into the tested scenarios and measured. VPN exploits encryption to provide data's confidentiality transmitted through the VPN tunnels. MPLS VPN connects sites over public networks using private labeled switched paths (LSPs) established on MPLS networks. IPSec certifying sender authentication, keeping data's confidentiality by encryption, and provides data integrity.**

The experimental results showed that IPSec is performed better than MPLS VPN in terms of end-to-end delay and packet delay variation. Moreover, OSPF protocol is employed as routing protocol also incurred more traffic in MPLS VPN than IPSec scenario. In addition, H.323 as a multimedia protocol is also recorded longer setup time in the case of MPLS VPN than IPSec scenario.

Keywords: MPLS VPN; IPSec; Tunneling; MPLS networks; VPN.

I. NTRODUCTION

Currently, MPLS is employed by almost all of Internet service providers (ISPs) and contents distribution networks across the world due to the strong features exhibited by MPLS networks such as security through MPLS contained virtual private networks (VPN), supports of convergence and integrity with other different networking technologies, tremendous availability by building connection-oriented network over public connectionless IP networks, transmission efficiency with short end-to-end delays, resiliency and scalability with support of quality of service (QoS) to different applications' requirements. MPLS employs labels to establish connection-oriented network over conventional TCP/IP datagram networks which is connectionless networks in a manner adopted from ATM or virtual circuit networks. Consequently, that introduced faster packet forwarding with reduced packet delivery delay, and provides reliability over TCP/IP connectionless networks by using and integrating MPLS into backbone communication networks all over the world. In addition, MPLS presented an important feature by including QoS concept in its frame format structure, which makes it an alternative solution to best-effort service provided by Internet.
However, the concepts of path establishment, label insertion and levels, FEC classification of data streaming and the binding made between them brought the scalability feature to the MPLS networks, as well as they all integrate different technologies into a one single label-based network. Other features include VPN, traffic engineering (TE), and recovery/alternative paths [1][2][3].

II. MULTIMEDIA NETWORKING

With multimedia networking a number of highly designs-concerns arise so it is a crucial design-work not a unstructured nor an arbitrary structure, such as huge bandwidth is required due to multimedia burstiness with dense traffic composing of multimedia scenes, multicasting as a nature of multimedia applications, and multimedia usually preferred to be watched on real-time by many users. Therefore, a lot of efforts have been made to facilitate a good user experience to multimedia over Internet by developing new protocols and processes, making emerged network infrastructures tools and technologies, redesigning network devices such as routers, refining models for improving QoS, and producing efficient multimedia applications. Furthermore, improvements included introducing traffic classifications, prioritizations, and resource allocations to multimedia flows. Also, special multimedia protocols such as real-time transport protocol (RTP), real-time control protocol (RTCP), real-time streaming protocol (RTSP), session initiation protocol (SIP), and resource reservation protocol (RSVP) [6][7][8][9]. However, RTP protocol is used instead of TCP protocol to overcome the slow start when congestion happens with TCP, to disable TCP unbounded retransmission delay and RTP introduced time-stamping which is a feature required by multimedia streaming playbacks. RTCP protocol is used to support RTP by collecting suitable information needed to improve multimedia sessions QoS, stability, and continuity. In addition, UDP is employed with RTP to escape from TCP congestion delays and to remove acknowledgement overhead associated with TCP protocol for time-sensitive real-time multimedia streaming applications. Still, TCP is used on the starting of any multimedia sessions to make session initiation period reliable, stable and synchronized with efficient flow control, before multimedia transmission starts between participants. RTSP is employed to allow clients to control multimedia servers to watch multimedia over Internet, while SIP is put in to initiate multimedia streaming sessions. Resource reservations along network paths are established by the RSVP protocol.

A. VoIP application

VoIP is a real-time inelastic application produces traffic at the rate generated by the voice codec irrespective to available capacity. Inelastic "real-time" application means the application requires the packets composing of the flow to be present on time at the right place on their stream at the receiver's end or otherwise assumed as lost packets. The VoIP uses codecs that is used by the sender to transform the voice analog signal to a digital form contains equivalent bit stream

and returns back the digital bit stream into an analog voice signal when received by the recipient of the VoIP call; keeping the accuracy of the received VoIP call. As mentioned earlier the VoIP is transported by RTP over UDP protocol in order to overcome the drawbacks of the TCP protocol retransmission behavior with undetermined delay limits that are not favorited with the real-time multimedia transmission. Furthermore, the VoIP flow is involving two phones or two PCs running VoIP application. However, two flows are associated with any VoIP session; one flow for transferring audio voice between participants while the second which is client-server flow type; used for call setup, maintenance, and teardown as seen in Figure (1).

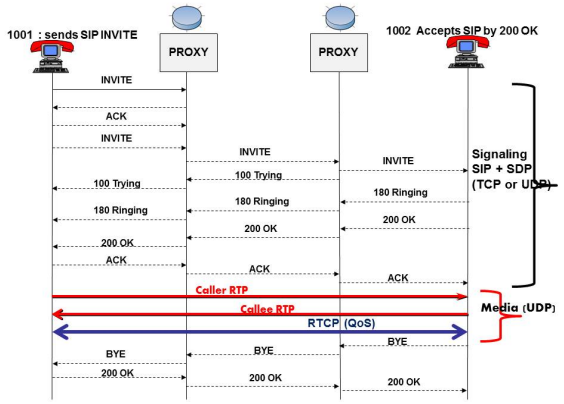

Fig. 1. VoIP session

Still, the end-to-end delay is an important quality measure of the VoIP transmission which is measured as one-way from sender to the receiver because it has significant influences on the admissibility and continuity of VoIP call perception decision. However, according to the ITU-T recommendations found in G.114 standard [11]; the call should be terminated when the end-to-end delay of the VoIP call reaches the 400ms value, while the end-to-end delay value of 150ms is acceptable [4] [11]. In addition, the VoIP is affected by packet re-ordering, usually the reordering has no high impact on QoS of VoIP; but the reordering may introduce more delay jitter on the flow of VoIP due to the differences of timing between the different paths that are followed by the packets composing of the VoIP stream. Therefore, that introduced delay jitter may degrade the QoS level slightly [19]. Furthermore, the throughput may has an impact on VoIP quality, where networks that are used to carry VoIP is usually designed efficiently to withstand congestion to a large extent to satisfy the steady flow of VoIP stream with sufficient bandwidth from the planed capacity that can handle the load expected on the network. However, availability and scalability need to be considered when planning bandwidth for the VoIP networking infrastructure to control delay jitter and packet loss requirements [4].

B. *Video streaming*

Video streaming is a transmission operation between clients and a multimedia server. The video streaming session is managed and their data is transmitted using the RTSP/UDP/RTP protocols after a successful session is setup using TCP protocol and then the playback can be started before the completion of the video download. Video streaming is either video on demand (VOD) as IP unicast transmission or broadcasting video channels with IP multicast way, as seen in Figure (2). The end-to-end delay from the server to the requested client is considered as the most important QoS factor, which needs to be controlled efficiently. The other factor is the delay jitter that can be eliminated by means of de-jitter buffers to make playback of the video stream accurate and continuous, which makes the variation delay and network delays as a constant value in order to make the sufficient user experience. However, the impact of the packet loss is also important in video streaming since it will produce some errors during the construction of the transmitted multimedia frames, thus error concealment techniques such as forward error correction is needed [4].

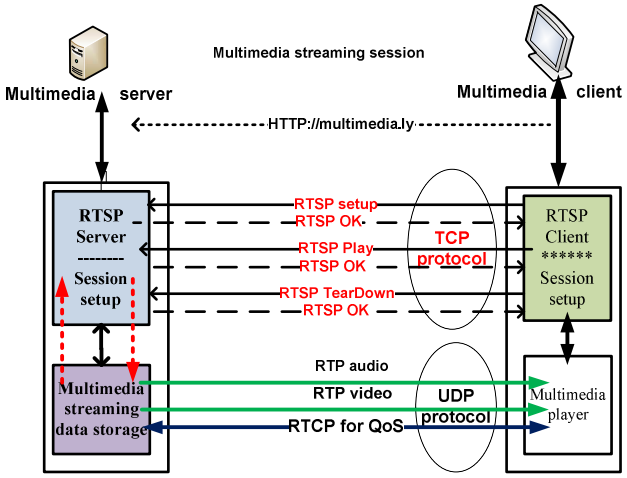

Fig. 2. Typical multimedia streaming session

C. *Video conferencing*

Video conferencing uses SIP or H.323 to establish and manage multimedia sessions. In video conferencing there are two different logical channels one for video and one for audio transmission are established to start multimedia transfer using RTP/UDP protocols with different UDP ports. However, packet loss is very important QoS metric in this application so it needs to be handled carefully by offering sufficient bandwidth to the video conferencing over the designed network. In addition both the end-to-end delay and delay jitter depend on the quality of the contents of the video conferencing stream itself, the higher the video stream's quality the higher synchronization is needed between video, and audio data composing of the video stream [4] [10].

III. MPLS

MPLS originally developed to combine some features of virtual circuits with IP datagram techniques. MPLS routers forward packets by using labels which has local significance as the paths and channels in virtual circuit networks, and labels have equivalent functions to those used with VPI/VCI which belongs to ATM technology [3]. Ordinary IP router is composed of control component and forwarding part. Control part contains routing protocols that exchange routing information among routers to establish routes that will be used

to build routing tables which needed to transfer users' data across the networks. However, forwarding tables is obtained from routing tables, which will be used by forwarding part of the router. Forwarding component contains all necessary functions and procedures that facilitate making applicable forwarding decision to move the packet on the way to its final destination through the appropriate interface of the router [5]. Therefore, IP router forwards packets by using packet IP prefix, however, all addresses with the same prefix will be forwarded through the same output interface of the IP router. On another hand, MPLS is constructing LIB table and associate IP prefix with so called forward equivalent class (FEC). Consequently, a label forward information base (LFIB) table is created to contain that information such as FEC and links it with a label that will be used as indicator to find which output interface of the router is selected to move the packet further toward its destination, since LFIB is indexed by means of incoming label.

IV. MPLS VPN

VPN applies encryption to offer confidentiality to data transmitted across it. MPLS VPN provides security means to traffic and segregates that traffic from other traffics over Internet as well as it offers network resources access with a well-defined policy. MPLS VPN employs LSPs that are established inside MPLS domain; unlike conventional VPN which transports users' data using specific tunneling protocol such as PPTP, L2TP, or GRE. Thus, MPLS VPN interconnects different sites over public networks using private LSPs, which allows different MPLS VPN to be linked together over running LSPs. In addition, MPLS VPN simplifies the any-to-any sites among different sites within any enterprise. As a result, this enhances the scalability feature of the MPLS networking technology [12]. Furthermore, MPLS VPN can handle different QoS requirements needed by real-time applications or other enterprise sensitive application. See Figure (3).

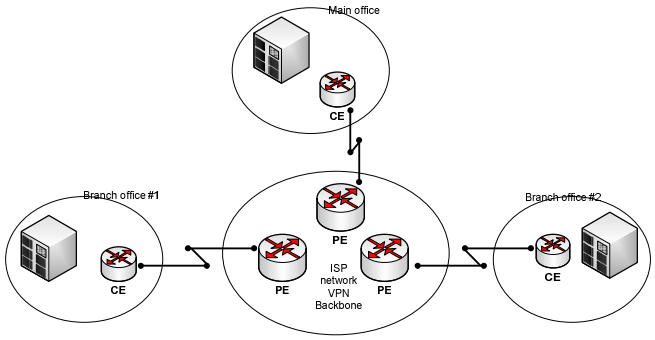

Fig. 3. MPLS VPN principle

MPLS VPN uses peer model where the customer's edge routers (CE router) are communicating their routes to SP' edge routers (PE) and BGP protocol is employed to distribute the information about the paths of specific VPN between PE routers belongs to such VPN. However, in order to make proper separation of different existed VPN, the PE routers send information to CE routers the routes learned from other side CE routers which are belongs to the desired VPN only. Thus, there are no peering occurs among CE routers together to prevent overlay in routing inside VPN.

V. IP SECURITY (IPSEC)

IPSec is a group of services and protocols works at network layer; used to provide security to TCP/IP networks with sufficient flexibility, scalability, and interoperability. IPsec contains two protocols; encapsulating security protocol (ESP) and authentication header (AH), supported with Internet key exchange (IKE). In addition, IPsec operates on two modes tunnel mode and transport mode while forwarding users' data through different networks. IPSec designed to satisfy the following requirements: ensuring sender authentication, sender data confidentiality by encrypting user's data before transmission, data integrity to ensure receiving data as it was sent by the sender, access control and protecting the receiver from spoofing and man-in-the-middle attacks.

D. IPSec protocols

IPSec contains the following components:

1) Authentication Header (AH)

AH it provides authentication and securing packet's integrity irrespective to the employed IPSec mode. In addition it offers replay protection and access protection, while it is used together with ESP protocol to complement integrity with confidentiality provided by ESP protocol. However, with IPSec tunnel mode, AH generates new IP header to every packet, while with the transport mode the IP address is replaced with the gateway's IP addresses.

2) Encapsulating security protocol (ESP)

ESP it is the second IPSec protocol which used to provide confidentiality by encrypting the packet's payload, as well as deals with authentication in IPSec v2. ESP works with symmetric cryptography to encrypt the IPSec packets, so both protected IPSec ends use the same encryption/decryption key with every packet.

3) Internet key exchange (IKE)

it is responsible for negotiation, definition, and management of the security association (SA). Thus, SA contains a sequence of approved keys, security protocols, and security parameters index (SPI) which intended to offer a secure tool for forming IPSec connections. However, SPI is a field found in AH header which is a unique 32 bit identifies each connection at every endpoint. Furthermore, IKE applies a Diffie-Hellman exchange mathematical algorithm in order to produce symmetrical keys for IPSec endpoint session usages.

IPSec contains a rich set of different features and options, which can lead to complexity during combinations selections, as a result the probability of vulnerabilities, will be increased with the protocol implementation. Thus, a special care with high effort configurations is needed while implementing IPSec protocol.

E. IPSec modes

IPSec includes two modes tunnel mode and transport mode; there structures are illustrated in Figure (4).

1) Tunnel mode

In tunnel mode the entire IP datagram is encapsulated within new IP datagram using IPSec protocol, which makes the tunnel mode is more secure than transport mode. However, in

this mode, a new IP header is added in front of IP packet so the whole IP packet is encrypted including its header, which will increase the size of the packet which protects that packet from different attacks.

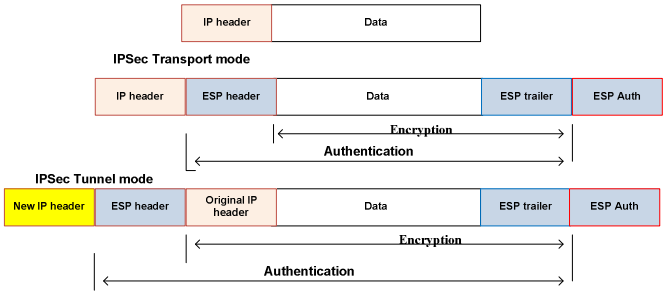

Fig. 4. IPSec modes' organizations: (transport and tunnel)

2) Transport mode

In transport mode the payload is encrypted individually, thus ESP or AH headers is placed between IP header and encrypted payload. However, in this transport mode of IPSec protocol the IP address is visible which make it visible to some attacks.

VI. Experimental Results

Modeling and simulation tools play an important role in performance evaluation and experimentation of computer networks due to cost encountered if the real networks need to be built to test new ideas and technologies. Therefore, OPNET modeling and simulation tool is engaged to implement analysis experiments to compare MPLS VPN with IPSec VPN models. This experiment has one MPLS-based baseline network case as shown in Fig. 5, with two main scenarios one for MPLS VPN while the other implementing IPSec. However, four applications are used to analyze the network: HTTP (heavy traffic), FTP (large files), video conferencing, and VoIP (100 call per sec), generating of a total traffic size 200.872 GB injected into the network by communicating two LANs (each has 50PCs) over MPLS network that have interconnection to Internet and two main HTTP and FTP servers.

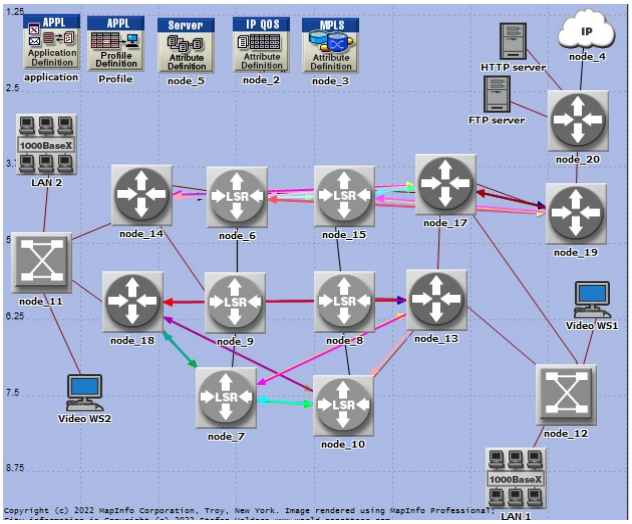

Fig. 5. The case study diagram

In all results the RED color represents MPLS VPN, while BLUE color represents IPSec curve.

FTP simulation results

Figure (6) show the results of FTP download response time; The results identifies that the implementation of the MPLS VPN network has lower download response time for FTP traffic than that produced by applying IPSec.

Figure (7) demonstrates the FTP upload response time; the result showing that IPSec recorded higher (worse) upload response time for FTP traffic in the middle of the test then it is results becomes better than MPLS VPN. However, MPLS VPN showed higher (worse) results at the beginning of the simulation run.

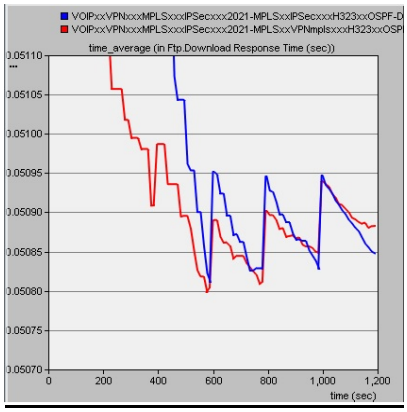

Fig. 6. FTP download response time

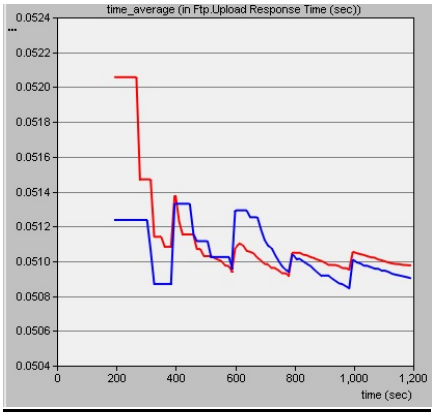

Fig. 7. FTP Upload response time

HTTP simulation results

Figure (8) illustrates the results of HTTP traffic, where it shows that MPLS VPN case registered higher (worse) object response time (0.00120sec) than the results of IPSec scenario which produced better result (lower response delay) tunneling (0.00115sec).

Figure (9) demonstrates the results of HTTP traffic for page response time. The figure describes that MPLS VPN produced (around 0.00300sec) worse results than IPSec scenario that recorded (0.00293sec).

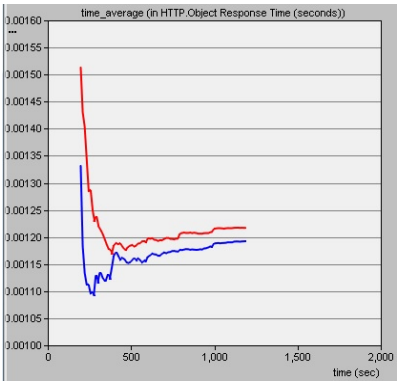

Fig. 8. HTTP object response time

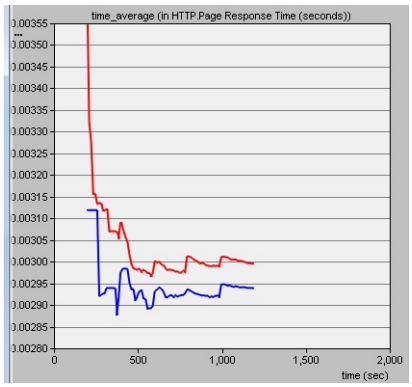

Fig. 9. HTTP page response time

Video conference simulation results

Figure (10) illustrates the results of video conferencing packet end-to-end delay. The figure clearly demonstrates that MPLS VPN scenario has recorded (0.0025sec) the worse results in terms of end-to-end delay for video conferencing traffic, while IPSec reported (around 0.0004sec) which is much better value than MPLS VPN.

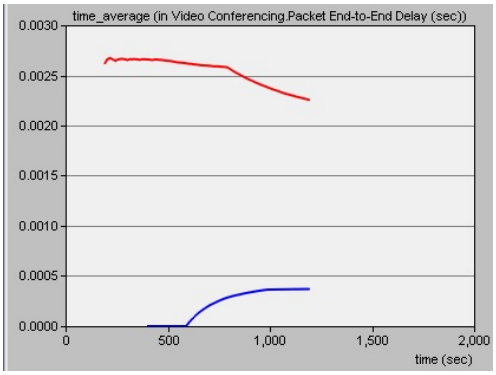

Fig. 10. Video conferecing packet end-to-end delay

VoIP simulation results

Figure (11) describes the results of the packet end-to-end delay for VoIP traffic. The results clearly show that the MPLS VPN scenario produced (0.0600270 sec) while IPSec case recorded (0.0600260 sec). However both values are nearly together but still IPSec reporting better results than MPLS VPN.

Figure (12) refer to the result of VoIP packet delay variation measurement, in which IPSec obtained very good result which is lower than the MPLS VPN.

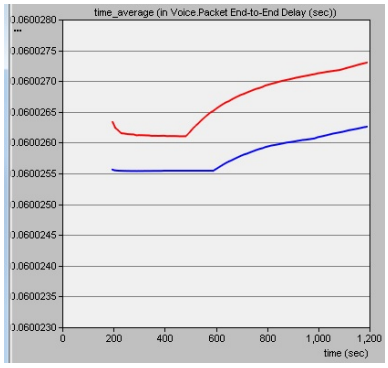

Fig. 11. VoIP packet end-to-end delay

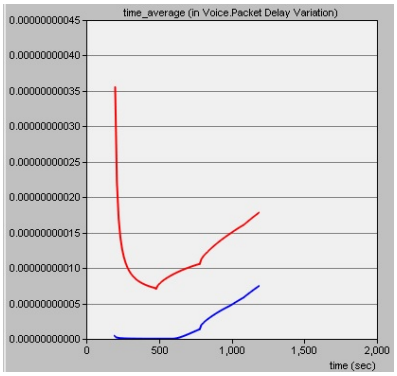

Fig. 12. VoIP packet delay variation

Other different simulation results

Figures below show the results of different protocols employed in the experimental study in order to make it more realistic one.

Figure (13) shows the results of H.323 signaling protocol which is used to establish VoIP and video conferencing sessions. However the figure exemplifies that H.323 protocol incurred higher setup time with MPLS VPN scenario than that of the IPSec scenario. Of course, this increases the delay for MPLS VPN while running VoIP and video conferencing applications.

Figure (14) illustrates the delay experienced from IP protocol background traffic, the figure describes that MPLS VPN has higher (worse) delay incurred from IP protocol background traffic.

Figure (15) describes TCP delay produced by transport layer during multimedia session setup and during transporting of HTTP and FTP traffic. Figure shows that MPLS VPN case study has recorded more TCP delay than IPSec scenario.

Figure (16) demonstrates how many OSPF traffic is generated during the simulation run of the scenarios. The figure clearly shows that MPLS VPN case study has much higher OSPF routing traffic than the IPSec scenario. Thus, inheriting more delay for MPLS VPN scenario that will consume part of the transmission capacity of the network.

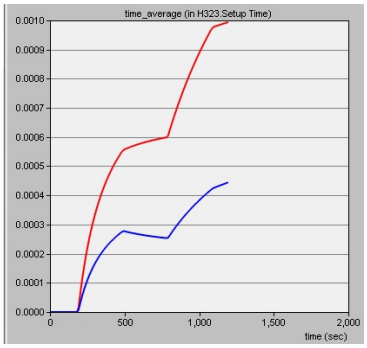

Fig. 13. H.323 protocol setup time

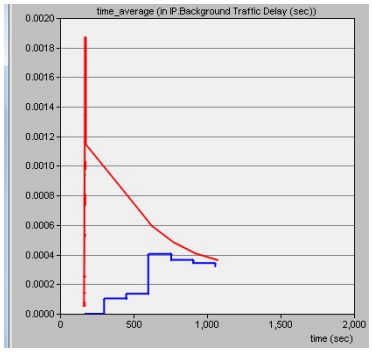

Fig. 14. IP protocol background traffic delay

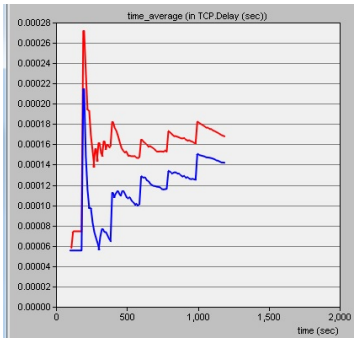

Fig. 15. TCP delay

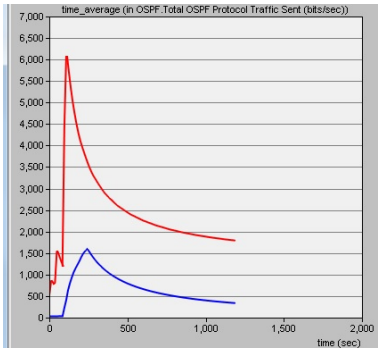

Fig. 16. OSPF routing traffic sent (bits/sec)

VII. Conclusion

Multimedia streaming applications have very strict transmission requirements. OPNET is a powerful tool used in performance evaluation of networks with different protocols, requirements, technologies [13-15]. However in this paper we have evaluated two very important VPN architectures currently have more attention in ISP providers. From the detailed figures produced as results of the simulation run. The IPSec has better results than MPLS VPN with multimedia applications in terms of end-to-end delay and packet delay variation. However, we found that MPLS VPN scenario has incurred a higher delay due to other delays produced by IP protocol, OSPF as routing protocol, TCP protocol, and H.323 protocol experienced higher setup time with MPLS VPN scenario than that of the IPSec scenario. all of them produced higher delay in MPLS VPN case study.

Reference

[1] James F. Kurose and Keith W. Ross: ComputerNetworking: A Top-Down Approach Featuring the Internet, Addison Wesley Publishers, USA, 2012.

[2] William Stallings: “Computer Networking with Internet Protocols and Technology,” Prentice Hall (Pearson Education), USA, 2004.

[3] Larry L. Peterson and Bruce S. Davie: Computer Networks: A Systems Approach, 4e, Morgan Kaufmann Publishers, Elsevier, 2007, San Francisco, CA, USA.

[4] John Evans and Clarence Filsfils: Deploying IP and MPLS QOS for Multiservice Networks: Theory and practice, Morgan Kaufmann Publishers, Elsevier, USA, 2007.

[5] Harry Perros: Connection-oriented Networks: SONET/SDH, ATM, MPLS and Optical networks, John Wiley & Sons Ltd Publisher, UK, 2005.

[6] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler: Session Initiation Protocol (SIP), RFC 2361, Internet Engineering Task Force (IETF), June 2002.

[7] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson : A Transport Protocol for Real-Time Applications (RTP), RFC 3550, Internet Engineering Task Force, July 2003.

[8] H. Schulzrinne, A. Rao , R. Lanphier: Real Time Streaming Protocol (RTSP), RFC 2368, Internet Engineering Task Force (IETF), April 1998.

[9] M. Handley, V. Jacobson: Session Description Protocol (SDP), RFC 4566, Internet Engineering Task Force (IETF), July 2006.

[10] Saleem N. Bhatti and Jon Crowcroft: QoS-Sensitive Flows: Issues in IP Packet Handling, IEEE Internet Computing, July-August 2000, pp.-48-57.

[11] ITU-T Recommendation G.114: ”International telephone connections and circuits – General Recommendations on the transmission quality for an entire international telephone connection One-way transmission time”, 05/2003.

[12] E. Rosen, Y. Rekhter : BGP/MPLS IP Virtual Private Networks (VPNs), RFC 4364, IETF, February 2006.

[13] Reema A. Saad, Mariam Abojella Msaad, Azeddien M. Sllame: Performance Evaluation of Multimedia Streaming Applications in MPLS Networks Using OPNET, in the IEEE 1st International Maghreb Meeting of the conference on Sciences and Techniques of Automatic control and computer engineering (IEEE MI-STA'2021), May 2021, Tripoli, Libya.

[14] Azeddien M. Sllame, Mohamed Aljafry: Performance Evaluation of Multimedia over IP/MPLS Networks, International Journal of Computer Theory and Engineering, Vol. 7, No.4,pp.283-291, August 2015.

[15] Azeddien M. Sllame: Evaluating the Impact of Routing on QoS of VoIP over MANET Wireless Networks, In Open Access Library Journal (OALib Journal), Scientific Research Publishing, Volume 4:e3361, No. 2, Feb. 2017.