Scientific Research Publishing

Journal of Computer and Communications, 2020, 8, 100-108
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

# Performance Evaluation of an Internet Protocol Security (IPSec) Based Multiprotocol Label Switching (MPLS) Virtual Private Network

**Conrad K. Simatimbe**[*]**, Smart Charles Lubobya**

Department of Electrical and Electronic Engineering, School of Engineering, The University of Zambia, Lusaka, Zambia
Email: *syakalima@gmail.com

**How to cite this paper:** Simatimbe, C.K. and Lubobya, S.C. (2020) Performance Evaluation of an Internet Protocol Security (IPSec) Based Multiprotocol Label Switching (MPLS) Virtual Private Network. *Journal of Computer and Communications*, **8**, 100-108.
https://doi.org/10.4236/jcc.2020.89009

**Received:** August 31, 2020
**Accepted:** September 22, 2020
**Published:** September 25, 2020

## Abstract

This paper evaluates the performance of Internet Protocol Security (IPSec) based Multiprotocol Label Switching (MPLS) virtual private network (VPN) in a small to medium sized organization. The demand for security in data networks has been increasing owing to the high cyber attacks and potential risks associated with networks spread over distant geographical locations. The MPLS networks ride on the public network backbone that is porous and highly susceptible to attacks and so the need for reliable security mechanisms to be part of the deployment plan. The evaluation criteria concentrated on Voice over Internet Protocol (VoIP) and Video conferencing with keen interest in jitter, end to end delivery and general data flow. This study used both structured questionnaire and observation methods. The structured questionnaire was administered to a group of 70 VPN users in a company. This provided the study with precise responses. The observation method was used in data simulations using OPNET Version 14.5 Simulation software. The results show that the IPSec features increase the size of data packets by approximately 9.98% translating into approximately 90.02% effectiveness. The tests showed that the performance metrics are all well within the recommended standards. The IPSec Based MPLS Virtual private network is more stable and secure than one without IPSec.

## Keywords

Multiprotocol Label Switching, Internet Protocol Security, Virtual Private Network, Video Conferencing, Voice over Internet Protocol, Jitter, End to End Delay

## 1. Introduction

There has been noticeable increase in organisations seeking to smartly integrate their business operations through various technological methods in Zambia. The preliminary survey shows that most of businesses have presence in all provinces of Zambia owing to the growth of business and technological space. The increased business space calls for a robust system to integrate inter branch operations in the quest to improve service delivery and attain market competitive edge.

This work seeks to evaluate the layer 3 Virtual Private Network with emphasis on Internet Protocol Security based Multiprotocol Label Switching (MPLS). [1], informs that MPLS technology is a modern core technology for most provider networks. Therefore the Internet Protocol Security (IPSec) seeks to immunize the network data packets from unauthorized access [2].

[3], conducted a study on the factors impacting the performance of data transferred through Virtual Private Network (VPN). The study indicated that most Information Technology managers and executives preferred the use of IPSec for site to site VPN. The internet bandwidth utilization, format of data and compressibility were also highlighted as the critical factors that affects data transfer performance in VPN implementation. [4], evaluated the impact of tunnel layer of IP, MPLS, MPLS VPN, and MPLS IPsec VPN on realtime applications. The evaluation criteria were based on jitter, latency, MOS score and loss rate and established that the IP network is affected by a high latency and a poor Mean Opinion Score. A study on Cloud based virtual private networks using IP tunneling for remote site interfaces was conducted by Ogbu and others [5], suggested that there is need for Internet Protocol (IP) technology in most organizations that creates a secure tunnel through a less secure public network [6], observed that header encapsulation increases the degradation in the flow of traffic and general performances, however recommended the implementation of IPSec to enhance security.

[7] studied the behavior of the core network equipment at the edge of the multiprotocol label switching network. The authors identified the devices as label edge router and label switch router that forwards labels through multiprotocol label switching network. They sought to elaborate how the packet that gets into the multiprotocol label switching network allocates labels through mapping of the label table with Internet Protocol table. The allocated label at the ingress label edge router was found to give the path information of the packet to get to the destination while the egress label edge router creates labels switch path dynamically [8], in their study the authors aimed at enhancing VoIP security using VPN (Virtual Private Network) technology. They developed an application using Android to support VoIP using Linphone, OpenVPN, and Asterisk. The study was effective and was able to generate anonymous packets. The study also showed that that the simultaneous invocation of VPN did not negatively affect the overall calling quality. The experiment was also successful in security and packet encryption procedures [9], studied the implementation of the premium services for MPLS IP VPNs. The authors provide that it is the Multiprotocol label switching

that enables networks to manage network costs, and brings the network to operate in a single domain thereby increasing resources sharing and reduce business operational costs. The MPLS technology guarantees traffic engineering and optimizes bandwidth usage achieved by virtual paths or routes creation between two sites.

The above studies have provided insights on hardware and software, protocols, operationalization of the network and its relevance to business communication. This study compares the performance of MPLS VPN that uses IPSec protocol against the performance of an MPLS VPN without IPSec protocol. It basically articulates by evaluating the behaviour of MPLS data packets in a secure environment.

## 2. Methodology

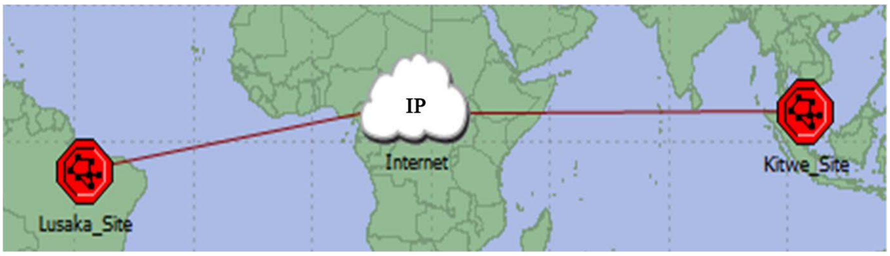
The study used both quantitative and qualitative methods. It used structured questionnaire and observation as data collection instruments. Simple and easy to follow questions were structured in the questionnaire. The observations method was used in the data simulations using the OPNET 14.5 simulation software and the results were examined, recorded and presented accordingly. A selection of protocols, hardware and software in the simulation software was done to make the network as close as possible to the study area.

### 2.1. The Virtual Private Network

Virtual Private Network comprise of more than one autonomous network. The Virtual Private Networks (VPN) provides for the smooth and safest way of inter-connecting geographically distant office locations. Although an organization can opt to have expensive dedicated tele-commuincation lines between branch offices, a VPN is the modern technology that brings about shared, cheaper, faster and secure inter-branch communications. [10], has defined VPN as a private data network that makes use of the public telecommunication infrastructure and maintains data privacy through a set of predefined security authentication in the VPN tunnel. Figure 1 below shows the VPN Topology.

### 2.2. Multiprotocol Label Switching (MPLS)

The MPLS is a Wide Area Networks (WAN) based technology developed by the



Source: Author.

Figure 1. VPN topology.

Internet Engineering Task Force (IETF) [4]. It is deployed mainly in core or service provider networks. An MPLS VPN therefore can be said to be a VPN deployed based on the Internet Service Provider's cloud providing communication tunnel between the customer sites [11]. As the data packet from the private or customer network enters the public network, it is given a specific Forward Equivalency Class (FEC) which in return assigns a label and a specific route to the destination host. The creation of the tunnel ensures that customer network is protected from the public network [12].

### 2.3. Internet Protocol Security (IPSec)

Security generally is made up of three variables commonly known as security triad. The security triad has Confidentiality, Integrity and Availability [13] [14], observes that the MPLS IPSec VPN is well known for good security features that are embedded in its architecture. [15] explain that the network layer is dominated by the Internet Protocol (IP). The IPSec protocol suites comprise of Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols, [16]. Security mechanisms include user authentication processes, data encryption and decryption, and tunnel creation. However, these security features are said to reduce the efficiency of the network. According to [17], security features cause delay and latency in the transmission process of the VPN packets. The IPSec features actually degrade the traffic flow as observed by [18]. Many authors including [2] [3] [4] [18] argue that with the increase in computer attacks that threaten data integrity and availability, it is now critically inevitable to have a secured network infrastructure. The Virtual Private Network (VPN) technology brings about this security aspect in the communication systems.

### 2.4. Performance Evaluation Methodology

The OPNET Modeller 14.5 Network simulator was used to simulate the IPSec based MPLS VPN. Two scenarios were developed as follows:

1) Scenario 1 is on the MPLS VPN network without Internet Protocol Security (IPSec).

2) Scenario 2 is on the MPLS VPN network with Internet Protocol Security (IPSec).

Both scenarios had 68 VPN users configured on one autonomous network while four (4) Servers were deployed on another *i.e.* VoIP, Video Conferencing, HTTP/Email and Database Servers.

There are two autonomous sites involved in this study. The first site is Lusaka and the second site is Kitwe which hosts all the servers and services. The Lusaka site is running on Class "C" network addressing system with network address 192.168.20.0/24. On the other site, Kitwe is running on Class "A" network addressing system with the network address being 10.10.10.0/16.

The Workstations at Kitwe and Lusaka sites are configured to use 100 Base-T cables that provide 100 MBPS to connect to the switch while all routers are interlinked with 10 GBPS cable.

There are four (4) configured set of attributes in this study. These are Profile Definition, Application Definition, IP_QoS definitions and MPLS definitions. These sets of attributes were used to condition the VoIP and Video conferencing traffic in the study. In Figure 2 below, the configuration of MPLS with IPSec protocol is shown.

## 3. Results Analysis

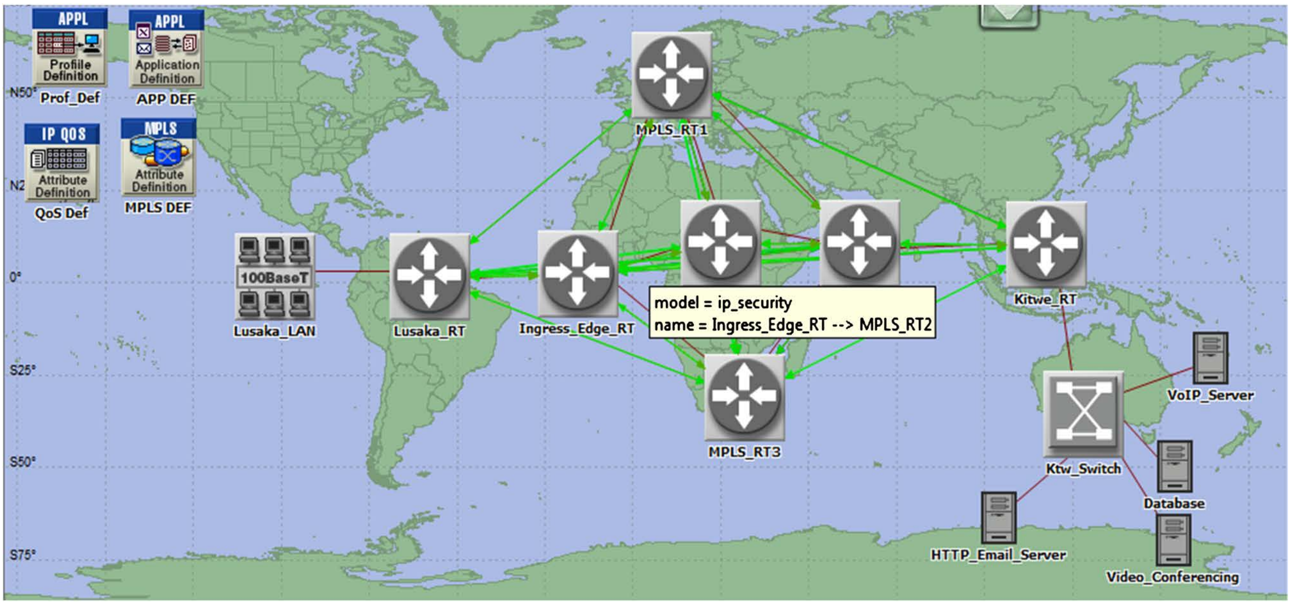
The results analysis presents the results generated from the simulation activities. There are two simulation results that are discussed in this part and these are VoIP, Video Conferencing.

### 3.1. Voice over Internet Protocol Evaluation Criteria

The Voice over Internet Protocol (VoIP) was evaluated in the area of Jitter, Latency and Mean Opinion Score (MOS). Jitter in this regard means variation of latency in a given space of time where latency represents the time required for data traffic to move from source to destination or the sum of delays in the network, [4]. The Mean Opinion Score is the measure of the quality of the reproduction of speech.

#### 3.1.1. Jitter

Figure 3 shows the Jitter in the data set produced by the simulation. The jitter was uniform from the beginning up to about the 180th second. The variation is seen improving in the MPLS_IPSec scenario more than in the MPLS without IPSec. The trend is observed improving towards negative numbers in MPLS_IPSec scenario which translates into better jitter or within acceptable margins. The



Source: Author.

Figure 2. IPSec MPLS network configuration.

routing process in the IPSec tunnel and the dual labeling methods in MPLS potentially brought about this difference in the two scenarios.

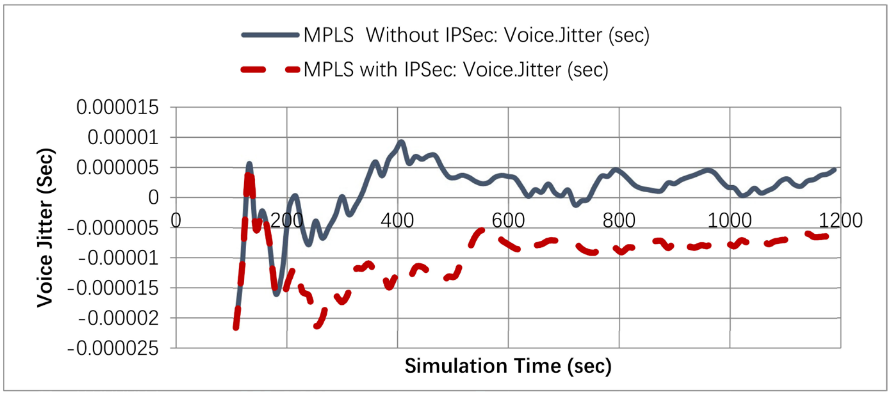
### 3.1.2. End-to-End Delay

In Figure 4 below, the VoIP end to end delay is presented which shows that the two scenarios had a closer delay although the IPSec based was slightly higher.

The end to end packet simulation curve indicated that IPSec based MPLS was on average slightly higher than the MPLS without IPSec arising from the encryption layer requirements of IPSec. However, we also note that the two scenarios presented reliable delivery (below 120 ms) of packets from source to destination on end to end delivery. Authors [18] [19] [20] provide that end to end delay should not exceed 200 milliseconds while jitter is expected to be below 60 milliseconds. This is consistent with the ITU-T standard that requires voice to be below 200 milliseconds [21].

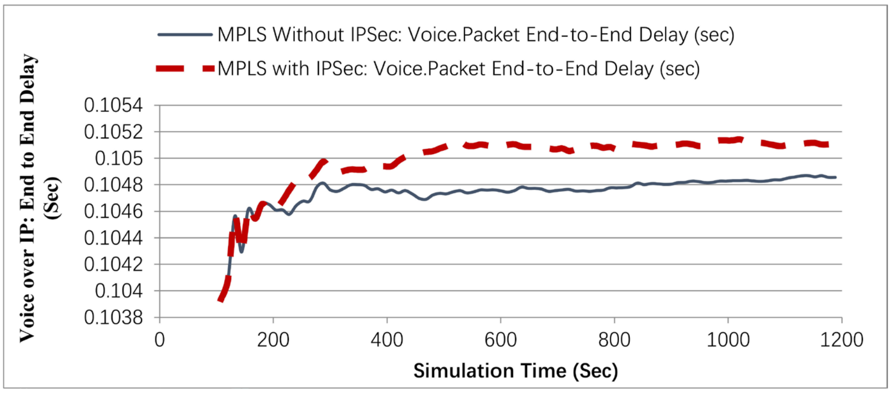
### 3.1.3. Mean Opinion Score

Figure 5 compares the Mean Opinion Score results between the two scenarios. The MOS is used to measure subjective quality of a call. On a score of 1 to 5, quality is said to be unacceptable at 1 while at 5 quality is scored excellent. The



Source: Author.

Figure 3. VoIP jitter evaluation results.



Source: Author.

Figure 4. VoIP end-to-end delay.

ITU-T provides that VOIP calls in the range 3 to 4 are acceptable.

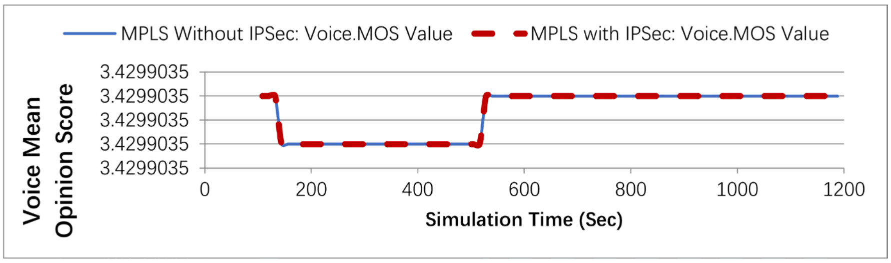
Based on Figure 5, both MPLS with IPSec and MPLS without IPSec scenarios have the same Mean Opinion Score below 3.5. This means that both configurations give the same speech quality. The quality therefore can be considered to be good in both scenarios.

### 3.2. Video Conferencing Evaluation Criteria

The Video Conferencing was evaluated on the basis of Jitter and End-to-End delay. The graph below shows that the MPLS with IPSec has lower jitter than the scenario for MPLS without IPSec.

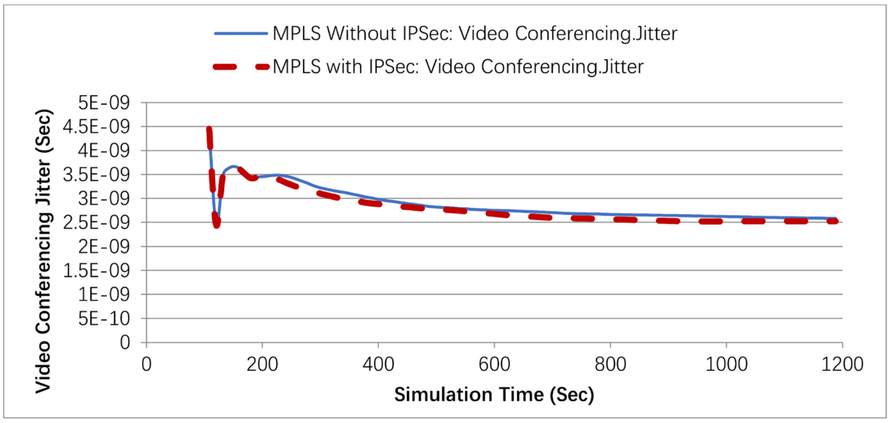
In Figure 6, it is observed that MPLS with IPSec has a better performance than in the MPLS without IPSec below 40 milliseconds. It is further observed that the performance improves on both scenarios as transmission progresses and falls within acceptable video transmission margins of less than 60 milliseconds. This can also be attributed to the buffering and video compression activities that Video requires at the onset of transmission. Therefore, we can conclude that both scenarios supported Video Conferencing within acceptable margins.

The IPSec based MPLS has shown better performance than the scenario without IPSec. In the Figure 7, we observe that there is a similar delay pattern from start up to the 200th minute of simulation. Thereafter, the IPSec based MPLS performance improves and maintains the trend to the end.



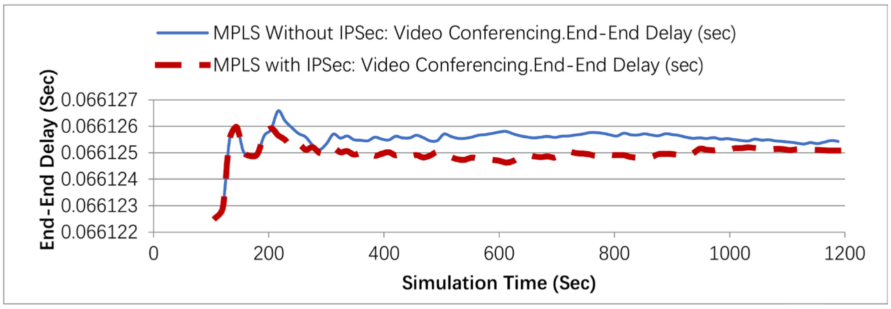
Source: Author.

Figure 5. MOS VoIP evaluation.



Source: Author.

Figure 6. Video conferencing jitter.



Source: Author.

**Figure 7.** Video conferencing end to end delay.

## 4. Conclusions

The conclusions of this research work have been drawn in line with the examined performance evaluation criteria. The results of the study have shown that even after adding extra packets, the MPLS with IPSec remain within acceptable operating levels. This was exemplified in the Video Conferencing where jitter remained within ITU-T acceptable margins below 60 milliseconds although started with a sharp rise due to call setup effects, it came down to normal margins. In the Voice over Internet Protocol (VoIP), all the three tests conducted; jitter was below 0, delay was less than 120 milliseconds and mean opinion score was less than 3.5 suggesting that voice communication was supported and within acceptable standards when compared in line with the ITU-T standards.

The study results have shown that Internet Protocol Security (IPSec) increases the size of the data packets by about 9.98%. Subsequently, this also increases jitter and delay in the IPSec based label switched network. It is also true that when IPSec is added to the MPLS virtual private network, the bandwidth usage tends to be higher than when IPSec is excluded.

In future, this work could be extended to compare the performance of VPNs in wireless network and performance in wired network setups. Furthermore, future studies could be skewed to look at video conferencing in detail and consider video compression activities and balancing of voice and video in a telecommunication network.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References

[1] Ahmed, F., Butt, Z.U.A. and Siddqui, U.A. (2016) MPLS Based VPN Implementation in a Corporate Environment. *Journal of Information Technology & Software Engineering*, **6**, 1-7.

[2] Shahzad, A. and Hussain, M. (2013) IP Backbone Security MPLS VPN Technology. *International Journal of Future Generation Communication and Networking*, **6**, 81-96. https://doi.org/10.14257/ijfgcn.2013.6.5.09

[3] Taneja, D. and Tyagi, S.S. (2019) Factors Impacting the Performance of Data

Transferred Via VPN. *International Journal of Innovative Technology and Exploring Engineering*, **8**, 2962-2966. https://doi.org/10.35940/ijitee.K1946.1081219

[4] Bensalah, F., El Kamoun, N. and Bahnasse, A. (2017) Analytical Performance and Evaluation of the Scalability of Layer3 Tunneling Protocols: Case of Voice Traffic over IP.

[5] Ogbu, M.N., Onoh, G.N. and Okafor, K.C. (2017) Cloud Based Virtual Private Networks Using IP Tunneling for Remote Site Interfaces. 2017 *IEEE* 3*rd International Conference on Electro-Technology for National Development* (*NIGERCON*), Owerri, 30-41. https://doi.org/10.1109/NIGERCON.2017.8281876

[6] Lee, Y., Bernstein, G., Li, D. and Martinelli, G. (2012) A Framework for the Control of Wavelength Switched Optical Networks (WSONs) with Impairments.

[7] Viswanathan, A., Rosen, E. and Callon, R. (2001) Multiprotocol Label Switching Architecture. RFC 3031.

[8] Surasak, T. and Huang, C.-H. (2019) Enhancing VoIP Security and Efficiency Using VPN. *ICNC* 2019, Vol. 1, 180-184. https://doi.org/10.1109/ICCNC.2019.8685553

[9] Kang, Y.-H. and Lee, J.-H. (2005) The Implementation of the Premium Services for MPLS IP VPNs. *The* 7*th International Conference on Advanced Communication Technology*, Phoenix Park, 1107-1110. https://doi.org/10.1109/ICACT.2005.246152

[10] Whitman, M. and Mattord, H. (2012) Principles of Information Security. Cengage Learning, Boston.

[11] Worster, T., Rekhter, Y. and Rosen, E. (2005) Encapsulating MPLS in IP or GRE.

[12] Zhang, J.Q., Wang, C. and Zhou, M.C. (2015) Fast and Epsilon-Optimal Discretized Pursuit Learning Automata. *IEEE Transactions on Cybernetics*, **45**, 2089-2099. https://doi.org/10.1109/TCYB.2014.2365463

[13] Adeel, A., Habib, M. and Talal, S. (2010) VoIP Performance Management and Optimization: Managing VoIP Networks. https://www.ciscopress.com/store/voip-performance-management-and-optimization-9780133433609

[14] Prayudi, Y. and Ashari, A. (2015) A Study on Secure Communication for Digital Forensics Environment. *International Journal of Scientific & Engineering Research*, **6**, 1036-1043. https://doi.org/10.14299/ijser.2015.01.010

[15] Alutaibi, K. and Trajković, L. (2012) Performance Analysis of VoIP Codecs over Wi-Fi and WiMAX Networks.

[16] Hung, T.C., Cuong, L.Q. and Mai, T.T. (2010) A Study on Any Transport over MPLS (AToM). *The* 12*th International Conference on Advanced Communication Technology* (*ICACT*), **1**, 64-70.

[17] Kaufman, C. (2005) RFC 4306 Internet Key Exchange (IKEv2) Protocol. Internet Engineering Task Force (IETF). https://doi.org/10.17487/rfc4306

[18] Lubobya, S.C., Dlodlo, M.E., de Jager, G., *et al.* (2018) Mesh IP Video Surveillance Systems Model Design and Performance Evaluation. *Wireless Personal Communications*, **100**, 227-240. https://doi.org/10.1007/s11277-017-5062-x

[19] Yu, J. and Al-Ajarmeh, I. (2007) Call Admission Control and Traffic Engineering of VoIP. *The Second International Conference on Digital Telecommunications* (*ICDT* 2007), San Jose, July 2007, 11-16. https://doi.org/10.1109/ICDT.2007.44

[20] Alvarez, A., Pozueco, L., Cabrero, S., Paneda, X.G., Garcia, R., Melendi, D. and Orueta, G.D. (2013) Subjective Evaluation of Critical Success Factors for a QoE Aware Adaptive System. *Computer Communications*, **36**, 1608-1620. https://doi.org/10.1016/j.comcom.2013.07.005

[21] Chen, Y., Farley, T. and Ye, N. (2004) QoS Requirements of Network Applications on the Internet. *Journal of Information Knowledge Systems Management*, **4**, 55-76.