# Impact of IPSec Protocol on the Performance of Network Real-Time Applications: A Review

Abdullah Abdulrahman Al-khatib and Rosilah Hassan
*(Corresponding author: Abdullah Abdulrahman Al-khatib)*
Research Center of Software Management and Technology (SOFTAM)
Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia
43600 UKM Bangi Selangor, Malaysia
(Email: khteb2003@gmail.com)
*(Received Feb. 2, 2017; revised and accepted July 13, 2017)*

## Abstract

Network real-time applications are gaining rapid prominence on today's Internet, particularly video and audio streaming, conferencing and telephony applications. The original design of those applications and their corresponding protocols did not consider security and privacy, which form a compelling requirement to many of the Internet users and in many of the involved applications. One of the most common solutions to impose security on network traffic is to use the IPSec security protocol, which adds authentication and encryption to network packets, by which securing network applications. In the context of time-sensitive application such as VoIP and similar real-time applications, an important question that arises is how, if any, the overhead of IPSec operations could affect the performance of network applications. This paper surveys a number of the most relevant works that addressed this question mostly within the last decade. The approach, metrics and findings of each study are briefly described and an overall summary of their main characteristics is presented.

*Keywords: IPsec; VOIP; VPN (Virtual Private Network)*

## 1 Introduction

The real time application is one type of applications make specific quality of service (Qos) demands to the communication network such as maximum delay, maximum loss rate, etc.; and the network once it accepts a connection guarantees the requested services quality. Traditional network protocols such as Ethernet are designed to deliver best effort performance. A best offer network strives to achieve good average performance, and makes no attempt to meet the individual deadline of task. These networks are intended for use in applications where long delays and high data loss under heavy load conditions are acceptable. It is needless to say that such network are insufficient for use in real-time applications. Also, the Current advances in communications technology have helped it possible to support applications in many different fields such as include the Internet, mobile/cell phones, land lines, instant messaging (IM), video conferencing, Internet relay chat, robotic telepresence and teleconferencing. Emails, blogs and bulletin boards are example of non-real-time applications, for which the performance metrics of interest are typically average message/packet delay and throughput. These applications also have strict reliability requirements; indeed, much of the complexity of traditional network protocols arises from the need for loss-free communication between non-real-time applications and data-oriented. Also, the properties of real-time applications are very different from those that are in the non-real-time. As in real-time computing, the distinguishing feature of real-time application is the fact that the value of the communication depends upon the times at which messages are successfully delivered to the recipient [16, 18, 38].

Furthermore, the real-time voice and video streams are isochronous in nature, that is, they can be through of as stream of finite size samples which are generated, transmitted and received at fixed time intervals, imposing a set of time constraints witch must never be exceeded [24, 31].

Many receivers located at geographically different places receive multimedia information from multimedia server. The multimedia information is usually in the form of streaming video and audio. Transmission and processing of these information have firm real-time requirements. Additionally, VoIP is all set to revolutionize voice communications. VoIP stands for Voice over IP, it Provide a generic transport capabilities for real-time multimedia applications and Supports both conversational and streaming applications such as Internet telephony, Internet radio, Videoconferencing, Music-on-demand and Video-on-demand [10].

VoIP applications are normally used with a simple microphone and computer speakers, but IP telephones can also be used, providing an experience identical to normal

telephoning. VoIP applications and services require firm real-time data transfer support [28].

## 2 IPSec

Most widely used and very important security technology is Internet Protocol Security (IPsec) [6]. It is used in the authentication and encryption in the public internet to provide the secure access. The IPsec is a set of protocols whose function is to secure communications over the Internet Protocol (IP) by authenticating and / or encrypting each IP packet in a data stream. IPsec also includes protocols for establishing encryption keys [11].

IPsec protocols act on the network layer, Layer 3 of the OSI model. Other extended Internet security protocols such as SSL, TLS and SSH operate from the application layer (Layer 7 of the OSI model). This makes IPsec more flexible because it can be used to protect Layer 4 protocols, including TCP and UDP [5, 15].

In addition, the feature of IPSec is its open standard nature. It complements perfectly with the PKI technology and, although it establishes certain common algorithms, for interoperability reasons, allows to integrate more robust algorithms cryptographic that can be designed in the future [14].

Among the benefits provided by IPSec, it should be noted that [12]:

- It enables new applications such as secure and transparent access to a remote IP node.
- It facilitates business-to-business e-commerce by providing a secure infrastructure on which to conduct transactions using any application. Extranets are an example.
- It allows building a secure corporate network over public networks, eliminating the management and cost of dedicated lines.
- It offers the teleworker the same level of confidentiality that would have in the local network of his company, being not necessary the limitation of access to the sensitive information by problems of privacy in transit.

It is important to note that when we cite the word "safe" we do not refer only to the confidentiality of the communication, we are also referring to the integrity of the data, which for many companies and business environments may be a much more critical requirement than Confidentiality. This integrity is provided by IPSec as a service added to data encryption or as an independent service. Within IPSec the following components are distinguished [35]:

- Two security protocols: IP Authentication Header (AH) and IP Encapsulating Security Payload (ESP) that provide security mechanisms to protect IP traffic.
- An Internet Key Exchange (IKE) key management protocol that allows two nodes to negotiate the keys and all the parameters necessary to establish an AH or ESP connection.

### 2.1 Authentication Header (AH)

The authentication header (AH) provides the data integrity and the authentication to check and replay the protection, but this authentication heard does not [29]. The AH protocol [21] is the procedure provided within IPSec to ensure the integrity and authentication of IP datagrams. That is, it provides a means to the receiver of the IP packets to authenticate the source of the data and to verify that said data has not been altered in transit. However it does not provide any guarantee of confidentiality, that is, the transmitted data can be viewed by third parties [22].

As its name indicates, AH is an authentication header that is inserted between the standard IP header (both IPv4 and IPv6) and the transported data, which can be a TCP, UDP or ICMP message, or even a complete IP datagram as shown in Figure 1.

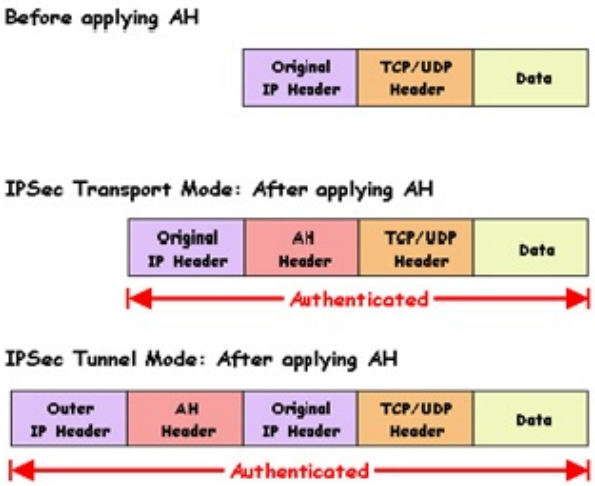


Figure 1: Structure of an AH datagram [27]

AH is actually a new IP protocol, and has assigned it the decimal number 51. This means that the IP header field contains the value 51, instead of the values 6 or 17 that are associated with TCP and UDP respectively. It is inside the AH header where the nature of the upper layer data is indicated. It is important to note that AH ensures the integrity and authenticity of the data transported and the IP header, except the variable fields: TOS, TTL, flags, offset and checksum as shown in Figure 1.

The function of AH is based on an HMAC algorithm [27], that is, a message authentication code. This algorithm consists of applying a hash function to the combination of an input data and a key, the output being a small string of characters that we call extract. This ex-

tract has the property that it is like a personal footprint associated with the data and the person who generated it, since it is the only one that knows the key.

### 2.2 Encapsulating Security Payload (ESP)

The main objective of the Encapsulating Security Payload (ESP) protocol [23] is to provide confidentiality by specifying how to encrypt the data that is to be sent and how this encrypted content is included in an IP datagram. In addition, it can offer data integrity and authentication services by incorporating a mechanism similar to AH.

Since ESP provides more functions than AH, the format of the header is more complex; This format consists of a header and a tail that surround the data transported. Such data can be any IP protocol (for example, TCP, UDP or ICMP, or even a complete IP packet). Figure 2 shows the structure of an ESP datagram, which shows how the content or payload travels encrypted [17].

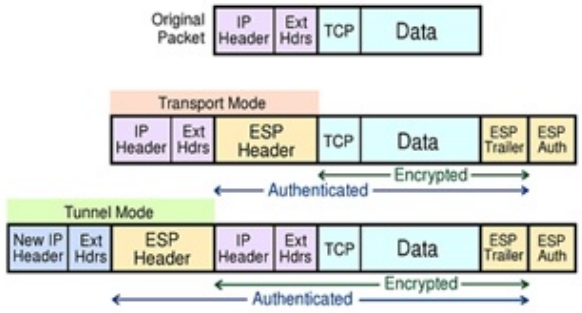


Figure 2: Structure of an ESP [17]

### 2.3 Internet Key Exchange (IKE)

IPsec uses Internet Key Exchange or IKE as the default protocol to control and convey the algorithms, keys, and protocols, and to validate the two parties. It is used to setup security associations [7]. An essential concept in IPSec is that of security association (SA): it is a unidirectional communication channel that connects two nodes, through which protected datagrams flow through previously agreed cryptographic mechanisms. By identifying only one unidirectional channel, an IPSec connection is composed of two SAs, one for each sense of communication. So far it has been assumed that both ends of a security association must be aware of the keys as well as the rest of the information they need to send and receive AH or ESP datagrams. As indicated above, it is necessary for both nodes to agree on both the cryptographic algorithms to be used and the control parameters. This operation can be done by means of a manual configuration, or by some control protocol that is in charge of the automatic negotiation of the necessary parameters; To this operation is called SAs negotiation [19].

The IETF has defined the IKE [20] protocol to perform both this automatic key management function and the establishment of the corresponding SAs. An important feature of IKE is that its utility is not limited to IPSec, but is a standard key management protocol that could be useful in other protocols, such as OSPF or RIPv2. IKE is a hybrid protocol that has resulted from the integration of two complementary protocols: ISAKMP and Oakley. ISAKMP generically defines the communication protocol and syntax of the messages that are used in IKE, while Oakley specifies the logic of how to securely perform the exchange of a key between two parts that are not previously known.

In this paper, we firstly reviewed the overview of IPsec and the main component of it. The other parts of this paper are organized as follows: Section 3 chronological survey of related works, we present some possible methods and techniques to ensure impact IPsec protocol on the performance of network RealTime Applications. Section 4 discussion attention of many researchers note from the works of several years; Section 5 is the conclusion of this paper.

## 3 Surveys of Relevant Works

Internet Protocol Security (IPsec) refers to a set of protocols used to secure communications over IP through the encryption and authentication of all data stream IP packets. It also includes protocols used to establish reciprocal authentication between agents at the start of a session and to facilitate the negotiation of cryptographic keys for use in the session. Several experiments have been conducted to measure IPsec performance and effects on Real-Time Applications.

### 3.1 VoIP Performance

Most of these studies the authors measure IPsec impact on the performance of VoIP with different experiences and network metrics, also the proportion of influence.

The experimental analysis reveals results relative to voice transmittal over secure communication links that employ IPsec [3]. This work reveals the important parameters that characterize real-time voice transmission over an Internet connection secured by IPsec and presents strategies to mitigate some VoIPsec (Voice over IPsec) limitations. The aim is to determine whether available VoIP applications can simply be replaced by VoIPsec. An efficient solution for packet header compression for VoIPsec traffic, which is called cIPsec, is also presented. Effective bandwidth was shown to decrease by up to 50 in terms of VoIP in case of VoIPsec. Meanwhile, voice traffic performance may be degraded by the cryptographic engine because access to this engine in order to prioritize traffic is difficult. Simulation results demonstrated a significant decrease in packet header overhead when the proposed compression scheme is used. This enhances

the transmission effective bandwidth to assess several parameters like effective bandwidth usage, crypto-engine throughput, the traffic delay affected by various QoS strategies, and impact of various encryption algorithms on packet delay, a number of tests have been conducted. When using IPsec, voice traffic is affected by two main factors. First, is the increased packet size attributed to the additional headers in the original IP packet. These headers include the ESP header for confidentiality and the new IP header for the tunnel. Second, is the time required to encrypt the payload and headers, as well as to construct new ones [4, 6, 9, 33].

The effects of encryption mechanisms on the quality of voice and speech in widely deployed wireless technologies, namely Bluetooth and 802.11 were experimentally compared [2]. The upper bound is assessed according to the number of simultaneous VoIP calls placed using a single cell of both networks with the application of security. E-Model is used to evaluate service quality. An E-Model-based QoS tool was found to evaluate the effect of the IPsec on VoIP traffic efficiently and objectively. A decrease in average MOS was noted with the increase in the number of simultaneous calls, but IPsec overhead significantly decreased compared with the case in which calls were placed without security [30].

IPsec-based VoIP performance (in terms of throughput, packet loss rate, latency and jitter) was assessed in a 3G-WLAN integration environment. The study was designed to provide guidelines for selecting the appropriate system parameter values for VoIP over WLAN. These works serve as a guide in the choice of system parameter setups that are suitable for VoIP service in a 3G-WLAN integration environment. An IEEE 802.11b access point was found capable of supporting 15 IPsec RTP streams with satisfactory latency, minimal jitter, and no packet loss. IPsec overhead is also reasonable [8, 39].

Experiments in a LAN environment were conducted to identify the influence of 6to4 encapsulation and IPsec on VoIP quality in future IPv6 networks. VoIP performance is assessed with varying background traffic, along with IPv6 and 6to4 encapsulation with and without NAT. Such performance is compared with that of IPv4. To make calls, soft phones are used, and background traffic is generated to simulate link and router congestion. Findings reveal the efficiency of the use of a single Linux box to handle IPsec, 6to4, and NAT processing. Voice quality was verified to remain satisfactory even when the network is operating close to its 100 Mbps capacity. VoIP performance is evaluated based on delta (packet inter-arrival time), packet loss, jitter, throughput, and MOS [13, 40]. The OPNET (Network Simulation Tool) was used to assess the negative effect of VoIP network security at different simulation times. Voice transmission over IPsec was found to increase end-to-end delay, delay variation (jitter), call setup time, and packet loss. Notably, authentication is less expensive than encryption. In the conclusion of their research on VOIPsec traffic, proposed an approach to the QOS issues linked to VOIPsec. This solution addresses the packet size increase associated with the use of IPsec. They use cIPsec, which is an IPsec version that performs internal header compression for a packet. This is done while the data in the internal headers of a packet remain constant or are duplicated in the outer header [34]. The analysis and experimental results are highlighted to facilitate the assessment of the voice traffic QOS. To study the effect of IPSEC VPN, a number of metrics are considered. Three scenarios, namely without firewall, with firewall, and with firewall and VPN, are compared. The results demonstrated that delay variation and packet end-to-end delay for voice traffic rises by using the IPSEC VPN. The key cause behind this is the additional encapsulation time required. MOS was not impacted by the IPSEC VPN. Whether IPsec encryption influences router CPU utilization, voice quality, and required bandwidth was determined. These parameters are functions of the number of calls placed. Integrated Services Cisco 2811 routers, which are suitable for small firms, were used to perform the tests. After IPsec deployment, a steep linear dependence of CPU utilization on the number of processed packets was observed. This could be addressed by adjusting the Voice Payload Size (VPS) to decrease the router packet load [26]. all the previous studies summarized the survey shown in Table 1.

### 3.2 Video Performance

Most of these studies the authors measure IPsec impact on the performance of Video with different experiences and network metrics, also the proportion of influence.

Voice and video communication performance in a LAN are measured. This includes such factors as the wireless hop, given that data transmissions alternately occur over the wireless hop, both through IPsec and plain IP. IPsec is found suitable for use to secure multimedia communications over a wireless link without a notable decrease in perceived quality. This experimental study primarily revealed that IPsec is suitable for using protect real-time communications interactive even when using a wireless link IPsec. When an infrastructure with sufficient bandwidth is used, the effect of IPsec cannot be perceived by users. The small differences in the network metrics become undetectable. The authors evaluated the measurements in terms of network parameters like delay, loss, and jitter and with respect to perceived quality. In this paper, it shows that the Internet security protocol (IPsec) can be used to provide secure multimedia communications over a wireless link without significantly degrading the perceived quality [25].

This work considered such metrics as End to End Packet Delay, Packet Delay Variation, Traffic Received, MOS (Mean Opinion Score), and Traffic Sent to assess the effect of encryption on IP network video transmission. To describe IPsec tunnels, AH header and ESP are used. These components provide confidentiality, safety, integrity, and non-repudiation, with HMAC-SHA1 and 3DES encryption used for confidentiality, and AES is em-

ployed in CBC mode. We also determine the effects of an OpenVPN on the transmitted video. The Experiment results identified video compression type as the most important component that influences video quality. The H264 codec achieves better encryption results, but worse packet loss results. In the latter part of measurement, a new network was created using IPsec tunnel. ESP and AH header are employed. Authentication was performed using a shared password (ISAKMP) and a hash function called SHA (HMAC variant). Symmetric ciphers AES and 3DES were used and their topologies are demonstrated to meet encryption standards [36].

An empirical investigation of the parameters influenced by IPsec implementation in IPv6 and 6to4 Tunnelled Migration Networks was conducted to assess the performance decay that ensues after incorporating security. IPsec significantly influenced the network, such that performance was degraded with security was incorporated. This performance decay impacted realtime applications, such as VoIP and video conferencing, which are highly sensitive to delay. The experiment employed various network scenarios: IPv6 with IPsec, IPv6 Only, and 6to4 Tunnelling (IPv6 to IPv4 Migration Technique) test-bed with two computers having the same specifications. One computer was used as the server, whereas the other was the client. Notably, no IPsec design exists for an IPv6-only network. The IPsec Tunnel was placed between Routers R2 and R1. We then verified the effect on the IPv6 to IPv4 migration network (6to4). Under these conditions, the server and PC-1 were running IPv6, while the network was IPv4. Moreover, a 6to4 Tunnel was designated as the IPsec Tunnel between R2 and R1 [37].

The authors studied the performance the real time multimedia with IPSec tunnel implemented with different operation system Windows 2000 and Novell Netware. The results from two platforms were not different between the encryption and unencrypting in this experimented. The implement of encryption tools (hardware and software) are affected in network performance with use different platform like Windows 2000 and Novell Netware, etc. and they focused on client-to-site VPN topology [1]. The authors analysis QoS in videoconference by using the IPsec with different type of encryption like AES are affected fundamentally in latency when is sent through a VPN because encryption and the traffic load. Also the packet lost for voice 1 and video 2 [32]. all the previous studies summarized the survey shown in Table 1.

# 4 Discussion

It is apparent from the related works that the impact of security (IPSec in particular) on the performance of real-time applications has attracted the attention of quite few researchers. We can make a few observations from the surveyed works. First, while the works vary on their results, it seems that more experimental works confirm the efficiency of IPSec. In particular, the perceptual quality of VoIP communication can be maintained with IPSec though at the expense of some bandwidth increase and end-to-end delay, which are deemed less than serious by some researchers. Second, a smaller part of the studies use simulations to estimate the effect of IPSec. This approach might be less reliable than a true test-bed based experimental approach, and it is noted that these works tend to highlight larger impact of IPSec on the network. Among those few works, the OPNET simulator is frequently the simulator of choice. Finally, we note that most of the previous studies are focused on the voice communications through the VoIP application, and did not give much attention to video. This might suggest a potential gap that can be filled by further research on various video conferencing as well as video streaming applications under the function of IPSec protocol.

# 5 Conclusions

This paper surveyed the most relevant works on the overhead caused by security on network performance. In particular, the survey focused on the works that studied the performance of real-time applications when IPSec protocol is employed. Both securing the transmission and ensuring minimum QoS measures are important in current networks, and the study of their interaction is imperative. Quite a few research works experimented with various scenarios of voice as well as video communications with IPSec, either in real test-beds or through OPNET-based simulations. Their work and findings have been summarized and a few observations have been made.

# Acknowledgments

The authors would like to acknowledge the assistance provided by the Network and Communication Technology Research Group, FTSM, and UKM in providing facilities throughout the research. This project is partially supported under the ETP-2014-008.

# References

[1] S. Al-Khayatt, *et al.*, "Performance of multimedia applications with IPSec tunneling," in *Proceedings of International Conference on Information Technology: Coding and Computing*, 2002.

[2] A. A. Al-khatib and W. A. Hammood, "Mobile malware and defending systems: Comparison study," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 116–123, 2017.

[3] A. A. Al-khatib, and R. Hassan, "Performance evaluation of AODV, DSDV, and DSR routing protocols in MANET using NS-2 simulator," in *International Conference of Reliable Information and Communication Technology*, pp. 276-284, 2017.

Table 1: Summary of the surveyed works on the overhead of IPSec on network real-time applications

| Authors | Year | Description | Findings | IP Protocol | Real-time Application | Measurement | Parameter | Type of study |
|---|---|---|---|---|---|---|---|---|
| *Barbieri* et al. | 2002 | Analysis reveals results relative to voicetransmittal over secure communication links that employ IPsec. | Results show decrease by up to 50 in terms of VoIP in case of VoIPsec. | IPv4 | VoIP | Effective bandwidth usage | Packet delay, Crypto engine throughput | Experimental testbed |
| *Klaue* et al. | 2005 | Video and Voice communication performance in LAN are measured. | The result IPsec is suitable for using protect real-time communications interactive even when using a wireless link. | IPv4 | VoIP, Video conferencing | Perceived quality | Loss, Delay, Jitter | Experimental testbed |
| *Nascimento* et al. | 2006 | The effects of encryption mechanisms on the quality of voice and speech in widely deployed wireless technologies, namely 802.11 and Bluetooth, were experimentally compared. | Found to evaluate the effect of the IPsec on VoIP traffic efficiently and objectively. | IPv4 | VoIP | Voice speech quality | Packet delay, Number of simultaneous VoIP calls, MOS (Mean Opinion Score) | Experimental testbed |
| *Sung and Lin* | 2008 | IPsec-based VoIP performance (in terms of packet loss rate, jitter, throughput and latency) was assessed in a 3G-WLAN integration environment. | The system parameter setups that are suitable for VoIP service in a 3G-WLAN integration environment. | IPv4 | VoIP | VoIP quality | Throughput, Packet loss, Latency Jitter | Experimental testbed |
| *Yasinovskyy* et al. | 2009 | Identify the influence of 6to4 encapsulation and IPsec on VoIP quality in future IPv6 networks. | Reveal the efficiency of the use of a single Linux box to handle IPsec, 6to4, and NAT processing. | IPv4, IPv6 | VoIP | VoIP quality | Throughput, MOS, Packet interarrival time, Jitter, Packet loss | Experimental testbed |
| *Salama* et al. | 2009 | The OPNET (Network Simulation Tool) was used to assess the negative effect of VoIP network security at different simulation times. | Increase delay variation (jitter), end-to-end delay, call setup time, and packet loss. Notably, authentication is less expensive than encryption. | IPv4 | VoIP | VoIP quality | End to end delay, Jitter, Packet loss, Call setup time | Simulation (OPNET) |

Table 2: Summary of the surveyed works on the overhead of IPSec on network real-time applications (Cont.)

| **Authors** | **Year** | **Description** | **Findings** | **IP Protocol** | **Real-time Application** | **Measurement** | **Parameter** | **Type of study** |
|---|---|---|---|---|---|---|---|---|
| *Babu* | 2012 | Study effect of IPSEC VPN, a number of metrics are considered. Three scenarios, namely without firewall, with firewall, and with firewall and VPN, are compared. | Delay variation and packet end-toend delay for voice traffic rises by using the IPSEC VPN. | IPv4 | VoIP | Voice quality | * Jitter * MOS * End to end packet delay * Traffic sent * Traffic received | Simulation (OPNET) |
| *Sevcik* et al. | 2014 | Study the metrics End to End Packet Delay, Packet Delay Variation, Traffic Received, MOS (Mean Opinion Score), and Traffic Sent to assess the effect of encryption on IP network video transmission. | Identified video compression type as the most important component that influences video quality. | IPv4 | Video transmission | Video quality | * Packet loss | Experimental testbed |
| *Mazalek* et al. | 2015 | IPsec encryption influences router CPU utilization, voice quality, and required bandwidth was determined. | Decrease the routers packet load. | IPv4 | VoIP | Voice quality | * CPU utilization * Bandwidth MOS | Experimental testbed |
| *Shah and Parvez* | 2015 | IPsec significantly influenced the network, such that performance was degraded with security was incorporated. | Performance decay impacted realtime applications, such as VoIP and video conferencing, which are highly sensitive to delay. | * IPv4 * IPv6 | * VoIP * Video conferencing | * VoIP * Video quality | * Throughput * IP end-to-end * Jitter * Delay * Packets drop rate Tunnel delay | Simulation based (OPNET) |

[4] M. Babu, "Performance analysis of IPSec VPN over VoIP networks using OPNET," *International Journal of Advanced Research in Computer Science and Software Engineering*, 2012. DOI: 10.5815/ijcnis.2015.12.01.

[5] M. Balfaqih, *et al.*, "Fast handover solution for network-based distributed mobility management in intelligent transportation systems," *Telecommunication Systems*, vol. 64, no. 2, pp. 325-346, 2017.

[6] R. Barbieri, D. Bruschi, and E. Rosti, "Voice over IPsec: Analysis and solutions," in *Computer Security Applications Conference*, 2002.

[7] B. K. Chawla, O. P. Gupta, and B. K. Sawhney, "A Review on IPsec and SSL VPN," *International Journal of Sientific & Engineering Research*, vol. 5, no. 11, 2014.

[8] W. E. Chen, "A call server integrated approach for QoS provisioning of SIP multimedia services in 802.11 wireless networks," in *Vehicular Technology Conference*, 2010.

[9] A. D. Elbayoumy, and S. J. Shepherd, "QoS control using an end-point CPU capability detector in a secure VoIP system," in *10th IEEE Symposium on Computers and Communications*, 2005.

[10] A. Elnashar, M. A. El-Saidny, and M. R. Sherif, *Design, Deployment and Performance of 4G-LTE Networks: A Practical Approach*, John Wiley and Sons, 2014.

[11] S. Frankel and S. Krishnan, *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*, RFC 6071, 2011.

[12] S. E. Frankel, *et al.*, "Guide to IPsec VPNs: Recommendations of the national institute of standards and technology," *NIST Special Publication*, Special Publication (NIST SP)-800-77, 2005.

[13] A. J. Ghazali, *et al.*, "Building IPv6 based tunneling mechanisms for VoIP security," in *13th International Multi-Conference on Systems, Signals and Devices (SSD'16)*, 2016.

[14] A. P. Hansen, *Public Key Infrastructure (PKI) Interoperability: A Security Services Approach to Support Transfer to Trust*, Dissertations Monterey, California: Naval Postgraduate School, 1999.

[15] R. Hassan, A. A. Al-Khatib, and W. M. H. W. Hussain, "A framework of Universiti Kebangsaan Malaysia patent: UKM patent," in *19th International Conference on Advanced Communication Technology (ICACT'17)*, 2017.

[16] X. Hei, and D. H. K. Tsang, "The Earliest Deadline First scheduling with active buffer management for real-time traffic in the Internet," in *International Conference on Networking*, pp. 45-54, 2001.

[17] P. Jokela, J. Melen, and R. Moskowitz, *Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)*, RFC 7402, 2015.

[18] N. S. Kambo, D. Z. Deniz, and T. Iqbal, "Measurement based MMPP modeling of voice traffic in computer networks using moments of packet interarrival times," in *International Conference on Networking*, pp. 570-578, 2001.

[19] C. Kaufman, *et al. Internet Key Exchange Protocol Version 2 (IKEv2)*, RFC 7296, 2014.

[20] C. Kaufman, *Internet Key Exchange (IKEv2) Protocol*, RFC 4306, 2005.

[21] S. Kent, *IP Authentication Header*, RFC 2402, 2005.

[22] S. Kent, R. Atkinson, *IP Authentication Header*, RFC 2402, 1998.

[23] S. Kent, *IP Encapsulating Security Payload (ESP05)*, RFC 4303, 2005.

[24] H. J. Kim, and S. G. Choi, "A study on a QoS/QoE correlation model for QoE evaluation on IPTV service," in *The 12th International Conference on Advanced Communication Technology (ICACT'10)*, vol. 2, 2010.

[25] J. Klaue, and A. Hess, "On the impact of ipsec on interactive communications," in *Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium*, 2005.

[26] A. Mazalek, Z. Vranova, and E. Stankova, "Analysis of the impact of IPSec on performance characteristics of VoIP networks and voice quality," in *International Conference on Military Technologies (ICMT'15)*, 2015.

[27] C. Madson and R. Glenn, *The Use of HMAC-MD5-96 within ESP and AH*, RFC 1321, 1998.

[28] R. Moraes, P. Portugal, F. Vasques, *et al.*, "Limitations of the IEEE 802.11 e EDCA protocol when supporting real-time communication," in *IEEE International Workshop on Factory Communication Systems (WFCS'08)*, 2008.

[29] M. Nakhjiri, and M. Nakhjiri, "Internet security and key exchange basics," *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility*, 2006.

[30] A. Nascimento, *et al.*, "Can I add a secure VoIP call?" in *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, 2006.

[31] K. Pulli, *et al.*, "Real-time computer vision with OpenCV," *Communications of the ACM*, vol. 55, no. 6, pp. 61-69, 2012.

[32] J. A. Perez, V. Zarate, A. Montes, "Quality of Service Analysis of site to site for IPSec VPNs for realtime multimedia traffic," in *Advanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services (AICT-ICIW'06)*, 2006.

[33] P. Radman, *et al.*, "VoIP: Making secure calls and maintaining high call quality," in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, 2010.

[34] G. I. Salama, *et al.*, "Performance analysis of transmitting voice over communication links implementing IPsec," in *Paper in 13th International Conference on Aerospace Sciences and Aviation Technology (ASAT'09)*, Military Technical College, Cairo, Egypt, 2009.

[35] K. Seo, and S. Kent, *Security Architecture for the Internet Protocol*, RFC 2401, 2005.
[36] L. Sevcik, *et al.*, "The impact of encryption on video transmission in IP network," in *Telecommunications Forum Telfor (TELFOR'14)*, 2014.
[37] J. L. Shah, and J. Parvez, "Impact of IPsec on real time applications in IPv6 and 6to4 tunneled migration network," in *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS'15)*, 2015.
[38] M. Shiwen, *et al.*, "MRTP: A multiflow real-time transport protocol for ad hoc networks," *IEEE Transactions on Multimedia*, vol. 8, no. 2, Apr. 2006.
[39] Y. C. Sung, and Y. B. Lin, "IPsec-based VoIP performance in WLAN environments," *IEEE Internet Computing*, vol. 12, no. 6, 2008.
[40] R. Yasinovskyy, A. L. Wijesinha, and R. Karne, "Impact of IPsec and 6to4 on VoIP quality over IPv6," in *10th International Conference on Telecommunications*, 2009.

# Biography

**Abdullah Abdulrahman Al-khatib** graduated from Al-Ahgaff College Hathramout-Yemen in year 2009. He is work in community college from 2009. He enrolled to study master in University Kebangsaan Malaysia (UKM) in computer science (Network Technology) in 2015. His research interest in (SDN) and IP Security (IPSec).

**Rosilah Hassan** works as an Engineer with Samsung Electronic Malaysia, Seremban before joining Universiti Kebangsaan Malaysia (UKM) in 1997. She obtains her Master of Electrical Engineering (M.E.E) in computer and communication from UKM in 1999. In late 2003, she went to Glassgow, Scotland for her PhD in Mobile Communication from University of Strathclyde. Her research interest is in mobile communication, networking, 3G and QoS. She is a senior lecturer at UKM for more than 10 years. She had received many award such as Top Ten Student for the Faculty of Engineering on the graduation day(certificated) in 1993. After that, on 1994-1996, she received JPA scholarship for undergrade study for Look East Policy Programmer.