2016 13th International Multi-Conference on Systems, Signals & Devices

Building IPv6 Based Tunneling Mechanisms for VoIP Security

Amzari J. Ghazali, Waleed Al-Nuaimy, Ali Al-Ataby, Majid A. Al-Taee
Department of Electrical Engineering and Electronics
University of Liverpool, UK
e-mail: {amzari.ghazali, wax, ali.ataby, altaeem}@liv.ac.uk

***Abstract*—Internet protocol version 6 (IPv6) was developed to resolve the IPv4 address exhaustion problem and support new features. However, IPv6 still comprises some defectiveness of IPv4 protocol such as multimedia security. This paper presents IPv6-based tunneling mechanisms for securing Voice over Internet Protocol (VoIP) network traffic using OpenSwan IPSec (site-to-site). IPSec with Triple Data Encryption Algorithm (3DES) is used to create a Virtual Private Network (VPN) on top of existing physical networks. Secure communication mechanisms can therefore be provided for data and control information transmitted between networks. Secure VoIP-oriented mechanisms on VPN IPv6 have been designed, implemented and tested successfully using open source approaches. The performance of the IPv6 VoIP network is assessed experimentally in terms of several performance metrics including jitter, throughput and packet loss rate. The obtained results revealed that the proposed IPv6-based tunneling mechanisms for VoIP have negligible impact on network performance when compared to the previously reported work in literature, with a slight increase in the price of CPU and memory resources.**

Keywords—IPv6 tunneling; IPSec; OpenSwan; Security; VoIP; VPN; OpenSwan.

I. INTRODUCTION

Rapid growth in the development of network-based computer system and the Internet has contributed to the depletion of IPv4 address space. Internet Engineering Task Force (IETF) has developed IPv6 as an upgrade of IPv4 as a plan to satisfy the perpetual increase in the Internet Protocol (IP) address needs [1]. IPv6 uses a 128-bit address which is allowed for 3.4×1038 addresses, enough for high usage for everyone in the world [2]. There are many advantages of the migration from IPv4 to IPv6, such as large address space, the capability of including media access control (MAC) addresses into IP addresses, enhanced security, mobility, streamlined encapsulation, transition capabilities, increase in network management and routing efficiency [3]. Considering the fact that there are many orginizations still using IPv4, deploying both IPv4 and IPv6 at the same time using the tunneling method is the best solution to overcome the migration process. IETF has created several tunneling methods such as Toredo, 6to4 and manual configuration [4]. Despite the benefits of using IPv6, there are still challenges and obstacles in implementing and practically using IPv6 VoIP [5]. The issues of the transition from the current IPv4 network to IPv6 as well as VoIP performance for both IP versions need to be assessed and compared.

Evaluation of VoIP performance with IPSec in IPv4, IPv6 and 6to4 networks using Teredo for NAT traversal in a test LAN was previously reported in [6]. The testbed used softphones to setup calls, and background traffic was generated to create congestion on the links and routers. The results demonstrated the feasibility of using a single Linux box to handle IPSec, 6to4 and NAT processing, and it was found that voice quality is acceptable as long as the traffic does not exceed network capacity.The study also showed that VoIP performance with IPSec is not adversely affected by the overhead due to 6to4 or Teredo. In [7], experiments in a LAN environment were carried out to determine the impact of IPSec and 6to4 mechanism on VoIP quality. The repored results showed that VoIP quality due to using IPSec with 6to4 mechanism and NAT in VPNs is negligible for both IP versions.

Evaluation of the transition mechanisms namely 6to4 tunneling in terms of data transmission was reported in [8]. A user-to-user network performance software was used to obtain the throughput, round trip time and tunneling overhead for transmission control protocol (TCP) and user datagram protocol (UDP). The performance of TCP and UDP through 6to4 and tunnelling was then compared over the native IPv4 and IPv6 environments. The findings proved the ease of TCP and UDP data transmission via the tunnel compared to both native networks. In [9] and [10], IPv4 security was implemented using various encryption algorithms [11] - [13], including utilization of open source software [14]. In this study, the overhead of an IPSec concerning IKE/ISAKMP key exchange showed that it was much larger than the ESP overhead. In [15], IPv6 IPSec VPN in Linux with OpenSwan was built and analyzed within the whole frame and modules of OpenSwan, then the Linux kernel recompiled to make it support IPv6, and

This work was supported by the Council of Trust for the People (Majlis Amanah Rakyat, MARA) agency under the Ministry of Rural and Regional Development in Malaysia.

978-1-5090-1291-6/16/$31.00 ©2016 IEEE

NETKEY module also been added. In the end, OpenSwan has been installed and configured with net-to-net mode.

Performance of 6to4 tunnelling without IPSec for TCP/UDP traffic was evaluated in [16] and [17], and it is found that the additional overhead due to tunneling was minimal but delayed reading was significantly different depending on the choice of transition mechanism and operating system used. An evaluation of IPSec with 6to4 mechanism is reported in [1]. The impact of this mechanism on end-to-end user application performance was studied using metrics such as throughput, latency, host CPU utilization, TCP connection time and number of TCP connections per second that a client can establish with a remote server. However, the study does not address VoIP performance. The experiments reported in [18] showed that the implementation of an IPSec VPN had a higher impact on smaller packets as compared to larger packets for both IPv4 and IPv6. The tests also showed that IPSec protocol has security advantages with minimal performance costs. In [19], the study compared VoIP performance on IPv4 and IPv6 LANs with the presence of background UDP network traffic, using open-source software. Results showed that the maximum jitter for IPv6 is slightly higher than that of IPv4, during high levels of background traffic while throughput for IPv6 is slightly faster than for IPv4.

This paper proposes an IPv6-based tunneling mechanisms for securing VoIP with 3DES encryption algorithm using open source approaches, and the focus will be on measuring the jitter, network throughput and packet loss with the variable packet size of background UDP traffic. VoIP performance over IPv4 and IPv6 will then be compared to assess the differences in terms of the requires system resources and impact of the larger IPv6 packet's header and packet payload. Unlike previous studies, this study focuses on open source configuration by building real traffic testbed network, and measuring the VoIP performance with the implementation of the IPSec encrypted using OpenSwan IPSec with 3DES encryption. The VoIP performance and the impact of tunneling mechanism with and without the implementation of IPSec security are investigated using both IPv4 and IPv6.

The remainder of this paper is organized as follows. Section II overviews various VoIP security aspects including potential threats and encryption algorithms. Section III describes the test network used in this study. In Section IV, configurations of IPv6 tunneling mechanisms are reported. Section V presents and discusses the obtained results. Finally, the work is concluded in Section VI.

II. VoIP Security

In VoIP networks, security has been a major concern and challenge, hence as VoIP deployments become more popular and widespread, it becomes a more attractive target for aggressive activities. Security issues related to VoIP need to be addressed, such as authentication, integrity and privacy. The authentication process ensures that each participant in the conversation which indeed the persons claim to be, the integrity process will check and validate whether the data and contents in the conversation has been compromised while transported between sender and receiver. Privacy is ensured by using encryption and decryption method in order to protect the data from interception and alteration.

A. VoIP Security Threats

The most common security threats and vulnerabilities against VoIP deployments, services, applications and end-users are outlined briefly as follows:

1) Social threats: It consists of misrepresentations of identity, authority, right and contents, mostly aimed directly against humans. This attack may lead to actions such as phishing, theft of service, unwanted contact or spam.

2) Eavesdropping, interception, and modification threats: An eavesdropping attack is defined as a method where an adversary can unlawfully and without authorization, capture the entire signalling and/or data stream between VoIP end users and participants. The attacker can then read and modify data sent on the VoIP networks unless incrypted.

3) Denial of services threats: Considered as interruption of a service which included Denial of Services (DoS) and physical intrusion. The potential of this attack is to deny users access to VoIP services, exploiting flaws in a call setup or in the implementation of services. The attack may also involve direct attack with physical and infrastructure components, for example Domain Name Server (DNS) and the Session Initiate Protocol (SIP) server.

4) Services abuse threats: This threat could be from a customer or employee of an ISP or a third party that improperly uses VoIP services. For example, traffic is artificially increased for the purpose of maximizing charges for billing or the other way around which is to reduce the billing charges. Others service abuse includes various forms of identity and account theft where the credentials of the rightful owner have been exploited and misused.

5) Physical access threats: Inappropriate and unauthorized physical access to VoIP devices or equipment are considered as a physical access threat, the attacker may tamper and gain access to any physical layer of the network.

6) Interruption of services threats: Problems which refer to non-intentional problems that can possibly contribute to inaccessibility of VoIP services for example, are loss of power due to weather and caused by nature, resource limitation caused by over-subscription and degraded call quality related to performance issues.

B. VoIP Encryption Algorithms

In VoIP encryption, several algorithms have been proposed and implemented to provide privacy, integrity and security during data communication and voice conversations. Block cipher encryption, such as DES, 3DES, AES and Blowfish among the common symmetric key encryption algorithms used to secure VoIP communication and services. In the present work, the 3DES encryption is adopted in the test network under investigation. The 3DES encryption algorithm was previously developed in 1998 as a replacement for DES; it used three round messages, which provides a stronger encryption by using 2^{168} possible combinations. By using 48 rounds in its computation and a key length of 168 bits, more security was obtained when compared with a previously reported DES encryption algorithm [20].

Fig. 1 shows a functional diagram for an improved algorithm based on 3DES encryption design in which the 3DES uses 3-times iteration of the DES encryption, hence increasing the encryption level with the penalty of increasing the average processing time. The 3DES and AES encryption algorithms are used in [20], [21] to evaluate the voice quality in wireless LAN. Similarly, 3DES algorithm was implemented in this work in IPSec experiment using LAN environment, benefiting from previous findings reported by the authors in [22]. In this study, a particular focus is given to the IPv6-based tunneling mechanisms.

III. TEST NETWORK AND EXPERIMENTAL SETUP

The test network has been designed and implemented as shown in Fig. 2, by using internet connection provided by Internet service provider (ISP). Several PCs are installed and configured with open source software. Internet connection was routed to our test network by using main Router #3 as provided by the ISP. Two different LANs were routed using Ubuntu Linux Router #1 and Router #2, with 100mbps Ethernet switches connected. An open source VoIP application; Ekiga softphone was installed on both clients and voice calls are made and established between each LAN.

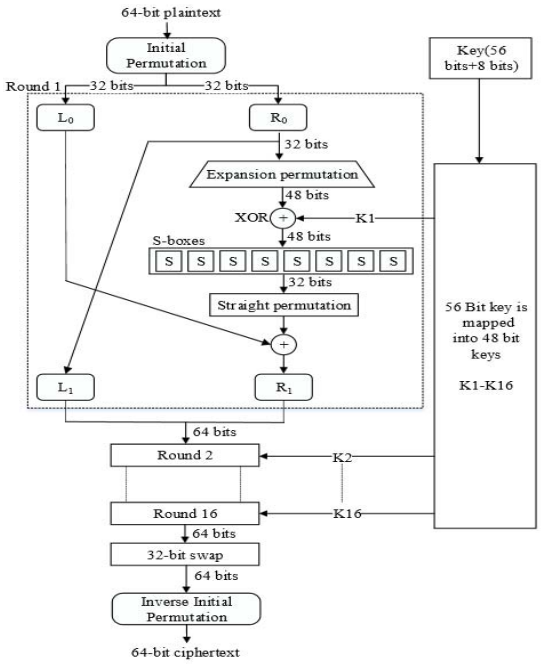

Fig. 1. Three DES encryption design [11]

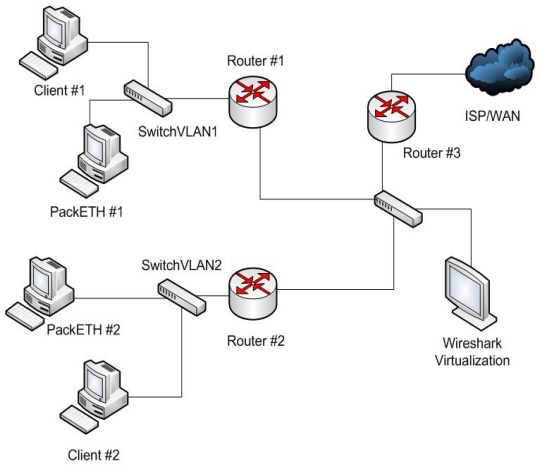

Fig. 2. Test network

Ekiga [23] is one of the well-known open sources, that establishes VoIP on Linux machines. It supports IPv6 and performs well under different operating systems. Router#1 and Router#2 use Ubuntu Linux 12.06 as the main operating system, while Router#3 represents the service provider end. The graphical user interface (GUI) of Router#1 and Router#2 packets activity can be accessed through Wireshark virtualization terminal, it can also be used as verification and validation for IPSec encryption. Wireshark Analyzer [24] are used to capture network traffic data and perform offline packet analysis.

The packet generator software is used to provide a sequence of packets on the Ethernet link to represent network background traffic. As a voice call is established between Client #1 and Client #2, VoIP traffic is competed with background UDP traffic sent by a pair of PackETH [25] traffic generator within each LAN. The GUI of PackETH 1.8.1 that supports adjusting UDP background traffic is used to assess the impact of background-traffic speed on the packet-loss ratio on VoIP network.

Numerous tools are available to measure the network traffic performance either by active or passive techniques. For example, Jperf [26] is one of active techniques that provide various parameters related to timing, buffers and protocols was used as the main measurement tool to perform in this test bed. It was the front-end of Iperf [27] which was written in the Java programming language. In this test bed, Jperf was also installed and set up on client #1 and client #2. During the call set up made between these two nodes (Clients #1 and 2#), Jperf was operated based on the UDP packet size sent from each client to produce network throughput and jitter values. In thist test, variable packet size that ranges from 128 to 1408 Kbytes were used, as suggested in [28]. The variety in packet size is needed to measure the impact of packet size variation during data transmission in order to maintain end-to-end network performance [29].

IV. IPv6 TUNNELING MECHANISMS

In this section three different configurations are considered; IPv6 tunneling, Dynamic host configuration protocol (DHCP) with a router advertisement daemon (radvd) and Internet Protocol Security Virtual Private Network (IPSec VPN).

A. IPv6 tunneling configuration

This configuration will allow connection from our IPv6 local area network (LAN) using native IPv4 gateway provided by Internet service provider (ISP). Table I shows a detailed configuration for the Router#3 to support IPv6 tunneling over ISP native IPv4.

B. DHCP with Radvd Configuration

All clients in the experiment were provided with automatic IP addresses by using DHCP server and radvd is used to implement a link-local advertisements as IPv6 routing prefixes to all clients. Details of the DHCP server and radvd configurations are shown in Table II.

C. IPSec with 3DES VPN Configuration

The platform under study involves an Ubuntu Linux operating system and IPSec implementation using OpenSwan [11] with 3DES encryption algorithm. The VoIP client routers are installed and configured with the commands shown in Table III.

TABLE I. TUNNELING IPV6 OVER IPV4 ISP ROUTER

Command	Function
nano /etc/network/interface auto he-ipv6 iface he-ipv6 inet6 v4tunnel endpoint 216.66.80.26 address fec0::244 netmask 64 up ip -6 route add default dev he-ipv6 down ip -6 route del default dev he-ipv6	IP configuration to allow IPv6 tunnel connection via IPv4 for Router#3.
nano /etc/sysctl.conf net.ipv6.conf.all.forwarding=1	Allows all IPv6 traffic through Router#3 to/from LAN clients.

TABLE II. DHCP AND RADVD COMMANDS

Command	Function
sudo apt-get install isc-dhcp-server	Install IPv6 DHCP server

nano /etc/dhcp/dhcpd6.conf
option domain-name "dhcpv6.com";
option domain-name-servers ns.dhcpv6.com;
default-lease-time 600;
max-lease-time 7200;
log-facility local7;
subnet6 fec0::/64 {
range6 fec0::100 fec0::110;}
host specialclient {
host-identifier option dhcp6.client-id 1f:ba:e3:60:b9:1f:01:23:45;
fixed-address6 fec0::1
	IPv6 address Pool and fix IP for Router #1 and Router #2

Nano /etc/radvd.conf
interface eth0 {
AdvSendAdvert on;
MinRtrAdvInterval 3;
MaxRtrAdvInterval 10;
prefix fec0::/64 {
AdvOnLink on;
AdvAutonomous on;
AdvRouterAddr on;
};
};
	Configuration of daemon to send advertisements through specified interfaces and auto-configures addresses with received prefix using the default route.

TABLE III. CONFIGURATION COMMANDS OF VOIP ROUTERS

Command	Function
apt-get install openswan xl2tpd ppp	Install OpenSwan IPSec on both VoIP client side
nano /etc/ipsec.conf auto=start keyingtries="0" connaddrfamily="ipv6" leftid="router1" left="fec0::1" 3des-cbc leftrsasigkey="0sAJKX....hIm"	Router#1 (VoIP Client 1) configuration files of settings, option defaults and connection.
nano /etc/ipsec.conf auto=start keyingtries="0" connaddrfamily="ipv6" rightid="router2" right=" fec0::2 3des-cbc rightrsasigkey="0sAJKX....hIm"	Router#2 (VoIP Client2) configuration files of settings, option defaults and connection.
/etc/init.d/ipsec start	Start OpenSwan in Router#1 and Router#2

V. Results and Discussion

Four different types of network traffic have been tested, which are IPv4 VoIP open system, IPv4 VoIP with IPSec, IPv6 VoIP open system and IPv6 with IPSec. By using 100mbps available bandwidth, a variety of packet size has been transmitted. Network throughput, mean jitter and packet loss were recorded with the influence of variable UDP background traffic size generated by PackETH, packet traffic generator starting from 0mbps, 50mbps, 100mbps, 150mbps and 200mbps traffic overload. By using Jperf, UDP data transmission from client #1 to client #2 during VoIP call setup, variable packet size was generated to perform and create overloaded links and enabled us to compare VoIP performance for IPv4 and IPv6 under heavy traffic and extreme conditions.

Fig. 3 shows the mean jitter recorded by Jperf when we tested with different sizes of UDP packets sent from end to end (Client #1 to client #2). It shows that VoIP, for both IPv4 and IPv6 was affected by the implementation of IPSec security, where the security payload imposed on IP packet increased the jitter. However the effect was still acceptable for VoIP services on IPv4 and IPv6 networks.

In Fig. 4, experimental results show that, IPv6 with IPSec on a smaller packet size, which was 384 bytes had the lowest network throughput, but it increased slightly faster when a larger packet size was transmitted. The IPv4 VoIP open system had a higher throughput almost for all packet sizes transmitted compared to other different types of network traffic tested in this experiment.

Fig. 5 shows the packet loss ratio when the generated UDP background traffic was varied in the range of 0 to 200 Mbps. Starting from 100mbps background traffic, packet loss started for all VoIP traffic except IPv4 VoIP open system. The highest packet loss occurred, which was 200mbps UDP background traffic on IPv6 with IPsec. Packet loss ratio with IPv6 as higher than IPv4 network traffic when dealing with bigger UDP background traffic, thus, IPv6 networks may need to be improved in the future to support better network quality of services.

There will be a trade-off that need to be considered in order to achieve a balance between service quality and secure communications. However, for multimedia streaming and VoIP in lossy networks, QoS mainly depends on the encryption type and network status [30], [31]. The results indicate that VPN using 3DES encryption algorithms contribute to the performance degradation on both IPv4 and IPv6 which related to the size of data that been transmitted during network communication. The security packet payload cause by IPSec will imposed to the increment on the size of the original IP header, hence time required to encrypt and decrypt the payload and the header (execution time) also will affecting to the jitter and network throughput.

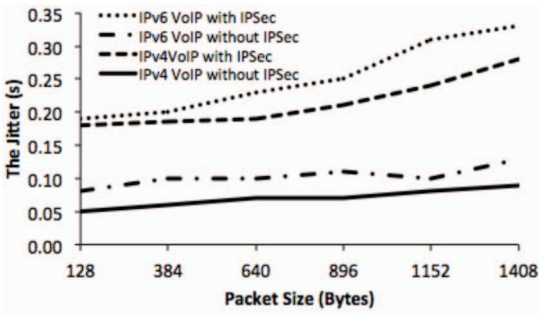

Fig. 3. Jitter comparison between IPv6 VoIP and IPv4 VoIP, with and without IPSec.

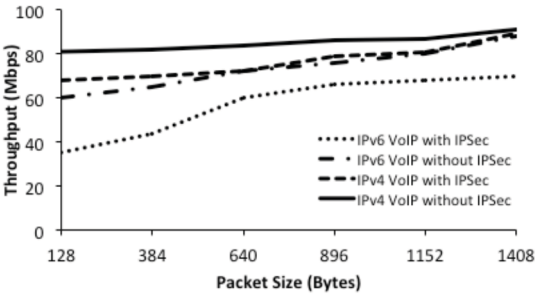

Fig. 4. Throughput comparison between IPv6 VoIP and IPv4 VoIP, with and without IPSec.

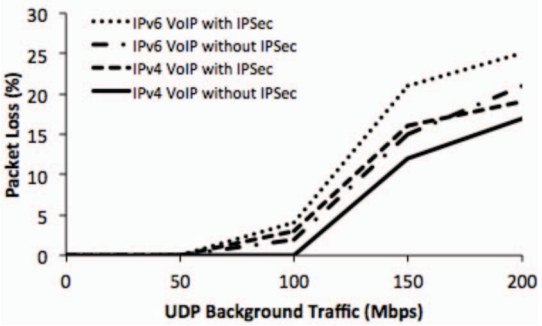

Fig. 5. Packet loss ratio comparison between IPv6 VoIP and IPv4 VoIP, with and without IPSec.

Network application and background traffic also will cause to increments of packet loss ratio, increasing UDP background traffic up to 200Mbps exceeded the maximum bandwidth and the network physical limitation in this case (100Mbps). By increasing the bandwidth and network physical, it can eliminate the packet loss ratio and improves QoS.

VI. Conclusions

In this paper, we presented an IPv6 tunneling mechanism for VoIP security, using 3DES encryption algorithm. Impact of implementing these

mechanism on the network performance has been compared to that of previously reported network based on IPv4. Variations of UDP packet size and background traffic with and without IPSec were considered in this study. Ekiga softphone running on the Ubuntu operating system was used for VoIP services on both clients and several parameters such as network throughput, jitter and packet loss ratio have been measured. Results showed that IPv6 with IPSec using 3DES encryption has a slightly higher jitter, lower throughput and higher packet loss ratio as compared to the other IPv4 and IPv6 traffic tested on the test bed. Nonetheless, it can still be considered negligible for VoIP traffic. However, the implementation of IPv6 and IPSec imposes larger packet size, additional security payload and thus it is expected to slightly increase the CPU and memory resources. Additional UDP background traffic may also contribute to degradation in network performance and voice quality as heavy overloaded network conditions up to 200mbps will rapidly increase the packet loss ratio.

REFERENCES

[1] I. Raicu and W. Lafayette, "Evaluating IPv4 to IPv6 Transition Mechanisms," Proc. 10th Int. Conf. on Telecommunications, 2003, pp. 1091–1098.

[2] A. S. Tanenbaum and D. J. Wetherall, Computer Networks, Prentice Hall, 5th ed, 2011.

[3] M. Tufail, "IPv6 - An opportunity for new service and network features," Proc. IEEE Int. Conf. on Networking and Services, Silicon Vally, CA, 16-18 Jully 2006, pp. 11.

[4] P. Amr and N. Abdelbaki, "VoIP performance evaluation over IPv4-6 and manually configured tunnels," Proc. IEEE Int. Workshop on Measurements and Networking, Naples, 7-8 October 2013, pp. 121 – 126.

[5] M. K. Sailan, R. Hassan, and A. Patel, "A comparative review of IPv4 and IPv6 for research testbed," Proc. int. Conf. on Electrical Engineering and Informatics, Selangor, 5-7 August, 2009, pp. 427–433..

[6] R. Asinovskyy, A. L.WIjesinha, and R. Karne, "VoIP performance with IPsec in IPv4-IPv6 transition networks," Inforcommunication Journal, Special Issue,. vol. LXV, no. 3, 2010, pp. 15–23.

[7] R. Yasinovskyy, A. L. Wijesinha and R. Karne, "Impact of IPsec and 6to4 on VoIP quality over IPv6," Proc. 10th Int. Conf. on Telecommunication, Zegreb, 8-10 June 2009, pp. 235-242.

[8] N. Bahaman, E. Hamid and A. S. Prabuwono, "Network performance evaluation of 6to4 tunneling," Int. Conf. Ion Innovation Management and Technology Research, Malacca, 21-22 May 2012, pp. 263–268.

[9] C. Shue, Y. Shin, M. Gupta and J. Y. Choi, "Analysis of IPSec overheads for VPN servers," Proc. 1st IEEE ICNP Workshop on Secure Network Protocols, 6 November 2006, pp. 25-30.

[10] C. A. Shue, M. Gupta, and S. A. Myers, "IPSec: Performance analysis and enhancements," IEEE Int. Conf. Communications, Glasgow, 24 – 28 June 2007, pp. 1527–1532.

[11] P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security," Int. J. Computer Applications, vol. 13, no. 15, 2013, pp. 33–38.

[12] M. A. Al-Taee, N. H. Al-Hassani, B. S. Bamajbour and D. Al-Jumeily, "Biometric-based security system for plaintext e-mail messages," Proc. Int. Conf. on Developments in e-Systems Engineering, Abu Dhabi, UAE, 14 – 16 December 2009, pp. 201-206.

[13] N. Qasrawi, M. A. Al-Taee, H. I'emair and R. Al-Asa'd, "Multilevel encryption of plaintext messages using a smart card connected to PC parallel port," Proc. 3rd Int. Conf. on Modelling, Simulation and Applied Optimization, Sharjah-UAE, 20-22 January 2009.

[14] Openswan, http://www.openswan.org/, (last accessed on 25 January 2016).

[15] L. Lian and G. Wen-mei, "Building IPsec VPN in IPv6 based on Openswan," Proc. IFIP Int. Conf. on Network and Parallel Computing, Liacning, 18-21 September, 2007, pp. 784–787.

[16] S. Narayan and S. Tauch, "IPv4-v6 transition mechanisms network performance evaluation on operating systems," Proc. IEEE 3rd Int. Conf. on Computer Science and Information Technology, Chengdu, 9-11 July 2010, pp. 664 – 668.

[17] S. Narayan and S. Tauch, "IPv4-v6 configured tunnel and 6to4 transition mechanisms network performance evaluation on Linux operating systems," Proc. 2nd Int. Conf. on Signal Processing Systems, vol. 2, Dalian, 5-7 July 2010, pp. V2-113– V2-117.

[18] M. Mujinga, H. Muyingi, and G. S. V. R. Krishna Rao, "IPSec overhead analysis in dual stack IPv4/IPv6 transition mechanisms," Proc. 8th Int. Conf. on Advanced Communication Technology, Phoenix Park, 20-22 February 2006, pp. 691-696.

[19] R. Yasinovskyy, A. L. Wijesinha, R. K. Karne and G. Khaksari, "A comparison of VoIP performance on IPv6 and IPv4 networks," Proc. IEEE/ACS Int. Conf. on Computer Systems and Applications, Rabat, 10-13 May 2009, pp. 603 – 609.

[20] A. Passito, E. Mota, R. Aguiar and L. Carvalho, "Evaluating voice speech quality in networks with VPN/IPSec," Proc. IEEE I7th Malaysia int. Conf. on Networks/Communication, 16-18 November 2005, pp. 161–165.

[21] R. Barbieri, D. Bruschi, and E. Rosti, "Voice over IPsec: analysis and solutions," Proc. 18th Annual Conf. on Computer Security Applications, 2002. pp. 261 – 270.

[22] A. J. Ghazali, W. Al-Nuaimy and A. K. Nandi, "Simulation of the encryption of NetFlow packet capturing system using IPSec," Proc. 5th Int. Conf. on Computers and Devices for Communication, Kolkata, 17-19 December 2012, pp. 1-4.

[23] Ekiga Softphone, http://www.ekiga.org, (last accessed on 30 January 2016).

[24] Wireshark. https://www.wireshark.org/, (last accessed on 30 January 2016).

[25] PackETH, http://packeth.sourceforge.net/packeth/Home.html, (last accessed on 28 January 2016).

[26] Jperf, https://code.google.com/p/xjperf/, (last accessed on 30 January 2016).

[27] Iperf, https://iperf.fr/, (last accessed on 25 January 2016).

[28] M. K. Sailan and R. Hassan, "Impact of TCP window size on IPv4 and IPv6 performance," Int. J. of Computer Science and Network Security, vol. 9, no. 12, 2009, pp. 129–133.

[29] R. Hassan and M. K. Sailan, "End-to-end baseline file transfer performance testbed," Information Technology J., vol. 10, no. 2, 2011, pp. 446 – 451.

[30] R. M. Dansereau, S. Jin and R. A. Goubran, "Reducing packet loss in CBC secured VoIP using interleaved encryption," Proc. Canadian Conf. on Electrical and Computer Engineering, Ottawa, May 2006, pp. 1320–1324.

[31] A. N. Murshid, A. F. Khalifa, and M. A. Al-Taee, "Quality of experience analysis of videoconferencing over lossy networks," Proc. IEEE Jordan Conf. on Applied Electrical Engineering and Computing Technologies, Amman, Jordan, 3-5 December 2013, pp. 1-6.