Impact of IPSec security on VoIP in different environments

Samad S. Kolahi, Keysha Mudaliar, Cheng Zhang, and Zhizhong Gu
Unitec Institute of Technology, New Zealand
skolahi@unitec.ac.nz

Abstract – **In this paper, the performance of VoIP on IPv4, IPv6 and 6in4 protocol with and without IPsec is compared. RTT (Round Trip Time), Throughput, Jitter and CPU usage are compared in VoIP networks. The results for throughput are almost same for both operating systems. CPU usage was higher on both operating systems with IPsec enabled and the results for RTT and Jitter were inconsistent. In general, the results indicated that Fedora 16 performance was better than Windows 7. The results show that although IPSec can add security, it can reduce the VoIP performance in terms of higher delay and higher CPU usage.**

Keyword: Performance, VoIP, IPsec, IPv4, IPv6, 6in4, Windows 7 and Fedora 16.

I. INRODUCTION

The purpose of network security is to provide confidentiality, integrity and authentication. VoIP is a revolutionary technology that takes analogue audio signals and turns them into digital data that can be transmitted over the internet. VoIP has the potential to completely rework the world's phone systems at cheaper rate than PSTN (Public Switched Telephone System). VoIP phone calls are cheaper as it uses a shared packet switched network as compared to circuit switched PSTN calls.

IPSec encryption can protect VoIP data as it travels over the network; if attackers bypass physical security precautions and intercept VoIP packets, they won't be able to decipher the encrypted contents. IPSec can make VoIP communications more secure than a traditional landline. Although IPsec is popular security technology for VoIP security, it affects VoIP performance due to added overheads involved with IPSec.

IPv6 is the later version of IPv4 that provided much more IP addresses (2^{128}), better mobility, better security, and better QoS features as compared to IPv4. In transition stages, where both IPv6 and IPv4 are present in a network, protocols such as 6in4 is required to handle computer networks including both IPv6 and IPv4 traffic. Currently the core of Internet is IPv4 but some companies might have immigrated to IPv6. We therefor compare the performance of these in IPSec encrypted VoIP environment using a test bed. The testing performance parameters were throughput, delay, and CPU usage. Data was obtained for IPv4, IPv6 and IPv6 to IPv4 environments.

To the authors' knowledge, there is little work in literature to evaluate VoIP in these environments. The motivation for this work is therefore to provide new results on the impact of IPSec on VoIP performance in IPv6, IPv6, 6in4 environments. We also compare the performance of window based system with Linux based system.

The organisation of this paper is as follows, next section is related works, section three is network set up, section four is data generation and traffic measurement tool used, section five is results, and section six is conclusions followed by future works and list of references.

II. RELATED WORKS

The previous research work on VoIP and IPsec are as follows. Barbieri, Bruschi and Rosti [1] discussed analysis and solutions of Voice over IPsec (experimental study of VoIP when an IPsec network is used). Their results show that the effective bandwidth can be reduced up to 50% with respect to VoIP in case of VoIPsec. The authors found an efficient solution for packet header compression for VoIPsec traffic. A new compression scheme to improve the effective bandwidth with security was proposed and preliminary performance results presented.

Ramakrishnan and Kumar [2] researched advantages and disadvantages of integrating all types of traffic onto a single IP network by comparing the performance of several SIP VoIP codecs. They analysed packet loss, jitter and delay. From the results that they obtained, a conclusion was made that G.711 is an ideal solution for PSTN networks with PCM scheme. G.723 is used for voice and videoconferencing however it offers lower voice quality. Music or tones such as DTMF cannot be transmitted reliably with G.723 codec. G.729 is mostly used in VoIP applications for its low bandwidth requirement.

Radman, Singh, Domingo, Arnedo and Talevski [3] investigated an end-to-end network with security and evaluated the impacts of QoS (Quality of Service) in VoIP. They researched methods for making secure calls and maintaining high call quality. The QoS was measured in terms of lost packet ratio, latency and jitter using no security, and different encryption algorithm. They used IP firewalls in Local and Wide Area Networks (LAN and WAN). The results of their laboratory tests showed that the impact on the overall performance of VoIP depends upon the bandwidth availability and encryption algorithm used. The authors stated that the implementation of any encryption algorithm in low bandwidth environments degrades the voice quality due to increased lost packets and packet latency. As bandwidth increased, encrypted VoIP calls provided better service compared to an unsecured environment. Their results also showed that the three factors of QoS - latency, jitter and lost packets are all improved through increased bandwidth.

Kazemi, Wijesinha, and Karne [4] evaluated IPsec overhead using a bare PC. In a bare PC softphone, the VoIP application runs directly on the hardware without any operating system. Such softphones are useful when security and/or performance concerns outweigh the need for a conventional system. The authors evaluated the overhead of IPsec for VoIP in a small test LAN using a bare PC softphone. The experimental results using a test LAN showed considerable processing overhead. The authors also compared tunnel mode verus transport mode.

Yasinovskyy, Wijesinha, Karne, and Khaksari [5] compared VoIP performance on IPv6 and IPv4 LANs in the presence of varying levels of background UDP traffic (using the same softphone on popular operating systems). They used a conventional softphone to make calls and a bare PC (with no operating system) softphone for control purposes (to determine the impact of system overhead). The performance measures were maximum and mean delta (the time between the arrivals of voice packets), maximum and mean jitter, packet loss, MOS (Mean Opinion Score), and throughput. The measurements of several parameters associated with call quality in the presence of varying levels of background traffic showed that there is no significant performance difference with IPv6 compared to IPv4. Measured throughput for voice data was close to the expected value only when there was moderate or no background traffic. For both IPv4 and IPv6, packet loss under overloaded conditions, resulted in poor voice quality and a significant drop in the MOS.

Impact of IPSec on performance of the wireless LAN networks is evaluated in [6, 7]. Impact of SSL security on network performance is evaluated in [8]. Results of these studies showed that IPSec and SSL lower bandwidth and increases RTT and CPU time.

III. NETWORK SETUP

The test bed is shown in Figure 1. In the two client-server computers, we first installed Windows operating system, and then Linux Fedora. The computes were connected via soft routers using a standard Category 5 cable between them. We set up IPsec on the client and server. The computer hardware comprised of an Intel (R) Core (TM) i7-2600 CPU3.40GHZ processer with Kingston 8 GB DDR3 1333MHz with a Westgate WDC WD 5000AAKX-001CAO 500 GB hard-drive and a Intel(R) 82579V Gigabit Network Card on these four computers (two soft routers and client-server).

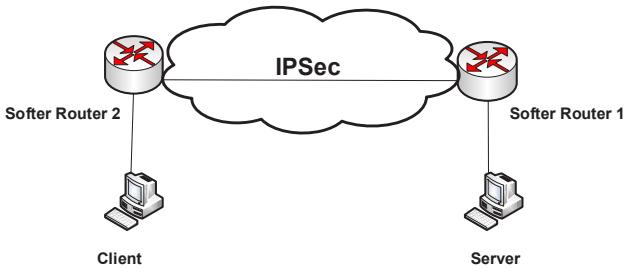

Figure 1, Network Test-Bed

IV. DATA GENERATOIN AND TRAFFIC MEASUREMENT TOOL

For traffic generation we used D-ITG software [9. 10]. It allows users to send traffic via both TCP and UDP for both IPv4 and IPv6. Users can modify the packet size and the quantity of the packets sent/received. For the VoIP traffic, it can support different voice Codec such as G729.2, G729.3, G711.1 G711.2 and G723.1. However, users can not modify packets for these Codec because they prefixed. It measures throughput, jitter, RTT, and packet loss. It can be used on different operating systems, Linux and Windows. Performance of various traffic generators and their properties is also compared in [10].

V. RESULTS

G711.1 had the highest throughput without IPsec for IPv4, IPv6 and 6in4 on Fedora16. On the other hand, G723.1 had the lowest throughput with IPsec for IPv4, IPv6 and 6in4 on Windows 7. On both operating systems, the difference in throughput between IPv4 and IPv4 with IPsec was barely noticeable for all codecs especially for G723.1, G729.2 and G729.3. The same could be said about IPv6 and 6in4. The results showed that UDP throughput was slightly lower when IPsec was enabled on IPv4, IPv6 and 6in4 although it can be concluded that the results showed an insignificant difference.

The results were consistent for both operating systems. All codecs showed steady decrease in throughput when IPsec was enabled. The throughput for G711.1 and G711.2 was much higher than the other codecs across all scenarios. The two codecs generally had slightly higher throughput on Fedora 16 as shown. Hence, the performance of Fedora 16 was slightly better than Windows 7 for the codecs G711.1 and G711.2. Results for the remaining codecs were almost the same for both operating systems.

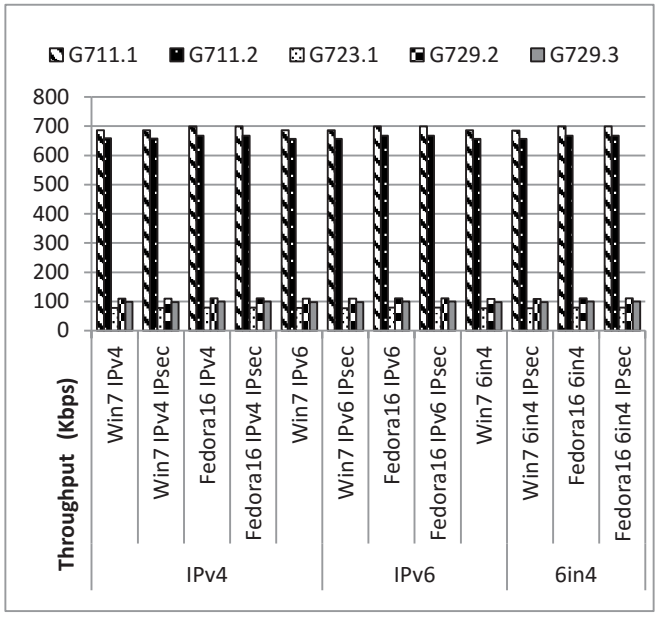

Figure 2, Impact of IPsec for VoIP Throughput on Windows7 and Fedora16

Figure 2 shows the UDP throughput for Windows 7 and Fedora 16 on IPv4, IPv6 and 6in4. Overall from the UDP throughput results, it was observed that as with IPv4, IPv6, 6in4 do not have a significant effect on UDP throughput.

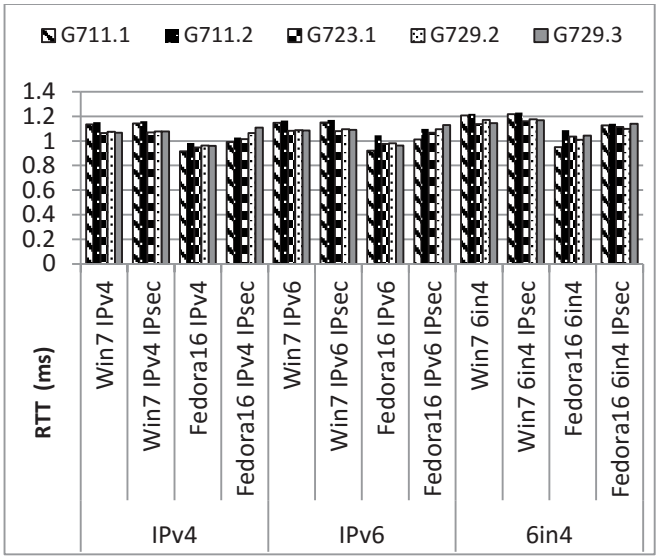

Figure 3, Impact of IPsec for VoIP Throughput on Windows7 and Fedora16

Figure 3 shows the UDP RTT for Windows 7 and Fedora 16 on IPv4, IPv6 and 6in4. Overall results show that G711.2 had the highest RTT (with IPsec) for IPv4, IPv6 and 6in4 on Windows 7. On the other hand, G711.1 had the lowest RTT (without IPsec) for IPv4, IPv6 and 6in4 on Fedora16. For both operating systems, increase in UDP RTT was observed when IPsec was enabled for all five codecs.

Compared to IPv4 and IPv6, the RTT increased on all codecs when tested on 6in4 both with and without IPsec. Windows 7 showed a steady increase in RTT when all codecs on IPv4 and IPv6, were compared with 6in4. The results for Fedora 16 were inconsistent for G711.1 G729.2 and G729.3. For G711.1 the difference between 6in4 with and without IPsec was higher than on IPv6 and IPv4.

Impact of IPsec for VoIP Jitter

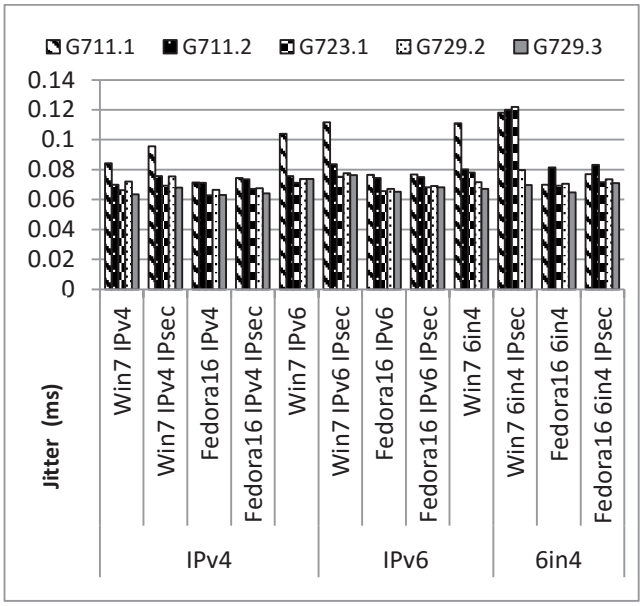

Figure 4 Impact of IPsec for VoIP Jitter on Windows7 and Fedora16

Figure 4 shows the UDP Jitter for Windows 7 and Fedora 16 on IPv4, IPv6 and 6in4. On the whole, G723.1 had the highest jitter on Windows 7 for 6in4 with IPsec. G723.1 also had the lowest jitter on Fedora16 for IPv4 without IPsec.

For Windows 7, G711.1 had the most inconsistent results which fluctuate as shown. The results were steady for G711.2 and G723.1 across all scenarios except for 6in4 with IPsec on Windows 7. The codecs G729.2 and G729.3 showed consistent results across all scenarios on both operating systems. The results were stable for all codecs on Fedora 16 with steady increase in jitter when IPsec was enabled.

The results show that the differences between IPv4 and IPv6 with IPsec were marginal for all codecs except G729.2 and G729.3. For IPv6 and 6in4 with IPsec, the differences were much higher for all codecs except for G711.1.

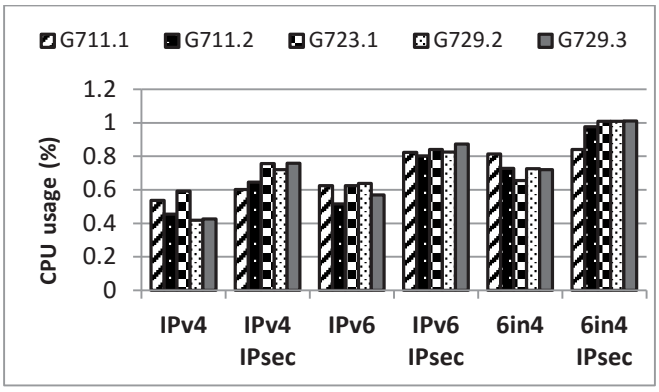

Figure 5, VoIP codecs CPU usage comparison for IPv4, IPv6 and 6in4 on Windows 7

Figure 5 shows the CPU usage for IPv4, IPv6 and 6in4 on Windows 7. Generally CPU usage increased when IPsec was enabled. The results show that CPU usage was higher when codecs were tested on 6in4 than on IPv6 and IPv4. As depicted, G729.3 had the highest CPU usage followed by the codecs G729.2 and G723.1 (on 6in4 with IPsec). On the other hand, G729.3 had the lowest CPU usage on IPv4.

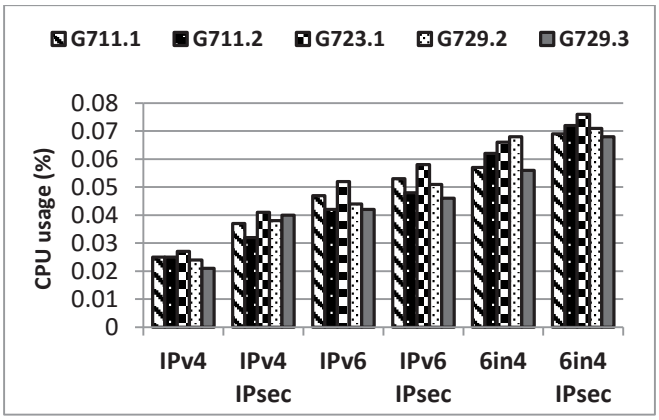

Figure 6, VoIP codecs CPU usage for IPv4, IPv6 and 6in4 on Fedora 16

Figure 6 shows the CPU usage for IPv4, IPv6 and 6in4 on Fedora 16. As shown, CPU usage increased when IPsec was enabled on all five codecs. The results show that CPU usage was higher when codecs were tested on 6in4 than on IPv6 and IPv4. G729.3 had the lowest CPU usage in all scenarios except on IPv4 with IPsec where CPU usage was the lowest for G711.2. On the other hand, G723.1 had the highest CPU usage in all scenarios except on 6in4 without IPsec. Overall, the highest CPU usage was observed for G723.1 (on 6in4 with IPsec) while G729.3 had the lowest CPU usage (on IPv4 without IPsec).

VI. CONCLUSION

In this research, we compared VoIP performance with and without IPsec for Windows 7 and Fedora 16

It was obvious from the results that the performance of IPv4 was generally better than IPv6 and 6in4 without IPsec for RTT, Jitter and CPU usage. There were small differences in UDP throughput for IPv4, IPv6 and 6in4. For most of tests conducted, the performance of IPv4 was the best without IPsec. On the whole 6in4 with IPsec had the highest RTT, Jitter and CPU usage as well as the lowest Throughput.

It was determined from comparison of results for the operating systems that Fedora 16 performed better than Windows 7 for RTT and Jitter. For Throughput, the results for Fedora 16 were slightly better for some codecs and the same for others. When IPsec was not enabled on Fedora 16 without IPsec, the results were steady for IPv4, IPv6 and 6in4 unlike for Windows 7. The results fluctuated more on Windows 7 both with and without IPsec.

In conclusion, it can be said that overall the results for IPv4, IPv4 and 6in4 without IPsec showed that the performance was better for each type of addressing. For some codecs the performance was much better without the encryption and overhead used in IPsec whereas for others the differences were insignificant. The results varied for each performance parameter.

VII. FUTURE WORKS

Future works include performing and comparing impact of IPsec on VoIP using IPv4, IPv6 and 6to4 in different network operating systems environments; Linux server and using Ubuntu as client operating systems over Gigabit Ethernet LAN's.

ACKNOWLEDGMENT

The authors would like to thank Unitec Institute of Technology for funding the research team and providing the inventory needed.

REFERENCES

[1] R. Barbieri, D. Bruschi, et al. Voice over IPSec: Analysis and solutions. 18th Annual Computer Security Applications Conference 2002, pp. 261-270.

[2] R. S. Ramakrishnan and P. V. Kumar, Performance Analysis of Different Codecs in VoIP Using SIP. The Conference on Mobile and Pervasive Computing 2008, pp. 142-145.

[3] P. Radman, J. Singh, et al. The Impact of Security on VoIP Call Quality. Journal of Mobile Multimedia, 7(1) 2011, pp. 113-128.

[4] N. Kazemi, A. L. Wijesinha, et al. Evaluation of IPsec Overhead for VoIP using a Bare PC. Computer Engineering and Technology (ICCET), 2010 2nd International Conference, 2, 2010, pp. 586-589.

[5] R. Yasinovskyy, A. L. Wijesinha, et al. A Comparison of VoIP Performance on IPv6 and IPv4 Networks. 2009 IEEE/ACS International Conference on Computer Systems and Applications 2009, pp. 603-609.

[6] S.S. Kolahi, Y.R. Cao, and H. Chen, Bandwidth-IPSec Security Tradeoff in IPv4 and IPv6 in Windows 7 Environment, Second International Conference on Future Generation Communication Technologies (FGCT 2013), December 12-14, 2013, London, UK, pp. 148-152.

[7] S.S. Kolahi, Y. Cao, and H. Chen, Evaluation of IPv6 with IPSec in 802.11n WLAN Using Fedora 15 Operating System. IEEE Symposium on Computers and Communication. July 7-10, Split, Croatia, 2013. pp 203-206.

[8] S.S. Kolahi, Y. Cao, and H. Chen, Impact of SSL Security on Bandwidth and Delay in IEEE 802.11n WLAN Using Windows 7. In 10th International Symposium on Communication Systems, Networks and Digital Signal Processing, 2016, pp 1-4.

[9] D-ITG Distributed Internet Traffic Generator Available:http://www.computer.org/comp/proceedings/qest/2004/2185/00/21850316.pdf

[10] S.S Kolahi, S.Narayan, D.D.T. Nguyen, and Y. Sunarto, "Performance Monitoring of Various Network Traffic Generators," UkSim 13th International Conference on Computer Modelling and Simulation (UKSim'11) Cambridge, UK, March 30 2011-April 1 2011, pp. 501 - 506.