Evaluation of IPv6 with IPSec in IEEE 802.11n Wireless LAN using Fedora 15 Operating System

Samad S. Kolahi, Yuqing (Rico) Cao, Hong Chen
Department of Computing, Unitec Institute of Technology, New Zealand
skolahi@unitec.ac.nz
caoyuqing.nz@hotmail.com
hongchen1127@gmail.com

***Abstract*—IPSec (IP Security) is a robust technique for securing communications over the Internet. Due to security algorithms used, transferring data using IPSec is known to be significantly slow. In this paper using a test bed environment for a site to site IPSec, we present new results on performance of IPSec for both IPv4 and IPv6 using Fedora 15 operating system and wireless network. Compared to open system, enabling IPSec results in approximately 50% and 40% less throughput for IPv4 and IPv6 networks respectively.**

Keywords- IPv6, IPSec, Wireless, Fedora Operating System

I. INTRODUCTION

Information on the Internet is carried using the Internet Protocol (IP), which does not inherently provide privacy or other securities. In today's IT environment, it is critical to protect user's data during data transmission via the Internet. As a result, IP Security (IPSec) was developed to provide secure communication to the Internet. The architecture of IPSec compliant system is defined in RFC 4301 (Security Architecture for the Internet Protocol) by the Network Working Group of the IETF [1]. IPSec is a point-to-point protocol. On one side of the network, IPSec encrypts the packet; and the other side decrypts the packet using shared key(s). IPSec is a collection of open standards that work together to establish data confidentiality, data integrity and authentication between site users [2].

According to the registers that allocate network addresses around the world, the current Internet Protocol version 4 (IPv4) has almost run out of network addresses. Internet Engineering Task Force (IETF) therefore developed a new version of Internet Protocol named IPv6 that not only provides the network addresses to 2^{128}, but also provides many additional benefits that lacks in IPv4, such as auto-configuration, mobility, secure communication and backward compatibility. New versions of operating systems have capability for IPv6 and hardware vendors, software developers and Internet Service Providers (ISP) are moving towards supporting IPv6.

Fedora 15 is the latest Linux operating system and is very popular at the time of this research.

The main objective of this paper is to produce new results for bandwidth for IPSec VPN for both IPv4 and IPv6 using Fedora 15 operating system and wireless 802.11n networks. Systems we compared are open system, DES-MD5 (Data Encryption Standard –Message-Digest 5), 3DES-SHA (Triple Data Encryption Standard –Secure Hash Algorithm), AES128-SHA (Advanced Encryption Standard-Secure Hash Algorithm), 3DES-MD5, AES256-SHA, DES-SHA, and AES192-SHA encrypted systems. We measured throughput for both TCP and UDP.

The organization of this paper is as follows. In the next section, the related work for IPSec, IPv4 and IPv6 are discussed. Section three covers the experimental setup. Section four covers information regarding the traffic measurement tool and the data generation. Section five covers the results produced and the last sections include the conclusions and future works.

II. RELATED WORK

Although there is little work on evaluation of IPSec in IPv6, performance evaluation and comparison of IPv4 and IPv6 with and without security, IPSec VPN, has been conducted by some researchers.

In 2002, Wei and Srinivas [3] presented a study of a secure wireless LAN using IPv4 and IPSec VPN tunneling protocol. Host to host IPSec was created between an Apple computer and an IPSec gateway. Their results demonstrated that the TCP throughput without IPSec was roughly three times than that with IPSec. In 2004, Zeadally and colleagues [4] conducted an empirical performance comparison of IPv4 and IPv6 protocol stack with three operating systems including Windows 2000, Solaris and Linux. Their results showed that there was a decrease in throughput and round-trip time performance for IPv6 compared to IPv4 on those three operating systems. In 2009, Narayan and colleagues [5] conducted a study of network performance of IPsec VPN on Windows server 2003, Windows vista and Linux operating systems. Two servers acted as software routers. Their studies concluded that throughput values varied for various operating systems used. In [6,7], Kolahi and colleagues studied the impact of security on the performance of IPv4 and IPv6 in a wireless 802.11n environment using various operating systems.

There has been no work done to date on performance of open system and IPSec for both IPv4 and IPv6 under Fedora 15 using networks connected by hard routers. The

lack of available research on impact of IPSec under Fedora 15 operating system was the main motivation behind this paper. The contribution of this paper is therefore to compare the performance of IPv4 and IPv6, IPSec (with various encryption systems) and open systems, on a site to site VPN network utilizing Fedora 15 operating system.

III. EXPERIMENT SETUP

The test-bed network setup remained constant for all experiments conducted and is shown in Figure 1.

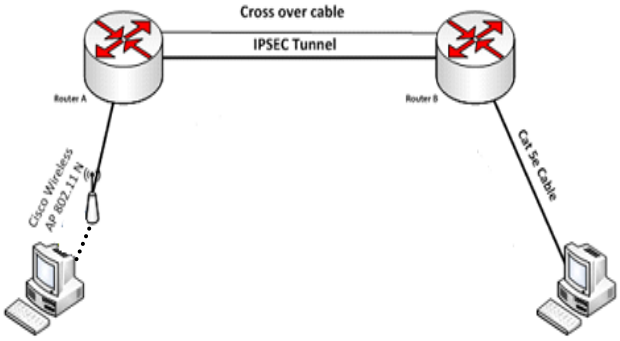

Figure 1: Testbed's Network.

Two hard routers were connected via Cross over Cat 5e cable, one client machine was connected wirelessly via Cisco Linksys WAP4410N 802.11n Access Point (AP). The other computer was directly connected to the Cisco 2811 router via Cat5e Cable.

The hardware benchmark was comprised of two computers with Intel® Core™ i5 2.80 GHz, 8.00 GB of RAM and two Cisco 2811 routers. For the efficient operation of Fedora 15, an Air Live Wn-5000 wireless PCI NIC and a Western Digital Caviar 160 GB hard-drive were installed on the two workstations.

IPSec VPN is commonly setup site to site, which will establish the VPN tunnel between two routers at two sites.

In the test-beds, Fedora 15 was installed in both computers. For each test bed we implemented open system, IPSec for both IPv4 and IPv6 measuring TCP and UDP throughput. In all options, the wireless link had WPA2 (Wireless Protected Access 2) security.

Throughput (the number of bits transmitted per unit time) depends on several factors in a network, such as process limitations and hardware design. In order to eliminate the effect of such conditions, hardware with same characteristics was used in all of the tests.

IV. DATA GENERATION AND TRAFFIC MEASUREMENT TOOL

Netperf 2.4.5 [8] was selected as the tool to analyze the performance of IPsec, IPv4 and IPv6, on Fedora 15 operating system over 802.11n WLAN. Netperf can be used to measure the performance of many different types of networks. It creates and sends TCP and UDP packets in either IPv4 or IPv6 networks and provides tests for throughput. Most performance evaluation tests were executed for 30 seconds, which usually generated 1 million packets per run. To ensure high data accuracy, each test was repeated at least 30 times and results averaged and runs continued until standard deviation of results was below 0.5% of the average.

V. EXPERIMENTAL RESULTS

Experiments were conducted using test bed of Figure 1, to evaluate and compare the throughput for TCP and UDP on open system and IPSec, for both IPv4 and IPv6. IPSec encryption methods compared were DES-MD5, DES-SHA, 3DES-MD5, 3DES-SHA, AES128-SHA, AES192-SHA and AES256-SHA systems.

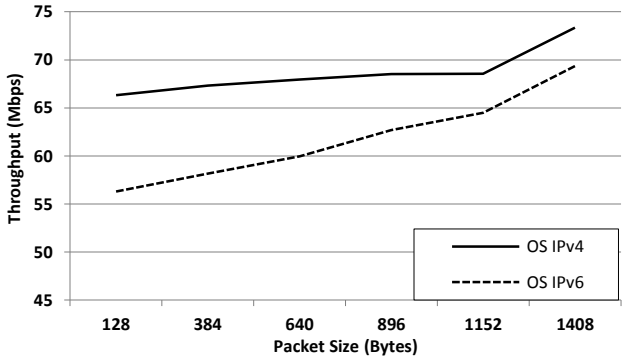

Figure 2: TCP Throughput Comparison for Open System for IPv4 and IPv6 on Fedora 15.

Figure 2 shows the TCP throughput comparison for open system for both IPv4 and IPv6 on Fedora 15 over 802.11n WLAN. From TCP throughput values, for all packet sizes, there were performance differences between IPv4 and IPv6. Comparing IPv4 with IPv6 (open systems), IPv4 had higher TCP throughput than IPv6 for all packet sizes. The maximum difference between IPv4 and IPv6 on open system was 10 Mbps for packet size of 128 Bytes and the minimum difference was 4 Mbps for packet size of 1408 Bytes. TCP throughput of open system with IPv4 and IPv6 both increased as the packet size increased.

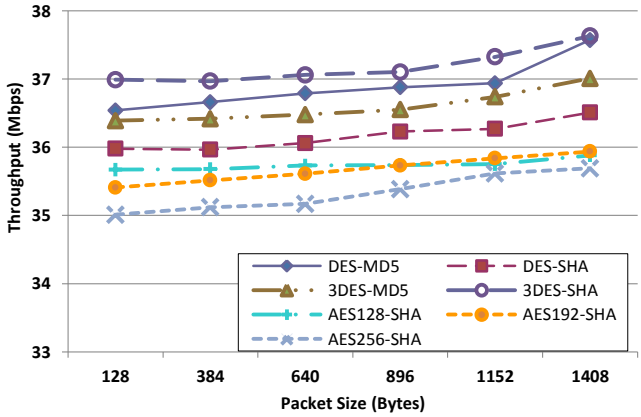

Figure 3: TCP Throughput Comparison of IPSec Encryption Methods for IPv4 on Fedora 15.

Figure 3 shows the TCP throughput comparison of IPv4 IPSec for different encrypted systems under Fedora 15 operating system. For TCP throughput, the bandwidth of 7 different encrypted systems increased as the packet size increased for all packet sizes. Compared with different encrypted systems, 3DES-SHA system had the highest TCP throughput than others while AES256-SHA system had the lowest TCP throughput than other scenarios.

From Figure 3, we can also see that the highest point of difference between the 7 encrypted IPSec systems can be noted at the packet size of 128 Bytes where 3DES-SHA system provided the highest TCP throughput of 36.99 Mbps and AES256-SHA system provided the lowest TCP throughput of 35.01 Mbps. The lowest point of difference was noted at the packet size of 1152 Bytes where 3DES-SHA system provided the highest TCP throughput of 37.33 Mbps and AES256-SHA system provided the lowest TCP throughput of 35.62 Mbps.

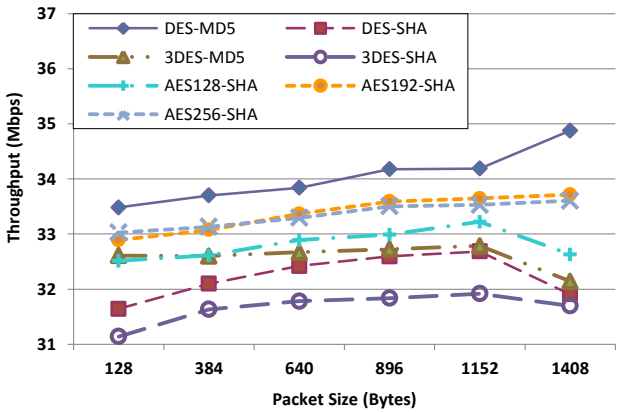

Figure 4: : TCP Throughput Comparison of IPSec Encryption Methods for IPv6 on Fedora 15.

Figure 4 shows the TCP throughput comparison of IPv6 IPSec for different encrypted systems. For TCP throughput, the bandwidth of 7 different encrypted systems increased as the packet size increased for all packet sizes with the exception of AES128-SHA, 3DES-MD5, DES-SHA and 3DES-SHA systems at packet size 1408 Bytes. Comparing the different encrypted systems, DES-MD5 encrypted system had the highest TCP throughput than others while 3DES-SHA encrypted system had the lowest TCP throughput than other scenarios for all packet sizes.

From Figure 4, we can also see that the maximum difference between the 7 IPSec systems was 3.18 Mbps at the packet size of 1408 Bytes and the minimum difference was 2.06 Mbps at the packet size of 640 Bytes.

Analyzing the impact of IPsec on TCP bandwidth for IPv4 and IPv6 on Fedora 15 operating system using wireless network (Figures 3 and 4), it can be seen that the throughput of both IPv4 and IPv6 was reduced when IPSec was enabled. For IPv4 network, compared to open system, the throughput of IPSec encrypted systems was decreased by a maximum of 37.65 Mbps (decrease rate of 51.33%) for packet size 1408 Bytes and by a minimum difference of 29.32 Mbps (decrease rate of 44.21%) for the packet size of 128 Bytes. For IPv6 network, compared to open system, the throughput of system using IPSec encrypted systems was decreased by a maximum of 37.64 Mbps (decrease rate of 54.29%) for packet size 1408 Bytes and by a minimum difference of 22.82 Mbps (decrease rate of 40.53%) for packet size 128 Bytes.

UDP results obtained from the test-bed for Fedora 15 operating system with IPv4 and IPv6 are presented in Figures 5 and 6.

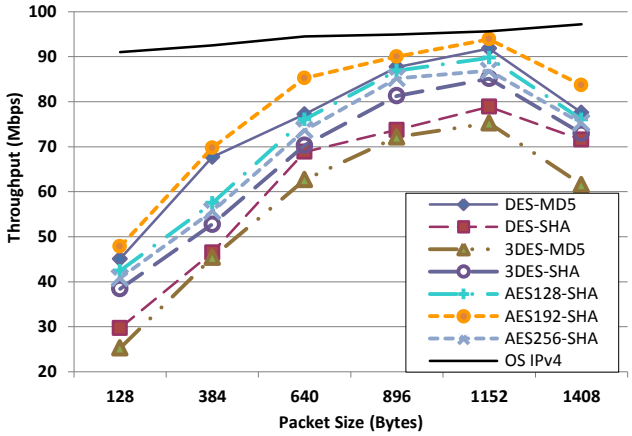

Figure 5: UDP Throughput Comparison for Open system and IPSec systems uisng IPv4 on Fedora 15.

Figure 5 shows the UDP throughput comparison for open system and IPSec encryption methods using IPv4, Fedora 15, and 802.11n WLAN. From UDP throughput values, for all packet sizes, the performance was reduced when IPSec was enabled. In addition, the UDP throughput was increased as the packet size increased for all packet sizes with the exception of packet size 1408 Bytes. In a few research work, we had inconsistent results at his packet size.

Comparing the 7 IPSec encrypted systems, AES192-SHA system gave the best UDP throughput performance while 3DES-MD5 system gave the worst UDP throughput performance.

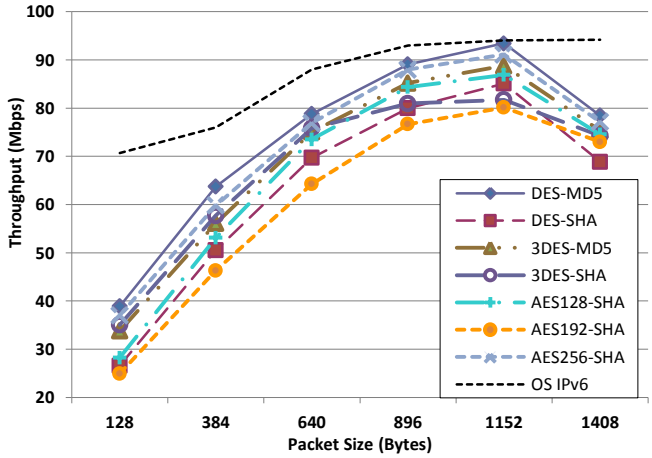

Figure 6: UDP Throughput Comparison for Open system and IPSec systems using IPv6 on Fedora 15.

Figure 6 shows the UDP throughput comparison for open system and IPSec using IPv6 on Fedora 15 over 802.11n WLAN. Comparing the 7 IPSec encrypted systems for open system, DES-MD5 system gave the best UDP throughput performance while AES192-SHA gave the worst UDP throughput performance. The UDP throughput was increased as the packet size increased for all packet sizes with the exception of packet size of 1408 Bytes.

Analyzing the UDP throughput impact of IPSec (Figures 5 and 6) for IPv4 and IPv6, it can be seen that the throughput of both IPv4 and IPv6 was reduced when IPSec was enabled. For IPv4 network, compared to open system, the UDP throughput of IPSec encrypted systems was decreased by a maximum of 65.76 Mbps (decrease rate of 72.25%) for packet size 128 Bytes and by a minimum difference of 1.80 Mbps (decrease rate of 1.88%) for packet size 1152 Bytes. For IPv6 network, compared to open system, the throughput of IPSec encrypted systems was decreased by a maximum of 45.72 Mbps (decrease rate of 64.70%) for packet size 128 Bytes and by a minimum difference of 0.64 Mbps (decrease rate of 0.68%) for packet size 640 Bytes.

Comparing the 7 different IPSec encrypted systems for both IPv4 and IPv6 network for TCP and UDP, it can be observed that if one encryption IPSec system performed well in IPv4 network, it might have a bad performance in IPv6 network. For example, for TCP throughput, the 3DES-SHA system performed the best in IPv4 network, whereas this encrypted system performed the worst in IPv6 network.

Comparing the two networks performance of throughput for both TCP and UDP, it can be observed that IPv4 had the higher TCP and UDP throughput than IPv6 for open system and the 7 encrypted systems. The lower throughput gained in IPv6 than in IPv4 is resulted by the drawback of having a larger overhead in IPv6 (which has a 40 Bytes header while IPv4 has a 24 Bytes header) over IPv4 [9]. The overhead increase in IPv6 has implication on the performance of IPv6, resulting in lower bandwidth.

The UDP throughputs are higher than the TCP on both open system and IPSec security enabled systems. This is due to UDP being a connectionless protocol and does not use any form of error correction and therefore does not send any acknowledgements. The source does not have to wait to receive any acknowledgements [10].

The gain in TCP and UDP throughput as the packet size increase is likely due to the amortization of overheads associated with larger user packet sizes [11].

The lower throughput results obtained when IPSec security is enabled (compared to open system with no security) is due to two reasons. The encryption and decryption take up CPU and memory resource, and the data packets become longer because of overheads associated with encryption. Although IPSec guarantees the security of data transmission, it leads to the decrease of throughput for both TCP and UDP [12].

VI. CONCLUSION

There was a bandwidth decrease when IPSec security was enabled for both IPv4 and IPv6 using Fedora 15. For system studied, enabling IPSec resulted in approximately up to 37.65 Mbps less TCP throughput than open system for IPv4 and up to 37.64 Mbps less TCP throughput than open system for IPv6. For IPv6, DES-MD5 encryption system had the highest TCP throughput while 3DES-SHA encrypted system had the lowest TCP throughput.

VII. FUTURE WORKS

In future, we plan to extend this study by incorporating Solaris and Windows 8 systems. In addition, the performance of other VPN technologies, such as SSL, PPTP and L2TP will be investigated.

REFERENCES

[1] R. Molva., "Internet Security Architecture" http://www.eurecom.fr/~nsteam/Papers/pap04.pdf.

[2] J.F. Roland, and M.J. Newcomb, CSVPN, Certification Guide, 2003, CISCO Press.

[3] Q. Wei and S. Srinivas. "IPSec-based secure wireless virtual private network". MILCOM 2002, pp. 1107-1112.

[4] S. Zeadally, R. Wasseem, and I. Raicu, "Comparison of End System IPv6 protocol Stacks", IEE Proc. Communications, vol 151 (3), 2004, pp. 238-242.

[5] S. Narayan, and K. Brooking, "Network Performance Analysis of VPN Protocols: An Empirical Comparison on Different Operating Systems." International Conference on Networks Security, Wireless Communications and Trusted Computing, NSWCTC '09, pp. 645-648.

[6] S. S. Kolahi, P. Li, M. Argawe, and M. Safdari, "WPA2 security-bandwidth trade-off in 802.11n peer-peer WLAN for IPv4 and IPv6 using Windows XP and Windows 7 operating systems". 2012 IEEE Symposium on Computers and Communications (ISCC), 2012, pp. 575 - 579.

[7] S. S. Kolahi, Z. Qu, B.K. Soorty, and N. Chand, "The Impact of Security on the Performance of IPv4 and IPv6 Using 802.11n Wireless LAN". Third International Conference on New Technologies, Mobility and Security, **IEEE** NTMS'2009, Cairo, pp. 1-5.

[8] R. Jones. Netperf 2.4.5 Available: http://www.netperf.org/netperf/NetperfNew.html

[9] R. Murugesan, S. Ramadas. R. Budiarto, "Improving the Performance of IPv6 Packet Transmission over LAN," 2009 IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009), October, 2009, pp. 182-187.

[10] S. S. Kolahi and P. Li, "Evaluating IPv6 in Peer-to-Peer 802.11n Wireless LANs," IEEE Internet Computing, Vol. 15 Issue 4, 2011, pp. 70-74.

[11] S. Zeadally and L. Raicu, "Evaluation IPv6 on Windows and Solars," Internet Computing, IEEE, vol.7, no. 3, 2003, pp. 51-57.

[12] E. Barka; K. Shuaib; H. Chamas, "Impact of IPSec on the Performance of the IEEE 802.16 Wireless Networks," New Technologies, Mobility and Security, NTMS '08, pp. 1-6.