The Influence of WPA2 Security on the UDP Performance of IPv4 and IPv6 Using 802.11n WLAN in Windows 7-Windows 2008 environment

Samad S. Kolahi, Hitesh Singla, Mohd Nash Ehsan, and Clarence Dong
UNITEC New Zealand
skolahi@unitec.ac.nz
hitzsingla@gmail.com

***Abstract*- The impact of WPA2 security-bandwidth trade-off for IPv4 and IPv6 on wireless 802.11n network implementing Windows 7-Windows Server 2008 is investigated. The highest point of difference between open system and WPA2 for UDP was noticed at packet size 1408 bytes where IPv4 provided 31.48 Mbps and IPv6 provided 24.33 Mbps higher throughput in the open environment. The performance of IPv4 and IPv6 are also compared.**

I. INTRODUCTION

IEEE 802.11 working group came up with a new 802.11n standard to meet the need for higher data rates. IEEE 802.11n is an amendment to the wireless networking standard to improve network throughput over previous standards, such as 802.11b and 802.11g with a significant increase in the maximum data rate from 54 Mbit/s to a maximum of 300+ Mbit/s using four spatial streams at a channel width of 40 MHz. To attain such a high data rate 802.11n uses multiple wireless signals and antennas also known as MIMO technology. Although the 802.11n is in its final stages of review, it is imperative to evaluate the 802.11n wireless performance so it will be easier for businesses to adopt this new technology into their networks.

Windows XP is the popular and dominant operating system in the market today and many businesses are reluctant to upgrade their operating system to a Windows Vista operating system due to countless negative reviews. Windows 7 is the new version of Windows operating system and is designed to answer the flaws that Windows Vista has. Windows 2008 Server is the newest network operating system that supersedes Windows 2003.

IPv6 is an upgrade to the next generation of the Internet Protocol to add better scalability and flexibility and a way to add new features in a standardized manner. The big blocks of IPv4 addresses that are assigned by Internet Assigned Number Authority (IANA) will be exhausted around 2010. Therefore it is imperative to perform a complete analysis of IPv4 and IPv6 performance over 802.11n wireless LAN. Several previous works have been carried out on evaluating IPv4 and IPv6 on other systems that have shown their performance to largely vary depending on the operating system used on the network [1].

In 2009, S.S. Kolahi et al [2] conducted a study on the impact of WPA2 security on performance of IPv4 and IPv6 on two client-server wireless 802.11n networks implementing Windows Vista-Windows Server 2008 and Windows XP - Windows Server 2008. Results indicated that for XP enabling WPA2 results in an average of approximately 7.07% less throughput than open systems for IPv4and 5.42% less throughput for IPv6. Enabling WPA2 on Vista results in an average of approximately 9.39% less throughput than open system for IPv4 and 17.02% less throughput for IPv6.With WPA2 security, IPv4 provides higher bandwidth than IPv6.

In 2008, S.S. Kolahi et al [3] conducted a study on the impact of security techniques for 802.11g on Windows XP, Windows Vista and Windows Server 2003. The main contribution of their paper was to investigate the impact of security on throughput and RTT (Round Trip Time) on those operating systems. Their results showed when adding encryption to open system, the TCP throughput reduced by approximately 10% for WEP-64 and 14% for WEP-128 on Windows XP. In 2007, Filho et al [4] studied bandwidth-security trade-off in Windows XP operating system, their results showed a drop in throughput of 4%, 7% and 5% when WEP-64, WEP-128 and WPA were applied to open systems.

In 2006, B. Ezedin et al [5] produced a paper based on the impact of security on the performance of 802.11g networks. The authors stated that the TCP throughput suffered a degradation of 4% on Windows XP when WEP-64 was enabled and 7.14% when the 128-bits key was enabled. The maximum degradation occurred (as much as 30%) with Windows Server 2003 when WEP-128 was enabled while Windows Vista and Windows XP displayed a 10% reduction in bandwidth.

In 2004, N Baghaei and R. Hunt [6] conducted a study on the impact of security performance on 802.11b networks using multiple clients. Their results showed that upon adding encryption to an open system network, the throughput reduced by approximately 7% for WEP-64 and 10% for WEP-128 using Windows XP.

There has been no work done to date on security-bandwidth tradeoff on the 802.11n wireless networks with IPv4 and IPv6

over network using Windows 7 as client operating systems and Windows Server 2008 as server network operating system. Given the fact that WEP-64 and WEP-128 are now regarded obsolete due to an increased number of vulnerabilities open to exploits, this paper focuses on the latest encryption protocol of WPA2 which is now used for security on most wireless 802.11n and 802.11g networks. The contribution of this paper is therefore to compare the UDP performance of IPv4 and IPv6 on a client-server wireless 802.11n network implementing Windows 7 and Windows Server 2008 whilst implementing WPA2 security and comparing the results with an open system 802.11n network.

The organization of this paper is as follows. In the next section the network setup is discussed. Section three covers information regarding the data generating and traffic measurement tool. Section four covers the results and the last sections include the conclusion, future works and acknowledgments followed by the references.

II. NETWORK SETUP

The hardware specifications for both the client and server machines consists of Intel Core 2 Duo E6300 1.87 GHz processor, 2 GB of RAM, one AirLive WN-5000 PCI wireless NIC located on the client machine, one Broadcom NetXtreme Gigabit Ethernet NIC installed on the server machine and two Western Digital Caviar SE 160 GB hard disks installed on both machines respectively.

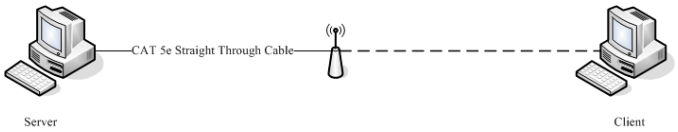

Figure1: Network test bed

A Linksys WAP4410N access point is connected to the Broadcom NetXtreme Gigabit Ethernet NIC via a Cat 5e crossover cable. The client will be connected wirelessly to the server via the Linksys WAP4410N access point. The client must join the domain and the time must be synchronized with the server before the experiments scenarios could be tested.This was done so as to maintain consistency with similar research shown in the past including the previous work done on 802.11n [2]. The distance between the access point and the workstations was well within two meters in-order to maintain the optimum signal strength.

The operating system installed was Microsoft Windows 7 as the client and Windows Server 2008 as the server. According to Killelea [7], throughput (the number of bits transmitted per unit time) depends on several factors in a network, such as process limitations and hardware designs. In-order to eliminate the effect of such conditions, the hardware was benchmarked and a similar setup was used for all the tests to negate the effect of the processor limitations and hardware design.

Characteristic parameters used for the access point configuration were:

(a) Channel bandwidth – In addition to the direction of the transmission, a channel is characterized by its bandwidth. In general, the greater the bandwidth of the assigned channels, the higher the possible speed of transmission. The access point provided two options here, 20 MHz for 802.11b and 802.11g networks and 40 MHz for the 802.11n networks. The latter was selected as the appropriate setting for the channel bandwidth.

(b) Guard Interval – Guard intervals are used to ensure that distinct transmissions do not interfere with one another. The purpose of the guard interval is to introduce immunity to propagation delays, echoes and reflections, to which digital data is normally very sensitive. This function was left appropriately to its default setting on the access point.

(c) CTS Protection Mode – This function boosts the access point's ability to detect all wireless connections but severely degrades performance, hence this setting was disabled to maximize performance.

(d) Beacon Interval – This function indicates the variable times in which clients meet the access point, this includes send and receive packets, and synchronism. This setting was best left at the default interval of 100ms.

(e) DTIM Interval – This setting specifies how often the access point broadcasts a Delivery Traffic Indication Message. According to the manual of the specific Linksys access point used in this project, lower settings ensure efficient networking. The default setting of 1ms therefore was left for achieving the best results.

(f) RTS Threshold – RTS (Request-to-Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data. This setting is used to decrease the problem of the hidden stations due to distance or signal blockage [8]. The manual for the Linksys access-point recommended that this be left at the default setting of 2347 for optimum performance.

(g) Fragmentation Threshold – This specifies the number of bytes used to fragment the frames with a purpose to increase transfer reliability. If the frame size is very big, it can cause heavy interference and elevate the retransmissions rate. On the other hand, if the frame is too small, it will create overhead during the transmission and reduce the throughput rate [4, 5]. The parameter value for this was left at the default setting of 2346.

III. DATA GENERATION AND TRAFFIC MEASUREMENT TOOL

Netperf [9] was selected as the traffic generating and measurement tool for its compatibility with Windows 7, Windows Server 2008 and for its powerful analysis of a wide range of quality of service parameters to acquire accurate

results. Netperf has extensively been used for similar researches on wireless local area networks including impact of various encryption techniques on performance of wireless 802.11g [3] and performance evaluation of security protocol over the mobile IP network [10].

IV. RESULTS

The UDP throughput was measured for IPv4 and IPv6 for various packet sizes. The range of packet sizes varied from 128 to 1408 bytes over a Windows 7-Windows Server 2008 client-server environment. The first phase of the evaluation involved measuring the throughput on an open system network with no encryption. In the second phase of the evaluation, WPA2 was enabled in-order to note the impact of its security mechanism on the IEEE 802.11n network.

This evaluation methodology comprised of performing 40 test runs and for each specific packet size (128 to 1408 bytes) in-order to get rid of any inconsistencies shown in the results.

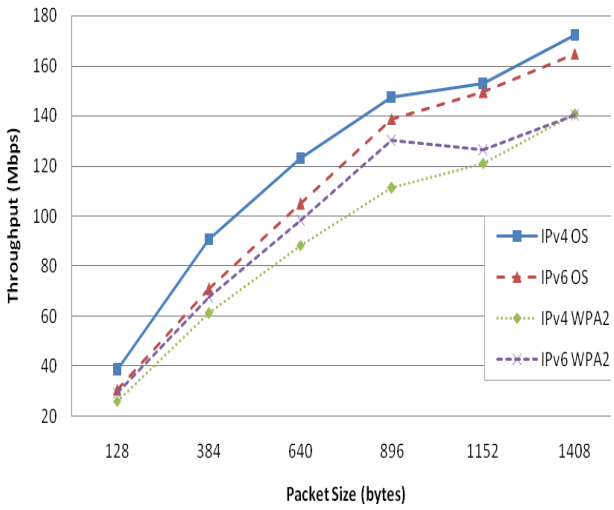

Figure 2: UDP Throughput Comparison for IPv4 and IPv6 on Windows 7 with Windows Server 2008 on Open System vs. WPA2

Figure 2 shows the UDP throughput for IPv4 and IPv6 on Windows 7 with Windows Server 2008 running on WPA2 and on an open system network with no security. For the lowest packet size, the differences are insignificant for all the scenarios. However as the packet size increases from 128 to 1408 bytes the throughput escalates consistently. With no security enabled, IPv4 on open system performs better than IPv6. The highest point of difference between IPv4 and IPv6 running on open system can be noted at the packet size 384 bytes where IPv4 provides a 28.18% higher throughput of 19.96 Mbps than IPv6.

On the same network with WPA2 security enabled IPv6 performed significantly better than IPv4 up to 896 bytes packet size. But for higher packets sizes both IPv4 and IPv6 provides almost same results. The highest point of difference between IPv4 and IPv6 for UDP with WPA2 enabled can be noted at packet size 896 bytes where IPv6 provides an 8.69% higher throughput of 10.43 Mbps than IPv4.

Analysing the impact of security on 802.11n network, for UDP as well open system performs better than WPA2. The highest point of difference between open system and WPA2 for UDP was noticed at packet size 1408 bytes where IPv4 provided 22.34% i.e. 31.48 Mbps and IPv6 provided 17.32% i.e. 24.33 Mbps higher throughput in the open environment.

The gain in UDP throughput as packet size increases is likely due to the amortization of overheads associated with larger user packet sizes (larger user payloads) [11]. Also, IPv4 running on open system clearly performs better than IPv6 for UDP protocol. On contrary with WPA2 security enabled IPv6 performs better than IPv4. Several previous works have been carried out on evaluating IPv4 and IPv6 that showed their performance largely vary depending on the Operating System used [1].

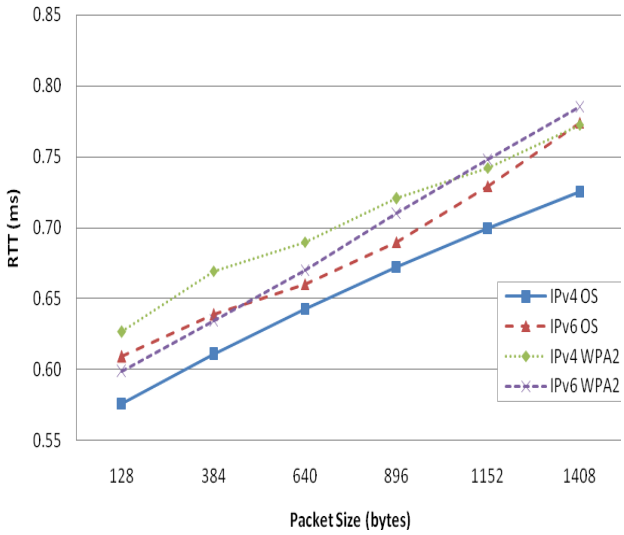

Figure 3: UDP RTT Comparison for IPv4 and IPv6 on Windows 7 with Windows Server 2008 on Open System vs. WPA2

Figure 3 shows the UDP RTT for IPv4 and IPv6 on Windows 7 with Windows Server 2008 running on WPA2 and on an open system network with no security. In both scenarios, as the packet size increase from 128 to 1408 bytes the RTT escalates consistently. On open system IPv4 outperforms IPv6 on all packet sizes by a large margin. The highest point of difference between IPv4 and IPv6 running on open system can be noted at 1408 packet sizes where IPv4 on an average provides a 5.19% lower delay rate of 0.04 ms than IPv6. On the same network with WPA2 security enabled IPv6 performed significantly better than IPv4 for all packet size except 1408 bytes. The highest point of difference between IPv4 and IPv6 for UDP with WPA2 enabled can be noted at

packet size 384 bytes where IPv6 provides a 5.97 % lower delay rate of 0.04 ms than IPv4.

V. CONCLUSIONS

In this paper the impact of WPA2 security for both IPv4 and IPv6 for UDP protocol in Windows 7- Server 2008 environment was compared. For both IPv4 and IPv6, it was observed that implementing security can adversely impact the bandwidth in 80211n environment. The highest bandwidth achieved for UDP was for IPv4 with open system at 175 Mbps.

VI. FUTURE WORKS

The future work includes testing more operating systems such as Linux with IPv4 and IPv6 using both open systems and WPA2.

ACKNOWLEDGMENT

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

REFERENCES

[1] S. Zeadally, R. Wasseem, and I. Raicu, "Comparison of end-system IPv6 protocol stacks," IEE Proceedings Communications, vol. 151, no. 3, 2004, pp. 238-242.

[2] Kolahi, S. S., Qu, Z., Soorty, B. K. & Chand, N. The Impact of Security on the Performance of IPv4 and IPv6 Using 802.11n Wireless LAN. Paper presented at the IEEE NTMS'2009, Cairo, Egypt.

[3] S.S Kolahi, S. Narayan, D.D.T, Y. Sunarto, P. Mani, "The Impact of Wireless LAN Security on Performance of Different Windows Operating Systems," IEEE Symposium on Computers and Communications, 2008, pp. 260-264.

[4] E.J.M.A. Filho, P.N.L. Fonseca, M.J.S. Leitao, and P.S.F. de Barros, "Security versus Bandwidth: The Support of Mechanisms WEP e WPA in 802.11g Network," *IFIP International Conference on Wireless and Optical Communications Networks, 2007. WOCN '07*, pp. 1-5.

[5] B. Ezedin, B. Mohammed, A. Amal, S. Hanadi Al, K. Huda, and M. Meera Al, "Impact of Security on the Performance of Wireless-Local Area Networks," *Innovations in Information Technology, 2006*, pp. 1-5.

[6] N. Baghaei, and R. Hunt, "IEEE 802.11 wireless LAN security performance using multiple clients," *Proceedings, The 12th IEEE International Conference on Networks, 2004. (ICON 2004)*, pp. 299-303 vol.291.

[7] P. Killelea, "Web Performance Tuning," http://www.amazon.ca/Web-Performance-Tuning-Patrick-Killelea/dp/product-description/059600172X.

[8] D. Akin, and J. Geier, "802.11 PHY layers," CWAP - certified wireless analysis professional official study guide, Mc.Graw-Hill, 2004, pp. 353-355.

[9] Jones, R. Netperf 2.4.5. from http://www.netperf.org/netperf/.

[10] Agarwal, A. K., Gill, J. S., & Wenye, W. (2004). An experimental study on wireless security protocols over mobile IP networks. Paper presented at the 2004 IEEE 60th, Vehicular Technology Conference, 2004. VTC2004-Fall.

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