The Performance of IPv4 and IPv6 using UDP on IEEE 802.11n WLANs with WPA2 Security

Samad S. Kolahi, Zhang Qu, Burjiz K. Soorty, and Navneet Chand
UNITEC New Zealand
skolahi@unitec.ac.nz
robert.zhang.qu@gmail.com

ABSTRACT
The IPv4 and IPv6 performance with UDP (User Datagram Protocol) on two client-server wireless 802.11n LANs implementing Windows Vista-Windows Server 2008 and Windows XP-Windows Server 2008 are compared. The impact of wireless security implementation (WPA2 security against no security) in IEEE 802.11n networks for IPv4 and IPv6 is investigated.

Keywords:
Wireless LAN 802.11n, impact WPA2 security, IPv4 and IPv6, Windows Vista, Windows XP, and Windows 2008 Server.

1. INTRODUCTION

IEEE 802.11n is designed to improve on the 802.11g in the amount of bandwidth available. 802.11n connections will support real-world data rates of well over 100 Mbps. This standard is expected to be finalized in November 2009 [1]. IPv6 is expected to replace IPv4 due to shortage of IP addresses. Windows Vista is the new version of Windows operating system, however, some businesses are undecided on an update from XP to Vista due to mixed reviews on Vista while some business have decided to updated to Vista due its better performance and that the recommended hardware benchmark for Windows Seven would remain the same as that for Vista[2]. Windows 2008 Server is the newest network operating system that supersedes Windows 2003. With the introduction of above new protocols, it is therefore important to perform a complete analysis of IPv4 and IPv6 over the new wireless standard and new operating systems.

Previous studies on performance comparison of IPv4 and IPv6 have shown their performance to largely vary depending on the operating system used on the network [3]. In 2008, S.S. Kolahi et al [4] conducted a study on the impact of overheads 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 throughput reduced by approximately 10% for WEP-64 and 14% for WEP-128 on Windows XP. For UDP traffic, Windows XP showed better throughput than Windows Vista by 3% on an open system network and 7% running WEP-128, whereas Windows Vista showed a 4% higher throughput than Windows XP for WPA.

In 2007, Filho et al [5] studied bandwidth-security trade-off in Windows XP operating system, their results showed a drop in UDP throughput of 4%, 7% and 5% when WEP-64, WEP-128 and WPA were applied to open systems.

In 2006, B. Ezedin et al [6] produced a paper based on the impact of security on the performance of 802.11g networks. The authors stated that the throughput suffered a degradation of 4% on Windows XP when WEP-64 was enabled and 7.14% when the 128-bits key was enabled. For UDP traffic, 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 [7] 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 Vista or Windows XP 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 to therefore compare the IPv4 and IPv6 performances using UDP on two client-server wireless 802.11n networks implementing Windows Vista-Windows Server 2008 and Windows XP-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, acknowledgments followed by the references.

2. NETWORK SETUP

The hardware benchmark comprised of an Intel® Core™ 2 Duo 6300 1.87 GHz processor with 2.00 GB RAM for the efficient operation of Windows Vista, a D-Link DWA-547 wireless NIC and a Western Digital Caviar SE 160 GB hard-drive on the two workstations. A Linksys WAP44110N was chosen as the appropriate access-point for this research.

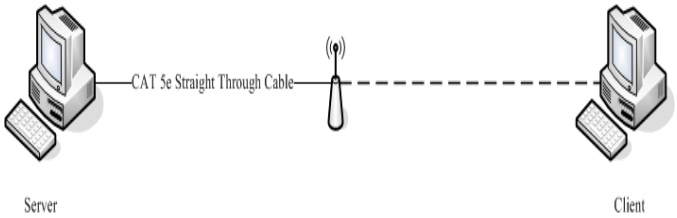

Figure1: Network test bed

The proposed network test-bed was setup through a direct connection via standard Category 5e cabling between the server and the access point. The connection between the access point and the client was wireless. The network setup was consistent with similar research shown in the past including the previous work done on 802.11g [4]. 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 Vista (plus Service Pack 1) as the client and Windows Server 2008 as the server in the first phase of the research. The second phase of the research involved Windows XP as the client with Windows Server 2008 being used as the server.

According to Killelea [8], 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.

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 [4,5]. 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 [9]. 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.

3. DATA GENERATION AND TRAFFIC MEASUREMENT TOOL

IP Traffic [10] was selected as the traffic generating and measurement tool for its compatibility with Windows Vista, Windows Server 2008 and Windows XP and for its powerful analysis of a wide range of quality of service parameters to acquire accurate results. IP Traffic has extensively been used for similar researches on wireless local area networks including impact of encryption effects on network performance [6] and performance evaluation of network security [7].

4. 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 Vista-Windows Server 2008 and Windows XP-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.

One run included sending 1 million packets of one particular packet size and protocol. The results were then averaged.

The impact of security on the IEEE 802.11n network was studied by comparing the performance of UDP throughput on IPv4 and IPv6 with WPA2 enabled to its performance in an open system environment.

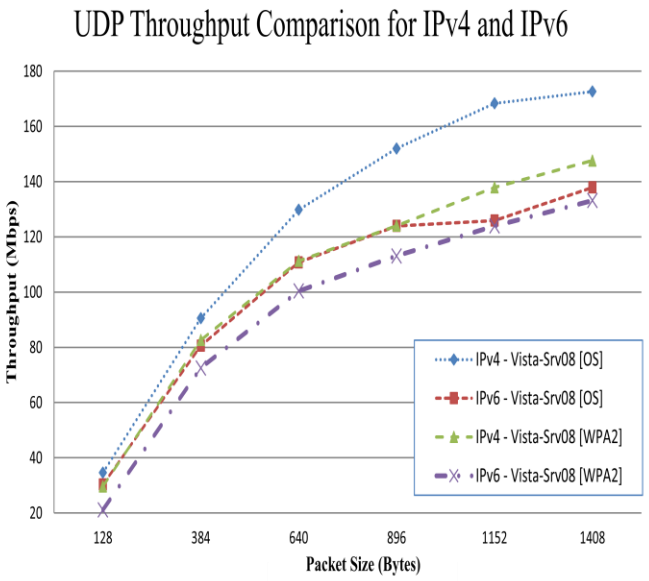

Figure 2: UDP Throughput Comparison for IPv4 and IPv6 on Windows Vista with Windows Server 2008 on Open System vs. WPA2

Figure 2 shows the UDP throughput for IPv4 and IPv6 on the Windows Vista (client) with Windows Server 2008 running on WPA2 and on an open system network with no security. As can be seen in Figure 2, as the packet size increases from 128 to 1408 bytes the throughput escalates. On the open system of the IEEE 802.11n network with no security enabled, the performance of IPv4 by far outperforms IPv6 by a large margin on all packet sizes. This margin of difference to a large extent increases with the growth in each packet size. The highest point of difference between IPv4 and IPv6 on an open system network is noted at the packet size of 1152 bytes where IPv4 provides 168.4 Mbps and IPv6 125.9 Mbps (42.5 Mbps difference). With security enabled in the form of WPA2 on the same network, IPv4 once again performs consistently better than IPv6 for all packet sizes, therefore corporate networks running IEEE 802.11n with WPA2 for UDP intensive applications such as VOIP can gain far better performance on IPv4 than they can on IPv6. The highest point of difference between IPv4 and IPv6 for UDP with WPA2 enabled is noted at the packet size of 1408 bytes where IPv4 provides 147.6Mbps and IPv6 133.2Mbps (14.4Mbps higher throughput than IPv6).

It can be concluded that enabling WPA2 results on average approximately 19.4% less throughput for IPv4 and 5.6% less throughput for IPv6. The highest point of difference between the open system and the WPA2 enabled network for UDP was noticed at the packet size of 1152 bytes for IPv4 and 896 bytes for IPv6 where IPv4 provided 30.5Mbps higher throughout (168.4 Mbps vs 137.9 Mbps) and IPv6 provided 10.9 Mbps higher throughput (124.0 Mbps vs 113.1 Mbps) in the open system environment. The lowest point of difference was noticed at the packet size of 128 bytes for IPv4 and 1152 bytes for IPv6 where IPv4 provided a 16.8% and IPv6 provided a 1.6% higher throughput in the open system environment (Figure 2). The highest bandwidth achieved was 172 Mbps for IPv4 and open systems.

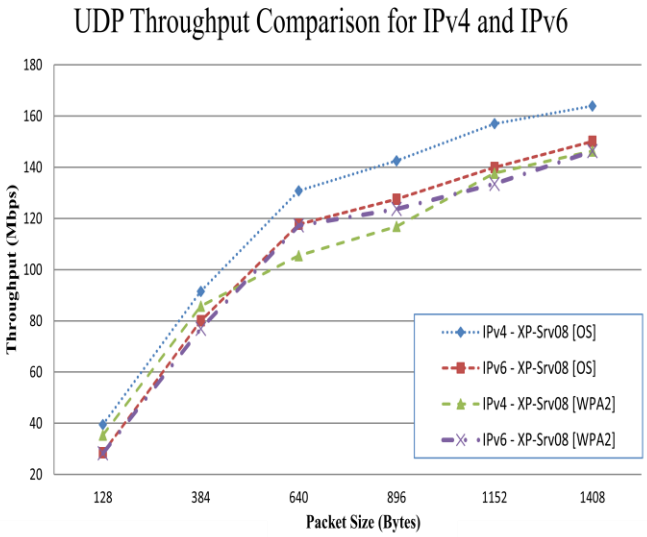

Figure 3: UDP Throughput Comparison for IPv4 and IPv6 on Windows XP with Windows Server 2008 on Open System vs. WPA2

Figure 3 shows the UDP throughput for IPv4 and IPv6 on the Windows XP as client with Windows Server 2008 running on WPA2 and on an open system network with no security. Throughput escalates substantially from packets 128 to 640 bytes before gradually increasing to 1408 bytes. On the open system of the IEEE 802.11n network with no security enabled, the performance of IPv4 again significantly increases compared to that on IPv6. The highest point of difference between IPv4 and IPv6 on an open system network is noted at the packet size of 1152 bytes where IPv4 provides a 23.5Mbps higher throughput than IPv6 (157 Mbps vs 133.5Mbps). With security enabled in the form of WPA2, the performance of IPv4 and IPv6 largely depends on packet size with IPv4 performing better on lower packet sizes 128 and 384 bytes and IPv6 performing better with the higher packet sizes of 640 to 1408 bytes, therefore corporate networks running IEEE 802.11n with WPA2 for UDP intensive applications such as VOIP can gain far better performance on IPv6 than they can on IPv4 provided the MTU (Maximum Transmission Unit) value to be traversed per frame is not customized to 384 bytes or less. The highest point of difference between IPv4 and IPv6

for UDP with WPA2 enabled is noted at the packet size of 640 bytes where IPv6 provides 11.7 Mbps higher throughput than IPv4 (117.2 Mbps vs 105.5 Mbps).

Comparing the performance of UDP throughput on IPv4 and IPv6 with WPA2 enabled to its performance in an open system environment, it can be concluded that enabling WPA2 reduces the average bandwidth by approximately 16.7% for IPv4 and 2.8% less throughput for IPv6. The highest point of difference between the open system and the WPA2 enabled network for UDP was noticed at the packet size of 896 bytes for IPv4 and 1152 bytes for IPv6 where open system with IPv4 provided 25.6Mbps higher bandwidth than WPA2 (142.5 Mbps vs 116.9Mbps) and open system with IPv6 provided higher throughput of 6.4 Mbps (139.9 Mbps vs 133.5 Mbps) compared to WPA2 environment. The lowest point of difference was noticed at the packet size of 128 bytes where IPv4 provided an 11.5% and IPv6 provided a 0.7% higher throughput in the open system environment.

Bothe graphs indicate increases in bandwidth with packet size. 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].

5. CONCLUSION

In this study, the throughput performance of IPv4 and IPv6 using UDP for wireless LAN networks with 802.11n and with and without security for two client-server networks were compared. For Vista-Server 2008 using open system, the 802.11n bandwidth varied from 34.6 Mbps to 172.4 Mbps for IPv4 and 30.3 Mbps to 133.9 Mbps for IPv6 while bandwidth variation using WPA2 security was 29.6 Mbps to 147.6 Mbps for IPv4 and 21.5 Mbps to 133.2 for IPv6. For XP-Server 2008 and no security, the IEEE 802.11n bandwidth varied from 39.5 Mbps to 163.9 Mbps for IPv4 and 28.5 Mbps to 150.1 Mbps for IPv6 while bandwidth variation using WPA2 security was 35.4 Mbps to 146.4 Mbps for IPv4 and 28.3 Mbps to 146.3 Mbps for IPv6.

ACKNOWLEDGMENT

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

REFERENCES

[1] S. McCann, "Official IEEE 802.11 Working Group Project Timelines - 07/22/09," 2009; http://www.ieee802.org/11/Reports/802.11_Timelines.htm.

[2] M. Oiaga, "Corporate IT Spending Feb 2009. Windows 7 Gets All the Love, Vista Gets Skipped," 2009; http://news.softpedia.com/newsImage/Windows-7-Gets-All-the-Love-Vista-Gets-Skipped-4.jpg.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

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

[10] ZTI Telecom, "IP Traffic - test & measure," http://www.zti-telecom.com.

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