The Impact of Wireless LAN Security on Performance of Different Windows Operating Systems

Samad S. Kolahi, Shaneel Narayan, Du D. T. Nguyen, Yonathan Sunarto, Paul Mani

UNITEC New Zealand
skolahi@unitec.ac.nz
snarayan@unitec.ac.nz

Abstract

This paper investigates the impact of various encryption techniques (WEP-64, WEP-128 and WPA) on performance of wireless LANs for Windows operating systems (Windows Server 2003, Windows XP and Windows Vista) and for both TCP and UDP protocols. The parameters considered are throughput and response time. The results indicate that security mechanism does influence the wireless performance and different operating systems provide various results.

Index Terms— Wireless, performance, throughput, response time, Windows operating system

1. Introduction

With the increased use of wireless local area networks (WLAN), the performance evaluation of these networks is becoming very important. As wireless uses air for transmission of data, wireless networks are not as secure as wired networks. In order to address security problem and offer confidentiality and integrity for data, various security encryption techniques are suggested. WEP-64 (Wireless Equivalent Protection), WEP-128, and WPA (WiFi Protected Access) are some of the encryption techniques suggested. Previous researchers have looked at some aspects of the influence of encryption on network performance. In [1], the impact of different wireless securities on the network performance for both TCP and UDP in Windows XP client and Windows 2000 server environment was investigated. The authors used IP-Traffic software as a tool and focused on studying IEEE 802.11b wireless protocol using a test environment with one server connected to an access point via cable and three other clients connected wirelessly to the access point. In [2], the performance of WLAN with various available security mechanisms was analysed in the IEEE 802.11b, IEEE 802.11g, and IEEE 802.11i environments. In a test bed environment, the authors in [2] increased the number of wireless nodes from one to 10 client machines and measured throughput. The authors developed and used a simulation software in Microsoft Visual C++ 6.0 and Microsoft Visual Basic 6.0 environments. In [3], the impact of security on bandwidth in IEEE 802.11g was evaluated by using a test bed consisting of one client connected to an access point via cable and three clients connected to the access point wirelessly.

To the authors' of this paper knowledge, there is no study available on impact of overheads of security techniques for most popular network operating systems such as Windows 2003, Windows XP, and Windows Vista. During September 2006 – August 2007 [4], our research shows 84.56% of desktop computer installed Windows XP operating system [4]. Recently many are installing Windows Vista to replace Windows XP on their desktop PC. The main contribution of this paper is to obtain new results when investigating the impact of the security encryption techniques on throughput and round trip delay for various commonly used operating systems discussed above.

In this study, Netperf [5] was used to measure the performance of these operating systems (Windows 2003, Windows Vista, Windows XP) in wireless LAN IEEE 802.11g environment and the performance was compared for different encryption techniques (and no encryption). Parameters investigated include throughput and RTT (round trip time) for both TCP and UDP protocols using IPv4 as the network layer protocol. Netperf [5] is the monitoring tool that can be used to measure the performance of many different types of networks as it provides test results for both throughput and end-to-end latency for either TCP or UDP protocol. Netperf can run on multi platforms such as: UNIX (all the major variants), Linux, and Windows operating systems, using command line as the interface. Netperf is commonly used by researchers to evaluate the performance of both the TCP and UDP networks, for example, researchers in [6] analyzed the TCP performance over

Ethernet LAN for Windows operating system using Netperf. Other researchers, Agarwal et al. [7], studied the wireless security protocols over the mobile IP network using Netperf as the network monitoring tool. Zeadally et al. [8] used Netperf for their research on end-to-end IPv6 protocol stack.

The organization of this paper is as follows. In next section, the network setup is discussed. Section 3 covers the results and discussions. The last sections present conclusions and future work followed by references.

.

2. Network Setup

The test bed for this study is setup as shown in Figure 1. Windows Server 2003 Enterprise Edition operating system (with Service Pack 2) was installed in both computers and various encryption techniques were implemented (no encryption, WEP-64, WEP-128, and WPA). The throughput and response time (RTT) were recorded using Netperf for both TCP and UDP. In the next phase, the same setup was used and Windows Server 2003 was replaced by Windows XP and then Windows Vista.

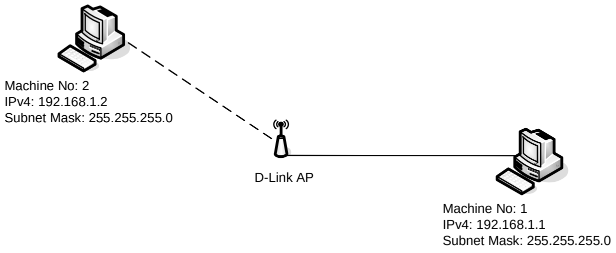


Figure 1: Network test bed

The hardware used for the experiments is two computers with Intel Pentium 4 3.00 GHz CPU, 1GB RAM, Intel Pro 100 Adapter NIC, 20 GB Seagate Barracuda series hard disk, and D-Link Airplus DWL-G520 wireless card. The access point used was D-Link 2100 with v1.01eu firmware. To maintain good signal during the experiments, the access point was located within 2 meters from both computers.

According to Killelea [9], throughput (the number of bits transmitted per unit time) depends on several conditions over the network like the processor limitations and the hardware designs. To eliminate the effect of these conditions, we benchmarked the hardware and similar set up was used for all the tests to negate the effect of the processor limitations and hardware designs. Other performance metric are characteristic parameters defined in the access point, such as:

1. Fragmentation threshold: the number of bytes used to fragment the frames with purpose to increase the transfer reliability. The frames can be fragmented in the band from 256 to 2346 bytes. 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 [3].

2. Beacons interval: the variable times in which clients meet the access point, this includes send and receive packets, and synchronism [3].

3. DTIM rate: the values that impacts receiving time of broadcast and multicast traffic for stations. The buffer traffic will be transmitted instantly after the beacon containing the list of the stations that go out from the save mode. The stations that are in the list, send other messages notifying their follow-on operation way and confirm that they are ready to receive the data [10].

4. RTC/CTS threshold: this is used to decrease the problem of the hidden stations due to distance or signal blockage [10].

We keep the above parameter values as default in all experiments for simplicity. The parameters used are in the following table:

Metrics	Value
Fragmentation thresholds	2346
Beacon interval	100
DTIM rate	1
RTS/CTS thresholds	2346

Table 1: Parameters values used in experiments

3. Results

Based on network of Figure 1, the experiments were initiated by measuring the throughput and response time for both TCP and UDP traffic in IEEE 802.11g network. For each encryption type a total of 50 runs were performed and streams of packets were generated from one computer to the other computer using Netperf as a tool. The standard deviation and averages of all the 50 records were recorded. The TCP throughput comparisons for the three windows operating system are in Figure 2.

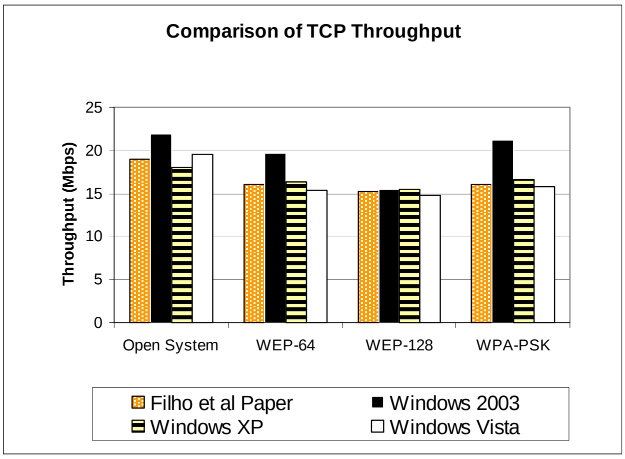


Figure 2: TCP throughput results

For TCP traffic, Windows 2003 records the highest bandwidth in all the encryption systems studied, for open system it leads at 21.9 Mbps, and for WEP-64 and WEP-128 record the highest throughputs of 19.7 Mbps and 15.5 Mbps respectively. For WPA, the Windows 2003 shows exceptionally high bandwidth of 21 Mbps and this is approximately 5 Mbps better than the second runner Windows XP. In the case of WEP-64 and WEP-128, Windows XP is again the second in bandwidth comparison with throughputs of 16.3 and 15.5 Mbps respectively. The only time Windows Vista gives better throughput than Windows XP is when no encryption is used (open system.) For the rest of the encryption systems tested, Windows Vista shows the least throughput.

Figure 2 shows that implementing the encryption reduces the TCP throughput. When WEP-64 was implemented the throughput of Windows 2003 and Windows XP was decreased by 10% but the maximum reduction of 22% was experienced by Windows Vista. In the case of WEP-128 the reduction in throughput was 29%, 14% and 24% for the Windows 2003, Windows XP and Vista operating systems. This reduction in the bandwidth was 8.7 Mbps when WEP-128 is implemented in Windows 2003. For Windows XP and Windows Vista the reduction in implementing WEP-128 was 2.4 Mbps and 3.1 Mbps respectively.

When WPA was implemented the bandwidth reductions were lower as compared to WEP-128. When implementing WPA with Windows 2003, Windows XP, and Windows Vista, the reductions were 3%, 8% and 19% respectively. We noticed only 1 Mbps reduction implementing WPA for Windows 2003 and 1.8 Mbps for Windows XP. But the least reduction in the throughput was 0.5 Mbps shown by Windows Vista when WPA was implemented.

When comparing to Filho et al [3] results, it is noticed that the results are close. In the case of WEP-64, WEP-128, and WPA, Windows XP bandwidth results was 2%, 2%, and 3% higher than Filho et al results respectively.

The results by Ezedin [11] showed that when the encryption mechanism WEP was implemented, the bandwidth was affected for both TCP and UDP traffic. The authors stated that the TCP throughput suffered a degradation of 4% when WEP-64 was enabled and 7.14% when the 128-bits key was enabled. The same trend but higher bandwidth degradation occurred in our experiment results when WEP-64 TCP traffic suffered degradation of 10% (Windows Server 2003 and Windows XP) and 22% (Windows Vista). In the case of WEP-128, the throughput experienced degradation of up to 29%.

The study by Baghaei in [1], used in IEEE 802.11b environment, showed when adding encryption to Open System, the throughput reduced by approximately 7% (WEP-64) and 10% (WEP-128) for Windows XP. Our results, using IEEE 802.11g and Windows XP, indicates 10% (WEP-64) and 14% (WEP-128) drop on throughput.

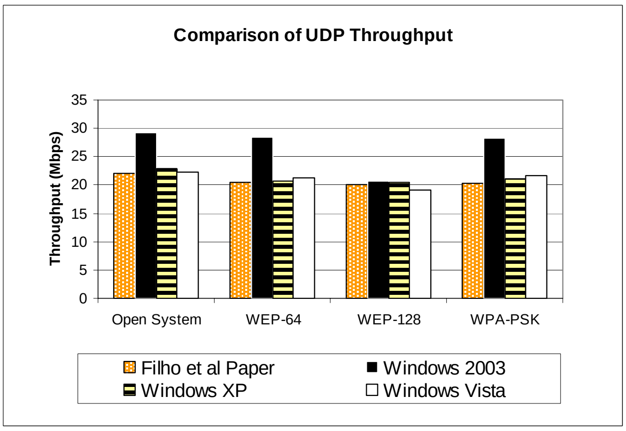
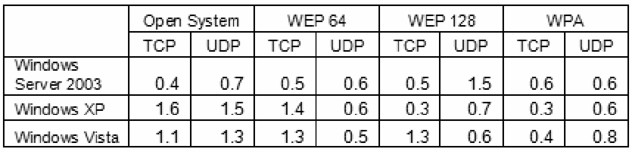


Figure 3: UDP throughput results

For the UDP traffic (Figure 3), Windows 2003 exhibits the highest bandwidths of the encryption systems studied with 29 Mbps in Open System (no security), 28 Mbps (WEP-64 and WPA), and 20 Mbps (WEP-128). Windows XP showed better throughput than Windows Vista by 3% (open systems) and by 7% (WEP-128). On the other hand, Windows Vista showed 4% higher throughput than Windows XP for WPA.

The results by Ezedin in [11] showed that in Windows Server 2003 when WEP-128 was enabled, the maximum bandwidth degradation occurred (as much as 30%) while Windows XP and Vista had 10% reduction in bandwidth. Comparing our results with Ezedin results in [11] shows similar trend when WEP-128 implemented, the throughput dropped by 29% for Windows Server 2003, 14% for Windows Vista, and 10% for Windows XP. Baghaei and Hunt results in [1] show that the throughput dropped approximately by 10% when WEP-64 and WEP- 128 were added in IEEE 802.11b. Our result confirmed this 10% reduction for Windows XP although we used IEEE 802.11g. Filho et al. [3] results showed throughput dropped by 4%, 7% and 5% when WEP-64, WEP-128 and WPA applied to Open Systems. Our results are much higher when compared with Filho, indicating 10% drop for WEP-64 (for both three operating system) and WEP-128 (for Windows XP and Vista). For WPA, both three Windows operating systems used in our study showed 10% drop while Filho result showed 5%.

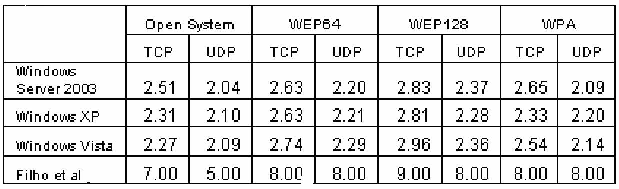
The standard deviation for the above results is shown in Table 2. Note that the standard deviations (and averages mentioned earlier) are for 50 data points.



	Open System		WEP 64		WEP 128		WPA	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
Windows Server 2003	0.4	0.7	0.5	0.6	0.5	1.5	0.6	0.6
Windows XP	1.6	1.5	1.4	0.6	0.3	0.7	0.3	0.6
Windows Vista	1.1	1.3	1.3	0.5	1.3	0.6	0.4	0.8

Table 2: Standard deviation for throughput

Results of round trip time (RTT) comparisons for the three windows operating systems and the results of the study by Filho et al [3] are shown in Table 3.



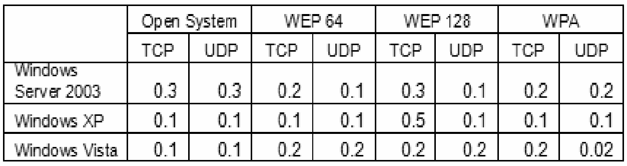
	Open System		WEP64		WEP128		WPA	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
Windows Server 2003	2.51	2.04	2.63	2.20	2.83	2.37	2.65	2.09
Windows XP	2.31	2.10	2.63	2.21	2.81	2.28	2.33	2.20
Windows Vista	2.27	2.09	2.74	2.29	2.96	2.36	2.54	2.14
Filho et al	7.00	5.00	8.00	8.00	9.00	8.00	8.00	8.00

Table 3: RTT results (msec)

Overall, the TCP traffic had higher RTT than UDP traffic and the highest RTT occurred in WEP-128 for both TCP and UDP traffic (Table 3). The results showed Windows Vista had the least RTT in Open System for both TCP and UDP. For TCP, Windows Vista RTT was 11% less than Windows Server 2003 and 2% less than Windows XP. For UDP the RTT reductions were respectively 2% and 0.5%. However, when encryption techniques were applied, Windows Vista had the highest RTT compared to other operating systems. In case of WEP-64 and WEP-128 for TCP traffic, Windows Vista had 4% higher RTT compared to Windows Server 2003 and Windows XP while for UDP the increased RTT was respectively 0.4% (Windows Server 2003) and 3% (Windows XP). When applying WPA with TCP traffic, Windows Vista experienced less RTT (by 4%) than Windows Server 2003 and higher RTT (by 8%) compared to Windows XP. On the other hand, when applying WPA to UDP, Windows Vista surprisingly had higher response time (by 2%) than Windows Server 2003 and less response time (by 3%) than Windows XP.

Filho et al [3] RTT results were much higher than our results. In average, results of our experiments for round trip time was approximately 2 ms while Filho et al results was up to 9 ms when encryptions was implemented in the network. Since Filho et al paper does not describe their testing environment clearly (distance, shadowing, equipments, etc.), this dissimilarity could be because of the different factors in Filho et al experiments which affect the response time. Moreover, the difference in results can be attributed to the different performance monitoring tools used to conduct these experiments.

The standard deviation of response time results is shown in Table 4.



	Open System		WEP 64		WEP 128		WPA	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
Windows Server 2003	0.3	0.3	0.2	0.1	0.3	0.1	0.2	0.2
Windows XP	0.1	0.1	0.1	0.1	0.5	0.1	0.1	0.1
Windows Vista	0.1	0.1	0.2	0.2	0.2	0.2	0.2	0.02

Table 4: Standard deviation for RTT

4. Conclusion

The performance in terms of throughput and RTT is affected when encryption technique is implemented, especially WEP. However, WEP provided less throughput when the key size increased because WEP added the Initial Value of its symmetric encryption key to the data sent and it used the rest of the key bits to initiate a key scheduling algorithm that generated a stream key for the stream data to be XORed [2]. As a result, WEP created some delay for sending/receiving encrypted/decrypted data. WPA supplied better throughput than WEP in the IEEE 802.1g wireless networks. Another interesting fact is that Windows Vista, latest operating system from Microsoft, did not provide better performance in terms of bandwidth and RTT than its predecessor in IEEE 802.1g wireless network. Adding WEP-128 had most impact in Windows 2003 while it did not have much impact when Windows XP or Vista was used. Windows 2003 records the highest bandwidth, for both TCP and UDP, in all of the encryption systems studied.

5. Future Work

The research team implemented only four common security mechanisms from many security mechanisms available in IEEE 802.11g wireless network. For future work, the research team would like to perform similar test using the following security mechanisms: MAC address authentication, WEP authentication only, WEP authentication with 40-bits key, WPA2, EAP-MSCHAP2 and EAP-TLS. Moreover, VPN is becoming more popular these days. VPN with various encryptions over wireless connection is an area of future work. Some examples are: Open System (no security), PPTP tunnelling with CHAP, IPSec tunnelling with CHAP, IPSec with CHAP and DES, IPSec with EAP-TLS and DES, IPSec with CHAP and 3DES, and IPSec with CHAP and 3DES.

6. References

[1] N. Baghaei and R. Hunt, "IEEE 802.11 wireless LAN security performance using multiple clients," in *Proceedings, The 12th IEEE International Conference on Networks, 2004. (ICON 2004)*, pp. 299-303 vol.1.

[2] G. Z. Gurkas, A. H. Zaim, and M. A. Aydin, "Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks," in *International Symposium on Computer Networks, 2006,* pp. 1-5.

[3] 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," in *IFIP International Conference on Wireless and Optical Communications Networks, 2007. WOCN '07.* , pp. 1-5.

[4] NetApplications, "Top operating system market share trend for September, 2006 to August, 2007," http://marketshare.hitslink.com/report.aspx?qprid=5&qpdt=1&qpct=4&qptimeframe=M&qpsp=92&qpnp=12.

[5] R. Jones, "Netperf 2.4.3," http://www.netperf.org/netperf/.

[6] K. A. Gotsis, S. K. Goudos, and J. N. Sahalos, "A test lab for the performance analysis of TCP over ethernet LAN on windows operating system," *IEEE Transactions on Education,* vol. 48, pp. 318-328, 2005.

[7] A. K. Agarwal, J. S. Gill, and W. Wenye, "An experimental study on wireless security protocols over mobile IP networks," in *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th,* 2004, pp. 5271-5275 Vol. 7.

[8] S. Zeadally, R. Wasseem, and I. Raicu, "Comparison of end-system IPv6 protocol stacks," *IEE Proceedings Communications,* vol. 151, pp. 238-242, 2004.

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

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

[11] 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," in *Innovations in Information Technology, 2006,* pp. 1-5.