Performance Analysis of Evolving Wireless IEEE 802.11 Security Architectures

Mohd Asri Bin Mohamad Stambul
Universiti Kebangsaan Malaysia
Bangi , Selangor
Email: mdasri.stambul@yahoo.com

Abstract

IEEE 802.11 Wireless LAN (WLAN) have gained increasing popularity in recent years, providing users with both mobility and flexibility in accessing information. Because of the poor performance, users always neglect the security parts in WLAN configuration setup. The WLAN performance depended on the technical options chosen during encryption, authentication and re-keying configuration. This research investigates the performance analysis of a range of security levels based upon variations of WEP, WPA and WPA2 in a variety of Wireless LAN architectures. This research also describes a performance analysis measured over a range of experiments run on testbed and using some tools.

1. Introduction

Wireless networks are becoming popular nowadays due to its mobility, portability, flexibility and seamless connectivity. Many people using this wireless networks especially in public places like shopping malls, airports, coffee cafes, hotels and in universities. However, wireless networks are naturally more vulnerable to attack and can suffer from variable performance in comparison with wired network.

IEEE 802.11i (WPA2) was developed to replace previous version of wireless LAN security protocol, WEP (Wired Equivalent Piracy) which was found weakness and vulnerabilities of its implementation. This paper describes the performance analysis of IEEE 802.11i and its variants in Wireless LANs and compares the result with WEP and WPA (WiFi Protected Access) variants.

In this review paper, we divided into a few section. Section 2 describes the issues that we have concluded from this paper. Section 3 highlights about the objectives of this paper while Section 4 describes of the previous related studied were done before. Section 5 describes about the methodology to run this experiments and the security levels tested. Section 6 were discuss the result from the experiments and lastly Section 7 covers the conclusions.

2. ISSUES

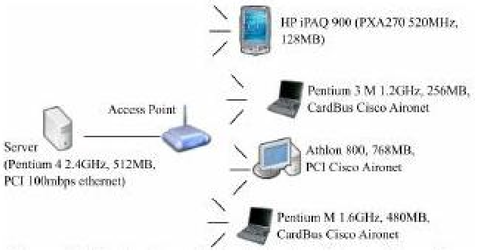
The reduced in performance has been a common reason for people to limit the usage of security in Wireless LAN equipment such as wireless PCs and embedded devices such as PDAs. Existing solutions for wireless LAN networks have been exposed to security vulnerabilities and previous study has addressed and evaluated the security performance of IEEE 802.11 wireless networks using single sever client architecture and simple traffic models.

The previous performance result has depended on technical options chosen for for encryption, authentication and re-keying. There are several protocol of wireless LAN or IEEE 802.11 such 802.11a, b, g and the latest is 802.11n. In terms of security, several security protocols related with wireless network was introduced such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and the latest IEEE 802.11i (also known as WPA2). Wireless LAN has more exposed to security vulnerabilities compared to wired network. For example, WEP protocols were heavily criticized because of the poor security handling, Adam Stubblefield and ATT publicly announced the first verification of the attack on WEP protocol. In the attack they were able to intercept transmissions and gain unauthorized access to wireless networks [5].

3. OBJECTIVE

This paper describes the performance analysis and practical measurement of a range of security levels based upon variations of WEP, WPA and WPA2 in a variety of Wireless LAN architectures. The results were compared from previous studies based on WEP (Wired Equivalent Privacy) and WPA (WiFi Protected Access) variants. The performance variation in operating performance is not only affected by the specific security protocol used (along with variables such as key length and reauthentication) but also network loading as well as the degree to which the security solutions are implemented in hardware.

And lastly this paper also investigates into the performance of the implementation and effects of the WPA2 security specification on the throughput of wireless local area networks and compares this performance with that of earlier existing WEP and WPA architectures.


HP iPAQ 900 (PXA270 520MHz, 128MB)
Pentium 3 M 1.2GHz, 256MB, CardBus Cisco Aironet
Access Point
Server (Pentium 4 2.4GHz, 512MB, PCI 100mbps ethernet)
Athlon 800, 768MB, PCI Cisco Aironet
Pentium M 1.6GHz, 480MB, CardBus Cisco Aironet

4. RELATED WORK

Previous studied by Barka [3] describes the effects of WEP security protocols on IEEE 802.11g wireless network performance. The result shown that the implementation of WEP security protocol will decreased the network performance.

Baghaei [2] extended this research by using multiple clients and evaluated with different security architectures. It also evaluated the effects of packet length on the network throughput with different security architectures. This study showed that WEP encryption reduced network performance when the network was congested. Network performance was also reduced as more clients were added to the network.

5. METHODOLOGY

A. Security Levels The following seven security levels were used to test the performance of the wireless network testbed. Each level has different degree of security and complexity. Each level represents a newer, more complex degree of security than the one preceding. The security layers defined are:

i. No Security ii. WEP shared key authentication and 40 bit encryption iii. WEP shared key authentication and 104 bit encryption iv. WPA with PSK authentication and RC4 encryption v. WPA with EAP-TLS authentication and RC4 encryption vi. WPA2 with PSK authentication and AES encryption vii. WPA2 with EAP-TLS authentication and AES

B. Network Performance Measurement Testbed and Traffic Generator Clients and a server were configured as illustrated in Figure 1. IP traffic generation tool, IPTraffic [5] was used in this test because its ability to generate TCP/IP and UDP/IP traffic over a range of statistical profiles and loads.

The experiment were using server that was ran Microsoft Windows Server 2003 Enterprise Edition with Service Pack 1 as a operating system. This server operated as a RADIUS server via Microsoft's Internet Authentication Service. All PC clients were running Windows XP Professional with Service Pack 2. A Cisco Aironet 1130AG series access point, operating in the IEEE 802.11a 5GHz 54 Mbps mode, was connected to the server via a 100 Mbps Ethernet connection. As all of the PC-based wireless network devices used in the experiment were using Cisco-based. This can avoid vendor interoperability problems. The wireless network adapters in the clients were based on the Atheros AR5212 and AR5112 chipsets, which like the access point, have hardware accelerated encryption. None of the computers were running any processes which could affect processor or network utilisation. An HP iPAQ 900 was also included in the experiments as a client to evaluate the impact of security on small embedded devices.

This experiment using two set of testing, the first set were synthetic benchmark tests which recorded the throughput of traffic flow between single and multiple client PCs, representing loaded and unloaded networks. For this testing, IPTraffic was used as the traffic generator and was configured as follows:

Total number of packets sent to a client per synthetic test: 20,000. This number ensured that there were no effects from transient conditions. Traffic Protocol: TCP. TCP Window: 8192 bytes (default for Windows XP). Packet payloads using synthetic throughput tests: A payload of 1460 bytes corresponds to the maximum payload of a TCP segment.

The second set of experiments consisted of downloading a large (11.2 MB) video file using the Cerberus FTP server. All results were analysed using ANOVA (Analysis of Variance) at the 95

6. RESULT

While several experiments were performed, only the results from the 1460 byte TCP synthetic transfer and FTP transfer are described here, as these can be directly compared with results found in the earlier studies.

A. Effects on Throughput In Figure 3a, the single client (light load) bars show the mean throughput for each of the security levels defined in Section 3.1. The differences are statistically significant for the single client-to-client transfer (F6,24 = 11.09, p ¡ 0.01). While statistically significant, in practical network usage, this difference is not large. Over all security levels the mean throughput is 8.12 Mbps (s.d. 0.26). A standard deviation of 0.26 Mbps is a relatively small variance when considering the overall mean transfer rate.

The results in Figure shows that different security levels have little effect on the throughput when modern hardware implementations of the security protocols are used. This result slightly different from the findings in [2] (Figure 2), which found that enabling the various security protocols radically decreased the throughput.

The second set of experiments involved an 11.2 MB FTP file transfer between Wireless LAN and PDA clients (Figure 1). Result shown performance did not degrade much across the various security levels. There are no statistically significant differences between the security levels (F6,24 = 2.00, p = 0.11). The mean throughput across all security

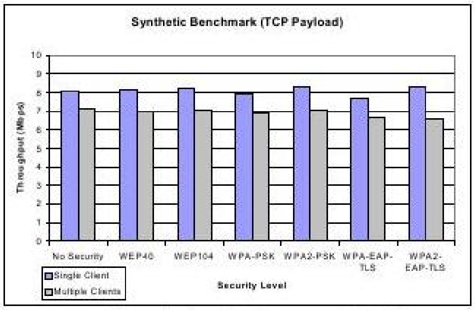


Figure 1. TCP Payload

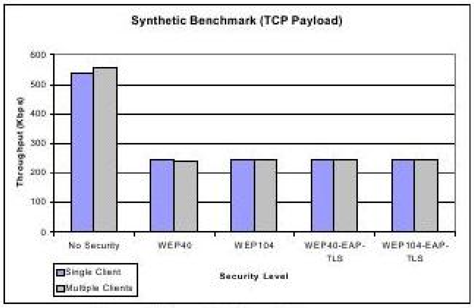


Figure 2. TCP Payload [2]

levels is 9.73 Mbps (s.d. 0.29) for PCs, while for the PDA client it is 2.40 Mbps (s.d. 0.07). Again these results differ significantly from [2] (Figure 2), where the stronger security levels resulted in considerably lower throughput.

B. Effects with Multiple Clients in Wireless LANs These experiments were continued with multiple clients, similar results are found where a pair of Wireless LAN PC clients were configured to saturate a third wireless PC. In Figure 3, the multiple client bars show the total mean throughput of both senders. The combined throughput of both clients in Figure 1 is lower than the throughput of the single client test, as the access point was configured to operate at 24 Mbps in order to produce saturation for these tests. The differences between the security levels are again statistically significant; (F6,24 = 2.82, p ¡ 0.05). As with the previous test, in practical terms this difference is not large; across all security levels, the mean throughput was 6.91 Mbps (s.d. 0.30).

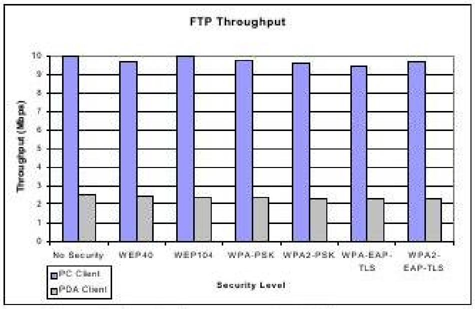


Figure 3. FTP Throughput

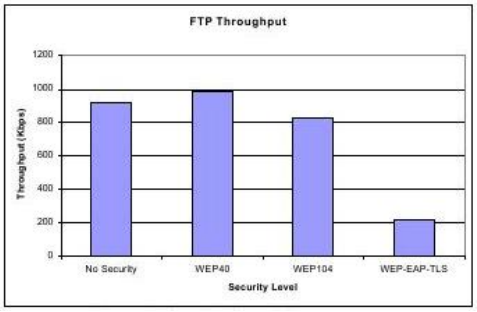


Figure 4. FTP Throughput [3]

Overall result shown various security levels have different effects on the throughput depending on the number of clients on the network. For the synthetic TCP transfer by number of clients, the interaction is significant (F6,24 = 3.20, p ¡ 0.05). Figure 3 shows the differences in throughput between single and multiple client transfers. The WPA2-EAP-TLS security level demonstrates the largest decrease in throughput, dropping by 1.68 Mbps, while the other security levels drop by an average of 1.21 Mbps. This test shows that WPA2-EAP-TLS drops by almost 0.5 Mbps more than the other security levels when more clients are connected to the network. This difference corresponds to roughly 7

7. CONCLUSION

This paper aimed to investigated the effects of the IEEE 802.11i security specification on the performance of wireless networks mostly where the security protocols were implemented in the hardware. It further aimed at drawing comparisons with the results of earlier experiments.

The results show that wireless network performance in Wireless LANs is basically unaffected over the range of security levels applied, provided that the protocol and algorithm implementation is primarily hardware- based. This is contrast with the results findings in [2] and [4], which found that performance decreased as more complex security levels were introduced.

Acknowledgment

I would like to thanks to Mr. Mohd Zamri Murah for introducing Latex software in order to write a paper. The preparation of this important document would not have been possible without the support, hard work and endless efforts from a number of individual.I would also like to gratefully acknowledge the support of some very special person in my

life, my belove wife. She helped me immensely by giving me encouragement and love.This paper is end of my journey in finishing LateX Assignment.

References

[1] A. Gin A and R. Hunt,*Performance Analysis of Evolving Wireless IEEE 802.11 Security architectures ,LaTeX*,International Conference On Mobile Technology, Applications, And Systems, 2008.

[2] N. Baghaei and R. Hunt, *IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients,LaTeX*,Networks, 2004. (ICON 2004). Proceedings. 12th IEEE International Conference, 2004.

[3] E. Barka, M. Boulmalf, A. Altenji, H. Al Suwaidi, H. Khazaimy and M. Al Mansouri, *Impact od Security on the Performance of wireless Local Area Networks, LaTeX*,United Arab University, 2006.

[4] A. Agarwal and W. Wang, *Measuring Performance Impact of Security Protocols in Wireless Local Area Networks,LaTeX*,The Second International Conference on Broadband Networks. October ,2005. Boston, Massachusette, USA.

[5] IPTraffic, http://www.zti-telecom.com/EN/IPTraffic_TM_KeyFeatures.html