Relative Encryption Overhead in 802.11g Network

Anuj Tripathi (anujt@it.iitb.ac.in), Om P Damani (damani@cse.iitb.ac.in)
Dept. of Computer Science & Engineering, IIT Bombay, India

Abstract— **We present a performance study of security overheads in 802.11g networks. At 54 Mbps, the security overhead becomes significant in single client scenarios for many of the popular security protocols. However, we find that the most secure protocol, WPA-2, is also the protocol with the lowest security overhead.**

Index Terms— **Wireless Networks, Security Overhead.**

I. INTRODUCTION

802.11 wireless networks are fast becoming the preferred choice for LAN environments. Given their limited bandwidth (54 Mbps in 802.11g) and the need for security in wireless setting, it is necessary to understand the relative overhead of different security protocols.

We present a performance study of security overheads due to three widely used security protocols in 802.11g networks. We have considered Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and WPA2. In WEP, we experimented with both 64-bit encryption and 128-bit encryption. In WPA mode, we have worked with WPA-PSK (Pre-Shared Key) mode with both TKIP and AES. In WPA2, we have considered AES encryption in PSK mode.

We find that at lower data rate (802.11b-11Mbps) encryption overhead is below 0.5% but at higher rate (802.11g- 54 Mbps) it is over 10 % for some of the popular security protocols. Our main finding is that the most secure protocol, WPA-2, is also the protocol with the lowest security overhead. This is not entirely unexpected since WPA-2 employs special hardware for integrity check.

In section II we present the background of various protocols. Section III describes related work. In Section IV and V, we present our aim and the experimental setup used. In section VI, we present our results for single client and multiple clients. Section VII contains an analysis of the results. Section VIII discusses the difficulties faced by us in conducting the experiments and Section IX concludes the paper.

II. BACKGROUND

In this section we will briefly see salient features of the protocols under consideration. WEP is a security scheme provided in the initial 802.11 protocol for providing privacy, integrity, and authentication. WEP uses the concept of a shared key that is same for all the users in the network. To make encryption keys different for different packets, WEP used a 24-bit initialization vector (IV). One of the major weaknesses of WEP is the small size of the initialization vector. Not surprisingly, WEP was found to have several vulnerabilities [2]. To address these vulnerabilities, Task Group-i (TGi) [1] came up with a new security protocol called WPA.

. WPA has two variants: AES and TKIP. AES (Advanced Encryption Standards) is a stronger encryption scheme than RC4, the encryption scheme in WEP. TKIP makes use of the RC4 algorithm for encryption and hence is backward compatible with the WEP hardware.

WPA2 made further changes to WPA by making AES encryption mandatory and using CCMP in place of MIC for integrity check [1].

WEP has been around for long, before WPA came in to existence. Due to WEP's widespread use, many chips have RC4 encryption implemented at the hardware level. This led to the wide acceptance of TKIP which is backward compatible with WEP and can be implemented by using a simple firmware/software upgrade over WEP. As per [7], in 2006, in Seattle, 85% people use WEP and 14 % WPA with TKIP. Hence it is important to compare the performance of WEP, TKIP, and WPA-2.

III. RELATED WORK

Wong [2] and Baghaei et. al. [4] discuss the impact of WEP combined with VPN on 802.11b networks. Carter [5] studies authentication delays and TKIP overheads in combination with authentication protocols like PEAP in 802.11b networks. WijeSinha et al [9] studied the behavior of security protocols with UDP in 802.11g networks. In contrast, we focus on MAC overheads alone in 802.11g networks. We adapt the methodology followed by Carter [5] and Atheros [8] for taking measurements in Wireless LAN. Our work is the first complete known study of the overhead caused due to *encryption schemes* like WEP-64 bit, WEP-128 bit, WPA and WPA2 in *802.11g* network for TCP and UDP.

978-1-4244-2751-2/08/$25.00 ©2008 IEEE

IV. OVERHEAD ANALYSIS AND MEASUREMENT

To analyze the bit overheads, note that the frame body (MSDU: MAC Service Data Unit) can have a maximum size of 2304 bytes in 802.11 networks. WEP, TKIP, and WPA-2 have bit overheads of 8, 20, and 16 octets respectively. Therefore, theoretically the minimum security overhead due to WEP, TKIP and WPA-2 should be approximately 0.34%, 0.86% and 0.69%, respectively. Considering the fact that generally wireless networks in turn are connected to an IP network, the Maximum Transfer Unit (MTU) is most likely to be 1500 bytes. On reducing the packet size from 2304 bytes to 1500 bytes, the security overhead increases to 0.53%, 1.33%, and 1.06% respectively. When we consider that there are many small packets like acknowledgements, beacons, probe requests and responses, the average packet size becomes smaller than 1500 bytes which implies even higher overhead.

These values do not take into consideration the overhead due to delays caused by processing of security parameters. For instance, there are steps like key mixing, MIC (message integrity code) generation, and encryption/decryption which have their own overheads. We attempt to measure these overheads in a 54 Mbps 802.11g environment. We target the throughputs at the user level for TCP and UDP connections, separately. Using UDP gives the maximum possible throughput as TCP has its own overheads of setting up the connection.

We define the security overhead as "*Extra amount of work done with a security scheme enabled, over the work done to push the same data without any security.*"

To measure the overhead, we measure the throughput with and without encryption for both TCP and UDP traffic. Let the throughput without encryption be T_1 and the throughput with encryption be T_2 for any given transport protocol.

Let W_1 (W_2) be the amount of work done and T_1 (T_2) be the throughput observed without (with) security enabled. Let Δ be the extra work due to the security protocol. It can be seen that

$$W_1 = \frac{1}{T_1} \qquad W_2 = W_1 + \Delta = \frac{1}{T_2}$$

Overhead can be given as $\dfrac{\Delta}{W_1}$

So the overhead comes to

$$Overhead = \frac{T_1 - T_2}{T_2}$$

V. EXPERIMENTAL SETUP

We have carried out the measurements for both one and two clients.

In the single client experiment, we send data from a wireless client A to a server B. The connections are as shown in the figure 1. Client A is connected to the access point AP through a wireless 802.11g connection. AP is connected to a switch through an Ethernet backbone which in turn is connected to a server B. Table 1 shows the configurations of the components used.

For two client scenario, we use a setup same as the one for single client, but with one more client C which also sends data to the server B.

To measure the bandwidth available at the user level, we use IPerf [3]. IPerf is one of the most lightweight tool available for performance measurement.

The results were taken at frequent intervals, to avoid effects of the changes in the settings and due to time. We took 20 readings for each setup and the five readings closest to the average were taken as final.

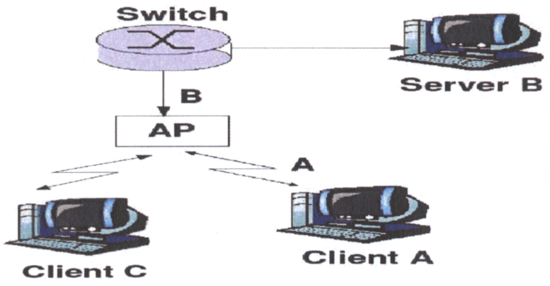

Fig.1 Experimental Setup.

Table.1. Configurations in Experimental Setup

Client A	Intel P4 CPU 3.2Ghz running Windows XP with SP2
Wireless card at A	Dlink- DWL G510
Access point AP and Switch	Linksys WRT54G version 7
Client B	Intel P4 CPU 3.2Ghz running Linux 2.17
Client C (Second Client)	Intel 1.7Ghz running MS XP SP2
Wireless Card at C	Linksys WPC54G

While calculating the UDP throughput, we attained maximum throughput with the following parameters. We pushed data at 140 Mbps (-b parameter in IPerf for bandwidth) and ran the experiment for 20 minutes. This gave the network enough time to stabilize. The packet size which gave maximum throughput was 1472 bytes. For TCP, IPerf does not need any parameters.

VI. RESULTS

Tables 2 and 3 show the average throughput and security overheads in 802.11g network for single client using TCP and UDP respectively. As expected, security overheads in 8021.11g networks are much more compared to 802.11b network, where the overhead for WEP-64 bit is only 0.45%. In 802.11g, at 54 Mbps the overhead for WEP-64 comes out to be 5.39% for TCP and 8.82% for UDP. As expected, WPA-TKIP has a higher overhead than WEP. It is higher than WEP by almost 4-7%. The most important result is that for AES in both WPA and WPA2. Despite having higher security features its overhead is lesser than TKIP.

Tables 4 and 5 show the average throughput and security overheads for two clients using TCP and UDP respectively. The security overhead drops considerably for the two client scenarios. For instance in UDP results for WPA-PSK the overall overhead comes down from 15.16% to 4.39%. A similar case can be seen for other protocols. This can be attributed to the slower data rate at the individual clients due to the sharing of the network bandwidth. At low bandwidths, the security protocol is not a bottleneck. Moreover AES encryptions in both WPA and WPA2 have almost nil CPU overhead.

Table.2. Security Overhead using TCP for single client

	Avg. Throughput In (Mbps)	Overhead
No Security	25.4	-
WEP-64	24.1	5.39%
WEP-128	23.72	7.08%
WPA-TKIP	23.26	9.20%
WPA-AES	24.26	4.69%
WPA2-AES	24.26	4.69%

Table.3 Security Overhead using UDP for single client

	Avg. Throughput In (Mbps)	Overhead
No Security	34.78	-
WEP-64	31.96	8.82%
WEP-128	32.08	8.41%
WPA-TKIP	30.2	15.16%
WPA-AES	34.08	2.05%
WPA2-AES	33.68	3.26%

VII. RESULTS ANALYSIS

We can draw the following inferences from the above results:

- The most secure protocol WPA2-AES is also the one with least overhead. The hardware for WPA and WPA2 supports CCMP for integrity check, making it faster than TKIP, which performs integrity check in software. WEP does not employ integrity check. WPA2 also benefits from better pipelining and pre-caching of keys in PSK mode.
- Even at the lowest level of encryption (64 bit), WEP has a considerable overhead of 8.82%, in the single client scenario. For both TCP and UDP, the overheads are not very different for WEP-64 and WEP-128. This indicates that WEP key size can be increased much more before it causes further noticeable performance hit.
- WPA-TKIP has the highest overhead.
- On increasing the number of active clients, the data rate at each client decreases. Hence the cpu cycles consumed for security purposes is no more a bottleneck and the overhead decreases drastically. For instance, we find the drop for WPA-PSK overhead in TCP from 9.20% for single client to 2.49% to for two clients. It can be safely presumed that as the number of active client increases, the individual data rate at each client will drop and hence security will not be a bottleneck.

During the experiments we came across an anomaly. As per [8], the maximum ideal UDP throughput for 802.11g networks should be 30.3 Mbps, but in our experiments we got the throughput to be over 33 Mbps. This could be attributed to any of the following:

1. 30.3 Mbps itself may not be the right figure.
2. IPerf might have some flaws in measuring the exact throughput.

VIII. EXPERIMENTAL DIFFICULTIES

We chose Dlink g510 for our experiments as it is supposed to have a driver support for Linux. G510 is a RALink based driver. Rt61pci driver is supposed to be running the card on linux. We faced the following problems in its installation :

- Rt61pci installation instructions did not work. After a lot of debugging we found that this driver had problems with G510. The solution was to install the drivers available at mad-wifi.
- The card once installed showed association with the access point but did not send any data across. On debugging we found that the driver crashed after a successful association.
- We solved this problem by using Ubuntu Linux. Ubuntu supports auto installation and plug-n-play support for different hardwares. The card still did not work and this time there were not any

associations too. It showed the card to be installed but could not scan for access points in vicinity.

- Through discussion lists we found that the card works easily with Ubuntu-dapper version. With this version, the card worked with the first time install but on changing any of the parameters (like IP or security policies) the card stopped working. On rebooting the system, the system hung at network starting stage.
- A brute solution to this problem which we later discovered was to use Live CD of linux and install the card afresh every time we need to change a parameter.

We also profiled the kernel to find the bottlenecks in various protocols. After spending considerable time in getting *Oprofil* tool to work, its limitations in profiling kernel at a high granularity betrayed us. We plan to take this up again in future as better tools become available.

IX. CONCLUSIONS

At the rate of 11 Mbps, the security schemes do not cause much overhead. At 54 Mbps, the security overhead becomes significant in single client scenarios for many of the popular security protocols. With the advent of even faster networks like 802.11a TURBO, which has a data rate of 108 Mbps, the security overhead will become even more pronounced and needs to be explored further.

However, the AES implementation shows that right hardware and careful coding can reduce the security overheads considerably even in high bandwidth networks.

REFERENCES

[1] TGi. (2002).Task Group 802.11i, IEEE,Inc. http://www.ieee80211.org/11 .

[2] Wong J. (2002). *Performance Investigation of Secure 802.11 Wireless LANs:Raising the Security bar to which level?*, Masters Thesis, University of Canterbury, Newzealand,2003,http://www.cosc.canterbury.ac.nz/research/reports/MastTheses/2003/mast_0301.pdf.

[3] Iperf, http://dast.nlanr.net/projects/iperf.

[4] N. Baghaei, R. Hunt, "*IEEE 802.11 Wireless LAN Security using Multiple Clients*", Proc. of. 12th IEEE Intl Conf on Networks, 2004.

[5] Harold Lars McCarter, *Analyzing Wireless LAN Security Overhead*, Masters Thesis, Virginia Polytechnic Institute and State University, 2006, http://scholar.lib.vt.edu/theses/available/etd-04202006-080941/unrestricted/mccarter_thesis.pdf

[6] Wijesinha A, Song Y, Krishnan M, Mathur V, Ahn J and Shyamsunder V, *Throughput measurement for UDP traffic in an IEEE 802.11g LAN.* Proc. 6th Intl. Conf. on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SAWN'05), 2005.

[7] Andrea Bittau, Mark Handley, Joshua Lackey, *The Final Nail in WEP's Coffin,* Proc. of the 2006 IEEE Symposium on Security and Privacy.

[8] ATheros, Methodology for Testing Wireless LAN Performance, http://www.super-ag.com/collateral/atheros_benchmark_whitepaper.pdf

[9] Wijesinha A, Song Y, Krishnan M, Mathur V, Ahn J and Shyamsunder V, *Throughput measurement for UDP traffic in an IEEE 802.11g LAN.* Proc. 6th Intl. Conf. on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SAWN'05), 2005.

Table.4 Security Overhead using TCP for two clients

	Client	**Avg. Throughput In (Mbps)**	**Total**	**Overhead**
No Security	A	11.08	25.58	-
	C	14.5		
WEP-64	A	10.96	24.96	2.47%
	C	14		
WEP-128	A	11.12	24.96	2.47%
	C	13.84		
WPA-TKIP	A	10.08	24.96	2.49%
	C	14.88		
WPA-AES	A	10.07	25.37	0.84%
	C	15.4		
WPA2-AES	A	10.76	25.28	1.17%
	C	14.52		

Table.5. Security Overhead using UDP for two clients

	Client	**Avg. Throughput In (Mbps)**	**Total**	**Overhead**
No Security	A	15.74	35.66	-
	C	19.92		
WEP-64	A	16.34	34.6	3.06%
	C	18.26		
WEP-128	A	14.42	34.36	3.78%
	C	19.94		
WPA-TKIP	A	15	34.16	4.39%
	C	19.16		
WPA-AES	A	14.16	35.36	0.84%
	C	21.2		
WPA2-AES	A	14.88	35.46	0.56%
	C	20.58		