This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.

Impact of encryption on the Throughput of Infrastructure WLAN IEEE 802.11g

Ezedin Barka, Mohammed Boulmalf

United Arab Emirates University
P.O. Box: 17555
Al-Ain, UAE

ABSTRACT — This paper investigates the impact of security on the performance of WLAN. More specifically, it analyzes the impact of applying encryption used by the well-known security protocol Wired Equivalent Privacy (WEP) on the throughput over an Infrastructure WLAN, IEEE 802.11g.

This paper also addresses the different issues related to the security protocols currently used in WLAN IEEE 802.11g and demonstrates how these issues affect the final results of the experiments conducted. The main result is that the security adds moderate degradation on the throughput that may affect some applications over infrastructure WLANs.

***Index Terms* — WLAN, WEP, Infrastructure Networks, Wireless Security.**

I. INTRODUCTION

The importance of Wireless Local Area Network (WLAN) was solidly established based on the constantly increasing number of clients that depend on the benefits provided by the wireless environment. However, the fact that wireless communication is based on broadcast radio frequency (RF) raises critical questions related to the security of communication on WLAN.

The introduction of certain security protocols that are specifically implemented for WLAN provided an enhancement to the confidentiality, integrity and authentication levels of the communicated traffic between different entities in the wireless environment.

The main contribution of this paper is analyzing the effect of adding encryption techniques of the well-known WLAN security protocol, Wired Equivalent security Protocol (WEP) to the wireless traffic on the overall WLAN performance. These analyses are carried out over actual experiments on IEEE 802.11g wireless test bed environment, by enabling WEP on different scenario with different keys sizes and then analyzing the throughput variation of different TCP and UDP traffic. The work in this paper starts by setting a test bed and analyzing the initial results to create a baseline, then conducting actual experiments and compare the results from the different experiments.

The rest of the paper is organized as following:
Section two provides a background on the different technology standards used in wireless LANs today; it describes some of the security issues facing WLANs, and presents some of the well known security protocols used for addressing these issues. Section three describes the conducted experiments and analysis their results. Section four introduces some related work, and finally, Section five concludes this paper.

II. WIRELESS LAN STANDARDS

A. Wireless Standards

There is several wireless networking standards discussed in the literature, and others that are considered proprietary. The following is a list of some the IEEE wireless standards:

1. 802.11b: This standard is the first widely accepted wireless networking standard, and has the following features:
   - Operates at 2.4 GHz band.
   - Provides a maximum signaling rate of 11 Mbps.
   - Average throughput in the range of 4 to 6 Mbps.
   - Provides maximum range about 76 meters when it operates at the lowest speed, and about 33 meters when it operates at the highest speed.
   - Supports Wired Equivalent Privacy (WEP) for confidentiality of data transmitted over the WLAN.

1525-3511/07/$25.00 ©2007 IEEE

2. 802.11a: This standard operates at 5 GHz band, and provides signaling rates up to 54 Mbps, with effective throughput in the range of 20 to 25 Mbps under average loads. Furthermore, 802.11a's maximum range is about 46 meters at the lowest speed, and about 23 meters at the highest speed. Unlike the 2.4 GHz band, the 5 GHz band is relatively free of interference. In addition, most of 802.11a's devices nowadays are backward compatible to 2.4 GHz, thus they can operate in both bands [1]. Moreover, IEEE 802.11a takes advantage of the size of this band to define only non-overlapping channels. Some countries make four channels available, some make eight, and others make even more for data networking.

3. 802.11g: The IEEE 802.11g standard offers the speed of 802.11a, the range of 802.11b, and backward compatibility of 802.11b. It uses the 2.4 GHz band but provides signaling rates of 6 to 54 Mbps. Moreover, it achieves its speed by using orthogonal frequency division multiplexing (OFDM) modulation, which is a technique that distributes the data to be transmitted into smaller pieces. In summary, the 802.11g standard is better than 802.11b and 802.11a in data transfer speed and in range, however, it suffer from the same interferences from the Bluetooth devices that operates in the same radio frequency [2][3]. Also, one of the limitations is being limited to maximum 3 channels without overlapping.

4. 802.11i: This standard is considered to be an enhancement of the current 802.11 MAC for providing improved security. It is a draft standard that describes two new security schemes for 802.11a, 802.11b and 802.11g WLAN standards. The first scheme is the Wi-Fi Protected Access (WPA) with some added options that will allow most WEP capable devices to be made 802.11i-compliant via firmware upgrades. The second scheme, which is called Robust Security Network (RSN), will require extra processing power, and therefore requires new hardware, to cope with the well-known Advanced Encryption Standard (AES).

B. Security in WLAN

Unlike its wired network counterpart, where the data remains in the cables connecting the end devices, the transmission in a wireless network takes the form of broadcast radio frequency (RF) signals, which uses the open air as a medium for its movements. Hence the broadcast nature of WLAN introduces a greater risk from intruders who may gain unauthorized access to, or even corrupt, the transmitted data. The following subsection briefly discusses some of the security limitations within wireless LAN and introduces some of the security protocols available in the market in order to counter such limitations.

1. *Threats:*

Among the well-known threats facing WLAN is that the wireless access points are configured to broadcast their service set identifier (SSID). In most cases, these access points use default SSIDs provided by the manufacturers, and usually are available for download from the internet, which makes it very vulnerable for sniffing attacks.

Another known problem facing WLAN is eavesdropping, in which case intruders do not have to physically tap into the network to be able to eavesdrop, they can passively sniff the network traffic without gaining physical access to it.

Also, In 802.11, the default authentication is open authentication, where the system will authenticate any user requesting a connection to the network. Usually, an access point has one or several methods available to control access to a wireless LAN [9], this includes the use of a common SSID, based on MAC address, and through WEP.

2. *WLAN Security Protocols*:

To defend the WLAN from the above listed security threats, and others, there are considerable number of security protocols that exist in the market today. Due to the limited size of this paper, we will discuss only the Wired Equivalent Privacy (WEP), which is considered as the industry standard for WLAN security.

WEP is an optional IEEE 802.11 feature that prevents disclosure and modification of packets in transit and also provides access control. WEP allows a person to set up a 40 or 128-bit security key that is shared between a mobile device and an access point. This key will encrypt all of the information that is transmitted on the network; however, in order for it to be effective, it must be configuration into all devices that connects to a wireless network through the access point [4].

One issue with this protocol is that WEP uses the RC4 as its underplaying algorithm. RC4 is a symmetric

algorithm. When WEP is enabled, each radio "station" has a key. The key is used to scramble the data before transmission of the data through the airwaves. If a station receives a packet that is not scrambled with the appropriate key, the station discards the packet and never delivers such a packet to the host.

Another issue is that name Wired Equivalency Privacy implies that WEP can provide users with the same degree of protection from eavesdropping as wired networks. Unfortunately, this isn't true. As it turned out, the encryption provided by WEP was fairly easy to crack.

- *WEP Encryption*

When WEP encrypts data, two processes are applied to the plaintext data: one to encrypt the plaintext, the other to protect against unauthorized data modification. The encryption process always begins with a plaintext message that needs to be protected [5-7]:

1. WEP performs a 32-bit cyclic redundancy check (CRC) checksum operation on the message. WEP calls this the integrity check value and concatenates it to the end of the plaintext message.
2. Take the 40-bit secret key and concatenate it to the end of a 24-bit initialization vector (IV), resulting in a 64-bit total key size.
3. Plug this IV + secret key combination into the RC4 Pseudo-Random Number Generator (PRNG) and it will output a pseudo-random key stream sequence based on the input key. The key stream is merely a series of 0s and 1s, equal in length to the plain text message plus CRC combination.
4. Perform a bitwise exclusive OR operation (XOR) between the plain text message plus CRC combination and the key stream.

The result is encrypted bytes equal in length to the number of data bytes that are to be transmitted in the expanded data, plus 4 bytes. This is because the key sequence is to protect the integrity check value (ICV, 32-bits) as well as the data. To protect against unauthorized data modification, an integrity algorithm (CRC-32) operates on the plaintext to produce the ICV [7].Figure 1 shows the WEP encryption algorithm.

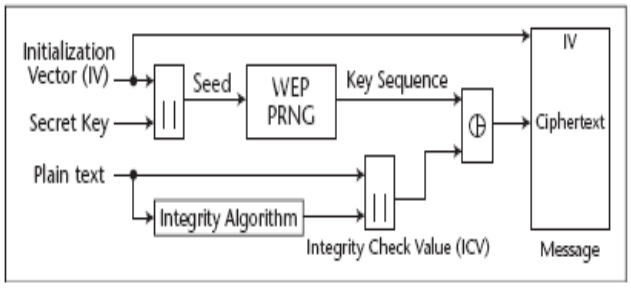

Figure 1: WEP Encryption Algorithm

Decryption in WEP follows the same process as that in the encryption, but in reverse. To decrypt the data stream, WEP goes through the following steps [8]:

1. Take the IV (which is sent in clear text) and append it to the secret key and plug that into the RC4 cipher to regenerate the key stream, which is necessary to decrypt the incoming message.
2. XOR the proper key sequence with the cipher text, which will result in the plain text value and ICV.
3. The decryption is verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV1 to the ICV transmitted with the message.
4. If ICV1 is not equal to ICV, the received message is in error, and an error indication is sent back to the sending station. Mobile units with erroneous messages are not authorized. Figure 2 shows the WEP decryption algorithm.

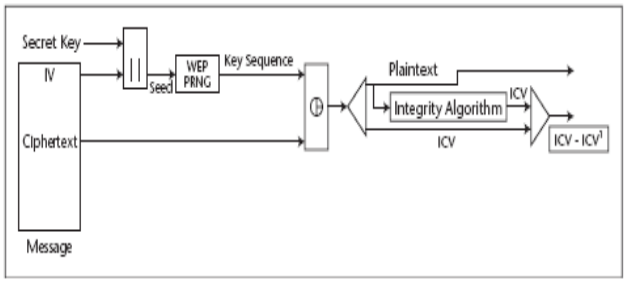

Figure 2: WEP Decryption Algorithm

- *WEP Authentication Methods*

WEP uses an open system authentication as the default authentication protocol for 802.11. With open authentication, the entire authentication process is done in cleartext, and a client can associate with an access point even without supplying the correct WEP key. “It is usually implemented where ease of use is the main issue". In open system mode, stations and access points are essentially using WEP as an encryption engine only” [7].

With shared key authentication, the access point sends the client a challenge text packet that the client must encrypt with the correct WEP key and return to the access point. If the client has the wrong key or no key, it will fail authentication and will not be allowed to associate with the access point.

It’s important to note that what are being authenticated here are the stations and not users. This authentication method can only verify that particular users belong to a certain group with access rights to the network; it cannot distinguish one mobile user from another.”

WEP allows an administrator to define a shared key for authentication. Access is denied to anyone who does not have an assigned key. The shared key used to encrypt and decrypt the data frames is also used to authenticate the station, but this is considered a security risk. However, the shared key authentication approach provides a better degree of authentication than the open system approach. For a station to use shared key authentication, it must implement WEP.

Other protocols used in the WALN are Wi-Fi Protected Access (WPA), and the WPA2, which is also called 802.11i security standard that was built for Robust Security Networks (RSN) that is meant to support addition software and hardware capabilities and is a backward compatible with existing WEP equipments.

III. EXPERMENTS

In this section, we present two experiment scenarios that were conducted for the purpose of establishing a baseline and for understanding the impact of adding encryptions, with different key sizes, used by WEP security protocol on UDP and TCP WLAN traffic. While the first experiment was for measuring the throughput under normal conditions (No encryption applied), the second experiment was to analyze the variation of traffic throughputs over an Infrastructure network when encryption is applied.

Next, we list the general software and hardware requirements for our experiments.

A. *General Design Requirements*:

The following is a list of the general design requirements for our experiments:

1. Software Requirements
   - LanTraffic™ packet generation V2 software
2. Hardware Requirements:
   - Two laptops
   - Ethernet Cables
   - Linksys Wireless-G Notebook Adapter (WAP45G)
   - Access point of Linksys Wireless-G Broadband Router (WAP45G)

B. *The Baseline Experiment Scenario:*

The baseline scenario is comprised of two different parts: The first part measures the throughput with respect to TCP traffic, while the second part deals with measuring the throughput with respect to UDP traffic. In both cases, the traffic is generated using LanTraffic™ V2 software. In the first part, laptop1 uses 802.11g wireless adapter is used to send TCP traffic of different data sizes and different inter-packets delays to laptop2, which is connected to an Access Point (AP) using an Ethernet cable. The second part of the experiment was conducted using the same environment variables described above, but this time UDP traffic generated using laptop1 and laptop2 to send traffic with different data sizes from laptop1 to laptop2. We varied the size of the data from 64 bytes to 1460 bytes and the inter-packet delay from 1 ms to 20 ms. The distance between the sender and the receiver was set to 5 meters to keep the signal strength very high. After generating, and transmitting, both traffic, it was determined that the maximum throughput for TCP traffic equals to 9800 Kbps and UDP traffic equals to 13144 Kbps. The reason for the throughput using UDP traffic is greater than that of the TCP traffic because UDP is not a reliable protocol.

C. *Infrastructure network with encryption Scenario*

Within the infrastructure mode, two sub-scenarios, wireless to wired and wireless to wireless scenarios, were used to analyze the affect of applying encryption, using different encryption key sizes of 64 bits and 128 bits of WEP security protocols, on the throughput of TCP and UDP traffic in IEEE 802.11g infrastructure wireless to wired communication mode. The following subsections discuss the two scenarios:

1. *Infrastructure wireless to wired communication mode*

In this scenario, the measurements were conducted on both TCP and UDP traffic as following:

In the case of TCP traffic, the data with a fixed size of 1460 bytes and 1ms as an inter-packet delay is sent from laptop1 using 802.11g wireless adapter to Laptop2 that is connected to the AP using Ethernet cable. See figure 3.

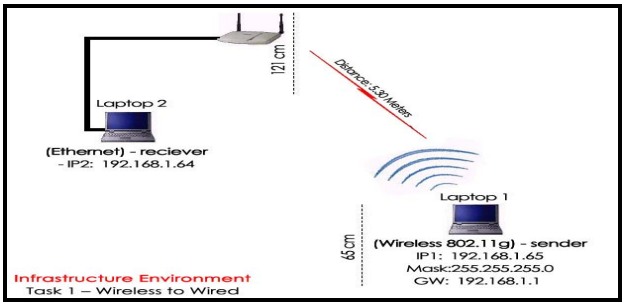

Figure 3: Wired to Wireless Infrastructure Mode

One fact worth mentioning about WEP is that in order to generate the security keys a pass phrase must be inserted to generate the key of the specified size in the access point after the security protocol is set , the

communicating laptop with the access point must also have the key that is usually exchanged using a secure channel.

In the case of UDP, the traffic was generated using the same laptops, laptop1 and laptop2, to send traffic of data size of 1460 bytes from laptop1 to laptop2.

For both UDP and TCP traffic the key sizes of the security protocol were varied after taking the results of the baseline throughput, were no encryption was involved, in order to have a comparative value to help determine the effect of adding encryption on the throughput.

- *Experiment Results & Analysis*

The table below (Table 1) indicates the different results of this experiment.

Table 1
Average throughput for TCP/UDP Traffic in Wireless to Wired Infrastructure Environment

Items Description	Baseline	WEP64	WEP128
Average Throughput/TCP	9800	9400	9100
Average Throughput/UDP	13144	13090	13000
Dropped TCP %	0%	4.08%	7.14%
Dropped UDP %	0%	0.41%	1.10%

Considering the results presented in the table above, the figure below depicts the throughput when encryption is applied.

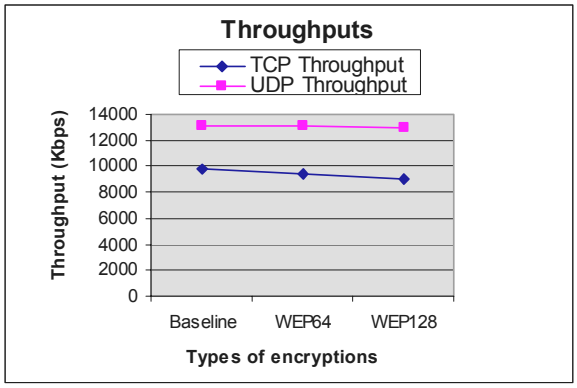

Figure 4: Infrastructure Wireless to Wired AverageThroughput Results

Figure 4 showed that for TCP traffic, the throughput had suffered a degradation of about 4% when WEP, with 64-bits key size, was enabled and a degradation of about 7.14% when WEP, with 128-bit key size, was enabled.

The figure also showed that for UDP traffic, the throughput had suffered a degradation of 0.41% when WEP, with 64-bits key size, was enabled and a degradation of 2.62% when WEP, with 128-bit key size, was enabled.

The reasons behind the traffic degradation as a result of enabling WEP can be summarized as following: The Initial Vector value of the key and the Integrity Check Value that are added to the IP payload before its being sent contributed to increasing the amount of data regularly transmitted. Also, WEP encryption algorithm uses a KSA algorithm that generate a key stream and XORs it with the payload to encrypt it, which requires more time and slow the sent stream of data. The degradation of the throughput in here is related to the increase of the packet size and time consumption which means more data to be sent in a slower rate.

UPD readings indicate higher throughput than that of the TCP due to the fact that the TCP is connection oriented reliable protocol that waits for acknowledgements before resending the next packets, which contributes to slowing the rate of sent data, while in the UDP its a un-reliable protocol that does not wait for confirmation and keeps on sending the packet stream on the wireless connection.

2. *Infrastructure wireless to wired communication mode*

The setup for this communication mode is similar to that of the wireless to wired communication mode. The only difference is that in this mode we have to air interfaces with one access point. Figure 5 depict this set up.

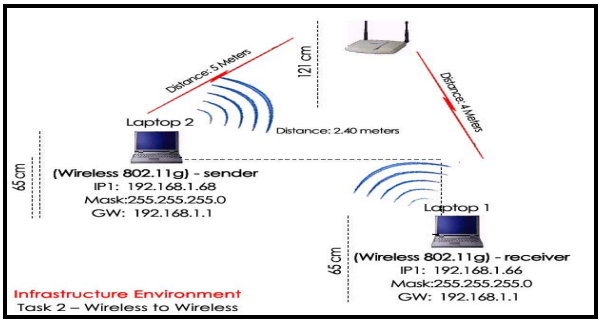

Figure 5: Wireless to Wireless Infrastructure Mode

- *Experiment Results & Analysis*

The results present the average throughput of the sent data and the percentage of drop in both TCP and UDP traffic using the previous equations related to both terms. The following table indicates the different results of this experiment.

Table 2
Average throughput for TCP/UDP Traffic in Wireless to Wireless Infrastructure Environment

Items Description	Baseline	WEP64	WEP128
Average Throughput/TCP	5194	5141	5071
Average Throughput/UDP	7872	7000	7198
Dropped TCP %	0%	1.02%	2.38%
Dropped UDP %	0%	11.09%	8.56%

Considering the results presented in the table above, the graph below depicts the throughput when encryption is applied.

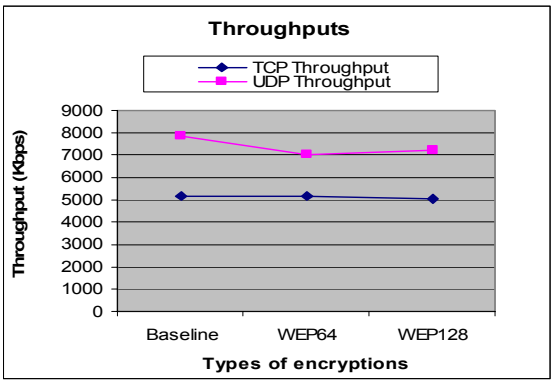

Figure 6: Wireless to Wireless Throughput Results

Results show the exact pattern of degradation in throughput of TCP traffic and approximately that same in UDP traffic when WEP was enabled in wireless to wireless environment. The degradation in performance in this scenario drops to about 9%, for UDP traffic, due to the fact that the there are two levels of encryptions provided in this scenario, from the first laptop to the AP and from the AP to the second laptop.

IV. Related Work

Since applying security to wireless networks is a very new yet an active area. Different researches were applied to delete the ambiguity of certain points in that field.

In [7] the authors presented an experimental effort in analyzing the effect of applying WEP on the traffic of an ADHOC networks. They examined the effect of applying WEP to different packet sizes and using different distance between the communicating machines. The authors' results indicated that the throughput decreases with the presence of security.

Another remarkable effort was presented in [8] to quantify the impact of different protocols on WLAN. The security protocols that were studied in the paper are WEP, EAP, SSL, IPSEC and RADIUS. The paper analyzed the strength of security functions presented by different protocols and compared among them. Results of the paper indicate that WEP will provide the least overhead in the established test beds.

V. Conclusion

In conclusion, the general observations taken from these experiments are:
Throughput decreases when security, WEP, is enabled. This is due to the fact that encryption operations performed by this protocol increases the amount of data transmitted and slows down the rate of data being sent or received.

For WEP when the key size increases the throughput slightly decreases that is due to the fact that WEP adds the Initial Value of its symmetric encryption key to the data sent and it uses the rest of the key bits to initiate a key scheduling algorithm that generates a stream key for the stream data to be XORed with. This regular process of RC4 encryption algorithm can impose a certain amount of delay to the data to be sent after encryption then received and decrypted.

In the wireless to wireless environment, the throughput suffered more degradation than that in the wireless to wired environment. This is due to the fact that in the wireless to wireless environment, there are double encryptions which resulted from having two air interfaces with one access point.

References

[1] Trulove, J. "Build your own wireless LAN" .McGraw-Hill. Two Penn Plaza, New York. 2002

[2] K. Shuaib and M. Boulmalf, "Co-existence of WLAN and WPAN Communication Systems" for the Handbook of Research in Mobile Business: Technical, Methodological and Social Perspectives" with IDEA group publishing (IGP), Hershey, PA, USA

[3] K.Shuaib, M. Boulmalf, F. Sallabi and A. Lakas, "Performance Analysis: Co-existence of IEEE 802.11g with Bluetooth", Second IFIP International Conference on Wireless and Optical Communication Networks, WOCN 2005, sponsored by IEEE., to be held in Dubai, March 6-9, 2005

[4] Khan, J and Khawaja, A. "Building Secure Wireless Networks with 802.11. Wiley Publishing, Inc. Indianapolis, Indiana, 2003.

[5] R.D.Vines. Wireless Security Essentials: Defending Mobile Systems from Data Piracy, Wiley Publishing Inc, 2002.

[6] Lee Barken, WEP Vulnerabilities—Wired Equivalent Privacy?, Dec 2003, retrieved on March, 2006, retrieved from http://www.informit.com/articles/article.asp?p=102230&seqNum=2

[7] Mohammad Saleh and Iyad Al Khatib, "Throughput Analysis of WEP Security in Ad Hoc Sensor Networks", The Second International Conference on Innovations in Information Technology (IIT'05), Dubai, 2005

[8] Avesh K. Agarwal, Wenye Wang ,"Measuring Performance Impact of Security Protocols in Wireless Local Area Networks", The Second International Conference on Broadband Networks. October ,2005. Boston, Massachusette, USA.