THE MEASUREMENT OF WLAN THROUGHPUT USING DIFFERENT SECURITY PROTOCOLS

B. Dekeris, L.Narbutaite

Telecommunication department, Kaunas University of Technology
Studentu str. 50, LT-51368 Kaunas, Lithuania
T, +370 37 300505; E,brunonas.dekeris@ktu.lt / lina.narbutaite@ktu.lt.

Abstract

802.11 wireless LANs continue to gain market momentum. Now, with this growing adoption of 802.11 wireless LANs, security has become a focal point regarding the decision to deploy a wireless LAN.

In this paper we analyze the wireless LAN throughput using different security protocols. While defining the right security layout, theoretical throughput of channel was calculated and compared to practical rates of wireless local area network channel, using different safety layouts.

This paper also addresses the different issues related to the security protocols currently used in WLAN IEEE 802.11 and demonstrates how these issues affect the final results of the experiments conducted. The results show that within the same access point range the security adds moderate degradation on the throughput that may affect some applications over both infrastructure and ad hoc WLANs.

1. Introduction

Over recent years, the market for wireless communications has experienced considerable growth. Wireless technologies have found an important place and popularity in business, the computer industry and medical clinics [1-2].

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 [3].

Since applying security to wireless networks is a very new yet an active area, intensive research was recently devoted to clarify remaining ambiguities, to identify limitations and difficulties, to propose solutions and to improve the performance of these networks[4].

2. WLAN security protocols

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

WEP was the original native security mechanism for WLAN developed by IEEE members in order to provide security through a 802.11 network. 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 [4-5]. WEP uses theRC4 as its underplaying algorithm. RC4 is a symmetric algorithm.

WPA enables 802.1x/EAP authentication along with Temporal Key Integrity Protocol (TKIP) encryption that is based on RC4. The components of WPA include:

WPA delivers a greatly enhanced encryption scheme called Temporal Key Integrity Protocol (TKIP). TKIP increases the key from 40 to 128 bits, and relies on dynamically generated session keys. 802.11i or WPA2 also provides a new encryption scheme called Advanced Encryption Standard (AES). AES enables security between workstations, and uses an algorithm that employs variable keys of 128, 192, or 256 bits [4].

A VPN creates a "tunnel" between each remote site and the host site allowing for communication. A VPN server is needed at the host site to terminate the "tunnel" as well as to provide the authentication and encryption. All traffic passing through the "tunnel" is encrypted. The more significant difference being, the traffic is protected by robust encryption techniques. Many times the encryption technique is IP-Sec, which is considered secure by government standards.

3. WLAN 802.11 throughput measurement

The objective of this research was How do different security mechanisms affect the performance (throughput).

3.1. Experimental configuration

The tested network structure is presented in Figure 1.

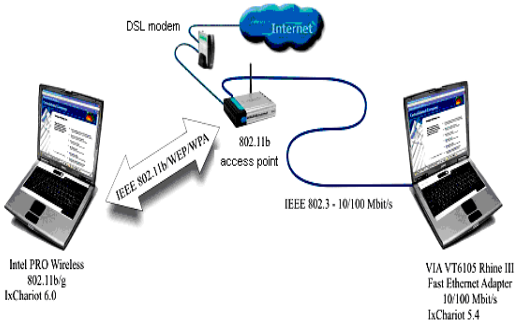

Figure 1. Tested network structure

The experiment were based upon Windows XP (clients). The measurement are used with IxChariot software equipment, SNR~69 dB. The measurement time of every case was 600 sec.

3.2. WEP, WPA measurement

For comparison our results, we used 3 case: non coding channel, WEP 128-bits key and WPA. The results are presented in figures 2-3.

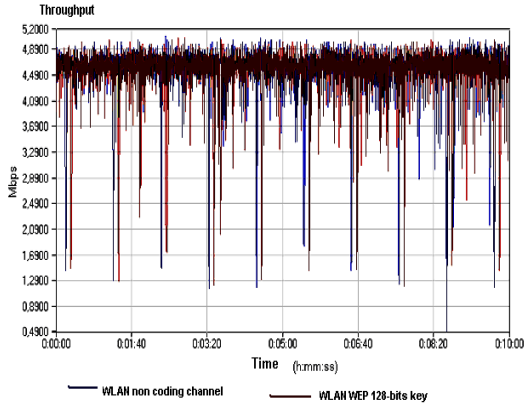

Figure 2. Throughput measurement using non coding and WEP 128-bit key channel

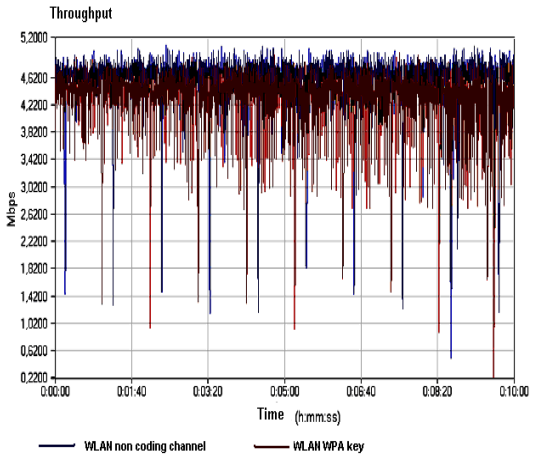

Figure 3. Throughput measurement using non coding and WPA protocol

Figures 2-3 indicate that using all 3 case we got the similar result:

- the maximum channel throughput is 5.06 Mbps;
- the average channel throughput is 4.49 Mbps.

3.3. IPsec VPN tunnel measurement

The tested network structure is presented in Figure 4.

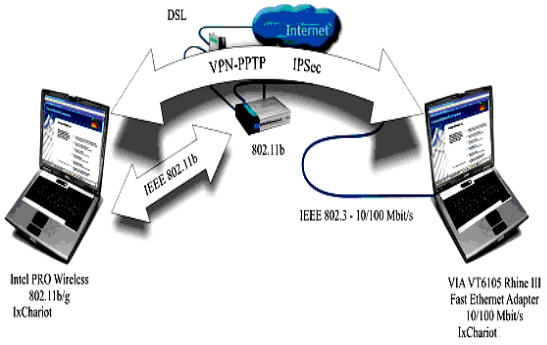

Figure 4. Tested network structure using VPN IPsec protocol

In this scenarios we used 1 and 2 VPN tunnels. The results are presented in Figure 5.

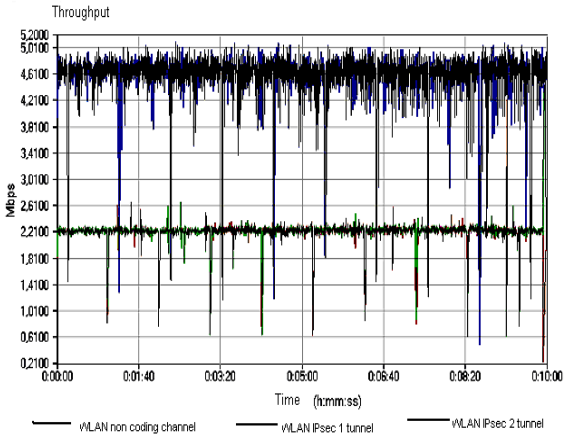

Figure 5. Throughput measurement using non coding and IPsec protocol

Comparison with results presented in the figures 2-3, we can see that in this case throughput decrease (2.2 time) than non coding channel throughput. This is due to the fact that encryption operations performed by these protocols increase the amount of data transmitted and slow down the rate of data being sent or received.

4. Theoretical WLAN throughput calculation

In order to determine the throughput of the system it is necessary to analyze the MAC layer of the IEEE 802.11b system. A data packet consists of overhead (preamble and header) and the data portion. The time to transmit this packet is shown below [6]:

$$T = DIFS + OH + \frac{M}{R} + SIFS + ACK \ , \quad (1)$$

where OH – overhead; M - data (bits); r – rate (bps).

DIFS, *SIFS* as well as *ACK* frame are considered here because they are necessary to ensure a correct reception of packet.

The average time for a correct transmission to be received is given by

$$T_{aver} = T + (1-p) \cdot \sum_{i=1}^{\infty} i \cdot p^i \cdot T \ , \quad (2)$$

where p – the probability of a packet being received in error (PER), it is calculated by formula

$$PER \ = 1-(1-P_{ber})^N \ , \quad (3)$$

where N – number pf bits in the packet, P_{ber} - the probability of bit error.

The P_{ber} is calculated [7]:

$$P_{ber} = \frac{2^{k-1}}{2^k - 1}\left(\sum_{m=1}^{M-1} \frac{(-1)^{m+1}\binom{M-1}{m}}{1+m+m8\Gamma} \right), \quad (4)$$

where $M = \frac{1}{2} \cdot 2^k$ - k is a number of bits in the symbol and $\Gamma = \sqrt{\frac{2E_b}{N_m}}$.

Then throughput is

$$C = \frac{M}{T}(1 - PER). \qquad (5)$$

MAC frame parameters: SIFS= 10μs, DIFS = 50μs, ACK = 112 μs, packet size= 1500 bytes.

The graphs for the throughput for four different rates are presented Figure 6.

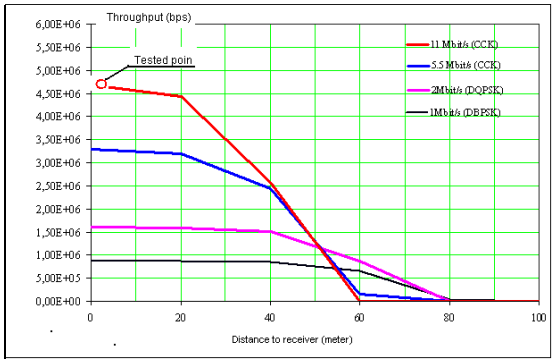

Figure 6. Theoretical throughput of the 802.11

From the figure 6 we can observe the efficiency of each data rate versus distance.11Mbps gives best throughput for the first 20 meters and throughput is 4.7Mbps.

5. Conclusions

The theoretical calculation and experimental throughput measurement results present that throughput decreases when security protocol WEP WPA and IPsec are enabled. Using WEP or WPA security protocol the theoretical differ from measurement throughput very small, but if we use VPN IPsec, the throughput decrease 2.2 time.

References

[1]. Karygiannis. "Wireless Network Security 802.11, Bluetooth and Handheld Devices".NIST, 2002, 119p.

[2]. Abderrahmane Lakas. "A Framework for SIP-Based Wireless Medical Applications", IEEE Communications,2004, pp1-5.

[3]. Brener P. A technical tutorial on the 802.11 protocol. 2004

[4]. Nilufar Baghaei. Security performance of loaded IEEE 802.11b wireless networks. Computer Communications 27, 2004, pp.1746–1756.

[5]. Aaron E. Earle. "Wireless Security Handbook", Taylor & Francis Group, 2006, p 347.

[6]. Rindzevičius,Grimaila.Pilkauskas, "Traffic analysis of the next generation wireless access technologies", IPSI - 2006 AMALFI , 2006, pp.1-7.

[7]. Fainberg M. "Performance analysis of the IEEE 802.11b local area network", 2001, pp 26-35.