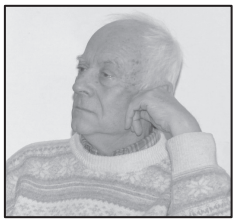

Prof. Dr. Eng. Anton POLICEC
Politechnica University of Timisoara
Electronics and Telecommunication Faculty
B-dul Vasile Pârvan Nr. 2, 300223
Timişoara, Romania

Drd. Eng. Gheorghe MÜLEC
Politechnica University of Timisoara
Electronics and Telecommunication Faculty
B-dul Vasile Pârvan Nr. 2, 300223
Timişoara, Romania
E-mail: george.mulec@rdslink.ro

SECURITY COST OF IEEE 802.11 WIRELESS LAN

NOTE: This paper was presented at the International Symposium "Research and Education in an Innovation Era", Section III, November 16-18, 2006, "Aurel Vlaicu" University of Arad, Romania.

ABSTRACT

Wireless network have gained popularity due to the flexibility and mobility that allow users access to the information. This research evaluated the effect of multiple security mechanisms of the performance for IEEE 802.11g wireless network using server-client architecture. The results showed that security mechanisms degrade the performance of network and we must know how much we pay for security features.

KEYWORDS

security mechanism, wireless network, topology.

I. INTRODUCTION

Since the ratification of the IEEE 802.11b standard in 1999, wireless LANs have became rifer. This is due the mobility of users by releasing the constraint of physical connections. Today, wireless LANs are widely deployed in places such as corporate office, conference rooms, airports, university campus.
Besides these advantages, inherent broadcast nature of wireless networks, the IEEE 802.11 – based wireless LANs present new challenges for information security administrators [1].
Network performance is characterized by certain parameters such as a time delay, system throughput, packet loss etc.
Wireless networks are highly susceptible to many kinds of attacks since interception and eavesdropping of data in transit is possible for anyone with access to wireless network due to their inherent broadcast nature and shared air medium [2],[3]. For maintaining a specific level of network performance it is vital to determine the performance impact caused by security services in wireless network. At the most basic level wireless security requires authentication and encryption. Wireless network use more levels of security for data protecting [4].

II. BACKGROUNDS

In the first stages of 802.11 development, the WLAN security was based on two mechanism: Service Set Identifier (SSID) and Wireless Equivalent Privacy (WEP). When the weaknesses of WEP were identified, IEEE ratified a new standard, IEEE 802.1X, that provides a way to leverage traditional strong authentication mechanisms such as RADIUS Server in a wireless network [5]. The IEEE 802.1x defines a mechanism for port-based network access control. It is based upon Extensible Authentication Protocol (EAP) to provide compatible

authentication and authorization mechanisms for devices interconnected by IEEE 802.11.

There are three main components in the IEEE 802.1x authentication system: supplicant, authenticator and authentication server. In a WLAN, *supplicant* usually is AP (Acces Point) that represents an *authenticator*. Authentication, Authorization, and Accounting (AAA) server such as RADIUS server is the *authentication server*. The *port* in 802.1x represents the association between supplicant and authenticator. Both supplicant and authenticator have a *Port Access Entity (PAE)* that operates the algorithms and protocols associated with the authentication mechanisms. The authenticator's *controlled port* is in unauthorized state. Messages will be directed only to the *Authenticator PAE*, which will further direct 802.1x messages to the authentication server.

The authenticator PAE will close the controlled port after the supplicant is authenticated successfully. IEEE 802.1X specifies how to run the EAP directly over a link layer protocol. EAP is a transport protocol that can used a variety of different authentication types known as EAP methods [6],[7],[8].

In **figure 1** is illustrate the 802.1X–EAP Message Flow for an authentication process. Among the EAP methods developed specifically for wireless networks are a family of methods base on public key certificates and the Transport Layer Security (TLS) protocols. These are EAP-TLS, EAP-TTLS and EAP-PEAP.

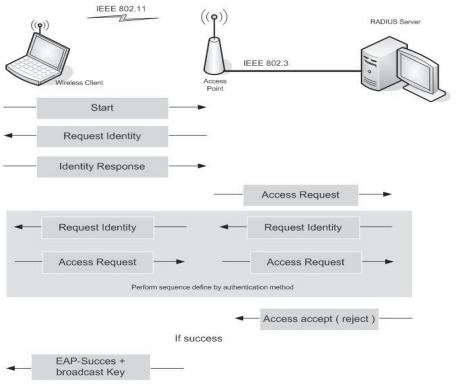

Fig. 1 - 802.1X – EAP Message Flow

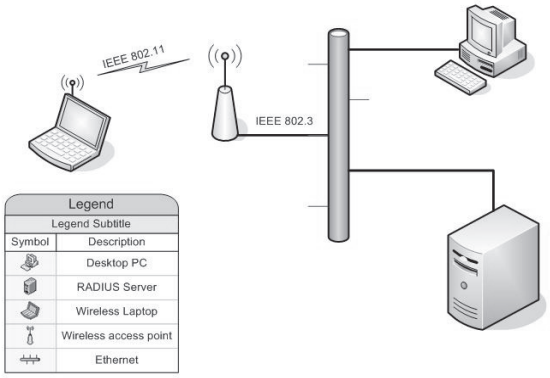

Fig. 2. Testbed architecture

III. EXPERIMENTAL PART

A. Configuration topology

Our test platform is a miniature of WLAN compound by an access point, an authentication RADIUS server, a local area network, a wireless laptop and a PC station. **Figure 2** shows the testbed architecture used on this experiment.

B. Hardware configuration

Access point (AP) used in experiment is a D-link DWL 2100AP [10]. At this access point, are wireless connected a wireless client with Laptop HP (Celeron 1.5 GHz, 256 MB RAM) and a D-link DWL G650 wireless cardbus adapter [10]. For RADIUS Server we used a desktop PC (P IV, 2.6 GHz, 512 MB RAM) and for PC station another desktop PC (AMD 1,3 GHz, 256 MB RAM). All the Ethernet adapter are fast adapter (100 Mbps).

C. Software configuration

All the system have installed Windows XP Home Edition as a operating system. We have installed following software components for various protocol used in testbed: RADIUS server is implemented with open-source software FreeRADIUS [11], X.509 Certificate (CA, Server, Client) are issued with open-source software OpenSSL [12], Capturing packets are made with Ethereal packet analyzer. [13], TCP / UDP tuning and throughput measurement are made with Iperf [14] and Qcheck [15]

D. Experimental analysis

Many factors affect network performance and some of them interact to provide overall performance results. Performance results depending on the choice of hardware device, software application, security policy and network topology. On the same conditions (hardware, software and network topology) we have measured the authentication time, throughput and response time for different types of security policy.

Authentication time is defined as the time involved in a authentication phase of security protocol.

Throughput refers to actual measured bandwidth, at a specific time of day, using specific routes, and while a specific set of data is transmitted on the network.

Response time is a measure of the delay in transmission of data between a sender and a receiver for a specific packet size.

For this experimental analyze we have used the "Iperf", "Qcheck" and "Ethereal" software programs.

1. Security configuration

IEEE 802.11 provides two mechanism of security: authentication and encryption. Authentication may be made with Shared key authentication mechanism and with different type of authentication mechanism run over the EAP protocol.

In our research we used the EAP based on 802.1x family protocol for authentication (EAP – TLS, EAP – TTLS, EAP –

PEAP).For data encryption we used WEP (40 and 128 bits), TKIP and AES encryption protocol.

2. Measurement methods

For each security service configured, experimental data were collected in two phases, in a not congested network (normal situation). The first phase collects measurements from authentication protocols. The second phase focuses on generating different traffic and measurement the throughput and response time.

In the first phase, we used "Ethereal" packet analyzer to capture the packets exchanged during authentication process. Data obtained here were used to compare the authentication time for different authentication protocols.

On the second phase we used "Iperf" and "Qcheck " for generate TCP and UDP traffic between Wireless Laptop and PC station for measures the throughput and response time .For all tests, the wireless link was at a constantly 54 Mbps with level of radio signal more than 95%.

IV. RESULTS AND DISCUSSION

1. Authentication Time

Figure 3 show authentication time (in sec) for EAP – TLS, EAP–TTLS, EAP–PEAP authentication protocols.

Our research is based only to the 802.1x authentication framework. The shared key authentication not achieves the mutual authentication and when the authentication is completed does not result a session key.

Authentication time for all the Certificates based protocol mention above is mostly the same. We can see that authentication process is smaller than 1 sec and appear after association phase.

2. Throughput

Figure 4 illustrates the throughput of TCP traffic for different encryption protocol. Performance measures were gathered by running seven repetitive tests at each encryption protocol. The throughput is smaller if we use the AES instead of TKIP (RC4) cipher. If we use the same protocol the throughputs decrease if increasing the secret key length.

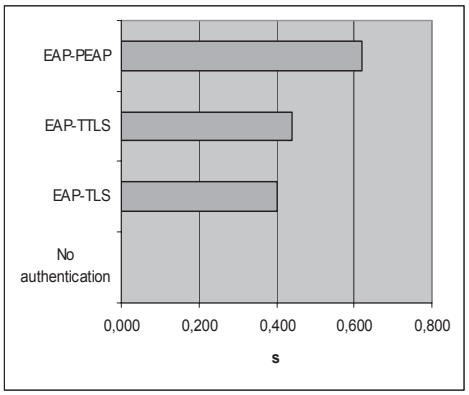

Fig. 3 Authentication time

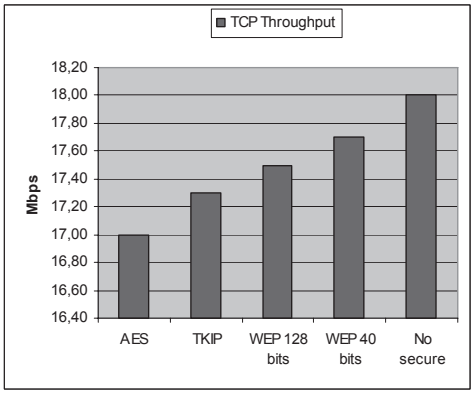

Fig. 4 Throughput for TCP

Figure 5 illustrates the throughput of UDP traffic for different encryption protocol. In this case, the "trend" is the same as in TCP traffic, but throughput is with cca. 20% lesser.

3. Response time

Figure 6 illustrate the response time for TCP and UDP traffic. In this case, we measure the response time for 1K byte packet size (in a not congested network).

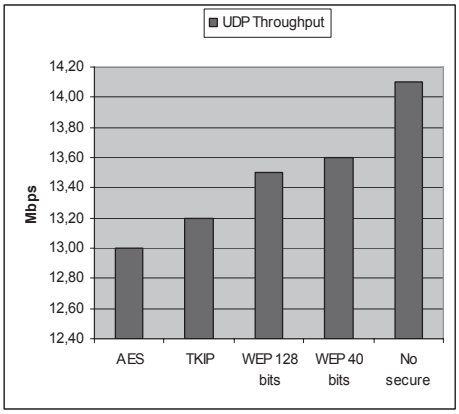

Fig. 5 Throughput for UDP

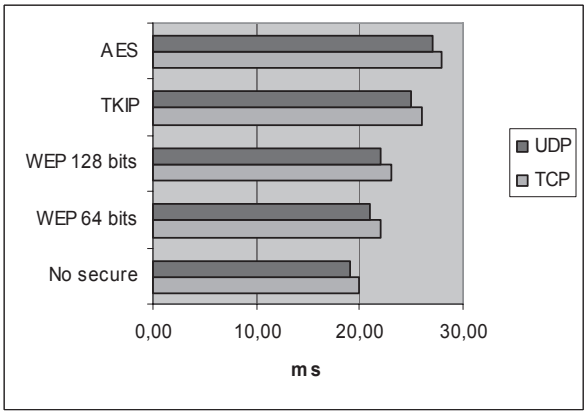

Fig. 6 Per packet response time

V. CONCLUSION

In this paper, we presented experimental results of impact incurred by security policies on system performance in a not congested network.
The results demonstrate that WEP policies cause least overhead, while AES and TKIP cause significant overhead but provide stronger security. Authentication process 802.1x with EAP-TLS cause lesser overhead than 802.1x with EAP-PEAP. The delay produce by the authentication process is smaller than 1 sec. Because the WLAN isn't very mobile (WLAN is implemented in relative limited area – college campuses, airports, shops) the need for authentication is not very frequent and the benefits of that is evident. The authentication delay is bigger for EAP-PEAP towards other authentication Certificate based protocols.
Using AES as encryption protocol we have obtained a smaller throughput and obviously the possibility of delivery less amount of data in a given time than in case of using TKIP or WEP , but this is the 'price' for having a higher security.

REFERENCES

[1] Y. Zahur and T.A. Yang, "Wireless LAN security and Laboratory design", Journal of Computing Science in Colleges, vol. 19, pp. 44-60, January 2004
[2] W. A. Arbaugh, N. Shankar, J. Wang and K. Zhang, "Your 802.11 network has no clothes", IEEE Wireless Communication Magazine, December 2002
[3] D.B. Faria and D.R.Cheriton, "DoS and authentication in Wireless Public Access Networks," pp. 47-56, September 2002.
[4] E Bertino, S. Jajodia , L. Mancini and I. Ray,"Advanced transaction processing in Multilevel secure File Stores", IEEE Transactions on Knowledge and Data Engineering, vol. 10 , pp. 120-135, February 1998
[5] "IEEE Std 802.1x-2001x: Port Based Network Access Control", http://www.ieee802.org/1/pages/802.1x.html, June 2001

[6] Blunk, L., & J. Vollbrecht. (1998). PPP Extensible Authentication Protocol (EAP), RFC2284: Internet Engineering Task Force.
[7] "IEEE 802 Standards", http://standards.ieee.org/getieee802
[8] IETF, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999
[9] Microsoft Wireless 802.11 Security Windows XP, http://www.microsoft.com
[10] http://www.d-link.com
[11] http://www.freeradius.org
[12] http://www.openssl.com
[13] http://www.ethereal.com
[14] http://www.iperf.org
[15] http://www.ixiacom.com