THE IMPACT OF VARIOUS SECURITY MECHANISMS ON THE WLAN PERFORMANCES

Nidal TURAB[1], Florica MOLDOVEANU[2]

În ultima decadă diferite tehnici de securitate au fost dezvoltate pentru îmbunătățirea securității comunicării în rețele WLAN (Wireless Local Area Networks). Implementarea lor într-o rețea poate degrada performanțele rețelei.

În acest articol se prezint rezultatele experimentelor realizate de autori privind capacitatea unei retele locale wireless de a transfera date in fisiere de dimensiuni diferite, în conditii de trafic normal şi congestionat, atunci cand în rețea sunt implementate diferite mecanisme de securitate. Măsuratorile au fost efectuate la două nivele de comunicație: TCP/UDP si FTP/HTTP.

Various security techniques were developed to improve the security of the communication in a WLAN. Their usage in a WLAN can degrade the network performances.

This paper presents the results of experiments conducted by the authors regarding the capability of a WLAN to transfer data files of different sizes, under normal and congested traffic loads, while various security mechanisms are used. Two levels of communication were chosen to carry out the measurements: TCP/UDP and FTP/ HTTP.

Keywords: network throughput, congested network, IEEE 802.11g , WEP, WPA, TKIP, EAP-TLS

1. Introduction

WLAN offers the organizations and private users many benefits such as mobility, increased productivity and low cost of installation. Deploying WLAN in any organization network can compromise the overall network.

Security of the wireless network is an important issue, because the transmission media is open (no physical control on the air). For protection purposes several security mechanisms have been developed over years. These security mechanisms differ in the degree of security they provide. In addition to the fact that they do not offer 100% protection they are not completely secure, they influence substantially the performance of the network.

[1] PhD, Dept. of Computers, University POLITEHNICA of Bucharest, Romania, nedalturab@hotmail.com

[2] Professor, Dept. of Computers, University POLITEHNICA of Bucharest, Romania, Florica.Moldoveanu@rdslink.ro

Various researches had studied in the past the performance of WLAN under the security protocol IEEE 802.11b. Neider [6] studied the performance of the TCP, UDP for IEEE 802.11b WLAN using WEP and WPA security protocols.

Wong [26] studied the performance of IEEE 802.11b WLAN for FTP and HTTP protocols under WEP and WPA security protocols. Site mirror software was used to simulate the WEB site in the experiments.

In this paper, we will present a study of the impact of different security mechanisms on the IEEE 802.11g networks throughput in an enterprise network, under normal and congested loads and various packet sizes. The measurements were made on TCP, UDP, FTP and HTTP transactions.

Section 2 of this paper shortly presents the main security mechanisms that were used in our experiments. Section 3 explains how the experiments have been done. Section 4 presents the measurements results emphasizing the relationship between the impacts of various security protocols on the network performance.

2. WLAN security protocols

This section provides a brief review of the standard WLAN security protocols.

2.1. WEP (Wired Equivalent Privacy)

The goal of the WEP was to make Wireless LAN communication as secure as wired LAN data transmissions. The IEEE 802.11 MAC specifies that WEP has two components of the wireless security architecture: authentication and confidentiality. It uses a shared key mechanism with a symmetric cipher called RC4. The key that a wireless client is using for authentication and encryption of the data stream must be the same key that the wireless access point (AP) uses. When the wireless station wants to associate with the wireless AP, it must authenticate itself to the AP. Once the authentication is successful the wireless station becomes associated with the AP.

WEP uses the stream cipher RC4 for encryption (the process of applying XOR operation of RC4 Key stream bit by bit with plaintext) and the CRC-32 checksum for integrity. WEP encryption standard uses a 40-bit key, which is concatenated with a 24-bit Initialization Vector (IV) to form the RC4 traffic key. Some WEP implementations use an extended 128-bit WEP protocol using a 104-bit key size. A 128-bit WEP key is a string of hexadecimal characters (0-9 and A-F). Each character represents 4 bits of the key, i.e.: 4 × 26 = 104 bits; adding the 24-bit IV will result 128-bit WEP key. The maximum key size of 128 bits represents a major security limitation in WEP, because some attacks (i.e. active attacks) may simulate the real traffic. There are also some other weaknesses in WEP, including the possibility of IV collisions as well as altered packets. Fig. 1 illustrates the WEP algorithm.

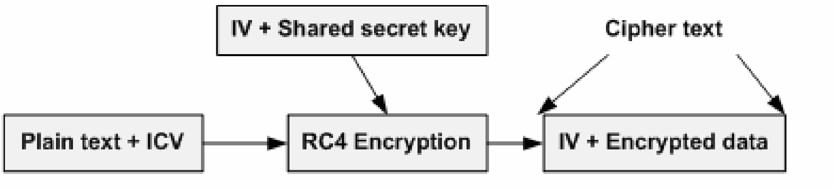

Fig. 1 WEP algorithm

2.2. Wi-Fi Protected Access (WPA)

WPA was intended to be intermediate mechanism, which will replace WEP while IEEE 802.11i was prepared. WPA was designed to be compatible with all old wireless network interface cards. It uses an IEEE 802.1x authentication server, which distributes different keys to each user. However, it can also be used in a less secure "Pre-Shared Key" (PSK) mode, where every user is given the same pass-phrase (a sequence of words that is similar to password but it is generally longer). In this mode, WPA requires that clients and access points use a shared network password (Preshared Key).

By increasing the size of the keys, the number of keys in use, and adding a secure message verification system, the usage of WPA makes breaking into a Wireless LAN very difficult.

WPA also employs the IEEE 802.1x access control protocol with Extensible Authentication Protocol (EAP), a universal authentication framework used in wireless networks and Point-to-Point connections.

In WPA, data is encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which uses a key scheme based on RC4. TKIP provides per-packet key mixing, a message integrity check and a rekeying mechanism. TKIP ensures that every data packet is sent with its own unique encryption key. Key mixing increases the complexity of decoding the keys. The message integrity check prevents forged packets from being accepted. Also TKIP hashes the initialization vector (IV) values, which are sent as plaintext, with the WPA key to form the RC4 traffic key, addressing one of WEP's largest security weaknesses.

In addition to authentication and encryption, WPA also provides improved payload integrity (usually known as MIC for "Message Integrity Code"). It uses an algorithm named "Michael”, to prevent reply attack and protect messages from being modified in transit. The MIC is calculated considering the destination and source addresses, three priority fields (reserved for future use) and the entire plaintext message payload. WPA algorithm is illustrated in fig. 2.

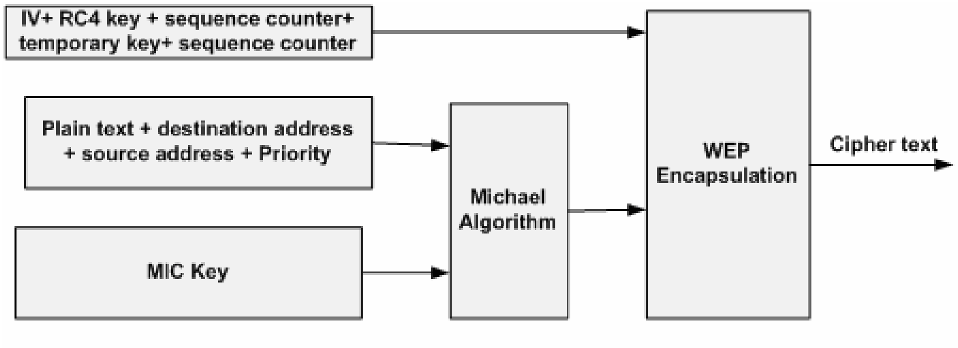
IV+ RC4 key + sequence counter+
temporary key+ sequence counter
Plain text + destination address
+ source address + Priority
MIC Key
Michael
Algorithm
WEP
Encapsulation
Cipher text

Fig. 2. WPA algorithm.

2.3. IEEE 802.11i

IEEE 802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in their 802.11a, 802.11b, and 802.11g, 802.11n (new) versions to provide wireless connectivity in the home, office and enterprise networks.

IEEE 802.11b works in the 2.4GHz band, with maximum data rate of 11Mbit/s; the modulation technique used is the Complementary Code Keying (CCK).
IEEE 802.11a works in the 5GHz band with data rate of 54 Mbit/s; this makes it incompatible with the IEEE802.11b
IEEE 802.11g is the third modulation standard for Wireless LAN, it works in the 2.4 GHz band (like IEEE 802.11b) but operates at a maximum raw data rate of 54 Mbit/s. IEEE 802.11g hardware is fully backward compatible with IEEE 802.11b hardware.

The modulation scheme used in IEEE 802.11g is orthogonal frequency-division multiplexing (OFDM) with data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s, and reverts to 1, 2, 5.5, and 11 Mbit/s using other modulation techniques such as Direct Sequence Spread Spectrum (DSSS) and Complementary Code Keying (CCK) that used with older wireless devices. Even though IEEE 802.11g operates in the same frequency band as IEEE 802.11b, it can achieve higher data rates [2, 7, 18].

The IEEE 802.11i architecture consists of the following components:

- **IEEE 802.1x:** port-based network access protocol. It provides authentication for point-to-point connection and can be used for wireless access points. It uses EAP and authentication server.
- **Robust Security Network (RSN)**: is an element of 802.11i authentication and encryption algorithms to be used for communications between wireless Access Point and the wireless clients.
- **Encryption algorithms:** The IEEE 802.11i includes two encryption algorithms:
    - **TKIP (Temporal Key Integrity Protocol)** - in order to support legacy devices, the IEEE 802.11i chooses TKIP as one of the encryption standards (similar with WPA).
    - **AES-based CCMP** (Advanced Encryption Standard based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) - encryption protocol, created to replace, together with TKIP, the insecure WEP protocol. It needs extra hardware for its implementation. The AES, also known as Rijndael (from the names of its developers Joan Daemen and Vincent Rijmen), is a block cipher. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. Due to the fixed block size of 128 bits, AES operates on a 4×4 array of bytes
- **Four-way handshake:** uses the key produced from IEEE 802.1x/EAP authentication (known as Pairwise Master Key PMK) to derive other keys necessary to encrypt broadcast and multicast traffic.

3. Experiments methodology

Fig. 3 illustrates the hardware configuration used by the authors to carry out several experiments.

Windows-based operating systems were used because Windows XP professional and Windows 2003 Server have a built in implementation of the IEEE 802.11 security mechanisms and 802.1x authentication protocol such as EAP-TLS [1, 3, 4].

The functions of the servers used in the experiments are:

- Active Directory server: acts as the information repository containing user, machine, group and user-specific policies based on lightweight directory access protocol (LDAP) technology. The application used was active directory (AD).This server is used in our network logon for the enterprise network. Users privileges can be controlled by the group policy template which is included in the Windows 2003 platform
- DNS server: provides name resolution service.

- DHCP server: provides the automatic IP-parameters distribution service for the network users.
- AAA server (RADIUS) can be integrated with the AD to provide a single sign-on to a network and provides single sign in services for remote users (wireless users in our study).
- Digital Certificate Server is the certificate authority that issues the digital certificates needed for EAP-TLS authentication (for IEEE 802.11i).
- WEB server contains IIS services. It was implemented a web page which is stored there in order to be downloaded by using HTPP and FTP protocols.

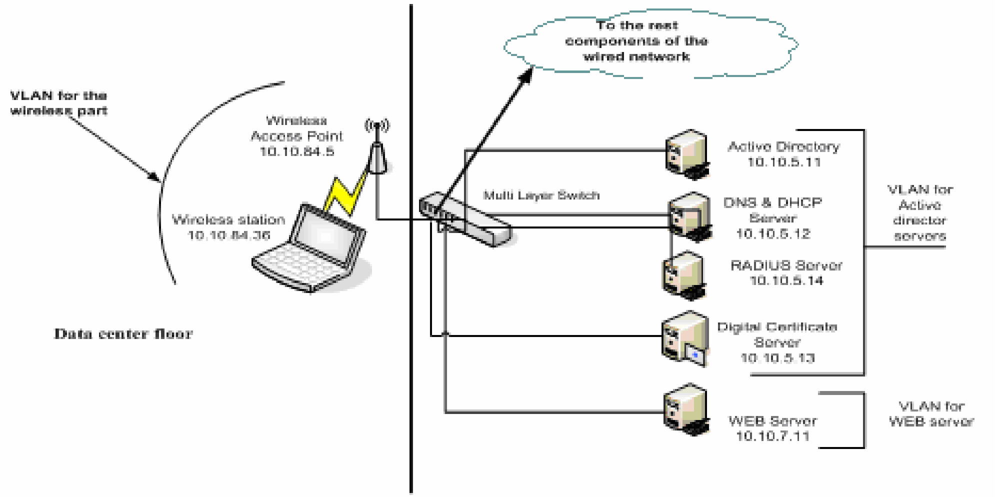
To the rest components of the wired network
VLAN for the wireless part
Wireless Access Point 10.10.84.5
Wireless station 10.10.84.36
Multi Layer Switch
Active Directory 10.10.5.11
DNS & DHCP Server 10.10.5.12
RADIUS Server 10.10.5.14
Digital Certificate Server 10.10.5.13
VLAN for Active director servers
Data center floor
WEB Server 10.10.7.11
VLAN for WEB server

Fig. 3. The hardware configuration used in our experiments.

The wireless access point used here is CISCO AP 1231G and the wireless client equipped with CISCO AIRONET wireless adapter. The multilayer switch executes the function of switching and routing, because in case of the presented experiments, different VLANs are used to maximize security and there is a need to route traffic between these VLANs. As routing between VLANs is handled by the wired part and has the same influence on all wireless security mechanisms that were used in our experiments, it was not considered.

The experiments were divided into three sets:

1) The first set of experiments was carried to study the impact of different security mechanisms on the network performance for TCP and UDP protocols, using variable packet lengths from 400 to 1500 bytes. A total of 60000 packets with random packet content were sent

2) The second set of experiments was carried to study the impact of different security mechanisms on the network performance in case of FTP and HTTP protocols.
3) The third set of experiments was carried to study the impact of the packet size on network performance under different security mechanisms. For TCP and UDP protocols, we used 60000 packets with random packet contents.

For the first and third sets of experiments, a real time traffic generator (IP Traffic - Test & Measure software version 2.4.1) [27] was used to generate both TCP and UDP traffic. This real-time software has the capability to control the number of packets sent, packet length, packet content and the transmission bandwidth.

Two bandwidths were used to send data from the wireless client to the access point:

- 9 MB/Sec, to represent a normal traffic;
- 56 MB/Sec. The IEEE 802.11g standard maximum speed is 54 MB/Sec so that 56 MB/Sec represents a congested traffic. Congested wireless network means that the wireless client sends much more data than the bandwidth between it and the access point can handle.

For the second set of experiments, we used a web page with two files of 11 MB for normal traffic and 64 MB for congested traffic. This web page was stored on the WEB server and then downloaded by the wireless client using FTP and HTTP protocols.

In all experiments, the transmission speed was 54 Mbps wireless connections between the AP and the wireless clients and 100 Mbps Ethernet connections between the AP and the servers. All the measurements were made at the server side using network traffic analyzer software (Wireshark [28]).
The following seven security mechanisms combinations (from lower security level to higher security level) were chosen to compare the security mechanisms available for WLAN [10, 12]:

1. **No security**: this is the default security setting provided by most hardware vendors;
2. **WEP 40 bit**: 40-bit encryption and authentication;
3. **WEP 128 –bit**: 128 bit encryption and authentication;
4. **WPA-PSK-TKI**P(WPA, Preshared Key, TKIP): Shared Key authentication with key management, and TKIP used for encryption;
5. **WPA-PSK-AES** (WIFI Protected Access, Preshared Key, Advanced encryption Standard): Shared Key authentication with key management and AES protocol are used for encryption. This combination of the WPA-PSK for authentication and key management and the strongest encryption

algorithm AES provides simplicity of implementation and configuration and an acceptable level of security;

6. **EAP-TLS–TKIP**: EAP-TLS is used for authentication using digital certificates to authenticate the users and TKIP is used for encryption. EAP-Transport Layer Security or EAP-TLS uses PKI (Public Key Infrastructure) to secure communication to the RADIUS authentication server or another type of authentication server. Even though EAP-TLS provides excellent security, the overhead of client-side certificates may be a drawback. The requirement of EAP-TLS is that both client and server have a valid certificate from a trusted certificate authority.
7. **EAP-TLS–AES**: EAP-TLS is used for authentication using digital certificates to authenticate the users and AES is used for encryption.

4. Results of the experiments

In this section we will provide and discuss the measurements results of the conducted experiments.

4.1. The impact of different security mechanisms on the network performance in case of TCP and UDP protocols

The Network throughput (the amount of transmitted date over a period of time expressed in Mbits/Sec) for TCP and UDP protocols under different security mechanisms, using the 56 MB/Sec and 9 MB/Sec bandwidth respectively are shown in table 1. The measured values represent the total number of bytes transmitted between the wireless and the wired networks over a period of time, using the two bandwidths (9 Mb/s and 56 Mb/s).

Table 1

Network throughput (in Mbits/Sec) for TCP and UDP

Security scheme nr.		B.W. 56 MB/Sec			B.W. 9 MB/Sec	
		TCP	UDP		TCP	UDP
1	No Security	16.53	17.45		11.26	9.7851
2	WEP40	16.11	16.37		10.765	9.537
3	WEP128	15.59	16.287		10.402	9.303
4	WPA-PSK-TKIP	15.49	16.288		10.181	9.194
5	WPA-PSK-AES	15.86	16.288		10.176	8.84
6	EAP-TLS-TKIP	15.61	15.755		9.14	8.139
5	EAP-TKIP-AES	15.11	15.109		9.114	7.79

The same results are represented graphically in Fig. 4 and 5.

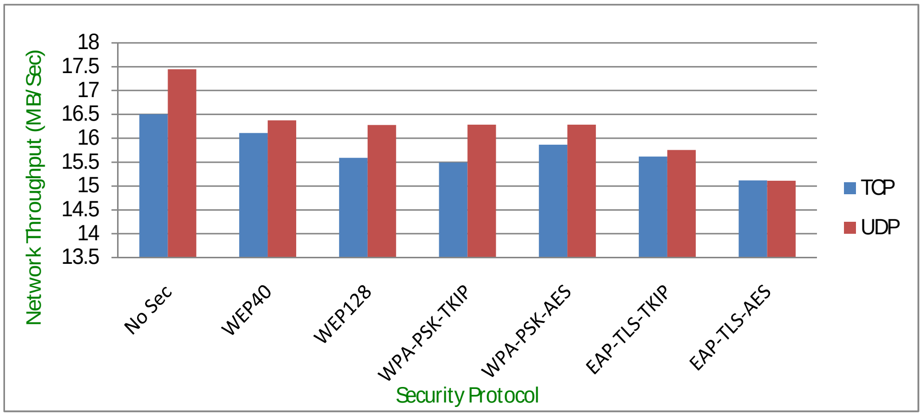

Fig.4. Network throughput for 56Mb/Sec bandwidth

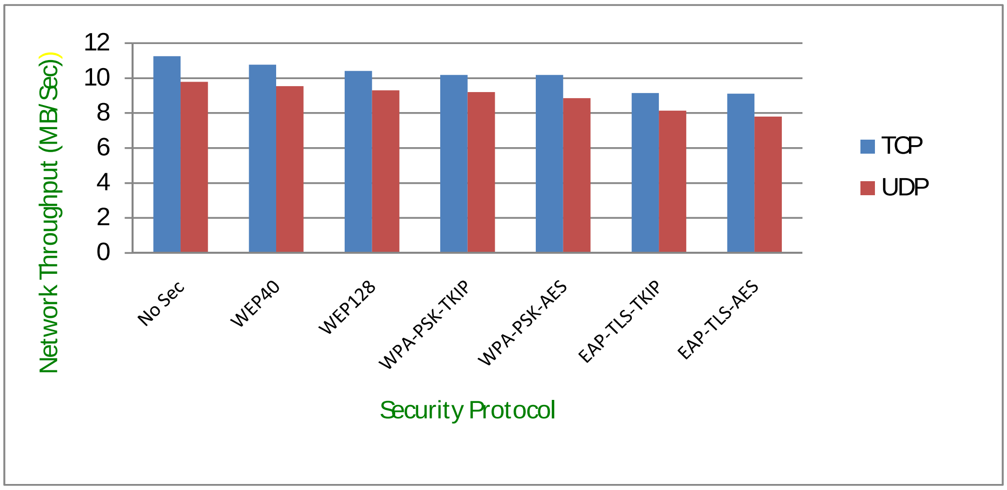

Fig. 5. Network throughput for 9Mb/Sec bandwidth

4.2. The network throughput in case of FTP and HTTP protocols under different security mechanisms

The network throughput for FTP and HTTP protocols under different security mechanisms to download the two files of sizes 64 MB and 11 MB respectively are shown in table 2.

Table 2

Network throughput (in Mbits/Sc) for FTP and HTTP protocols

		64 MB			11 MB	
Security scheme nr.		FTP	HTTP		FTP	HTTP
1	No security	22.242255	21.505		20.207	20.8465
2	WEP-40	21.0155	2.6257		16.628	16.7575
3	WEP 128	21.691	20.01		16.6953	16.9575
4	WPA-PSK-TKIP	21.104	20.1435		16.236	16.78
5	WPA-PSK-AES	21.21425	20.4915		16.982	16.78
6	EAP-TLS-TKIP	20.3115	19.8995		16.2865	17.5495
5	EAP-TLS-AES	21.48325	18.83375		14.8415	17.5495

The same results are graphically represented in Fig. 6 and 7.

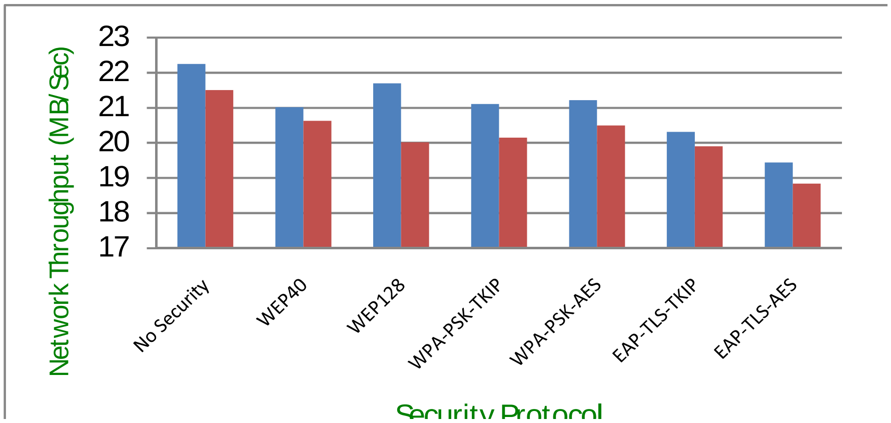

Fig.6. Network throughput for FTP and HTTP protocols to download a file of size 64 MB

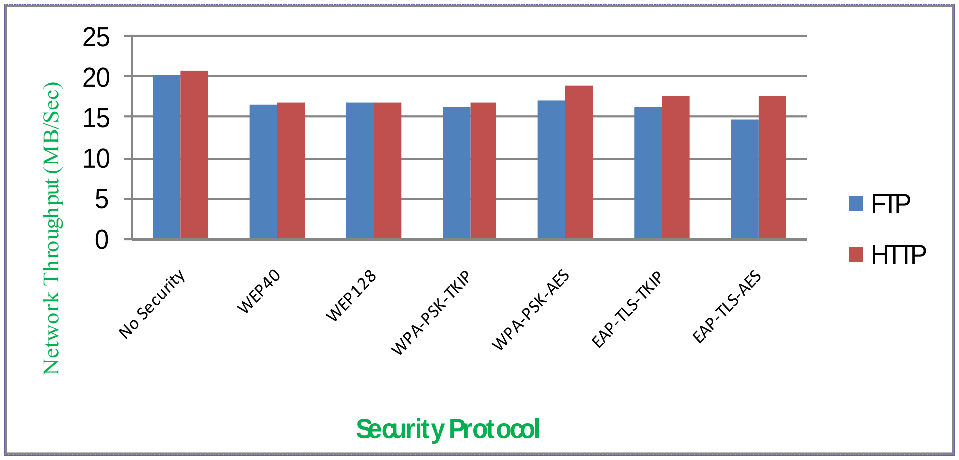

Fig.7. Network throughput for FTP and HTTP protocols to download a file of 11 MB

From fig. 4, 5, 6 and 7 results that the network throughput decreases as the security level increases, for both congested and normal traffic, because different authentication methods created different levels of performance overhead. EAP-TLS generated the longest delay and decreased throughput, as it provides mutual authentication and key management. A comparison of the authentication mechanisms can be summarized as follows: EAP-TLS > WPA > WEP.

Congested network traffic results in better performance than the normal network traffic. In addition, for congested traffic, the UDP (connectionless) traffic type performed better than TCP (connection oriented), because of the nature of TCP mechanisms for congestion avoidance and error control. Unlike UDP, TCP protocol detects packet drops and retransmit them, which gives lower network throughput.
The same situation results also in case of FTP and HTTP traffic types. FTP performed better than HTTP, because of the nature of HTTP mechanisms for congestion avoidance and error control.

Security scheme Nr. 5 (see table 1) offers the same or even higher network performance than security schemes 2, 3 and 4 (see table 1) which are less secure. This result is explained by the fact that - unlike WEP and TKIP processing which is done by software only - AES processing is done faster by means of hardware and the overhead produced by encrypting each individual packet is significantly smaller than in case of WEP and TKIP

4.3. Impact of Packet Length on the network performance under various security mechanisms

From the results in the previous experiments, it is clear that a congested network performs better than a normal network. In this set of experiments there were used a congested network to investigate the effect of the packet length on the network throughput for both TCP and UDP protocols under various security mechanisms.
Packet lengths of 100, 500, 1000, 1300 and 1500 bytes were chosen to simulate traffic consisting out of a mixture of short, normal and long packets.
Tables 3 and 4 contain the throughputs of congested network traffic, for UDP and TCP.

Table 3

Throughputs (in Mbits/Sec) for different packet sizes, using UDP

	NO SEC	WEP40	WEP128	WPA-PSK-TKIP	WPA-PSK-AES	EAP-TLS-TKIP	EAP-TLS-AES
100	3.937368	3.8527	3.74896875	3.8125	3.8125	3.9375	3.8125
500	12.86345	12.700	13.0263181	13.026355	12.86348	12.701506	12.863486
1000	19.50701	20.750	20.0780311	19.6764718	20.078125	19.867974	19.87734
1300	23.055	24.718	23.277139	22.84970	23.0352	23.2772463	23.0555581
1500	16.28185	19.900	13.867	15.54321	17.1148	15.53312	15.7386

Table 4

Throughputs (in Mbits/Sec) for different packet sizes, using TCP

	NO SEC	WEP40	WEP128	WPA-PSK-TKIP	WPA-PSK-AES	EAP-TLS-TKIP	EAP-TLS-AES
100	14.253	26.233	15.19875	14.75	14.75	14.406	15
500	18.248	18.2505	18.124	18	18.25	18.87775	18.25
1000	23.499	22.2505	23.157	23.5	23	23.40875	23.25
1300	26.002	24.25175	25.87625	26.25	26	25.823	26
1500	47.837	43.771	41	41	44.75	47.45	45.5

The same results are illustrated graphically in fig. 8, where 100-UDP represents a packet length of 100 bytes for UDP traffic type; 100-TCP represents a packet length of 100 bytes for TCP traffic type and so on.

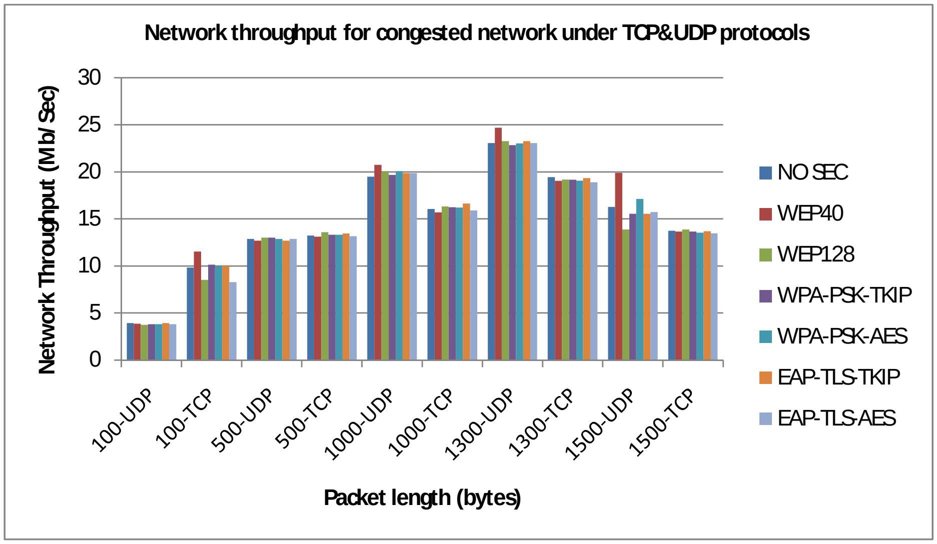

Fig. 8. Impact of packet length on network performance

Fig. 8 shows that the packet size of 1300 bytes gives the best network throughput for both TCP and UDP protocols, under various security mechanisms.

In case of packet sizes of 100 and 500 bytes, TCP performs better than UDP, while for packet sizes 1000 and 1300 UDP (connectionless) performed better than TCP (connection oriented), because of the nature of TCP mechanisms for congestion avoidance and error control. This is consistent with the results obtained when we studied the impact of different security mechanisms on the network performance in case of TCP and UDP protocols.

For a packet length of 1500 bytes the packets were fragmented, because the configuration of the networking devices used in our experiments was set up to fragment packets of 1500 bytes and larger; every IP based network has a Maximum Transmission Unit (MTU) size; the MTU is the size of the largest packet which that network can transmit before fragmentation occurs, which yields to network performance decrease. The packets of smaller lengths (500, 1000 and 1300) were not fragmented.

5. Conclusions

In this paper, we studied the impact of the traffic type (TCP, UDP, FTP, and HTTP), network traffic (normal and congested) and packet size on the network throughput, under different WLAN security mechanisms. From the obtained results, we can conclude that as we apply more secure mechanisms the network throughput decreases. Longer packet sizes can lead to best network performance under any security protocol.

Also from the results it is obvious that, choosing the security scheme Nr. 5 (WPA-PSK-AES) a very good network performance and a good security level is obtained. The vulnerability of offline dictionary attack can be mitigated through the use of the new Wi-Fi protocol (Wi-Fi Protected setup), ratified in Jan 2007 [24]. It provides secure and easy way for distributing keys for WPA protocols for midsize networks and can be used in an enterprise network for users that require only Internet services and file sharing.

By selecting the appropriate security mechanism for a particular network one must take the above results into consideration. That is, if the security is a major concern, especially for an enterprise network, then a more secure mechanism must be chosen. On the other hand, if security is a less concern one can choose a less security mechanism which means increase in network performance by less requirements for extra hardware or/and administration overhead.
Our proposed solution is to assign dedicated VLAN for users that require only simple services like Internet surfing and file sharing. To that VLAN security scheme no. 5 (see table 1) using the Wi-Fi protected Setup protocol for automatic key distribution. This configuration can achieve high performance and good security level. Wireless users that require access to the enterprise internal network can be assigned to a secure VLAN that has a higher security mechanism i.e. schemes 6, 7 to protect the internal network, on the expense of experiencing a lower network performance.

TABLE OF ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
AD	Active Directory
AES	Advanced Encryption standard
AP	Access Point
CCK	Complementary Code Keying
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security

ICV	Integrity Check Vector
IIS	Internet Information Services.
IV	Initialization Vector
LDAP	Lightweight Directory Active Protocol
MIC	Message Integrity Code
OFDM	Orthogonal Frequency Division Multiplexing
RADIUS	Remote Authentication Dial In User Service
TKIP	Temporary Key Integrity Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

REFERENCES

[1]. Secure Wireless Access Point Configuration, URL: http://www.microsoft.com/ downloads/ details.aspx?FamilyID=27390BD4-D920-43AF-98A1-0F53FBB90A02& displaylang =en

[2]. *Changhua He, John C Mitchell, "*Analysis of the 802.11i 4-Way Handshake", URL: http://byte.csc.lsu.edu/~durresi/7502/reading/p43-he.pdf

[3]. *Jim Burns, "*Best Practices Wireless LAN Security' URL: http://www.mtghouse.com/ best_practices.pdf

[4]. *Cisco* − Cisco Secure ACS for Windows v3.2 With EAP−TLS Machine Authentication*, URL: http://www.cisco.com/warp/public/480/acs-eap.pdf*

[5]. *Vijay Chandramouli*, "A detailed study of wireless LAN technologies", URL: http:// crystal.uta.edu/~kumar/cse6392/termpapers/Vijay_paper.pdf#search='A%20Detailed%20Study%20on%20Wireless%20LAN%20Technologies

[6]. *Nedier Janvier Sena,* "IEEE 802.11 Wireless LAN Security Performance Using Multiple clients" http://www.cosc.canterbury.ac.nz/research/reports/HonsReps/ 2003/ hons_0304 .pdf

[7]. *Stanley Wong,* "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards", URL: http://www.sans.org/rr/ whitepapers /wireless/ 1109.php

[8]. *TakehiroTakahashi,* "WPA Passive Dictionary Attack Overview", URL: http:// www.tinypeap .com / docs/WPA_Passive_Dictionary_Attack_Overview.pdf

[9]. *Changhua He, John C Mitchell,* "Security Analysis and Improvements for IEEE 802.11i " http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/NDSS05-1107.pdf

[10]. *Janice Reynolds* "Going WLAN: A practical guide to planning and building an 802.11 network", CMP Books 2003 ISBN-10: 1578203015

[11]. Certified Wireless Network Associate Official Study guide, McGrew-Hill, 2nd edition, 2003.

[12]. EEE 802.11i, URL:http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[13]. *Kevin Tyrrell, "*An over view of Wireless security issues" GSEC V1.4b SANS Institute

[14]. *Jesse R. Walker*," IEEE 802.11 Wireless LAN Unsafe at any key size; an analysis of the WEP encapsulation", URL:http://citeseer.ist.psu.edu/558358.html

[15]. *Wong Stanley,* GSEC "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards", SANS institute.

[16]. *Adam Stubbleefield,* "Strengthening 802.11i Implementations with Additional Standards-based Mechanisms", URL: http://www.lancs.ac.uk/ postgrad/grech/ 802.11i_white_paper .pdf

[17]. *John Ioannidis,* "A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP) ", URL: http:// www.cs.jhu.edu/ ~rubin/ courses/ sp04/ wep.pdf

[18]. *Anrech Mishra, William A. Arbaugh*, "An initial security analysis of IEEE 802.11x standard" , URL: http://www.cs.umd.edu/~waa/1x.pdf

[19]. *Wade Williamson,* "Best Practices For Securing Your Enterprise WLAN",URL: http://www.airmagnet.com/products/wp-index.htm

[20]. *Dan Simon, Bernard Aboba, Tim Moore,* "IEEE 802.11 Security and 802.1X", URL: http:// www.ieee802.org /1/files/public/docs2000/8021xSecurity.PDF

[21]. *Davin Akin,* "802.11i authentication and key management (AKM)", URL: http:// www.cwne.com/learning_center/search_details.php?doc_id=duge

[22]. *Sean Convery, Darrin Miller, Sri Sundaralingam,* "Cisco SAFE: Wireless LAN Security in Depth", URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

[23]. "802.11i, WPA, RSN and What it all Means to WLAN Security**",** , URL: http: //www.microsoft.com/downloads/details.aspx?FamilyID=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en, 11-2005.

[24]. "Introducing Wi-Fi Protected Setup", URL: http://www.wi-fi.org/files/ wp_18 _ 20070108 _Wi-Fi_Protected_Setup_WP_FINAL.pdf , Jan 2007

[25]. *Harold Lars, McCarter,* "Analyzing Wireless LAN Security Overhead", URL: http:// scholar.lib.vt. edu /theses/available/etd-04202006-80941/unrestricted/ ccarter_thesis.pdf

[26]. *Jenne Wong,* "Performance Investigation of Secure 802.11 Wireless LANS: Raising the security Bar to Which Level?", URL: http://www.cosc.canterbury.ac.nz/ research/reports/ MastTheses/2003/ mast_0301.pdf

[27]. IP Traffic - Test & Measure software version 2.4.1, URL: http://www.pds-test .co.uk/products/ip_test_measure

[28]. Wireshark Traffic analyzer software, URL: http:// 1.0.0. http://www.Wireshark .org/ download.html.