A COMPARISON BETWEEN WIRELESS LAN SECURITY PROTOCOLS

Nidal TURAB[1], Florica MOLDOVEANU[2]

Articolul prezintă o analiză a protocoalelor WEP, WPA şi IEEE 802.11i din punct de vedere al cerinţelor de securitate pentru reţelele locale wireless (WLAN). Acestea sunt apoi comparate prin prisma a două criterii: nivelul de securitate a reţelei pe care-l asigură fiecare dintre ele şi influenţa pe care o au asupra performaţei reţelei.

The paper presents an analysis of the WEP, WPA and IEEE 802.11i protocols, from the WLANs security requirements point of view. Then, they are compared by two criteria: the network security level that each one assures and their influence on the network performance.

Keywords: - IEEE 802.11i, WEP, WPA, TKIP, CCMP and WPS.

1. Introduction

Security is the major weakness in the wireless technology, because there is no control over the communication channel (the wireless medium). In the wired networks each communication party has to have physical access to the communication media (i.e. wire). Wireless communication media is an open media where each user with a device equipped with wireless interface can use and share the airwave transmission medium with other users. Some of the weakness WLAN drawbacks are:

- no physical control over wireless network connections;
- weak built-in security measures;
- unmonitored, untrusted connection to wired network core.

In the past years several security protocols (i.e. WEP, WPA, IEEE 802.11i) were developed to add more authentication, confidentiality, message integrity of the WLAN.

Any security mechanism used in WLAN must provide the following features:

[1] PhD, Dept. of Computers, University POLITEHNCA of Bucharest, Romania, e-mail: nedalturab@hotmail.com
[2] Professor, Dept. of Computers, University POLITEHNCA of Bucharest, Romania, e-mail: Florica.Moldoveanu@rdslink.ro

- o Confidentiality - keeping information unreachable for unauthorized users;
- o Authentication - the process of determining whether the user is actually the same as he claims to be or not, before he can gain access to the network resources;
- o Integrity - how one can be sure that a message he received wasn't modified in transit.

This paper presents an analysis of the most important and used security mechanisms implemented to overcome the security problems of WLANs. We identify their strength and weaknesses from the security point of view. This comparison, combined with results obtained regarding the influence of these mechanisms on the network performance, ca be a valuable guide in deciding what security protocol to choose for a particular WLAN.

2. WEP (Wired Equivalent Privacy)

Wired Equivalent Privacy (WEP) was developed to provide a WLAN security equivalent to that of a wired LAN. WEP algorithm uses a XOR operation applied on plaintext (bit by bit) with a pseudorandom key sequence of equal length.
WEP is a symmetric algorithm where the same key is used for encryption and decryption.
Encryption begins with a secret key that has been distributed to the wireless stations .The secret key is concatenated with an initialization vector (IV) and the resulting seed is input to a pseudorandom generator (PRNG). The PRNG generates a key sequence (K) of pseudorandom octets equal in length to the number of data octets that are to be transmitted plus 4 (since the key sequence is used to protect the Integrity Check Value (ICV) as well as the data). The encryption process of WEP is depicted in fig. 1.

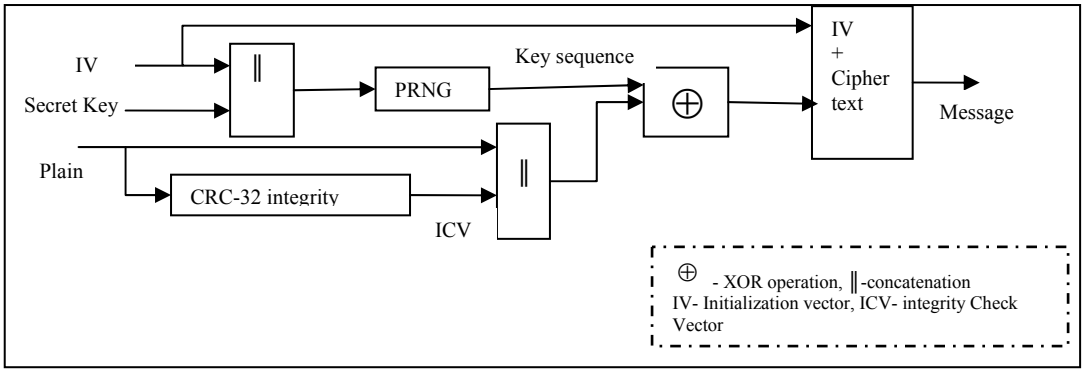

Fig. 1 WEP encryption process

The IV may be changed for every packet and, since it travels with the message, the receiver will always be able to decrypt any message. The IV is transmitted as clear text since its value must be known by the recipient in order to perform the decryption.
The decryption process begins with the arrival of a message. The IV of the incoming message shall be used to generate the key sequence necessary to decrypt the incoming message. Combining the ciphertext with the key sequence yields the original plaintext and ICV. Correct decryption is verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV to the ICV transmitted with the message. If the both values are not equal then the received message is considered as being corrupted. As desiccated in fig. 2.
WEP uses encryption keys only; it does not perform data authentication. Therefore, it does not have data integrity keys.

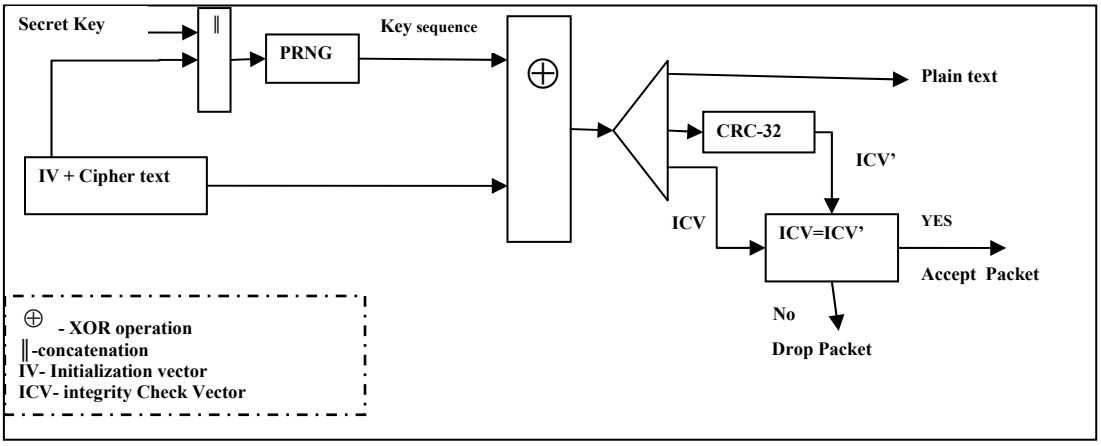

Fig. 2 WEP decryption process

2.1 WEP problems

- **IV limited space**: One of the problems of WEP is that IV is only 24 bits long. A 24 bit IV means there are 2^{24} combinations =16777216, which means there can be 2^{24} frames transmitted before the IV space is exhausted. Once this happened, the IVs will begin to cycle through previously used values for the IV. These possibilities of IV combinations are not so large, thus for IEEE 802.11g, WLAN operates at 54 Mb/s = 6750000 bytes sent per second, with packet length of 1500 bytes which yields to 6750000 / 1500 = 4500 packets / second
2^{24} / 4500= 3728 seconds = about 1 hour. This period will be shorter for packets less than 1500 bytes

- **Passive Attack**: refers to traffic decryption; an eavesdropper can intercept all wireless traffic, until an IV collision occurs (two packets that use the same IV). By XORing these two packets, the attacker obtains the XOR operation of the two cipher texts to obtain the two plain texts as follow :
  Let CT'_1, CT'_2 be the two cipher text that use the same IV; PT_1, PT'_2 the two plain texts.
  $CT'_1 = PT_1 \oplus RC4\ (IV, K)$ and $CT'_2 = PT'_2 \oplus RC4\ (IV, K)$ then:
  $CT'_1 \oplus CT'_2 = (PT1 \oplus RC4\ (IV, K)) \oplus (PT'_2 \oplus RC4\ (IV, K))$
  $= PT'_1 \oplus PT'_2$.
  Once it is possible to recover the entire plaintext for one of the messages, the plaintext for all other messages with the same IV follows directly, since all the pairwise XORs are known.
- **Active attack:** refers to traffic injection in case an attacker knows the exact plaintext for one encrypted message. He can use this knowledge to construct correct encrypted packets. The procedure involves constructing a new message, calculating the CRC-32, and performing bit flips on the original encrypted message to change the plaintext to the new message. The basic property is that $RC4(X) \oplus X \oplus Y = RC4(Y)$. This packet can now be sent to the access point or wireless device and it will be accepted as a valid packet. Other form of this attack is to flip selected bits in a message and successfully adjust the encrypted CRC, to obtain a correct encrypted version of a modified packet. If the attacker has partial knowledge of the contents of a packet, he can intercept it and perform modifications on it.
- **Transitive trust:** If the WLAN is a part of the enterprise network, the intruder can use a wireless device to launch a transitive trust attack by using a wireless device as rouge node in the network or as rouge access point so that all the wireless stations will try to associate with the rouge device rather than the real access points.
- **Denial of Services (DoS):** denial of services attacks can be launched by using a powerful transmitter to generate powerful radio signals that interfere with WLAN transmission which makes wireless devices unable to use the radio path.

3. WPA (Wi-Fi Protected Access)

The Wi-Fi Protected Access (WPA) standard was developed by the Wi-Fi alliance as an interim replacement for WEP. As an interim version of the IEEE 802.11i security specification, WPA adopts TKIP to fix flaws in WEP protocol and includes packet integrity.

WPA has two modes of authentication process: Preshared Key (PSK) and IEEE 802.1x.
1) In the PSK authentication method, a key is manually set into each device of the wireless network. The PSK is used directly as the Pairwise Master Key (PMK) which is produced to create other keys used for encryption. Since the PSK method is simpler, it has some disadvantages that are not present when using IEEE 802.1x authentications. PSK key manually set may be changed if needed, on each device on the wireless network [21, 23].
2) In case of the IEEE 802.1x authentication method, special authentication server software known as ***AAA (Authentication, Authorization and Accounting***) server is required. The Access Point (AP) needs to authenticate itself to the wireless client and to derive encryption keys that used to encrypt the traffic. By means of EAP message exchange (Extensible Authentication Protocol -EAP- which defines the end-to-end message formats used in a simple request-response mode of interaction between the client and authentication server) the shared secret key PMK is provided. This key will last the entire session. Therefore the four-way handshake is used to establish another key called the Pairwise Transient Key (PTK). The PTK is generated by concatenating the following attributes: PMK, access point nonce (ANonce), station nonce (SNonce), access point MAC address and station MAC address; the resulting string is then put into MD5 cryptographic hash function.
The handshake also yields the Group Temporal Key (GTK) [3], used to decrypt multicast and broadcast traffic. The actual messages exchanged during the handshake are depicted in fig. 3.

- The access point sends a nonce-value to the station (ANonce). The client now constructs the PTK.
- The station sends its nonce-value (SNonce) to the access point together with a MIC (MIC: "Message Integrity Code" will be explained later).
- The AP sends the GTK and a sequence number together with another MIC. The sequence number is the sequence number that will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
- The station sends a confirmation to the AP.

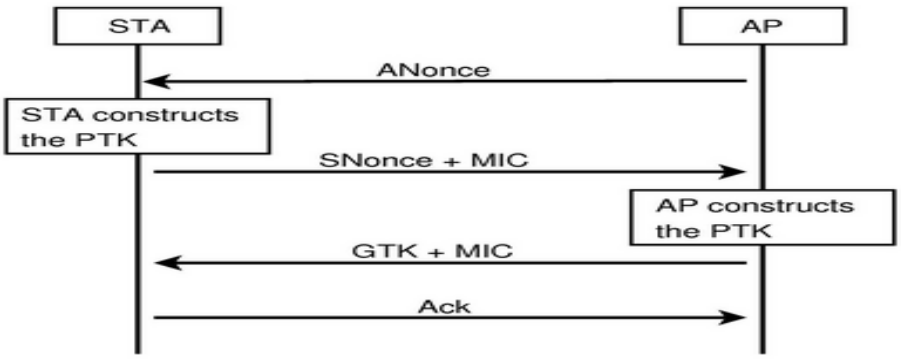

Fig. 3 Four-Way Handshake process

As soon as the PTK is obtained it is divided into three separate keys:

- EAPOL-Key Confirmation Key (KCK) - the key used to compute the MIC for EAPOL-Key packets.
- EAPOL-Key Encryption Key (KEK) - the key used to provide confidentiality for EAPOL-Key packets.
- Temporal Key (TK) - the key used to encrypt the actual wireless traffic.

Extended Authentication Protocol (EAP) is an authentication framework that provides some common functions and a negotiation of the desired authentication mechanism. When EAP is invoked by an 802.1x authentication device such as wireless AP, EAP methods can provide a secure authentication mechanism and negotiate a secure PMK between the client and authentication server. The PMK can then be used for the wireless encryption session which uses TKIP (Temporal Key Integrity Protocol) or CCMP (CCMP: Counter mode with Cipher block chaining Message authentication code Protocol will be explained in Sec.4.3.1).
One of the EAP methods used in IEEE 802.1x is EAP-TLS, which uses Public Key Infrastructure PKI to secure communication to the RADIUS authentication server or any type of authentication server. The requirement of EAP-TLS is that both client and server have a valid certificate from a trusted certificate authority. So even though EAP-TLS provides excellent security, the overhead of client-side certificates may be a drawback.

The encryption algorithm used in WPA is the ***Temporal Key Integrity Protocol (TKIP***), it uses IV and RC4, but the IV has been extended to 48 bits, and is used as TKIP Sequence Counter (TSC). The first 16 bits of the TSC are stored in the WEP IV field, while the remaining 32 bits are stored in a field known as the extended IV. As a result the protocol data unit is expanded to accommodate this

additional field. The 48 bit TSC is an increasing counter initialized to 1 when the TKIP Temporal Key is initialized or changed. Each frame received must have a TSC greater than the TSC in the previous frame received from the same sender. This provides protection from replay attacks. The TSC space is 48 bits. This means over 248 =281474976710656 (more than two trillion) frames can be sent before all TSC values are reused for a single temporal key. An access point operating at 54Mbps continuously sending 1500 byte packets will require more than 1983 years exhausting the TSC space, e.g. For IEEE 802.11 g WLAN operating at 54 Mb/s = 6750000 bytes sent per second, with packet length of 1500 byte which yields to 6750000 / 1500 = 4500 packets / second. Which yields to 248 / 4500= 62549994824 seconds = 17374998 hour = 1983 years.

TKIP has a 64 bit Message Integrity Code (MIC) called Michael, to protect messages from being modified in transit. The MIC is calculated over the destination and source address, a priority field, three reserved octets and the entire plaintext message payload [3, 19, 22].

MIC detects active attacks and countermeasures can be employed to prevent further attacks. The WEP ICV is still used in conjunction with the MIC to prevent false detection of MIC failures, and therefore false countermeasure initiation.

3.1 WPS (Wi-Fi Protected Setup)

This newly emerging protocol created by the Wi-Fi Alliance and officially launched on January 2007, called Wi-Fi Protected Setup (WPS) is designed for easy and secure establishment of a wireless network. The standard defines four methods to add a new device to the network, two mandatory and two optional. We will explain the mandatory options as stated in [23]:

- PIN method: a PIN (Personal Identification Number) has to be read from a sticker on the new station. This is the mandatory method; every Wi-Fi Protected Setup certified product must support it.
- Push Button Configuration (PBC) method: the user simply has to push a button, either an actual or virtual one, on both the Access Point and the new wireless client device. Support of this model is mandatory for Access Points and optional for wireless stations.

The WPS protocol defines three types of devices in a network:
1) Registrar: A device with the authority to issue and revoke credentials to a network. A Registrar may be integrated into an Access Point, or it may be separate from it.
2) Enrollee: A device seeking to join a wireless LAN network.

3) Authenticator: An Access Point functioning as a proxy between a Registrar and an Enrollee

For secure distribution key and network configuration, Wi-Fi protected setup uses two modes of operation: in-band and out-of-band.
In case of " In-band" configuration" PIN or password is used .
In case of "Out-of-band" configuration, a USB flash drive or NFC (Near Field Communication) is used.

WPS also defines the concept of Registration Protocol as logical three party in-band protocols to assign a Credential to the Enrollee. The protocol operates between the Enrollee and the Registrar and may receive support through a proxy.
In case of Registration Protocol the user is prompted to enter the device password, then the Registrar sends a message containing the Registrar's description to the Enrollee. This message enables Enrollees to give appropriate instructions to the user and direct them to use the correct Registrar. Other Registration Protocol messages incrementally demonstrate mutual knowledge of the device password, and then the encrypted configuration data is exchanged. Cryptographic protection for the messages is based on a key derivation key (KDK) that is computed from the values of the Diffie- Hellman secret, nonces, and Enrollee MAC address.

3.1.1 Security of WPS

The Wi-Fi Protected Setup Registration protocol is designed to provide strong protection against passive attacks and also to detect and to protect the system from active brute force attack for both in-band and out-of-band configurations.

For in-band configuration, if a Registrar detects an attacker that pretends to be a legitimate Enrollee, it first detects that the attacker does not know the password. This detection occurs before the Registration protocol gives enough information to expose the password to brute force attack. To address the brute force attack, if a PIN authentication or communication error occurs after sending specific message, the Registrar warns the user and will not automatically reuse the PIN. The Registrar will not accept the same PIN again without warning the user of a potential attack. If a strong device password with at least 32 bytes of randomness is used instead of a PIN, the Registrar is permitted to use this password multiple times without warning the user when failures occur.

For out-of-band configuration, large device passwords (such as 256 bit random values) can be sent to the Registrar. The hash of the Enrollee's public key is also included.

Encrypted key can use a key derived from the Diffie-Hellman public key of the Enrollee obtained over the in-band channel, along with that of the Registrar, to encrypt settings for that specific Enrollee.

In Out-of-band configuration, a USB flash drive or NFC (Near Field Communication; it is a contact less technology for very short-range operation less than 10cm) are used. If the USB or NFC is used to enter the device password, the Registrar also provides the hash of the Enrollee's Diffie-Hellman public key. This process strengthens the authentication of the Enrollee to the Registrar.

3.2 Vulnerability of PSK mode of WPA

The PSK version of WPA suffers from offline dictionary attack because of the broadcasting of information required to create and verify a session key. In case of WPA, the PMK (master key) is generated in order to create the PTK and install it on both sides.

The PMK is generated by inputting the string of the pass phrase, Service Set Identifier SSID (unique, case sensitive alphanumeric name of the wireless network) and the SSID length into the hashing algorithm, which is set to hash 4096 times and generate a value of 256 bits. Since the SSID is easily recoverable, it should be noted that only the pass phrase would have to be guessed in order to determine the valid PMK.

Furthermore, in the generation of the PTK for cracking purposes, only the PMK needs to be determined since all other fields can be trivially discovered; the first step in the 4 way handshake provides ANonce and access point MAC address while the second step provides SNonce and station MAC address, and the signature of the PTK just generated. After receiving the first packet of the 4way handshake traffic, the client generates the PTK and runs MD5 hash function on the KCK and the EAP packet to be sent. This hash is then added to the EAP packet and sent over the network as the 2nd step. Now, an intruder can utilize the hash portion of this packet and match it with the hash result of his guessed PTK and collected EAP packet; the correctly guessed pass phrase produces the same signature. Hence the intruder, by passively sniffing two of the EAPOL packets, can begin an offline dictionary attack. [19] This attack is illustrated in fig. 4.

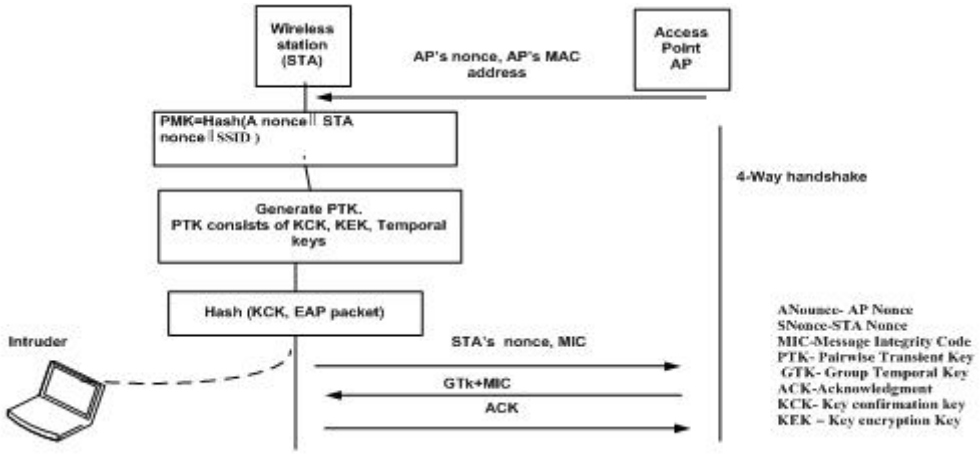

Fig. 4 WPA passive dictionary attack.

4. IEEE 802.11i

The IEEE 802.11i specification is a solution of the IEEE 802.11 for improving the security problems of WEP. The IEEE 802.11i includes several key features:

- Encryption algorithms
  - o TKIP - in order to support legacy devices, the IEEE 802.11i chooses TKIP as one of the encryption standards (similar with WPA).
  - o CCMP – IEEE 802.11i also includes another encryption protocol known as AES-CCMP. AES stands for advanced encryption standard, which is a strong encryption algorithm; AES-CCMP requires extra hardware to be used.
- Message Integrity – A strong data integrity algorithm (Michael Message Integrity Check) is applied (similar as in case of WPA).
- Mutual Authentication – 802.11i uses 802.1x/EAP for user authentication (similar as in case of WPA).
- Other security features - secure Independent Basic Service Set (IBSS), secure fast handoff (wireless device can move from one access point to a second access point without disrupting data transmission), and secure deauthentication and disassociation.
- Roaming Support

The IEEE 802.11i defines two classes of security algorithms for IEEE 802.11 networks:

1) Algorithms for creating and using a Robust Security Network Association, called RSNA algorithms (TKIP, CCMP, RSNA establishment and termination procedures, including use of IEEE 802.1X authentication and Key management procedures).

2) Pre-RSNA algorithms (WEP authentication).

A wireless station can simultaneously operate pre-RSNA and RSNA algorithms.

4.1 Security associations

IEEE 802.11i uses the notation of a security association to describe secure operation. A security association is a set of policies and keys used to protect information. The information in the security association is stored by each party of the security association, and it must be consistent among all parties, and it must have an identity.

There are four types of security associations supported by an RSN STA:

1) Pairwise master key security association (PMKSA): the result of a successful IEEE 802.1X authentication exchange between the station and Authentication Server (AS) or from a preshared key (PSK), PMK information, or PMK cached via some other mechanism.

2) Pairwise transient key security association (PTKSA): the result of a successful Four-Way Handshake exchange between the station and Authenticator.

3) Group temporal key security association (GTKSA): the result of a successful group temporal key (GTK) distribution exchange via either a Group Key Handshake or a Four-Way Handshake.

4) STA Key security association (STAKeySA): the security context for direct station-to-station communication in an infrastructure basic service set (BSS).

4.2 Pre-RSNA security methods

In an extended service set ESS (two or more wireless access points and wireless stations, while the access points are connected to the wired network), each wireless station must complete an IEEE 802.11 authentication exchange with the access point prior to association. Such an exchange is optional in an IBSS network. (The Independent Basic Service Set consists of minimum two wireless stations without any access point).

As IEEE 802.11 authentication is performed between pairs of stations, broadcast/multicast authentication is not allowed. Shared Key authentication is deprecated and should not be implemented except for backward compatibility with pre-RSNA devices.

4.3 RSNA data confidentiality protocols

IEEE 802.11i defines two RSNA data confidentiality and integrity protocols: TKIP (as in WPA) and CCMP. Implementation of CCMP shall be

mandatory in all IEEE 802.11i RSNA compliant devices. Implementation of TKIP is optional for an RSNA. The aim for TKIP was that the algorithm should be compatible with the devices that supporting only WEP; only firmware upgrade is required to support TKIP. RSNA devices should only use TKIP when communicating with devices that are unable or are not configured to communicate using CCMP**.**

CCMP (CTR with CBC-MAC Protocol)

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) provides confidentiality, authentication, integrity, and replay protection. CCMP is an IEEE 802.11i encryption protocol, created to replace, together with TKIP, the insecure WEP protocol, and use AES encryption algorithm. CCMP combines CTR for confidentiality and CBC-MAC (Cipher Block Chaining Message Authentication Code used for constructing a message authentication code from a block cipher) for authentication and integrity. CCMP protects the integrity of the transmitted data. CCMP is mandatory for RSN compliance.

All AES processing used within CCMP uses a 128-bit key and a 128-bit block size. CCMP is a generic mode that can be used with any block-oriented encryption algorithm.

CCMP requires a fresh temporal key for every session. CCMP also requires a unique nonce value for each frame protected by a given temporal key. CCMP uses a 48-bit packet number (PN) for this purpose. Reuse of a PN with the same temporal key violates the security of the CCMP.

CCMP processing expands the original size of MPDU (Medium access control Protocol Data Unit), is the unit of data exchanged between two peer MAC entities [3]) by 16 octets, 8 octets for the CCMP header field and 8 octets for the MIC field.

The CCMP header field is constructed from the packet number (PN), ExtIV, and Key ID subfields. CCMP does not use the WEP ICV.

The ExtIV subfield of the Key ID octet, that CCMP header field extends the MPDU header by 8 octets, compared to the 4 octets added to the MPDU header when WEP is used. The ExtIV bit is always set to 1 for CCMP.

CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting cipher text, which involves the following steps:

I. Increment the PN (which is a 48-bit) by a positive number for each MPDU. The PN shall never repeat for a series of encrypted MPDUs using the same temporal key.

II. Use the fields in the MPDU header to construct the additional authentication data (AAD) for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD.
III. Construct the CCM Nonce block from the PN, A2, and the Priority field of the MPDU where A2 is MPDU Address 2. The Priority field has a reserved value set to 0.
IV. Place the new PN and the key identifier into the 8-octet CCMP header.
V. Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and MIC. This step is known as CCM originator processing: The CCM originator processing provides authentication and integrity of the frame body and the AAD as well as confidentiality of the frame body. The output from the CCM originator processing consists of the encrypted data and 8 additional octets of encrypted MIC.
VI. Form the encrypted MPDU by combining the original MPDU header, the CCMP header, the encrypted data and MIC.

The CCMP encryption process is illustrated in fig. 5

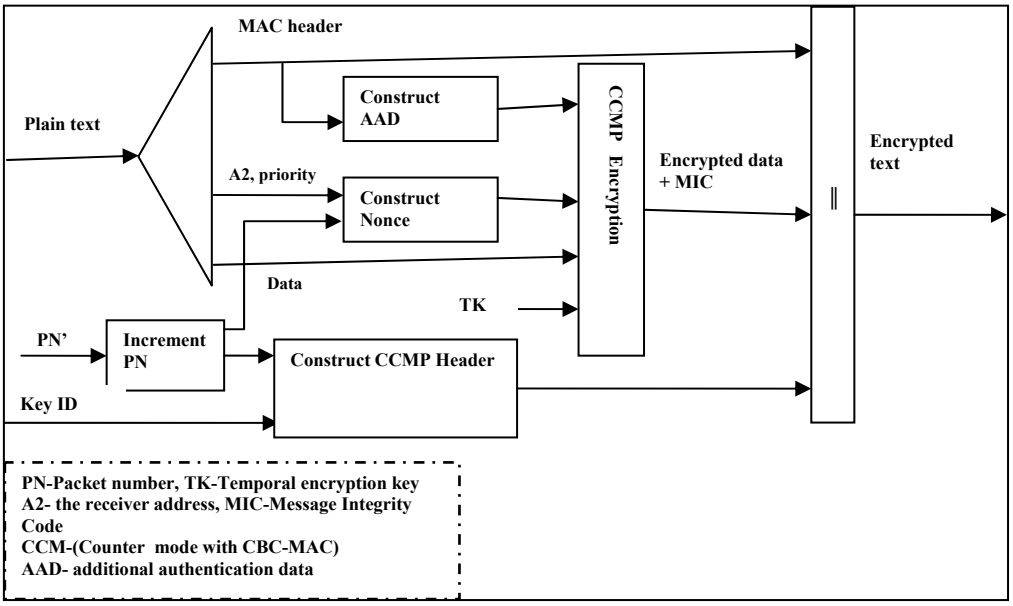

Fig. 5 CCMP encryption process.

CCMP decrypts the payload of a cipher text MPDU and decapsulates a plaintext MPDU using the following steps:

I. The encrypted MPDU is parsed to construct the AAD and nonce values.
II. The AAD is formed from the MPDU header of the encrypted MPDU.
III. The nonce value is constructed from the A2, PN, and Priority Octet fields (reserved and set to 0).
IV. The MIC is extracted for use in the CCM integrity checking.
V. The CCM recipient processing uses the temporal key, AAD, nonce, MIC, and MPDU cipher text data to recover the MPDU plaintext data as well as to check the integrity of the AAD and MPDU plaintext data.

The received MPDU header and the MPDU plaintext data from the CCM recipient processing may be concatenated to form a plaintext MPDU.

The decryption processing prevents replay of MPDUs by validating that the PN in the MPDU is greater than the replay counter maintained for the session [3,7,16,18].

The decapsulation process succeeds when the calculated MIC matches the MIC value obtained from decrypting the received encrypted MPDU. The original MPDU header is concatenated with the plaintext data resulting from the successful CCM recipient processing to create the plaintext MPDU. The CCMP decryption process is illustrated in fig. 6.

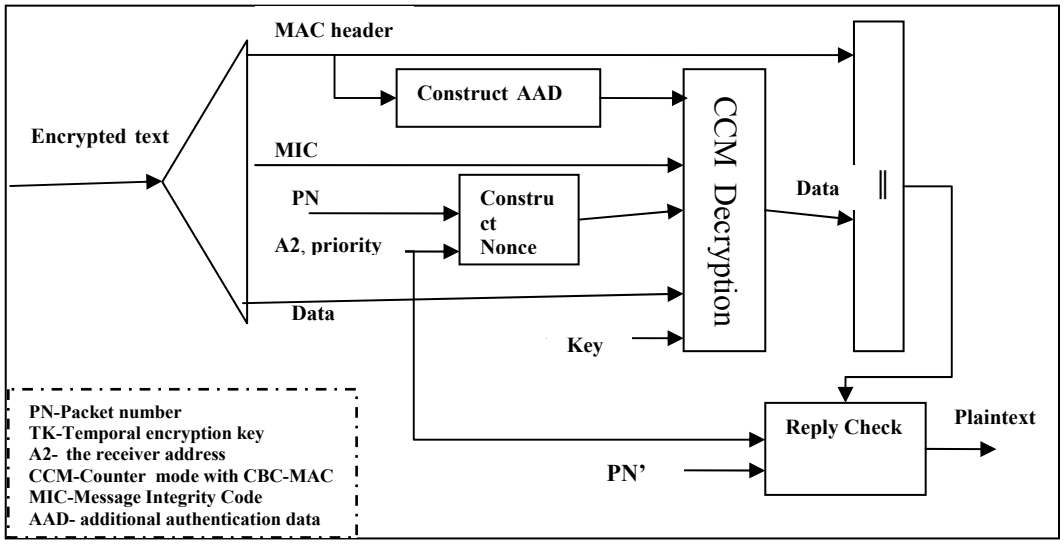

Fig. 6 CCMP decryption process.

4.4 Vulnerability

The possible vulnerability of IEEE 802.11i is the DoS (Denial of Service) attack that was discussed by Changhua He John C Mitchell in [16] where the authors stated that ”*since the management frames and control frames are*

unprotected in a WLAN, an adversary can easily forge these frames to launch a DoS attack. Among the management frame attacks, the most efficient attack is to forge and repeatedly send Deauthentication or Disassociation frames. This vulnerability can be mitigated by using Central Manager to handle these frames specifically and identify the forged frames by their abnormal behavior". Table 1 illustrates a comparison between security protocols used in WLAN, from Security Vulnerabilities point of view.

Table 1

Security Vulnerabilities of different security protocol

Security threat	Does the protocol open to the threat		
	WEP	**WPA**	**IEEE 802.11i**
Weak encryption	Yes	No (TKIP and AES are strong Encryption protocols	No (TKIP and AES are strong Encryption protocols
Off line dictionary attacks	Yes	Pre-shared key Mode is exposed	No((IEEE820.1x is used)
Illegitimate message Deletion and insertion	Yes	No (MIC is used)	No (CCMP is used)
Man in the Middle attack (MITM)	Yes	Pre-shared key Mode is exposed	No (IEEE820.1x is used)
Media Access Control (MAC) spoofing	Yes	Pre-shared key Mode is exposed	No (IEEE820.1x is used)
Man in the Middle attack (MITM):	Yes	Pre-shared key Mode is exposed	No (IEEE820.1x is used)
Rouge Access point	Yes	Yes (unless IEEE802.1x is used)	No
Denial-of-Service attacks (DoS)	Yes	Yes	Yes

5. Comparison of the security protocols

When evaluating the security protocols for WLAN, there are different criteria that should be considered such as:

- The level of security offered by different security protocols.
- How much contribute these protocols to decrease the network performance?
- The required hardware and software upgrades for implementing different security protocols.
- The possibility of implementing these protocols on old wireless hardware?
- What security protocol is suitable for a specific network size (small, medium or large)?

From the above discussion of the security protocols we can conclude that WEP is easy to implement and does not require any software or hardware upgrade, but it is the weakest security protocol and has several vulnerabilities like:

IV limited space, active attacks, passive attacks and transitive trust attack. It is suitable for home use only.
WPA provides well defenses against WEP threats, because:

- the TKIP Sequence Counter (TSC) is increased for each packet to prevent replay attacks,
- the 48 bit TSC long overcomes the problem of IV limited space,
- protects against active and passive attacks because there will be no two packets with the same IV number.

For encryption, WPA uses TKIP encryption algorithm with RC4 and IV in the same way like WEP but the larger space of TKIP key makes it stronger than WEP. TKIP uses MIC algorithm to prevent message modification in transit.

Possible vulnerability of WPA when it is used in the PSK mode is the offline dictionary attack. This attack can be mitigated by using the Wi-Fi Protected Setup protocol to automatically distribute keys and network configuration. This automated process is secure because it uses *Diffie-Hellman authentication*. WPA is suitable for use in small and medium networks.

Finally IEEE 802.11i gives the best security level of all protocols, because it uses a stronger encryption algorithm (AES based on CCMP), data integrity (CBC-MAC), replay protection (Packet Number) and stronger authentication (IEEE 802.1x/ EAP-TLS). In addition IEEE 802.11i includes also other security features like for instance: secure fast handoff, secure deauthentication, disassociation and Roaming support.

On the other hand, IEEE 802.11i does not support backward compatibility with the legacy devices and requires additional hardware and software implementations (e.g. authentication server, valid digital certificate, and support of CCMP).

The influence of various security schemes on network performance was studied by the authors of this paper with regard to the IEEE 802.11g networks throughput, under different network loads (normal and congested) and for various traffic packet sizes (from 100 bytes to 1500 bytes). The obtained results [28] show that for all network loads and packet sizes WEP offers the best network performance. The usage of WPA leads to moderate network performance (using TKIP encryption) and almost the same network performance as WEP using AES encryption instead of TKIP. Finally, IEEE 802.11i offers the weakest network performance due to the extra required processing of the authentication, encryption, and creation of the security associations. IEEE802.11i is a very good choice for the WLAN security in large scale networks environments. Table 2

contains a comparison between the main factors of security protocols used in WLANs.

Wireless access points and network cards form hardware vendors (such as CISCO, 3Com and Siemens) support all the WLAN security protocols. These products are suitable for large networks. As WPS can be used to simplify the security setup and management of small and medium wireless networks, we recommend using wireless products that support WPS such as: 3Com, Belkin, Broadcom, Brother, Buffalo, Linksys, D-link, Fujitsu, Intell and HP.

Table 2

Comparison between the main factors of different security protocol

	WEP	**WPA**	**IEEE 802.11i**
Encryption	WEP (RC4)	TKIP (RC4)	CCMP (AES)
Key length	40 bits or104 bits	128 bits encryption	128 bits or higher
Data integrity	CRC-32	Michael	CBC-MAC
Replay protection	N/A	Packet number	Packet number
Authentication	Open or Shared Key	IEEE 802.1x or Pre-shared Key	IEEE 802.11X
Network performance	High network performance than WPA and IEEE 802.11i	Less than or almost the same as WEP performance and higher than IEEE 802.11i	Less network performance than WEP, WPA

6. Conclusions

The use of wireless local area networks is growing rapidly. Although the early WLANs were not designed to enhance strong security, meanwhile standards and methods are emerging for securing WLANs. With IEEE 802.1x and IEEE 802.11i protocols, there are now good solutions for encryption and authentication. These emerging security features must be implemented in order to assure the security of information on the wireless networks.

In this paper we presented the security protocols of WLAN (WEP, WPA and IEEE 802.11i) and identified their advantages and drawbacks from the security point of view.

Selecting the appropriate security protocol to be implemented in WLAN should not ignore the performance of the network under that protocol.

We concluded that the selection of the appropriate security protocol depends on three factors: the organization size (network infrastructure, available

hardware and software), desired security level and the acceptable network performance. Because there is trade off between security and performance, and the decision depends on the above three factors, this is why if the desired level of security is high, then IEEE802.11i is the best choice on the expense of lower network performance. If the desired security level is moderate then WPA is a good choice, especially if it is mixed with the AES encryption to give stronger security and higher network performance. Finally, because of the weak security features of WEP it is recommended to use WEP security methods only on legacy devices and for home devices.

TABLE OF ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption standard
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
EAP	Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security
GTK	Group Temporal Key
ICV	Integrity Check Vector
IV	Initialization Vector
KCK	Key confirmation Key
KDK	Key Derivation Key
KEK	Key Encryption Key
MIC	Message Integrity Code
NFC	Near Field Communication
PIN	Personal Identification Number
PMK	Pairwise Master Key
PTK	Pairwise Transient Key
PSK	Preshared Key
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
TK	Temporal Key
TKIP	Temporary Key Integrity Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

R E F E R E N C E S

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

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

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

[4] *Kevin Tyrrell*, "An over view of Wireless security issues" GSEC **V1.4b** SANS Institute 2003

[5] *Jesse R. Walker*," IEEE 802.11 Wireless LAN Unsafe at any key size; an analysis of the WEP encapsulation" Oct27, 2000, URL:http://citeseer.ist.psu.edu/558358.html

[6] *Wong Stanley GSEC* "The evolution of wireless security in 802.11 networks: WEP, WPA and 7802.11 standards" **Practical v1.4b**, SANS institute.

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

[8] *TakehiroTakahashi* "WPA Passive Dictionary Attack Overview" 2003, URL: http:// www.tinypeap.com / docs/WPA_Passive_Dictionary_Attack_Overview.pdf

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

[10] *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*

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

[12] *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'

[13] *Nedier Janvier Senat "IEEE 802.11 Wireless LAN Security Mean throughput Using Multiple clients"*http://www.cosc.canterbury.ac.nz/research/ reports/HonsReps/2003/hons_0304.pdf

[14] *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*

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

[16] *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

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

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

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

[20] *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

[21] "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

[22] *N. Cam-Winget, T. Moore, D. Stanley, and J. Walker, "*IEEE 802.11i Overview," in NIST 802.11 Wireless LAN Security Workshop, http: //csrc.nist.gov/ wireless/ S10_ 802. 11i% 20Overview-jw1. pdf.

[23] "Introducing Wi-Fi Protected Setup", URL:http://www.wi-fi.org/files/ wp_18_20070108_Wi-Fi_Protected_Setup_WP_FINAL.pdf

[24] *Andrew Gin*" The performance of the IEEE 802.11i Security Specifications on Wireless LANs" URL: http://www.cosc.canterbury.ac.nz/research/ reports/HonsReps/2005/hons_0505.pdf

[25] *P. Ding, J. Holliday, and A. Celik* " Improving the security of Wireless LANs by managing 802.1X Disassociation." In Proceedings of the IEEE Consumer Communications and Networking Conference (**CCNC'04**), Las Vegas, NV.

[26] "Wi-Fi Protected Setup Specification Version 1.0h" , http:// www.wi-fi.org/pressroom_overview.php?newsid=7

[27] *John Ioannidis* "A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP) ", September 2005, URL: http://www.cs.jhu.edu/~rubin/ courses/ sp04/wep.pdf

[28] *Nidal Turab, Florica Moldoveanu*, " The Impact of various security mechanisms on the WLAN performances", U.P.B. Sci. Bull., Series C, **Vol. 70**, No. 4, 2008.