IEEE 802.11 Wireless LAN Security Overview

Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen

Department of Electrical and Computer Engineering – Sultan Qaboos University, Oman.

Summary

Wireless Local Area Networks (WLANs) are cost effective and desirable gateways to mobile computing. They allow computers to be mobile, cable less and communicate with speeds close to the speeds of wired LANs. These features came with expensive price to pay in areas of security of the network. This paper identifies and summarizes these security concerns and their solutions. Broadly, security concerns in the WLAN world are classified into physical and logical. The paper overviews both physical and logical WLANs security problems followed by a review of the main technologies used to overcome them. It addresses logical security attacks like man-in-the-middle attack and Denial of Service attacks as well as physical security attacks like rouge APs. Wired Equivalent Privacy (WEP) was the first logical solution to secure WLANs. Hiwever, WEP suffered many problems which were partially solved by IEEE802.1x protocol. Towards perfection in securing WLANs, IEEE802.11i emerged as a new MAC layer standard which permanently fixes most of the security problems found in WEP and other temporary WLANs security solutions. This paper reviews all security solutions starting from WEP to IEEE802.11i and discusses the strength and weakness of these solutions.

Key words:

WLAN, wireless LAN, security, IEEE802.11.

1 Introduction

Wireless Local Area Networks (WLANs) succeeded in providing wireless network access at acceptable data rates. The Institute of Electrical and Electronics Engineering (IEEE) have set standards and specifications for data communications in wireless environment, IEEE802.11 is the driving technology standard for WLANs [1]. WLANs are deployed as an extension to the existing fixed/wired LANs and due to the fact that the nature of WLANs are different from their wired counterparts, it is important to raise the security of WLANs to levels closer or equal to the wired LANs. In general IEEE802.11 can operate in two network topology modes, Ad hoc and Infrastructure modes. This paper discusses WLANs in infrastructure mode. In the infrastructure topology, wireless stations (STAs) communicate wirelessly to a network access point (AP) which is connected to the wired network, this setup forms a WLAN. The establishment of connections between STAs and AP goes through three phases; probing, authentication and association [1]. In probing phase, the STA can either listen passively to AP signals and automatically attempts to join the AP or can actively request to join an AP. Next is the authentication phase, the STA here is authenticated by the AP using some authentication mechanisms described later in the paper. After successfully authenticating, the STA will send an association request to the AP, when approved, the AP adds the STA to its table of associated wireless devices. The AP can associate many STAs but an STA can be associated to one AP only at a time. Figure 1 shows the three phases in WLANs.

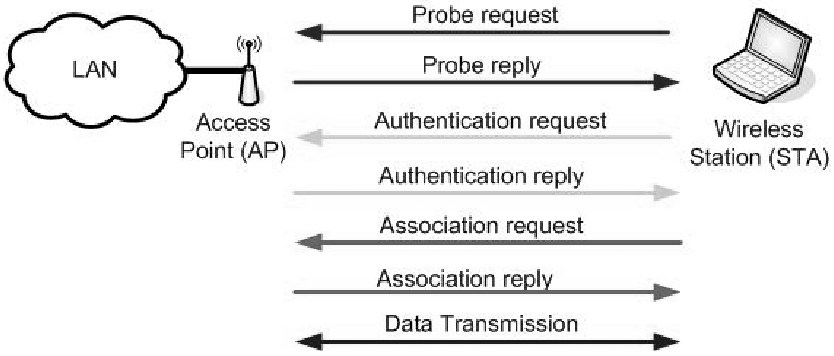

Fig. 1 The three phases undergone through WLAN for the establishment of connections between STAs and AP. These are probing, authentication and association

A breach of the security of the WLAN will eventually harm the security of the wired LAN. There are many issues regarding the security of WLANs like using Radio Frequency (RF) as a medium of transmitting information and the fact that all messages are broadcasted to wherever the coverage of that WLAN can reach [1]-[2]. The propagation of air waves can not be blocked or locked in a room so there is a big risk of eavesdropping and Man-in-the-middle-Attacks [3]. The situation is different in wired LANs where critical servers can be locked in a special room and data transmission is carried out by cables that can be monitored and controlled to some extent. When dealing with WLANs it is important to keep three security goals in mind, Authentication to the WLAN, Confidentiality and Integrity of the data transmitted [4]. In terms of authentication, there is a need to implement a mechanism to allow STAs to authenticate to grant access to the WLAN. These mechanisms have to be efficient, scalable and reliable.

Confidentiality means hiding high sensitive data during information transmission between STAs and AP. This is done to deny other users from listening to the communication. Integrity means preserving the accurateness and the correctness of information transmitted between STAs and AP [5]. Any security solution should achieve these three goals together. The security and management problem become huge as more APs are installed in the network. So there is a need to centralize and manage security issues in small WLANs as well as large ones and a need to develop techniques to counter security threats. As WLANs applications like wireless Internet and wireless e-commerce spread very fast, there is a need to assure the security of such applications. Many papers have been written to address WLANs security problems (see [3], [4], [6]-[12], [18] and [21]). This paper reviews WLANs security problem in both physical and logical aspects and discusses the current available solutions to these problems. The following sections will therefore discus major threats affecting WLANs security and available security protocols and technologies used to counter these threats.

2 WLAN Security attacks

There are many security threats and attacks that can damage the security of WLANs. Those attacks can be classified into logical attacks and physical attacks.

2.1 Logical attacks

2.1.1 Attacks on WEP

Wired Equivalent Privacy (WEP) is a security protocol based on encryption algorithm called "RC4" that aims to provide security to the WLAN similar to the security provided in the wired LAN [2]. WEP has many drawbacks like the usage of small Initialization Vector (IV) and short RC4 encryption key as well as using XOR operation to cipher the key with the plain text to generate cipher text. Sending the MAC addresses and the IV in the clear in addition to the frequent use of a single IV and the fact that secret keys are actually shared between communications parties are WEPs major security problems [4]. WEP encrypted messages can be easily retrieved using publicly available tools like WEPCrack [13] and AirSnort [14]. More discussion about WEP is addressed in later sections.

2.1.2 MAC Address Spoofing

MAC addresses are sent in the clear when a communication between STAs and AP takes place. A way to secure access to APs and hence to the network is to filter accesses based on MAC addresses of the STAs attempting to access the network [7]. Since MAC addresses are sent in the clear, an attacker can obtain the MAC address of authorized station by sniffing airwaves using tools like ethereal [15] or kismet [16] to generate a database of legitimate wireless stations and their MAC addresses. The attacker can easily spoof the MAC address of a legitimate wireless station and use that MAC address to gain access to the WLAN. Stealing STAs with MAC addresses authorized by the AP is also possible. This can cause a major security violation. The network security administrator has to be notified of any stolen or lost STA to remove it from the list of STAs allowed to access the AP hence the WLAN.

2.1.3 Denial of Service attack

Denial of Service attacks or DoS is a serious threat on both wired and wireless networks. This attack aims to disable the availability of the network and the services it provides [5]. In WLANs, DoS is conducted in several ways like interfering the frequency spectrum by external RF sources hence denying access to the WLAN or, in best cases, granting access with lower data rates [3]. Another way is sending failed association messages to AP and overloads the AP with connections till it collapses which, as a result, will deny other STAs from associating with the AP. Attempts are maid by researchers to overcome such attack by introducing new network elements like Admission Controller (AC) and Global Monitor (GM) [36]. AC and GM allocates specific bandwidth to be utilized by STAs and in the case of heavy traffic on AP, they can de-route some packets to neighboring AP to deter DoS attacks on APs. Also attackers try to exploit the authentication scheme used by APs; this will force the AP to refuse all legitimate connections initiated by valid STAs. Little is done so far to counter DoS attacks [11], the fact that DoS attacks are serious and tools to counter them are minimum attracted attackers to vandalize WLANs using such attacks.

2.1.4 Man-in-the-middle attack

This is a famous attack in both wired and wireless networks. An illicit STA intercepts the communication between legitimate STAs and the AP. The illegal STA fools the AP and pretends to be a legitimate STA; on the other hand, it also fools the other end STA and pretends to be trusted AP. Using techniques like IEEE802.1x to achieve mutual authentications between APs and STAs as well as adopting an intelligent wireless Intrusion Detection System can help in preventing such attacks. Figure 2 shows how this attack is conducted [17].

2.1.5 Bad network design

WLANs function as an extension to the wired LAN hence the security of the LAN depends highly on the security of the WLAN. The vulnerability of WLANs means that the wired LAN is directly on risk. A proper WLAN design should be implemented by trying to separate the WLAN from the wired LAN by placing the WLAN in the Demilitarized Zone (DMZ) with firewalls, switches and any additional access control technology to limit the access to the WLAN. Also dedicating specific subnets for WLAN than the once used for wired LAN could help in limiting security breaches. Careful wired and wireless LAN network design plays important role to secure access to the WLAN [9].

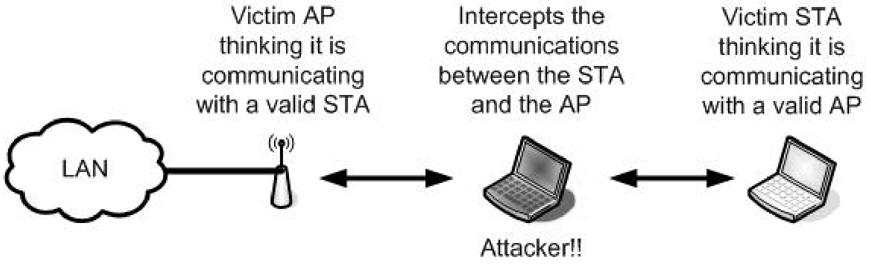
Victim AP thinking it is communicating with a valid STA
Intercepts the communications between the STA and the AP
Victim STA thinking it is communicating with a valid AP
LAN
Attacker!!

Fig. 2 Representation of the famous Man-in-the-middle attack for both wired and wireless networks.

2.1.6 Default AP configurations

Most APs are shipped with minimum or no security configuration by default. This is true because shipping them with all security features enabled will make usage and operation difficult for normal users. The aim of AP suppliers is to deliver high data rate, out of the box installation APs with- out sincere commitment to security. Network security administrators should configure these AP according to the organizations security policy [18]. Some of the default unsecured setting in APs shipped today are default passwords which happens to be weak or blank.

Service Set Identifier (SSID) is the name given to a certain WLAN and it is announced by the AP, the knowledge of SSID is important and works like the first security defense. Unfortunately, by default, some APs disable SSID request which means users can access the WLAN without proving the knowledge of SSID [12]. On the other hand, Some APs don't disable SSID request, in fact the SSID request is enabled but the SSID name itself is broadcasted in the air. This is another security problem because it advertises the existence of the WLAN. SSID requests should be enabled and SSID names shouldn't be broadcasted so users have to prove the knowledge of WLAN's SSID prior establishing communication. Another default configuration in APs is that Dynamic Host Configuration Protocol (DHCP) is ON so users can obtain IP addresses automatically and hence access the WLAN easily. Simple Network Management Protocol (SNMP) parameters are also set to unsecured values [10]. Network security administrators have the responsibility to change these configurations to maximize APs security.

2.2 Physical attacks

2.2.1 Rogue Access Points

In normal situations, AP authenticates STAs to grant access to the WLAN. The AP is never asked for authentication, this raises a security concern, what if the

AP is installed without IT center's awareness? These APs are called "Rogue APs" and they form a security hole in the network [18]. An attacker can install a Rogue AP with security features disabled causing a mass security threat. There is a need for mutual authentication between STAs and APs to ensure that both parties are legitimate. Technologies like IEEE802.1x can be used to overcome this problem [7]. Network security administrators can discover Rogue APs by using wireless analyzing tools to search and audit the network.

2.2.2 Physical placement of APs

The installation location of APs is another security issue because placing APs inappropriately will expose it to physical attacks. Attackers can easily reset the APs once found causing the AP to switch to its default settings which is totally insecure. It is very important for network security administrators to carefully choose appropriate places to mount APs.

2.2.3 AP's coverage

The main difference between WLANs and wired/fixed LANs is that WLANs relies on Radio Frequency (RF) signals as a communication medium. The signals broadcasted by the AP can propagate outside the perimeter of a room or a building, where an AP is placed, allowing users who are not physically in the building to gain access to the network. Attackers use special equipments and sniffing tools to find available WLANs and eavesdrop live communications while driving a car or roaming around CBD areas. Because RF signals obey no boundaries, attackers outside a building can receive such signals and launch attacks on the WLAN. This kind of attack is called "war driving" [19]. Publicly available tools are used for war driving like NetStumbler [20]. Hobbyists also chalk buildings to indicate that signals are broadcasted from the building and the WLAN in it can be easily accessed. This marking is called "war chalking". In War chalking, information about the speed of the connection and whether the authentication scheme used is open or shared keys are mentioned in the form of special codes agreed upon between war-chalkers. There are a lot of doubts and debates in the wireless network community regarding the legality of war chalking and war driving activities. Network security administrators can test the propagation of APs by using special tools to verify to what extent the signals can reach. Accordingly they can control the propagation of APs by lowering the signal strength or by using smart type of antennas to control the direction of the signal or move the AP to a place where it is guaranteed that the signal will not travel beyond the building premises [7]. Some work has been done in the area of smart antennas in APs to direct the propagation of traffic [38]. Directing the propagation of traffic as well as managing the power of signals originating form the APs can be helpful in restricting the coverage of APs to specified regions.

Sometimes public and open access to the WLAN is preferable, such public WLANs are called "hot spots" [9]. Implementing hot spots is subject to many of the mentioned security problems. It is important to understand that breaking the security of a hot spot will result in breaking the security of wired network connected to that hot spot. The control and monitoring of APs is minimal because it is installed in a public area like hotel lobbies, coffee shops, and airport lounges so preventing physical access to AP is more difficult as the site has to be monitored all the time. In this case, there is a tradeoff between giving users the mobility and the flexibility to log in to the network in public areas versus the security of the network infrastructure. The network backbone can be highly secured but a breach in the security of the network access node (i.e. AP) can always lead to a breach in the security of the backbone behind the node.

3 WLAN Security Technologies

There are several security technologies introduced to solve the authentication problem and to preserve the privacy and integrity of data transmitted on air. IEEE802.11 specified three basic security technologies to authenticate access to the WLAN and to preserve the privacy of data transmitted, they are open system authentication, shared key authentication and WEP [1]. Because of the shortcoming of security technologies in IEEE802.11, Wi-Fi Alliance released a new security standard for the industry called "Wi-Fi Protected Access" (WPA) [8]. WPA added two more technologies, namely, IEEE802.1x to improve authentication and TKIP for privacy and integrity of information. Recently IEEE published a new security standard for WLANs, the new standard is IEEE802.11i [22], the new standard provides enhancements of the security shortcomings of WEP and it comprises all security technologies in WPA. In addition to that, IEEE802.11i adopts recently certified encryption algorithm called the "Advanced Encryption Standard" (AES).

The usage of security technologies to discover and fix security holes and to maintain security in a WLAN environment has to be compatible with a security policy issued by the organization's management to achieve best results [23]. The security policy defines who are alleged wireless users, wireless user's responsibilities, network security administrator's responsibilities, what to be done in the case of security violations and general guidelines in implementing and maintaining WLAN security. Such security policies are to be adhered and enforced in order to be effective.

3.1 Authentication techniques

IEEE802.11 defines two types of authentication methods used to access WLANs, open-system and shared key [1]. In the open-system method all communications between the STA and the AP are in the clear (i.e. visible and not hidden). In this method it does not matter if the WEP keys (section 3.3) used to access the WLAN are correct, the AP will allow accessing the WLAN even if the keys used are invalid, the only requirement here is the network SSID (section 3.2). However, APs broadcast their SSID by default so using open-system authentication is totally insecure. In the shared key method, the AP sends a challenge text to the STA; this challenge is encrypted by WEP keys then it is returned back to the AP to either grant access to the WLAN or not. The AP will decrypt the received challenge and compare it with the original challenge it stores. If the decrypted challenge found identical to the original challenge then it implies that the AP and the STA are using the same WEP key; hence the STA can be authenticated. In this scenario, the authentication of STAs is mandatory while AP authentication is not important [1]. This means that a legitimate STA can connect to an illicit AP.

Another problem in shared authentication scheme is that an attacker can sniff the data traffic, especially the challenge text and the encrypted response to the challenge, doing that, it will be possible to find out the secret encryption keys and as result infringing the security of the network. Unfortunately the default authentication method in most APs is the open-system method [12]. Another authentication technique also used is based on the STA MAC address information. Accessing the WLAN can be filtered on the bases of STA's MAC addresses. This means that all authorized STA's MAC addresses have to be listed in a lookup table stored in the AP or a network connected Authentication server. Only STAs which their MAC addresses listed in the table will be able to access the WLAN. The problem in this technique is the ease of data traffic monitoring hence it becomes trivial to capture the MAC address of an authenticated wireless station. Doing that and with the help of some publicly available tools, an attacker can spoof the AP by using an authenticated MAC address and breach the security of the WLAN. This does not mean that such technique can never be used, in fact it can be used in some special situations but it is not recommended in public WLANs. Some researchers tried to develop new techniques to discover attacks using false or spoofed MAC addresses [25].

3.2 Service Set Identifier (SSID)

SSID is a network identifier number broadcasted by APs [4]. Without knowing the SSID number, STAs can not access the network. This seems fine but the problem with SSID is that it is actually broadcasted by the AP. Unauthorized stations can capture the SSID of a WLAN and use it to gain access. It is useful to stop SSID broadcast, this means that wireless stations have to actively search for the SSID correspondent to the WLAN they want to access to. It is also recommended to change the value of the SSID frequently but that will overload network administrators if many APs exist in a WLAN with the absence of central management scheme to control all of them at once. SSID is not a very efficient access control technique; however, it is one hurdle that could be tuned to make it difficult for non-skilled attackers to access the WLAN.

3.3 Wired Equivalent Privacy (WEP)

WEP is the security protocol in use since the early IEEE802.11 standard [1]. It is used to secure communications between APs and STAs and to provide secured authentication schemes; the aim was to provide security to the WLAN similar to the security provided in the wired LAN. It is based on a stream cipher encryption algorithm called "RC4". WEP is used to control access to the WLAN and to encrypt confidential information. It was proved theoretically and practically that WEP failed as a security protocol because of many problems. References like ([3], [4], [12], [24], and [27]) discuss the details of WEP and their problems. This paper summarizes the operation of WEP and explores its vulnerabilities.

To access a WLAN in a shared key authentication scheme, both STA and AP should have the correct shared secret key; this key is used to encrypt confidential information. The length of this key is 40-bits; this is a very short key length. The main drawback of WEP is the use of this 40-bit key even though RC4 encryption algorithm can support up to 104 bit key but 40-bit key is the default key size shipped with WLAN products. Using key sizes higher then 40-bit is possible but it will cause problems when communicating with other devices because other devices might be using the default setting, which is 40-bits. WEP is still considered weak even if it uses 104-bit key for encryption, the key can be disclosed in less then 15 Minutes as this reference states [26].

Another problem with WEP is the use of a short Initialization Vector (IV), typically 24-bit, not to mention that it is sent in the clear and it is being reused multiple numbers of times. The WEP encryption key, also called the RC4 key stream, is generated from the concatenation of the short shared secret 40-bits key and 24-bit IV. The 64-bit WEP encryption key stream and the 40-bit shared secret keys are the secret elements in the security system. Due to the short shared key length (40-bits), the frequent reuse of this key, short IV length, and again the frequent reuse of IV value, the generated WEP encryption key stream repeats it self after a period of time which means that the cipher text generated by this key stream is easily breakable. Figure 3 shows the operation of WEP. WEP also provides simple integrity service (not shown in Figure 3), a checksum value is calculated for the message using a special Integrity Algorithm, and this checksum, also called Integrity Check Value ICV, is attached to the message. The receiver runs the same integrity algorithm on the message to output its own ICV then it compares it with the received ICV. The message is assured to be error-free when both ICVs are identical.

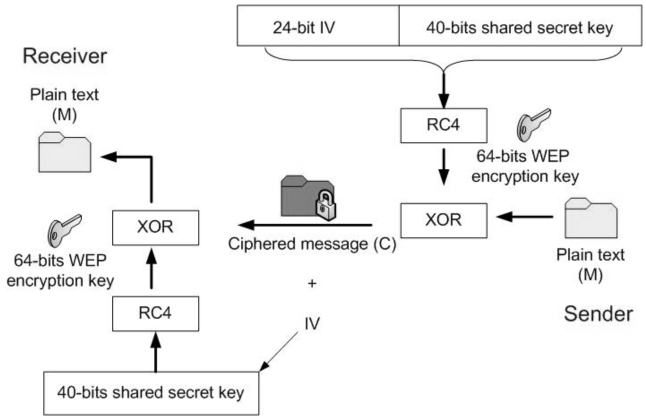
24-bit IV
40-bits shared secret key
Receiver
Plain text (M)
RC4
64-bits WEP encryption key
XOR
Ciphered message (C)
+
IV
Plain text (M)
Sender
64-bits WEP encryption key
XOR
RC4
40-bits shared secret key

Fig. 3 Schematics of the Wired Equivalent Privacy (WEP) protocol used to control access to the WLAN and to encrypt confidential information.

The cipher text (C) is generated from a simple XOR operation between the WEP encryption key (K) and the plain text message (M) as illustrated in equation (1) and Figure 3. XORing the cipher text with the plain text message will result in the encryption key as illustrated equation (2). XORing two cipher text messages is equal to XORing two plain text messages as shown in equation (3). If one of the plain text messages is known, or at least parts of it, finding the WEP encryption key will becomes trivial [24]. Knowledge of plain text message and its corresponding cipher text message can be easily done by eavesdropping the initial challenge sent from the AP to the STA and the reply of that challenge.

The main problem here is that there is a direct relationship between WEP encryption keys and the IV used in a single session, so it is easy for an attacker who knows the WEP encryption key (using equations 1-3) to capture its corresponding IV. Because the length of the WEP encryption key and IVs are short, they are going to be repeated after a while. The attacker can build a database of IV's and their corresponding WEP keys. The attacker can monitor encrypted transmissions and captures IVs, lookup the corresponding WEP key and easily decrypts the transmission. This scheme is shown in Figure 4.

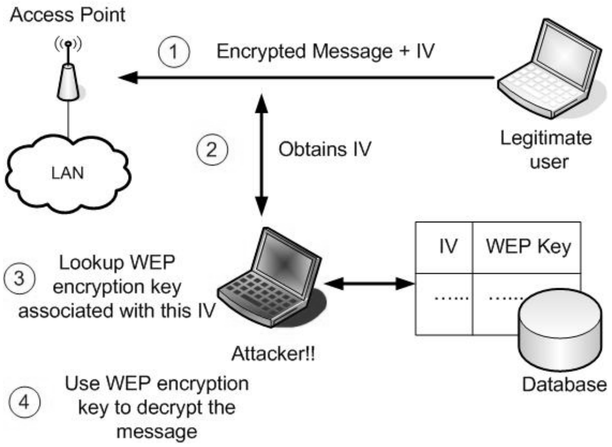
Access Point
1 Encrypted Message + IV
LAN
2 Obtains IV
Legitimate user
IV
WEP Key
……
……
3 Lookup WEP encryption key associated with this IV
Attacker!!
Database
4 Use WEP encryption key to decrypt the message

Fig. 4 Illustration of a Wired Equivalent Privacy (WEP) weakness. The attacker can monitor encrypted transmissions and captures IVs, lookup the corresponding WEP key and easily decrypts the transmitted data.

WEP also lacks key management solutions, there is no solid key distribution policy and a single key is reused frequently. This problem will not only make the AP vulnerable to attacks but it will make all other APs and STAs vulnerable as well. Even worse, key distribution is static by default which means all STAs have to have the key entered manually and when the key compromised, all STAs have to revoke it and use a new key. Generally, WEP lacks key management and distribution system. Reference [37] provides a possible solution to key distribution problem by distributing the keys by Dynamic Host Configuration Protocol (DHCP) server. DHCP server distributes WEP keys as part of DHCP frame options.

WEP does not provide a defense mechanism against replay attacks. An attacker can record a WEP encrypted message and illegally use it later on in a multiple number of times to derive information about the encryption key or to access the WLAN as a legitimate user. It has been proved mathematically and practically that WEP is insecure at all and it is not recommended if high security is required. Nonetheless, WEP protected WLANs adds a hurdle against attackers and definitely such WLANs are better then non WEP-protected WLANs.

3.4 IEEE802.1x

IEEE802.1x is a port-based network access control protocol used to achieve mutual authentication and efficient key exchange mechanism between clients and servers in wired and wireless LANs [7]. It is based on three network elements, supplicant, authenticator and authentication server [28]. In the context of wireless LANs, the supplicant is the wireless station which tries to access the network. An authenticator is a network access node which allows STAs to access the network (i.e. AP) and the authentication server is any server with authentication mechanism. The advantage of having a single AS to authenticate STAs is the existence of a centralized management and authentication server to authenticate and/or control security management aspects of the WLAN. IEEE802.1x was designed first to be used in the wired networks but with wireless networks security problems, the technology found its way to the wireless world. In both open-system and shared key WLAN authentication techniques, only STAs are authenticated but the AP and the wired network behind it are not. IEEE802.1x provides a mechanism to authenticate the STA by an Authentication Server connected to the AP and optionally authenticate the AP to defend against rogue AP attacks.

IEEE802.1x uses Extensible Authentication Protocol (EAP [29]) messages to handle authentication requests and replies [10]. EAP messages traveling between supplicants and the authenticator in wired or wireless LAN environment are encapsulated in an encapsulation technique called EAP over LAN or EAPoL [28], the terms EAPoL and EAP are used interchangeably when working in a LAN environment. Beside authentication, IEEE802.1x plays important role in key management, series of EAP messages travel from supplicants to the authenticator to securely distribute encryption keys. EAP messages are extensible because they can be used to achieve different authentication mechanisms with IEEE802.1x like login usernames and passwords, smart cards, digital certificates and others. Indeed, different types of EAP messages are used in today's wired and wireless LANs to reflect the variety of authentication mechanisms like EAP-TLS, EAP-TTLS and PEAP [6]. EAP-TLS [30] implements the Transport Layer Security protocol defined by IETF [31] where it achieves authentication between supplicants and authentication server by means of public key cryptography and digital certificates. EAP with Tunneled TLS and Protected EAP (PEAP) can achieve authentication by the commonly used login usernames and passwords. As far as implementation is concerned, it depends on the infrastructure of the organization and the complexity of its network to decide on which authentication mechanism, consequently, EAP messages to implement to secure wired and Wireless LAN communications.

The operation of IEEE802.1x in WLAN environments starts first by ignoring all packets arriving to the AP’s Port Access Entity (PAE) except EAP traffic generated from the STA which requests to access the WLAN [10]. At this instance, the AP's PAE is called "uncontrolled port", protected communication should take place in the "controlled port" but the controlled port is blocked till the AP receives the correct EAP message from STA. STAs start by sending the EAP-Start message to the AP then the following sequence of events takes place as shown in Figure. 5

1- STA and AP agree to use IEEE802.1x as the authentication standard and EAP messages during the Association phase
2- The AP blocks all messages sent by the STA to its PAE , uncontrolled port, except EAP messages attempting to log in to the network
3- The wireless user has to provide username and password or any authentication mechanism (example fingerprint) to prove his/her identity
4- The AP will extract EAP messages and sends it securely to the Authentication Server (AS) in the wired LAN (the de-facto protocol to secure communications between AS and AP is Remote Authentication Dial-In User Service (RADIUS)) [33]. Note that APs have no part on authentication, they just allow EAP messages to pass, and authentication servers decide whether STAs should be granted access or not.
5- The STA and the AS will mutually authenticate themselves using IEEE802.1x and EAP messages by exchanging series of challenge/response messages
6- The AS and the STA agree on a WEP key (example. KAS-STA)
7- AS pushes KAS-STA to the AP. The AP will generate a new WEP key (example KAP-STA) and will send it to the wireless station encrypted by the KAS-STA key
8- Finally, the controlled port is unblocked and the AP and the STA will use the new key (i.e. KAP-STA) for communication during that session as well as the KAS-STA key to encrypt all communications between them.

APs have to be IEEE802.1x compliant to allow the STA to be authenticated by the AS. IEEE802.1x helps in defending against rogue APs because only legitimate APs will be connected to the AS. IEEE802.1x is independent of WEP and it does not replace it. The implementation of IEEE802.1x is essential in IEEE802.11i standard and it is used as the authentication protocol. However some parts of it are refined for better security.

3.5 Temporal Key Integrity Protocol (TKIP)

TKIP is a major enhancement over traditional WEP protocol. Since legacy APs and wireless interface cards are equipped with hardware necessary for WEP, TKIP is introduced to work on the same hardware for backward

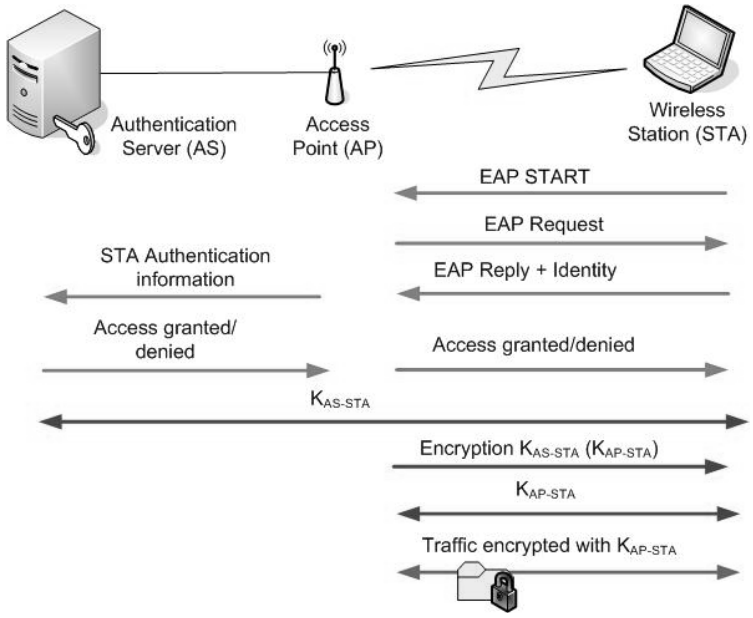

Fig. 5 Illustration of IEEE802.1x network access control protocol operation that is used to achieve mutual authentication and efficient key exchange mechanism between clients and servers in wired and wireless LANs.

compatibility but with software enhancement for additional security [32]. To overcome WEP problems permanently, it is required to design a new security protocol from scratch and to use a stronger ciphering technique than RC4 which will require new hardware in APs and wireless interface cards; this adds extra cost to wireless equipment and less efficient utilization on current ones. TKIP, although it is a short term solution, it is the economical and feasible solution to WEP problems in the current time where it provides more security with no extra hardware.

Even though TKIP is based on RC4 stream cipher but it uses long IV and encryption/authentication keys. TKIP uses 48-bits IV, 64-bit authentication key and 128-bit encryption key [8]. WEP can only accommodate 24-bit IV and maximum of 104-bit encryption key, in comparison with TKIP, the later provides more security against exhaustive key search attacks. The security improvement in TKIP is due to the longer key and IV lengths used as well as using different keys per packet and avoiding key reuse.

The communication between STAs and the AP utilizes different encryption keys every time a packet is transmitted. These keys are generated from the combination/mixture of a shared base key, sender’s MAC address and packet sequence number, also called TKIP sequence number. Figure 6 shows a block diagram that explains the construction of TKIP per-packet keys.

TKIP sequence number is in fact a sequence counter that increments every time a packet is sent, this counter reside in the IV (4 octets) and extended IV (4 octets) fields of WEP data unit. TKIP interprets the IV and extended IV fields of WEP data unit as TKIP Sequence Counter (TSC) and as an input to two key mixing functions to produce a per-packet key and IV to feed the WEP encryption algorithm. Simple XOR as well as AND logic operations constitutes the key mixing functions. TSC is a good tool to defend against replay attacks which was missing in legacy WEP protocol.

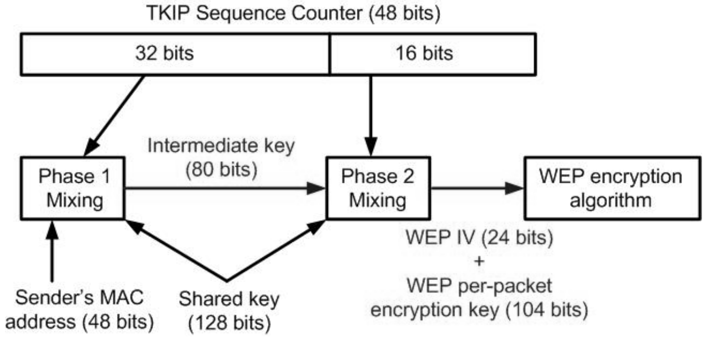
TKIP Sequence Counter (48 bits)
32 bits
16 bits
Intermediate key (80 bits)
Phase 1 Mixing
Phase 2 Mixing
WEP encryption algorithm
WEP IV (24 bits)
+
WEP per-packet encryption key (104 bits)
Sender's MAC address (48 bits)
Shared key (128 bits)

Fig. 6 Construction of TKIP based on RC4 stream cipher which uses long IV and encryption/authentication keys. The per-packet keys use 48-bits IV, 64-bit authentication and 128-bit encryption keys. Note that TKIP is economical and feasible solution to WEP problems in the current time and provides more security with no extra hardware.

TSC requires synchronization between sender and receiver; packets received have to hold a sequence number grater than previously received packets to assure that the packet is not under replay attack. MAC address is used to derive TKIP per-packet encryption key, this is important to guarantee that every STA and AP will generate a different per-packet encryption key, this key will continuously change for every packet in transit as a direct effect of incrementing TSC for every new packet. This new key mixing mechanism highlights couple of advantages, firstly, due to MAC addresses differences, every station will generate different set of WEP per-packet encryption keys which eliminates key reuse problem in WEP, secondly, the mechanism breaks any one to one relation between TKIP per-packet encryption keys and WEP IV, lastly, the mechanism can be completely implemented on software to save the investment done in hardware.

One of greatest WEP disadvantages was the direct relation between the IV and the WEP encryption key, so the knowledge of IV, which was sent in the clear, leads to knowing the WEP encryption key. This problem is resolved in TKIP because TSC is sent in the clear and it is used to derive the IV and TKIP per-packet encryption keys by means of key mixing functions explained earlier. When TSC is obtained by attackers, it will have no relation with the TKIP per-packet encryption key so it gives no extra information to the attacker. TSC is initialized by both sender and receiver, when the 128-bit shared key changes, the TSC will reset to some offset value. The question now is how to distribute the shared key securely? Section 3.6 will discuss in details novel key management strategy to securely distribute encryption keys.

TKIP also overcomes attacks on data integrity by including a cryptographic protocol called Message Integrity Code (MIC) or Michael [22]. MIC uses a cryptographic one-way hash which accepts 64-bit authentication key and the message as inputs and produces a special tag as an output. The tagging function consists of XOR operation, bit swapping and bit addition to result a special tag of each message. The message and its corresponding tag are sent to the receiver. The receiver uses a verification procedure to generate a tag from the message received and compares it with the tag received by the sender. If both tags are identical, it means that the original message has not been tampered. MIC is used to protect the payload as well as the source and destination addresses to care for MAC address spoofing attacks and redirection to unauthorized stations. Figure 7 shows how MIC operates.

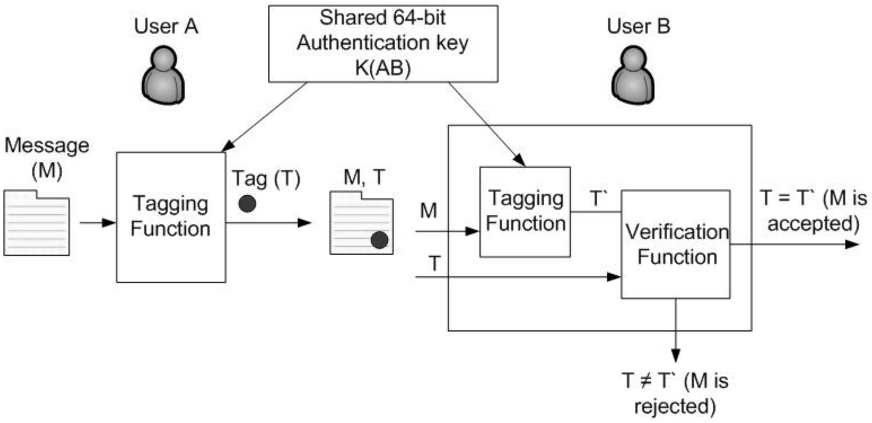

Fig. 7 Bloc diagram of Message Integrity Code (MIC) operation . MIC is included in TKIP to overcome attacks on data integrity.

TKIP adds more features on top of WEP like guard against integrity attacks, privacy attacks, replay attacks and usage of longer key and IV lengths. Never the less, it is based on RC4 encryption which is weak. Moreover, using TKIP will affect the overall network performance due to heavy cryptographic computations per-packet. All this makes TKIP a more short term solution rather than long term solution. Finally it is a solution achievable by the hardware shipped with current APs and wireless interface cards. TKIP is not the best solution but due to hardware constraint it is a major security enhancement than WEP. A permanent solution requires designing a new security protocol that will take advantage of more advanced hardware capabilities.

3.6 IEEE802.11i

3.6.1 Overview

To solve the roots of the problems in WEP and TKIP, IEEE specified a new standard that provides enhanced security as well as support to legacy protocols for backward compatibility. IEEE802.11i [22] is based on IEEE802.11 with security enhancement in the MAC layer; it was approved in July 2004. IEEE802.11i elevates the level of security shipped with WLAN products like APs and wireless network interface cards. A specific task group in the IEEE called "Task Group i (TGi)" developed and still updating this standard, the group tried to specify a standard that will achieve most important security goals, authentication, confidentiality and integrity.

RSN IEEE802.11i defines the concept of Robust Security Network (RSN). RSN, according to IEEE802.11i, is the description of the network that can establish an RSN Association (RSNA) between its entities. As Figure 1 shows, any communication between entities in WLAN starts with an association, whether an STA associates with AP in an infrastructure topology or an STA associates with another STA in ad hoc topology. With this new framework, IEEE802.11i defines RSNA-equipment which has the capability to establish RSNA. On the other hand, there are pre-RSNA equipments which are equipments that do not have the capability to establish RSNA.

RSNA equipments use pre-RSNA security framework which includes authentication and encryption protocols like shared key authentication and WEP encryption protocol to communicate with pre-RSNA equipment. RSNA equipments use RSNA security framework which includes two encryption protocols, Counter mode with CBC-MAC protocol (CCMP) and TKIP as well as enhanced authentication protocol based on IEEE802.1x and advanced key management algorithm called the 4-way handshake when it communicates with RSNA equipment. IEEE802.11i specifies that when two RSNA equipments communicate, they should first use pre-RSNA authentication methods then they carry on with RSNA security framework. The specification mandated the use of open system authentication as the pre-RSNA authentication method in this case. In the case where both communicating parties are pre-RSNA equipments, shared key authentication could be used with WEP encryption protocol, this feature is supported by IEEE802.11i for backward compatibility.

When an STA searches for AP signal by sending probe requests or when it passively receives probe messages from the AP, the probing frames contains a special header in the frame body called RSN Information Element (RSNIE). RSNIE identifies the security capabilities of the sender; whether AP or STA. RSNIE frames are important in the negotiation stage of the WLAN communications because every entity in this early stage will discover other entities security capabilities and accordingly will negotiate to settle on the most secure and mutually understandable security protocols. RSNIE holds information like cipher suites (i.e. CCMP – Default, TKIP, WEP-104, etc…) and authentication mechanism like IEEE802.1x, key selections and other security capabilities required to secure communications. Figure 8 illustrates the exchange of RSNIE during a session in a WLAN where both entities are RSNA-equipments; the result of such exchange is the establishment of a secured association between the STA and AP. RSNIE frames are exchanged in, probe reply association request and messages 2 and 3 of the 4-way handshake protocol.

RSNIE should be protected because an attacker can disclose it and have an idea on the security protocols agreed among network entities. More dangerously, skilled attackers can modify and resend RSNIE frames after setting it to its lowest security capability.

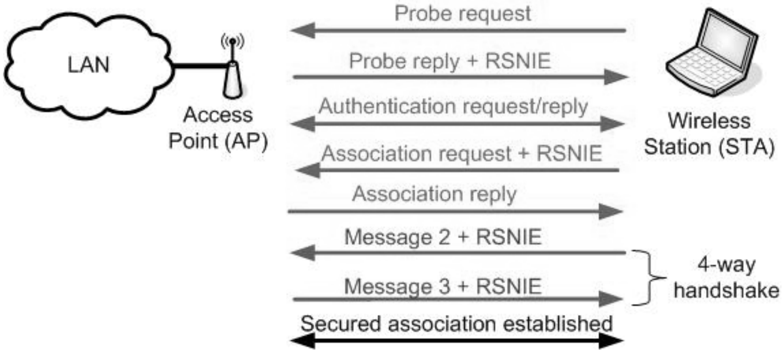

Fig. 8 Illustration of the exchange of RSNIE during a session in a WLAN where both entities are RSNA-equipments which results in the establishment of a secured association between the STA and AP. RSNIE frames are exchanged in, probe reply association request and messages 2 and 3 of the 4-way handshake protocol.

3.6.2 Key management

Key management was a major problem in WEP; one of the biggest drawbacks of WEP was key abuse by using the same key over and over again. With the help of IEEE802.1x/EAP, a novel key management scheme was developed. This key management scheme can be used with TKIP and IEEE802.11i security standard. IEEE802.11i names this key management scheme the “4-way handshake”. Overview of key management handling in IEEE802.11i is illustrated in Figure 9. Initially the STA listens to AP signals passively or actively probes for it. Then the STA authenticates using open system authentication method. Then STA associates with the AP. When the association is established, they both authenticate themselves using IEEE802.1x authentication. Further, STA and AS exchange EAP messages to derive PMK. In situations where AS does not exist, AP and STA share a secret key, PSK, here PMK takes the value of PSK. Next, the 4-way handshake protocol is performed between STA and AP to derive and install PTK and GTK (optional). All previous communications takes place in the 802.1x uncontrolled port; i.e. the 802.1x controlled port is blocked. The establishment of a secured association completes when the 4-way handshake is achieved. Data traffic is now ready to be sent through 802.1x controlled port. If there is a need to update GTK or install new GTK, Group key handshake protocol takes place.

Figure 10 details the 4-way handshake protocol. The protocol takes place only in an RSNA framework. Initially, an STA uses open system authentication to authenticate to the AP as specified by IEEE802.11i, then the STA associates with the AP. When that is done, IEEE802.1x is used to assure mutual authentication of STAs and AP. After successful authentication, STAs and AS share a secret key, AAA key if RADIUS is used. AAA key is used to derive a Pairwise Master Key (PMK), the PMK should change in the case of re-association or when the STA associates with a different AP. Next, the AS will securely push PMK to the AP. IEEE802.11i does not specify a particular network security protocol to protect the link between the AP and AS, however this link could be protected by widely implemented protocols like TLS, IPsec. [35], RADIUS or any security protocol that assures mutual authentication, the protocol should also assure the protection of keys exchanged between the AP and the

AS as well as providing a channel to exchange keys between STAs and AS [10]. As states earlier, RADIUS is the de-facto protocol. Both AP and STA should have PMK installed before the 4-way handshake scheme starts. In cases where AS is not available, a pre-shared key (PSK) could be installed in AP and STAs manually or any out-of-band methods, here the PMK takes the value of PSK. 4-way handshake protocol exchanges 4 messages between STA and AP to derive and install fresh keys for encryption and authentication. IEEE802.11i uses EAPoL key frames for exchanging messages, the frames contain information like the key length, key IDs, nonces and other key related information necessary for the successfulness of the 4-way handshake. The 4 messages are explained in details next.

1- Message 1: this message is sent from the AP to the STA, the message contains key information and a random number generated by the AP called, APnonce. nonces should be random or pseudo-random numbers. The STA keeps track of Replay Counter field in the EAPoL frame to make sure that the value in this field is always greater than the previous values received for that association. If the value in the Replay Counter field is less or equal to the value received before, the message is discarded. If the check returns positive, the STA generates an Snonce. STA will then input the APnonce, Snonce, PMK, AP MAC Address (APA) and STA MAC Address (SA) to a special Pseudo Random Function to generate Pairwise Transient Key (PTK). Note here that PTK depends on random numbers like APnonce and Snonce, it also depends on APA and SA. This means that the key changes automatically whenever the inputs change. PTK is 384 bits in length and it consists of three keys. Key Conformance Key (KCK) bits 0-127 of PTK, Key Encryption Key (KEK) bits 128-255 of PTK and Temporal Key (TK) bits 256-383 of PTK. KCK is used to calculate MIC to provide authenticity and integrity in 4-way handshake and group key handshake. KEK is used to encrypt keys in EAPoL frame during 4-way handshake and group key handshake. TK is the key used to encrypt normal traffic between STA and AP.

2- Message 2: this message is sent from the STA to the AP. EAPoL frame contains key information, Snonce and MIC. MIC is calculated using KCK and it is used to provide authentication and integrity of the message. RSNIE of the STA is also sent in message 2. Upon receiving message 2, AP will check the Replay Counter, if the value is correct it will proceed to derive PTK the same way PTK was derived by the STA. Then it is going to calculate MIC using KCK got from the derived PTK and compares it with the MIC received, if both MICs match, it will compare the RSNIE of the STA with the one received in the (Re)Association request, both RSNIE should be identical. If Replay Counter value do not match with previous counter value or when the calculated MIC value found not identical with received MIC, the message is discarded and association is terminated otherwise the AP will start constructing message 3.

3- Message 3: this message is sent from the AP to the STA. EAPoL frame contains key info, APnonce (same as APnonce in message 1) and MIC. It is possible to send Group Temporal Key (GTK) at this stage if both AP and STA agree on that. When it happens, GTK will be encrypted with KEK, generation of GTK is explained in details in group key handshake. RSNIE of the AP and MIC is also sent to assure authenticity and integrity of the message. At reception, the STA checks the replay counter as specified before, checks if RSNIE is the same RSNIE sent in the probe reply message, checks if the received APnonce is the same APnonce received in message 1. If all tests return positive, STA calculates new MIC value and compares it with the received one, if the last test is also positive, the STA will start constructing the last message in the 4-way handshake.

4- Message 4: this is the last message in the 4-way handshake protocol, this message is sent from the STA to the AP. EAPoL frame contains key information and MIC only. This message is like an acknowledgment from the STA that everything is fine and PTK and GTK (optional) are now installed. By the end of this message, AP and STA are holding fresh PTK and GTK and the secured association between them is established.

APnonce, Snonce, APA and SA plays important role to defend against man-in-the-middle attack. If an attacker in the middle tries to intercept communications and change these values, the association will be terminated because this attempt will be directly reflected in a failed MIC computation. Note here that MICs are encrypted with KCK, and KCK is part of PTK, further PTK is constructed using APnonce, Snonce, PMK, APA and SA. If any of these values where tampered during communication, MIC validation will fail which means there is a possible man-in-the-middle attack. Skilled attackers can pre-compute nonce values and hence can fool the 4-way handshake protocol, this can only happen if the selection of nonces is done in a deterministic way. IEEE802.11i specifies that the selection of nonce values should be purely random to avoid this problem.

By the end of 4-way handshake, PTK should be installed in STA and AP. GTK could also be installed if it was agreed upon between STA and AP during security capabilities negotiation. GTK is used to encrypt multicast/broadcast traffic between AP and STAs. IEEE802.11i specifies a protocol for generating new GTK by AP or updating GTK held by all STAs, it is called "group key handshake protocol", it is shown in Figure 10. Updating GTK takes place when an STA is disassociated or deauthenticated. Group key handshake protocol starts after the 4-way handshake protocol and its aim is to derive a fresh GTK. The protocol starts first by deriving a new GTK by the AP. The AP generates a new random nonce value called Gnonce and inputs it along with its MAC address and a Group Master Key (GMK), which is configured in the AP, to a PRF. The output of the PRF is GTK (256 bits in TKIP, 128 bits in CCMP). The first message sent from the AP to the STA contains GTK encrypted by KEK, Key information, Gnonce and MIC calculated using KCK. When this message is received, STA will check the Replay counter, similar to 4-way handshake, and it will compute a new MIC and compares it with the received one. If both tests return positive, STA will decrypt GTK by KEK and install it in its MAC. STA replies to the first message by sending key information and MIC, i.e. STA acknowledges installing GTK.

It is very important to complete the 4-way handshake before starting the group key handshake because KEK and KCK are derived from PTK which can be distributed using the 4-way handshake protocol. Communication between individual STAs and the AP is encrypted using TK associated with each STA. Broadcast communications between the AP and all STAs in its range are encrypted using GTK. This key hierarchy scheme solves key management problems in legacy security protocols like WEP and TKIP.

3.6.3 CCMP

IEEE802.11i mandates the use of a protocol to protect confidentiality and integrity of data transferred, named Counter mode with CBC-MAC Protocol (CCMP). CCMP provides confidentiality and integrity of the data transferred and authenticity of the sender. It is based on the Advanced Encryption Standard (AES) block cipher. AES is the most reliable block cipher to date, it uses a minimum of 128-bit key length and text blocks of 128-bits as well [4]. This is a great advancement over traditional WEP protocol which is based on weak RC4 stream cipher. CCMP consists of two important protocols, Counter Mode AES encryption (CTR-AES) and Cipher Block Chaining – Massage Authentication Code (CBC-MAC) based on AES. CTR-AES encrypts data transferred (i.e. achieves confidentiality) and CBC-MAC provides integrity of data and authentication of the sender by calculating the Message Integrity Code (MIC) of the message. Figure 11 shows how MIC is calculated using CBC-MAC based on AES block cipher.

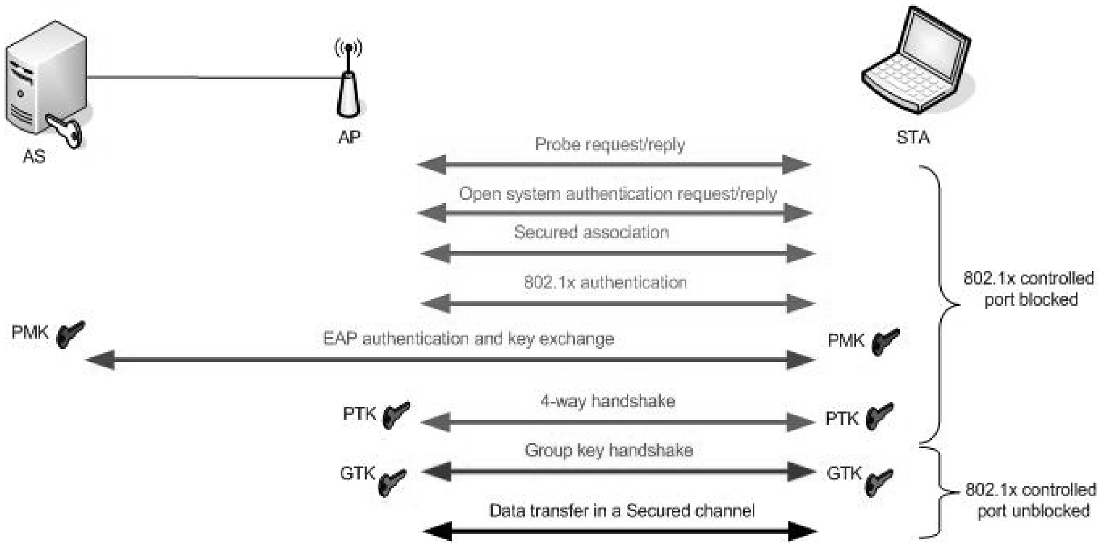
AS
AP
STA
Probe request/reply
Open system authentication request/reply
Secured association
802.1x authentication
PMK
EAP authentication and key exchange
PMK
PTK
4-way handshake
PTK
GTK
Group key handshake
GTK
Data transfer in a Secured channel
802.1x controlled port blocked
802.1x controlled port unblocked

Fig. 9 Key management structure in IEEE802.11i protocol.

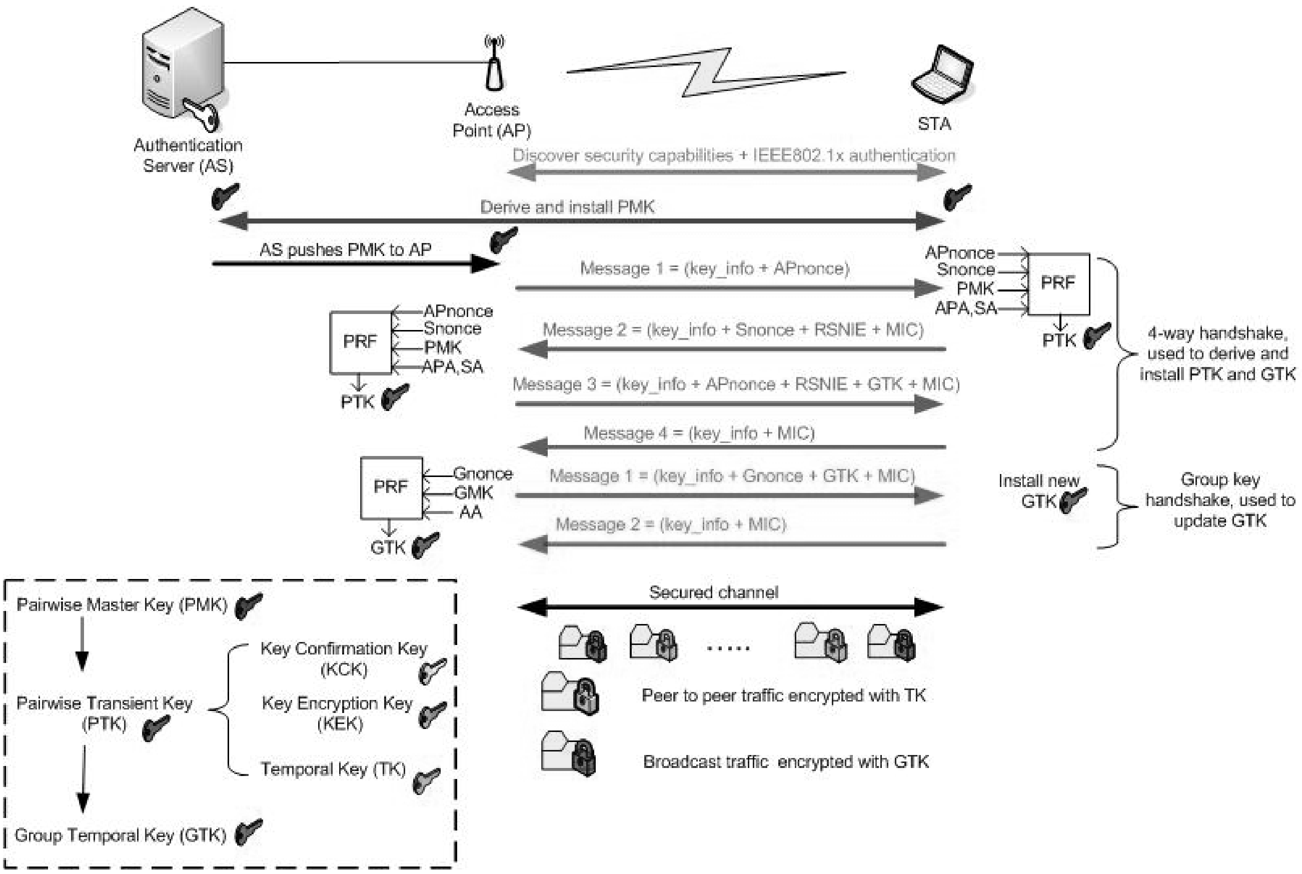
Authentication Server (AS)
Access Point (AP)
STA
Discover security capabilities + IEEE802.1x authentication
Derive and install PMK
AS pushes PMK to AP
Message 1 = (key_info + APnonce)
APnonce
Snonce
PMK
APA,SA
PRF
PTK
Message 2 = (key_info + Snonce + RSNIE + MIC)
Message 3 = (key_info + APnonce + RSNIE + GTK + MIC)
Message 4 = (key_info + MIC)
4-way handshake, used to derive and install PTK and GTK
Gnonce
GMK
AA
GTK
Message 1 = (key_info + Gnonce + GTK + MIC)
Message 2 = (key_info + MIC)
Install new GTK
Group key handshake, used to update GTK
Pairwise Master Key (PMK)
Pairwise Transient Key (PTK)
Key Confirmation Key (KCK)
Key Encryption Key (KEK)
Temporal Key (TK)
Group Temporal Key (GTK)
Secured channel
Peer to peer traffic encrypted with TK
Broadcast traffic encrypted with GTK

Fig. 10 802.1x/EAP operation as refined by IEEE802.11i protocol.

The cipher text output of the first round of CBC-MAC is fed back as an input to second round of CBC-MAC, this operation continues till the nth round. The output of the nth round is the MIC of the plain text. STA and AP share KCK, 128-bits minimum, derived from PTK and used to calculate MIC. Assume that MIC generated by STA is called MIC(STA), similarly MIC generated by AP is called MIC(AP). MIC(STA) will be sent to the AP as well as the original message. The AP will receive the original message, calculates MIC(AP) based on the message received and compares it with MIC(STA). If both MICs are identical, then this indicates that the message has not been tampered while transmission which also means integrity is preserved. Further, if MIC(STA) = MIC(AP) then there is a very high probability that the message came from STA because only STA holds a shared secret key, KCK in this case, with the AP. Figure 12 shows integrity and authentication protocols of CBC-MAC.

CTR-AES is one mode of AES operation, this mode is based on a counter that increment an initial value. CBC-MAC requires an IV to start its operation, the counter in CTR-AES and the CBC-MAC IV are constructed from the concatenation of Packet Number (PN) and miscellaneous data like the sender's MAC address and some priority bits reserved for future use. CTR-AES is used to encrypt the traffic between AP and STA and vise versa. Both parties obtain an encryption key from PTK or GTK to encrypt messages as well as generate MIC using CBC-MAC, this key is 128-bits and it is called, Temporal Key (TK). A block diagram of CCMP protocol is illustrated in Figure 13. The diagram shows how CBC-MAC IV and CTR-AES counter are constructed. CBC-MAC IV is fed into the CBC-MAC encryption along with the message, MAC header and TK to generate MIC. Note here that only selected elements of the MAC header are fed into CBC-MAC operation like sender and receiver MAC addresses while other fields are set to Zero. MIC generated is used to preserve the integrity and authenticity of the message and MAC header, MIC will become an input to CTR-AES so it can be protected from modifications.

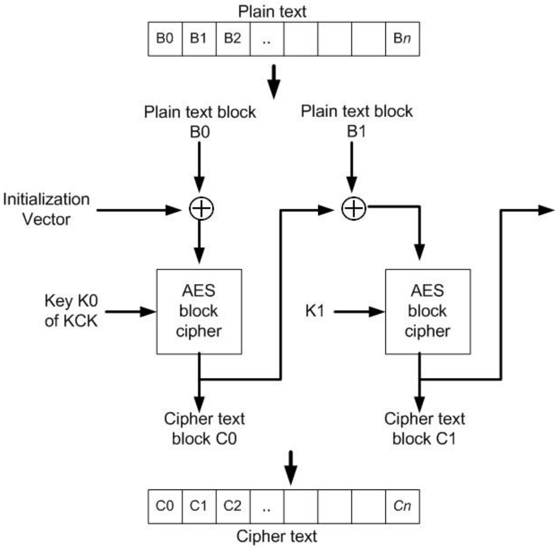

Fig.. 11 Illustartion of Calculation of MIC using CBC-MAC AES based bloc cipher.

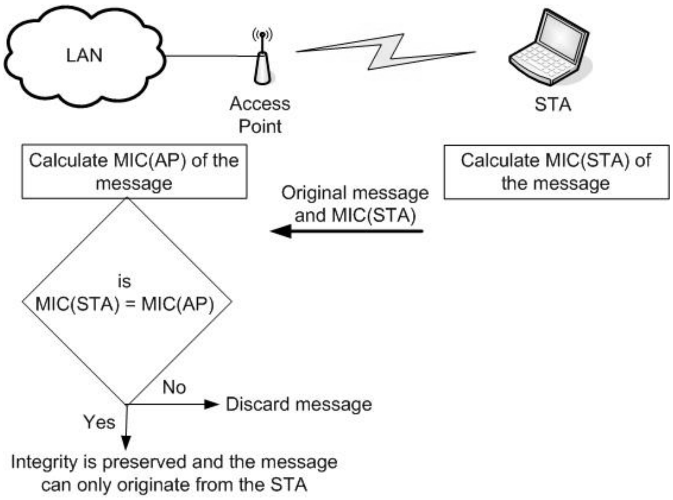
LAN
Access Point
STA
Calculate MIC(AP) of the message
Calculate MIC(STA) of the message
Original message and MIC(STA)
is MIC(STA) = MIC(AP)
No
Discard message
Yes
Integrity is preserved and the message can only originate from the STA

Fig. 12 CBC-MAC protocol used for the calculation of MIC as shown in Fig. 11.

CTR-AES counter value is fed into CTR-AES encryption along with TK, the message and MIC. Moreover, a special header is constructed for CCMP. CCMP header contains information like PN which is necessary to counter replay attacks. Extended IV is a one bit flag which is always set to one when CCMP protocol is used. The final output from the CCM encryption block is the message and it MIC in an encrypted form, MAC header is added, some parts of MAC is already in MIC to provide authenticity and integrity, then CCMP header is injected between the encrypted message and MAC header. The packet containing the encrypted message with its MIC, CCMP header and MAC header is now sent over the insecure channel. The receiver will decrypt the message and MIC using TK, a new MIC will be generated from the decrypted message and some parts of MAC header, the two MIC's are compared to insure validity of the message as well as authenticity of sender.

CCMP uses PN efficiently; PN helps in resolving problems faced by WEP and its successor TKIP encryption protocols. A fresh PN is required for every message, this is achieved by continuously incrementing it. IEEE802.11i specifies that PN should be initialized to one whenever TK is changed. On the receiver side, the PN number is compared to the previous PN number received, if the fresh one is greater than the previous one while using the same TK, this means that the message is not under replay attack. Incrementing PN for each message sent will assure that PN is never repeated with the same TK.

In general, IEEE802.11i will overcome all shortcomings of WEP and TKIP, the following points summarizes the advantages of CCMP protocol

- Protects the privacy of messages using CTR-AES encryption which is a powerful encryption algorithm.
- Protects the integrity of the message, counters forgery packets and proofs the authenticity of the sender using MIC. Additionally, it protects the source and destination addresses from modification hence defending against man-in-the-middle attack and MAC address spoofing.
- Protect users from replay attacks because it uses packet sequence numbers.
- Prevents key reuse. CCMP uses TK which is derived from the 4-way handshake scheme shown in Figure 10. IEEE802.11i specifies that CBC-MAC IV and counter of CTR-AES are never repeated with the same TK.

3.6.4 Other services

IEEE802.11i is optionally supporting TKIP to provide backward compatibility with legacy systems and with systems that does not support AES hardware. TKIP keys are obtained from PTK and GTK, 128-bits minimum, TKIP will benefit from the key management scheme offered by IEEE802.11i to solve key distribution problems. IEEE802.11i offers extra features like pre-authentication capabilities for secured roaming, pre-authentication can only be used when the 4-way handshake is completed. When STAs roams from an AP to another, it could send a special EAPoL-Start message to its currently associated AP which will forward this message to the AS and the targeted AP. Next, the AS will forward the STA’s information to the new AP. When the STA becomes in radio range with the targeted AP, it can directly start the 4-way handshake protocol and save the time usually spent on open system authentication. Pre-authentication can only be utilized if the new AP advertises the capability of pre-authentication in its RSNIE.

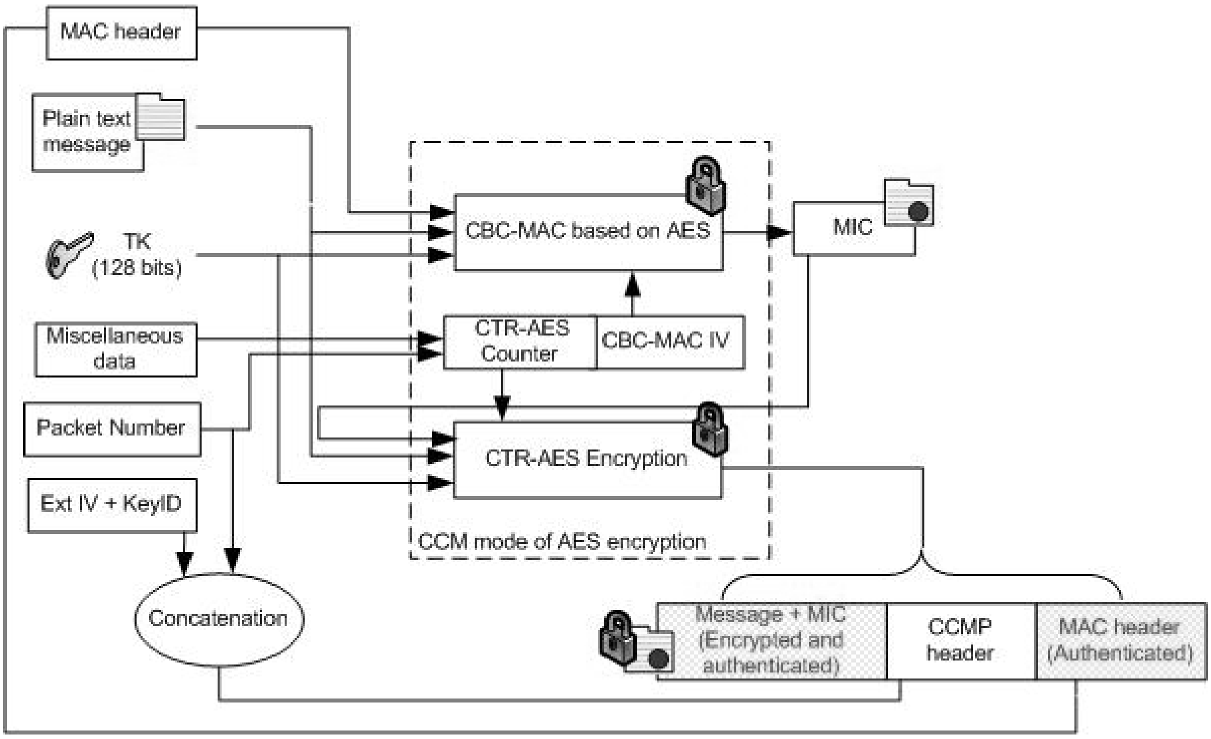

Fig. 13 Block diagram of CBC-MAC Protocol (CCMP) based on the Advanced Encryption Standard (AES) block cipher. It shows how CBC-MAC IV and CTR-AES counter are constructed. CBC-MAC IV is fed into the CBC-MAC encryption along with the message, MAC header and TK to generate MIC. Note here that only selected elements of the MAC header are fed into CBC-MAC operation like sender and receiver MAC addresses while other fields are set to Zero. MIC generated is used to preserve the integrity and authenticity of the message and MAC header, MIC will become an input to CTR-AES so it can be protected from modifications.

Before the standardization of IEEE802.11i, the industry pushed towards another proprietary standard released in the first quarter of 2003 by Wi-Fi Alliance to substitute WEP [34]; this industry standard is called "WiFi Protected Access" (WPA). WPA is forward compatible with IEEE802.11i standard; in fact it is a subset of IEEE802.11i. WPA includes support for IEEE802.1x based authentication, TKIP, WEP 104-bit encryption key and Message Integrity Check (MIC) but it does not support AES encryption. The next version of WPA, WPA2 will support AES encryption. WPA can be looked at as a software security upgrade and temporary solution that can be adopted faster in the industry while waiting for IEEE802.11i to be fully implemented in future wireless devices.

To adapt to IEEE802.11i specifications, current hardware in wireless NIC have to be replaced with ones that can carry on AES computations including new STAs and APs. Communication security will better be achieved by IEEE802.11i but the cost to achieve it will be higher since current hardware can not support AES computations which are the basic building block of IEEE802.11i [7]. Reference [39] proposed a new processor design that can be used in wireless network cards and APs which can efficiently implement

IEEE802.11i technologies. The main purpose of the WLAN security processor is to relief the host's main processor from calculating AES computations and key generation.

4 Conclusion

IEEE802.11 was initially designed to interconnect wireless devices to wired networks; the aim was to achieve networking with minimum or no security. Security was not an important issue at that stage, however, with the successful of WLANs and the fast adoption of this technology, security became important and achieving security became a primary concern. Wired Equivalent Privacy (WEP) security protocols was the first to be adopted in an attempt to satisfy the need for securing wireless networks, soon WEP became vulnerable and there was a demand for a better security protocol. Industries already invested in wireless devices so any new protocol should consider the hardware capabilities of such devices. TKIP came into picture with promise of a better security using the same hardware. An upgrade in software is what made TKIP more secured than WEP. However, the core encryption algorithm is still the same, weak RC4 stream cipher, with this encryption algorithm and the design flaws it experiences, TKIP believed to be a short-life solution. IEEE recognized the need for a new protocol that is more secure and long lasting. IEEE finally answered the call by working on a new security standard, IEEE802.11i. The standard was approved in June 2004. This new standard addresses new security protocols and introduces the adoption of strong block encryption algorithm, Advanced Encryption Standard (AES), also introduces a new key management scheme. Attacks on privacy, integrity, and authentication can be overcome by IEEE802.11i.

As far as the logical attacks are concerned, IEEE802.11i provides adequate solutions to defend against WEP weaknesses, man-in-the-middle attacks, forgery packets attacks and replay attacks. However, DoS attack is not addressed properly and there are no solid protocols or implementations to stop such attacks basically because the attacks target the physical layer of the TCP/IP stack like interfering with the frequency band. Most research activities in wireless security are done on the data link and upper layers. Researchers are working hand to hand with the industry to provide the best solution for logical attacks but there is negligence in the area of physical attacks in which human behavior and human interaction with devices takes place. There is no meaning to use IEEE802.11i equipped AP that sits behind a firewall and allocated a dedicated subnet and uses long AES encryption keys to encrypt transmissions if this AP is placed somewhere visible to attackers or placed in such a way that signals propagate outside the premises. As simple as resetting the AP, a catastrophe could happen in the network.

The human factor and the way they deal with device settings, placements and overall managements have significant value in wireless security. Education and training in wireless security issues and their differences comparing to wired security issues as well as defining an appropriate wireless security policy are important factors to achieve overall security. Adequate compromise between ease of usability versus security is required in APs shipped today. APs should be easy to implement and use by normal users and at the same time some critical security features should not be left disabled.

All in all, wireless LANs are becoming more and more secure especially with the arrival of IEEE802.11i complaint wireless hardware. Sensitive information and highly secured communications can be transmitted with a higher confident than few years back that no illicit user around can actively or passively tamper with the data transmitted providing a careful, skilled personnel is in charge of configuring and installing the APs.

References

[1] IEEE Standard for local and metropolitan area networks, “Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications”, ANSI/IEEE Std 802.11, 1999 Edition (R2003).

[2] Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A., “Wireless network security and interworking”, Proceedings of IEEE, Volume 94, Issue 2, pp 455 – 466, February 2006.

[3] Wang Shunman, TaoRan, WmgYue and ZhangJi, "Wireless LAN and it's security problem". Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003.

[4] Matthew S. Gast, 802.11 Wireless Networks, O’REILLY, 2002.

[5] William Stallings, Cryptography and Network Security, Principles and Practices, 3rd Edition, Prentice Hall 2003.

[6] Matija Sorman, Tomislav Kovac and Damir Maurovic, "Implementing Improved WLAN security", 46th International Symposium Electronics in Marine. ELMAR-2004, Zadar. Croatia, 16-18 June 2004.

[7] Joon S.Park and Derrick Dicoi, "WLAN Security: Current and Future". IEEE Computer Society, October 2003.

[8] Nancy R. Mead and Gary McGraw. "Wireless Security’s Future". IEEE Computer Society, IEEE Security and Privacy, August 2003.

[9] Joseph Williams, "Providing for Wireless LAN Security, Part 2". IEEE IT Pro, November | December 2002.

[10] Jyh-cheng Chen, Ming-chia Jiang, and Yi-Wen Liu, "Wireless LAN Security and IEEE802.11i", IEEE Wireless Communications, February 2005.

[11] William A. Arbaugh. “Wireless Security is Different”, IEEE Computer Magazine, August 2003.

[12] William A. Arbaugh, Narendar Shankar, Kan Zhang and Y. C. Justing Wan. “Your 802.11 Wireless network has no cloths". IEEE Wireless Communications, December 2002.

[13] WEPCRACK, Software, http://www.sourceforge.net/projects/wepcrack .

[14] AirSnort Software, http://airsnort.shmoo.com

[15] Ethereal Software, http://www.ethereal.com

[16] KISMET Software, http://www.kismetwireless.net

[17] Brown, B. "802.11: the security differences between b and I", IEEE Potentials, October/November 2003.

[18] Joel W. Branch, Nick L.Petroni JR, Leendert Van Doorn and David Safford, "Autonomic 802.11 Wireless LAN Security Auditing". IEEE Security & Privacy, 2004.

[19] War driving website, http://www.wardriving.com/

[20] NetStumbler Software, http://www.netstumbler.com

[21] Cisco Systems. "Wireless LAN Security". February 2001, (online) [Available: http://mithras.itworld.com/WhitePapers/Cisco/WLAN_WP_BW7012.pdf] .

[22] IEEE Standard for local and metropolitan area networks , “Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications, Medium Access Control (MAC) Security Enhancements”. ANSI/IEEE Std 802.11i, 2004 Edition.

[23] Tom Karygiannis and Les Owens, " Wireless Network Security: 802.11, Bluetooth and Handheld Devices", National Institute of Standard and Technology. November 2002.

[24] Jesse Walker, 2002. "802.11 Security Series Part I: The Wired Equivalent Privacy (WEP)". February 2002. (online) Intel Corporation. [Available: http://www.intel.com/cd/ids/developer/asmo-na/eng/technologies/mobile/20501.htm]

[25] Joshua Wright, “Detecting Wireless LAN MAC Address Spoofing”, January 2003. (online) [Available: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf]

[26] Sean Convery, Darrin Miller and Sri Sundaralingam. "Cisco SAFE: Wireless LAN Security in Depth". October 2003. (online). Cisco Systems [Available: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

[27] Nikita Borisov, Ian Goldberg and David Wagner. "Intercepting Mobile Communications: The insecurity of IEEE802.11", 7th Annual International Conference on Mobile Computing and Networking. July 2001.

[28] IEEE Standard for local and metropolitan area networks, “Port-based Network Access Control” , IEEE Std 802.1x, 2001 Edition (R2004).

[29] IETF, RFC 3748, “Extensible Authentication Protocol (EAP)” (online) IETF Website [Available: http://www.ietf.org/rfc/rfc3748.txt]

[30] IETF, RFC2716, “PPP EAP TLS Authentication Protocol” (online) IETF Website [Available: http://www.ietf.org/rfc/rfc2716.txt]

[31] IETF, RFC 2246, “The TLS Protocol Version 1.0”. (online) IETF Website [Available: http://www.ietf.org/rfc/rfc2246.txt]

[32] Jesse Walker. "802.11 Security Series Part II: The Temporal Key Integrity Protocol (TKIP)". April 2002 (online). Intel Corporation. [Available: http://www.intel.com/cd/ids/developer/asmo-na/eng/technologies/security/topics/19181.htm

[33] Nancy Cam-Winget, Tim Moore, Dorothy Stanley, Jesse Walker. "IEEE 802.11i Overview" December 2002 (online). [Available: http://csrc.nist.gov/wireless/S10_802.11i%20Overview-jw1.pdf]

[34] http://www.wi-fi.org/OpenSection/protected_access_archive.asp

[35] IETF, RFC2401, “Security architecture for the Internet Protocol” (online) IETF Website [Available: http://www.ietf.org/rfc/rfc2401.txt]

[36] Mohit Virendra, Shambhu Upadhyaya, “SWAN: A Secure Wireless LAN Architecture”. Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN’04) , 2004.

[37] Narendar Shankar, William A. Arbaugh and Kan Zhang, “A Transparent Key Management Scheme for Wireless LANs Using DHCP” September 2001. (online) HP Website [Available: http://www.hpl.hp.com/techreports/2001/HPL-2001-227.pdf]

[38] Joseph M. Carey and Dirk Grunwald, “Enhancing WLAN Security with Smart Antennas, A Physical Layer Response for Information Assurance”. IEEE 60th Vehicular Technology Conference, VTC2004, Fall 2004.

[39] Neil Smyth, Máire McLoone and John V. McCanny, “Reconfigurable hardware acceleration of WLAN security”.IEEE Workshop on Signal Processing Systems SIPS, 2004.