Chapter 3
Security in Wireless Local Area Networks

Chao Yang[1] and Guofei Gu[2]

Abstract

Wireless Local Area Networks (WLAN) allow end users to wirelessly access Internet with great convenience at home, work, or in public places. WLANs are currently being widely deployed in our real life with great success. However, it is still in its infant stage as long as security is concerned. In this chapter, we briefly overview the security issues in the Wireless Local Area Networks (WLAN). After a short introduction to the background of WLAN, we present WLAN security requirements and categories of current real-world WLAN attacks. We then describe some details of several representative WLAN security protocols such as WEP, WPA, WPA2, and WAPI. We also survey security issues of the WLAN access points such as rogue access points and evil twin attacks. Finally, we overview other security mechanisms that can be used to enhance WLAN security, including Wireless Firewalls, Wireless VPN, and Wireless IDS.

3.1 Introduction to WLAN

3.1.1 WLAN Background

With people's huge demand of accessing the Internet wirelessly and the wide deployment of Wi-Fi equipments, wireless local area networks (WLANs) are nearly everywhere and are easy to find no matter at the coffee shops, restaurants, hotels, airports, private home, enterprises, universities, or government

1 Texas A&M University, College Station, Texas, USA. E-mail: yangchao@cse.tamu.edu.
2 Texas A&M University, College Station, Texas, USA. E-mail: guofei@cse.tamu.edu.

L. Chen et al., *Wireless Network Security*

facilities. A wireless local area network is a network linking two or more devices by using wireless distribution methods (typically spread-spectrum or orthogonal frequency-division multiplexing radio), and usually providing a connection through an access point to the wider Internet[14]. In practice, a WLAN consists of two main categories of components: wireless-enable clients such as laptops, PDAs and smart phones equipped with wireless cards and wireless access points (APs) such as wireless routers. The main functions of the wireless access points are to receive and transmit radio frequencies for the wireless clients.

To achieve the goal of standardizing the implementations of WLANs, IEEE LAN/MAN Standards Committee (LMSC) creates and maintains a set of IEEE 802.11 standards[6] for WLANs. The services specified in IEEE 802.11 for the implementations of WLANs include both radio standards and networking protocol standards. These standards guarantee the acceptability of the wireless connectivity to fixed stations, portable stations, and moving stations within the specific area of the network.

3.1.2 WLAN Architecture

In an 802.11 WLAN, all the components belonging to the WLAN are referred to as "stations". A set of stations can form a basic building block called "basic service set" (BSS). The stations in the basic service set communicate with each other obeying the same networking protocol under the same, shared wireless medium, which may generate medium access collisions. Every BSS has a unique identification (ID) called BSSID, which is the MAC address of the access point servicing the BSS. Multiple BSSs connected through a wired or wireless distribution system can form an extended service set (ESS). Each ESS also has an ID called service set identifier (SSID) which can be up to 256 characters long now.

From the viewpoint of the network architecture, WLANs can be divided into two categories: infrastructure-based WLANs and Ad Hoc WLANs. The majority of current WLANs are infrastructure-based, such as IEEE 802.11 WLANs. In an infrastructure-based WLAN, each device connects to the network by establishing a wireless connection to a pre-installed base station to transmit and receive packets. The base stations in the WLAN are usually connected through high bandwidth wired connections. In this way, the communication typically takes place between the wireless clients and the base station rather than directly between the wireless clients. The main aim of the infrastructure-based networks is to provide wireless services to users in a fixed network area. An example of an infrastructure-based WLAN can be found in Fig. 3.1.

Unlike the infrastructure-based wireless network, the stations in an ad hoc network communicate with each other directly peer to peer (P2P) without the need of any pre-existing fixed infrastructure or base stations. In this way,

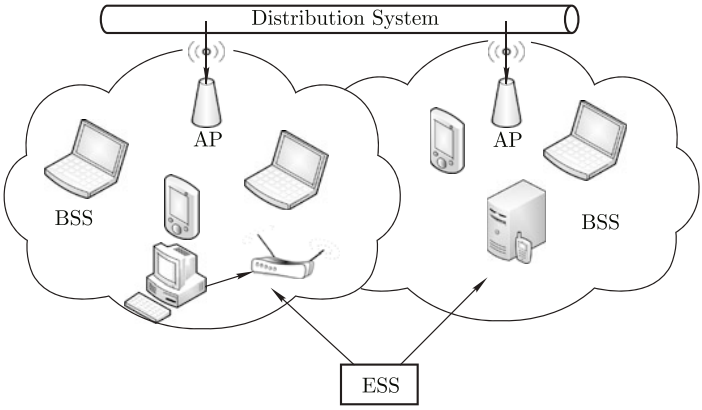

Fig. 3.1 An example of an infrastructure-based WLAN.

the Ad Hoc network can offer the service to users without the constraints of certain geographical situations. An example of an Ad Hoc WLAN can be seen in Fig. 3.2.

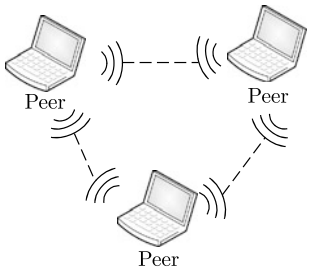

Fig. 3.2 An example of an Ad Hoc WLAN.

3.1.3 WLAN Applications

Current applications of WLANs have been extended into many areas such as LAN extension, public service, multimedia transmission, and mobile communication. WLANs are broadly being utilized from personal home networks to public places such as airline lounges, coffee shops, restaurants, stores and libraries, also ranging from personal service such as mobile IP and VoIP to public business such as education, healthcare, hospitality, financial industries, and public safety.

3.2 Current State of WLAN Security

The ubiquity, convenience and powerful strength of WLANs are not merely enticing to legitimate users but also to malicious attackers. Especially, attackers can utilize the vulnerabilities in the existing authorization and authentication policies in WLANs and the broadcast nature of the wireless communication to greatly compromise the security of legitimate wireless users. Thus, wireless LAN security has become a serious concern for an increasing number of wireless organizations. According to reference [44], nearly two-thirds (61%) of people consider security as the second most important WLAN characteristic after reliability (64%) and nearly half (49%) describe the ability to simplify WLAN security deployment as "very important". In this section, we will show a brief outlook of the current state of WLAN security.

3.2.1 WLAN Security Requirements

WLAN security is an important, dynamic, and even evolving topic. Novel threats, attacks, technologies and solutions are emerging almost every day. However, although diverse WLANs may have different infrastructure components and support distinct practical applications, to be effective, stable, and trustworthy, the security requirements of the WLANs essentially fall into the following five broad categories: confidentiality, authentication, access control, integrity, and intrusion detection and prevention.

- *Confidentiality*: Confidentiality prevents the disclosure of the data or information to unauthorized individuals or systems, when that information is transmitted across the shared communication medium. Confidentiality can be achieved through the utilization of encryption techniques to encode the information in a manner so that the information can only be decoded, understood and analyzed by the authorized parties.
- *Authentication*: Authentication provides a service that verifies and confirms the authenticity of a sender or receiver's identity that it claims to be. Essentially, robust authentication mechanism in the WLANs not only ensures that the information can be transmitted from/to the authentic entities in the two-side parities of the communication, but also avoids these information to be interfered or impersonated by a third party. Without such an authentication mechanism, attackers can gain full access to the information transmitted in the WLANs or even control the WLANs.
- *Access Control*: Access control service enables an authority to grant authorized users the corresponding access right to the resources in the WLANs. In this way, sophisticated implementations of access control policies in the WLANs allow for granting different users or groups with different security settings and with different levels of access rights to the resources after authenticating these users' or groups' identities.

- *Integrity*: Integrity assures the consistency of the data when it is transmitted in the WLANs. This requirement is also usually achieved by the utilization of encryption techniques. Strong integrity is essentially crucial for wireless traffic, as wireless network packets can be easily intercepted, modified, or even compromised by the attackers in the WLANs due to the broadcast nature of the wireless communication.
- *Intrusion Detection and Prevention*: Due to the continually increasing attacks to the WLANs, in addition to the above requirements, a robust WLAN also needs to provide wireless intrusion detection and prevention services (Wireless IDS/IPS). These services can identify and remove threats, but still allow neighboring WLANs to co-exist while preventing clients from accessing each other's resources[24]. It involves detecting rogue access points, regulating network access and defending against wireless Denial-of-Service (DoS) attacks.

To effectively and efficiently meet the above security requirements in the WLANs, it is significant and indispensable to design and implement robust security policies for the WLANs. These policies should not only layout the security schemas for the installations, managements, and usage procedures, but also be flexible in terms of the supported technologies and functions. Whenever the security policies are implemented in terms of these security challenges in the WLANs, deeply understanding WLAN specific vulnerabilities and existing attacks will be necessary and beneficial to designing more robust security policies.

3.2.2 Real-World WLAN Attacks

As mentioned before, despite the productivity and convenience that the WLAN offers, the improper human configurations or the operations, and the vulnerabilities in the existing WLAN security policies can still be utilized by the attackers to make legitimate wireless users at a risk. "To advance irresistibly, push through their gaps." In order to design more robust security mechanism and more powerful defense methods to enhance the WLAN security, it is very useful and meaningful to understand current real-world WLAN attacks. Although attacks against WLAN technologies are increasing in number and sophistication over time, we can summarize most current real-world WLAN attacks into the following categories: deauthentication, eavesdropping and interception of wireless traffic, traffic jamming, brute force attacks against access point passwords, attacks against security protocols and misconfiguration.

- *Deauthentication*: This kind of attacks attempt to defeat the authorization mechanism in WLANs. By launching this kind of attacks, the attackers can steal legitimate wireless users' identities or authorized wireless access points' deployment rights to mimic as authenticated users or deploy rogue access points without going through security process and review.

  - *MAC Spoofing*: By modifying the wireless client's MAC address, the attackers can bypass the MAC filtering policies widely utilized in the most current wireless systems. Specifically, many wireless systems can use a white list of MAC addresses to authorize the wireless clients. Only the wireless clients whose MAC addresses are in the white list can gain access to the network. However, by utilizing some software that can make a wireless client to pretend to have any customized MAC address[18], the attacker can easily get around that hurdle.
  - *IP Spoofing*: By modifying the source IP address contained in the packet header, an attacker can evade IP address based authentication and pretend itself to be a legitimately authenticated user who is communicating with others.
  - *Rogue Access Points*: Rogue access points are unauthorized access points that are deployed in the WLANs. In this way, the unauthorized clients can gain the open access to the WLAN through the rogue access points. Also, these rogue access points can also be settled as "honeypot" or "phishing" access points to achieve attackers' malicious goals.

- *Eavesdropping and Interception of Wireless Traffic*: This kind of attacks can eavesdrop or intercept legitimate wireless traffic by compromising the legitimate users' wireless communication channel. Through this kind of attacks, the attackers could achieve all the sensitive and important information sent by the legitimate users.
  - *Traffic Eavesdropping*: Attackers can break the confidentiality of the data by eavesdropping the whole WLAN. Due to the broadcasting nature, all the information is passing from the network interface cards (NIC) across a communication medium and the centralized device intentionally radiates the network traffic into space. In this way, an attacker can simply utilize some wireless network sniffers such as Kismet[7], Wellenreiter[11], Airtraf[3] and Airfart[1], to eavesdrop the wireless traffic in the whole WLAN. In the WLANs, traffic eavesdropping is typically the first step for an attacker to launch other attacks.
  - *Man-in-the-middle Attacks*: In this attack, an attacker can sit in the middle of the two-way communicating parties. In this way, by successfully cheating the senders and receivers that they are communicating under a private and reliable connection channel, the attacker could not only obtain all the transmitted information, but also intercept, modify and even impersonate the communication. Especially, evil twin attack is one of the representative man-in-the-middle attacks. It is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers[5].
  - *Network Injection*: In this kind of attacks, an attacker can inject bogus network traffic into the legitimate traffic. By inserting this bogus traffic, the attacker could achieve malicious goals like sending

re-configuration commands to the access points to fully control them.
  - *Session Hijacking*: This kind of attacks can be achieved by stealing a legitimate authenticated conversation session ID. As a result, the attacker could control the whole conversation session when it is still going on.
- *Traffic Jamming*: The goal of this kind of attacks is to heavily consume the bandwidth of the WLAN in order to overwhelm legitimate traffic. This kind of attacks can be achieved by flooding either valid or invalid messages, or high radio frequency signals.
  - *Denial of Service (DoS) Attacks*: Denial of service attacks are also easily applied to wireless networks, where legitimate traffic cannot reach the destinations due to the flooding of high-frequency radio signals or messages. Since the high bit rates of WLANs can overwhelm low bit rates of WLANs, an attacker can easily launch a denial of service attack by using a proper equipment that can flood higher radio frequency signals, corrupting all other legitimate signals until the whole WLAN ceases to function. In addition, an attacker can also use a wireless device to flood other wireless clients with bogus packets to create a denial of service attack.
  - *Spam Attacks*: Like spam in the traditional Internet security that can consume bandwidth and generate phishing attacks, attackers can also launch spam attacks by flooding spam messages over the whole wireless network channels. In this way, legitimate users cannot obtain normal service afforded by the WLAN due to the overflowing spam messages.
- *Brute Force Attacks Against Access Point Passwords*: Since most access points only use a single shared password with all connecting wireless clients, attackers can use brute force dictionary attacks to compromise this password by testing every possible password. As a result, the attacker could control the access point and even take over the whole WLAN.
- *Attacks Against Security Protocols*: To meet the security requirements, 802.11 standards have designed and utilized different security protocols such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). However, the vulnerabilities of these standards have been utilized by the attackers to crack them. For example, there are several WEP crackers such as AirSnort[2], Wepcrack[12] and Wep tools[13], which can be used by attackers to compromise WEP protocol.
- *Misconfiguration*: Many WLAN attacks are generated due to the limited security knowledge of the administrators of the WLANs, and human misconfigurations or improper operations to the access points. For example, access points are usually sold with an unsecured and common configuration with a goal of easing consumers' usages. Unless administrators with certain wireless security knowledge and properly configure the access points, these access points will remain at a high risk for being attacked. However, many studies (e.g., reference [26]) have pointed out that

many users would keep the default security configurations of the access points when they are deploying their WLANs. Obviously, these WLANs are very vulnerable and can be easily compromised by attackers.

3.3 WLAN Communication Security

After knowing about a bunch of real-world WLAN attacks, we also need to understand the advantages and weakness of existing WLAN security standards that are deployed to satisfy WLAN security requirements. Thus, this section will describe the security details of two existing representative IEEE 802.11 security standards — Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). Also, this section will give a brief introduction to other standards such as 802.1x, 802.11i (WPA2), and WAPI.

3.3.1 WEP Protocol

Wired Equivalent Privacy (WEP) is the first IEEE 802.11 security protocol, which was designed in September 1999. The main goal of this protocol is to guarantee the confidentiality, authentication and integrity by implementing encryption techniques in the MAC layer to protect link-level data communication security between the clients and the access points. Basically, WEP is implemented from the initial connection between the clients and the APs. The clients can only successfully connect to the APs by using the correct passwords. Also, WEP achieves the security goals by encrypting the transmission so that only the receivers who own the correct decryption key can decrypt the transmitted information.

3.3.1.1 WEP Framework

WEP utilizes RC4 encryption algorithm, CRC-32 (Cyclic Redundancy Code) checksum algorithm, and a pre-established shared secret key (the base key) to encrypt the transmission between the clients and APs. The original base key with a fixed value was 40 bits long. The key had been increased by most manufactures to 104 bits with a security concern.

Furthermore, WEP utilizes a generated traffic key which is the base key added with an initialization vector (IV). The initialization vector is a randomly-generated 24-bit sequence, converting the original 104-bit key to a new 128-bit key. In this way, since the values of the IV vary when different packets are generated, the encryption keys are also different for encrypting different packets. Thus, the same plaintext may generate different cipher text at different times.

3.3.1.2 WEP Vulnerabilities

Nowadays, WEP is no longer considered as a secure mechanism for WLAN, because it contains several vulnerabilities and can be compromised by the attackers. The major WEP vulnerabilities can be summarized into the following four categories[41]:

- *No forgery protection*: There is no forgery protection provided by WEP. Even without knowing the encryption key, an adversary can change 802.11 packets in arbitrary, undetectable ways, deliver data to unauthorized parties, and masquerade as an authorized user. Even worse, an adversary can also learn more about the encryption key with forgery attacks.
- *No protection against replays*: WEP does not offer any protection against replays. An adversary can create forgeries without changing any data in an existing packet, simply by recording WEP packets and then retransmitting later. Replay, a special type of forgery attack, can be used to derive information about the encryption key and the data it protects.
- *Misusing the RC4 encryption algorithm*: Although RC4 encryption algorithm should not be blamed, WEP misuses the RC4 encryption algorithm in such a way to expose the protocol to the weak key attacks. An attacker can utilize the WEP IV to identify RC4 weak keys, and then use known plaintext from each packet to recover the encryption key.
- *Reusing initialization vectors*: It is known that if the same traffic key should not be used twice for a stream cipher such as RC4. Since the length of the IV in IEEE 802.11 WEP is 24, there are only 16 777 216 possible values of the IV. In a large and busy network, an access point may exhaust the space of IVs and thus reuse the same IV after several hours. Furthermore, due to the well-known birthday paradox, for a 24-bit IV, there is a 50% probability the same IV will repeat after 212 (4096) packets. Thus, WEP enables an attacker to decrypt the encrypted data without ever learning the encryption key or even resorting to high-tech techniques by using the brute force attack.

3.3.1.3 WEP Attacks

Due to the above vulnerabilities in WEP, attackers have already launched attacks on WEP by compromising these vulnerabilities. This section describes the following three major attacks on WEP: Brute force attack, Key Stream Re-uses, and Weak IV attacks[23].

- *Brute force attack*: As mentioned before, there are around 17 million possible values of the IV, the brute force attack will try all possible keys either by manually or by the computers until the correct one is found. Attackers can utilize the computers to find the key within the time period of less than several days by a continuous search.
- *Key Stream Re-use attacks*: According to the policy of the Shared Key Authentication in WEP, the authenticator will first send a clear text to the supplicant also known as authentication peer. Then, the supplicant will be authenticated by replying with the correctly encrypted message

of the text. If an attacker can steal the ciphertext and plaintext pair by snooping the authentication communication, the attacker can simply recover the key stream by using RC4 algorithm on the ciphertext and plaintext pair. Once the attacker successfully recovers the key stream, he can decrypt all the data which is associated with that key stream.

- *Weak IV attacks*: By collecting sufficient data packets using weak IVs, the attacker can re-calculate the accurate WEP key[27]. Specifically, a single weak IV reveals a correct key byte 5% of the time. By gathering a high number of statistics (IVs), the most probable key may be calculated within several days.

3.3.1.4 WEP Cracking Tools

Due to WEP's vulnerabilities, many public tools have been developed to crack WEP. This section will briefly introduce several WEP cracking tools[40].

- *AirSnort*: One of the most famous WEP cracking tools is AirSnort[2]. By displaying an intuitive human-machine interface, AirSnort is very convenient for people to use to discover networks and crack WEP. Besides cracking WEP, AirSnort can also be used to dump wireless packets and to save them as pcap-format files.
- *Wepcrack*: As one of the first few WEP cracking tools implementing theoretical attacks into practice, Wepcrack[12] consists of a collection of Perl scripts such as WEPcrack.pl, WeakIVGen.pl, and prism-getIV.pl. It can collect packets with initialization vectors (IVs) and save the weak IVs in a log file called IVFile.log. Then, attackers can simply use the following command to crack WEP protocol: (assuming the wireless network interface is wlan0)

  ```
  root:# tcpdump - i wlan0 -w - | perl prism-getIV.pl
  ```

- *Wep_tools*: Wep_tools[13] is a WEP cracking toolkit implementing brute-force and dictionary attacks. By compromising the 40-bit WEP-from-passphrase generation algorithm, it is efficient to crack original 40-bit WEP keys. For the 128-bit WEP keys, attackers are limited to launch dictionary attack by using practical terms. Wep_tools can be run on Linux machines using the following command[40]:

  ```
  root:# ./wep_crack
  Usage: ./wep_crack [-b] [-s] [-k num] packfile [wordfile]
  -b       Brute force the key generator
  -s       Crack strong keys
  -k num   Crack only one of the subkeys without using a key generator
  ```

3.3.2 WPA Protocol

As an enhanced WLAN security protocol, Wi-Fi Protected Access (WPA) is invented by Wi-Fi Alliance (WFA) in the year of 2002 to improve the initial

security standard WEP. Essentially, WPA is implemented by designing more complex encryption and authentication methods in place of merely using WEP's basic RC4 encryption.

WPA contains two modes: Enterprise/commercial WPA and Personal/ WPA-PSK (Pre-Shared Key) WPA. In Enterprise mode, WPA functions as a Remote Authentication Dial In User Service (RADIUS) server. It provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. In Personal mode, it utilized Pre-Shared Key (PSK) containing the network SSID and the WPA key generated by the access point to provide authenticity to wireless networks.

3.3.2.1 WPA Framework

WPA achieves the goal of designing a more secure wireless standard by mainly using the Temporal Key Integrity Protocol (TKIP) and Message Integrity Check (MIC). In the TKIP protocol, it has two different keys: a 128-bit key, which is used by a mixing function to produce a per-packet encryption key, and a 64-bit key, which is used to guarantee message integrity.

As discussed before on WEP's vulnerabilities, one major weaknesses of WEP was the small size of its initialization vector. In TKIP, the size of IV is increased from 24 to 40, which can effectively reduce the probability of generating key collisions. In addition, every key in the TKIP has its own fixed lifetime. The key will automatically be replaced when the key reaches its lifetime. Although WPA also uses RC4 algorithm like WEP, the per-packet key mixing function and re-keying mechanism in the WPA can guarantee that keys are frequently updated when using RC4. With the larger key size and the dynamic key encryption method, WPA can defend against stronger attacks. Also, instead of using Cyclic Redundancy Check (CRC) in the WEP standard, WPA guarantees the message integrity by using Message Integrity Check (MIC). The purpose of MIC is to prevent an attacker from capturing, altering and/or re-sending data packets. Essentially, it achieves this by appending 64 bits Cryptographic Message Integrity Code with the IV.

3.3.2.2 WPA Vulnerabilities

In general, WPA is a stronger encryption standard than WEP by using the TKIP protocol. However, it may still be an interim solution due to its several vulnerabilities, which will be described in this section.

Since WPA still utilizes the RC4 cipher stream algorithm, an attacker can also brute force two distinct RC4 keys to recover the 128-bit temporal key in WPA, known as temporal key recovery attack[34]. Once an attacker achieves the key, he can nearly do anything before current temporal key expires.

In Personal WPA mode, it utilizes the Pre-Shared Keys (PSKs) for the authentication rather than using a dedicated authentication server. Due to the broadcasting nature of the wireless device to create and verify a session key, the attacker could steal the information about the key by passively sniffing the wireless communication channel. Also, the attacker can launch an

offline dictionary attack on the keys, when WPA tools are using handshake process for exchanging the data encryption keys between the access point and the end user. Thus, PSK, requiring simple deployments, is designed to meet the security requirement in the small and less critical wireless networks. However, the risk of using PSK can still not be neglected.

3.3.2.3 WPA Attacks

Similar to the situation of WEP, attackers also utilize WPA's vulnerabilities to launch their attacks. As the problem of the PSKs mentioned in the previous section, any key generated from a passphrase of less than about 20 characters is highly vulnerable to the offline PSK dictionary attack[35].

In addition, although WPA utilizes more sophisticated methods and protocols to prevent key attacks, the attacker can still launch an improved version of ChopChop attack[22] to decrypt the wireless traffic by sending customized packets to the network. In addition, WPA may also suffer from DoS attack. For example, when the WPA wireless device receives two packets of unauthorized data within one second from the same user, it will assume it is under attack and automatically shut down itself. In this way, the attacker can launch the DoS attack by rapidly repeating sending authentication packets to the wireless device.

3.3.3 Other Security Protocols

In addition to the above two traditional and representative WLAN security protocols, we also briefly introduce other security standards such as 802.1x, 802.11i (WPA2), and WAPI in this section.

3.3.3.1 802.1x

As part of the 802.11i standard, IEEE 802.1x protocol is designed for the Port-based Network Access Control (PNAC). It provides an authentication mechanism for the wireless devices to connect to a LAN or WLAN. It also guarantees the security requirement of the data transmission for the components that are connected with each other through different 802.11 LANs.

The 802.1x authentication system has three major components: a supplicant, an authenticator, and an authentication server. The supplicant is a wireless client device wishing to connect to the WLAN. The supplicant refers to the software running on the client that provides credentials to the authenticator. The authenticator is usually a network device (e.g., a wireless access point) that transmits this information between the supplicant and the authentication server. The authentication server is typically a network device, such as an Ethernet switch or wireless access point, running software to support the RADIUS and Extensible Authentication Protocol (EAP), which is defined in the 802.1x standard. In this way, the authenticator, validating and authoring the supplicant's identity, acts like a security guard to protect

the WLAN.

3.3.3.2 802.11i (WPA2)

After the 802.1x standard, IEEE 802.11i, also known as WPA2, is an additional specification that is finalized in fall 2004 in order to provide replacement technology for WEP security in the WLAN. Generally, to provide enhanced WLANs' security, WPA2 defines data confidentiality, mutual authentication, and key management protocols.

Compared with WEP and WPA, one of the significant improvements of WPA2 is that it utilizes a single component, named as counter mode with CBC-MAC Protocol (CCMP), for authentication, key management and message integrity. CCMP is built based on an enhanced version of encryption algorithm — Advanced Encryption Security (AES), which is one of the most secured encryption standards. Specifically, CCMP consists of two components: Counter mode, used in AES to encrypt the data that provides data protection from unauthorized access, and Cipher Block Chaining Message Authentication Code (CBC-MAC) mode, creating a Message Integrity Check (MIC) code to provide message integrity. In addition, WPA2 use 802.1x or pre-shared keys (PSKs) to authenticate the wireless client and the authentication server. It also defines the Robust Security Network Association (RSNA) protocol to provide mutual authentications.

In brief, the comparison of WEP, WPA, and WPA2 can be summarized in Table 3.1.[36]

Table 3.1 The comparison of WLAN security protocols

Security Protocol	WEP	WPA	WPA2
Major Component	IV	TKIP	CCMP
Stream Cipher	RC4	RC4	AES
Key Size	40 bit	128 bit (encryption) and 64 bit (authentication)	128 bit
IV Size	24 bit	48 bit	48 bit
Key Management	Not Available	IEEE 802.1x/EAP	IEEE 802.1x/EAP/CCMP
Date Integrity	CRC-32	MIC	CBC-MAC

As shown in Table 3.1, the main advantages of the WPA2 standard can be listed as follows[30]:

- Providing more excellent security by using advanced encryption algorithms;
- Using stronger key management policies;
- Protecting against the man-in-the-middle attacks by using the two-way authentication process;
- Providing improved message integrity by using CBC-MAC.

Although WPA2 is designed to cover up for the weaknesses of WEP, it still

has its own drawbacks. First, WPA2 is costly. Due to the requirements of the implementation of the advanced properties designed in WPA2 (e.g., CCMP), a lot of money and effort will be costed on upgrading existing hardware and software. Also, due to the need of bidirectional authentication between users and access points, WPA2 requires more hardware to achieve the security goal. Second, WPA2 is still vulnerable to DoS attacks[36]. Attackers can send large amount of authentication requests to the authentication server simultaneously so that the 8-bit space of EAP packet will be exhausted, leading the network under DoS attacks. Third, WPA2 is also prone to attacks such as security level rollback attack, reflection attack, and Time Memory Trade Off (TMTO) attack. Specifically, when Pre-RSNA and RSNA algorithms are both used in a single WLAN, an adversary can launch a security level rollback attack, avoiding authentication and disclosing the default keys[29]. Also, if a device is implemented to play the roles of authenticator and supplicant (in ad hoc networks, typically not in infrastructure networks), attackers can launch the reflection attack during the 4-Way Handshake. Current studies[33] also show that attackers can launch TMTO pre-computation attack, if they have sufficient knowledge about the WLAN so that they can successfully obtain the initial counter value used in the AES of CCMP.

3.3.3.3 WAPI

Besides internationally well-acknowledged WLAN security standards, to adapt to the rapid developments of Chinese WLANs and to meet the security requirements of Chinese wireless users, China has also finalized its own national WLAN security standard in 2003 — WLAN Authentication and Privacy Infrastructure (WAPI)[15]. According to WAPI protocol specification[16,17], WAPI consists of two modules: Wireless Authentication Infrastructure (WAI) and Wireless Privacy Infrastructure (WPI). Specifically, WAI is designed for the authentication process and key management and WPI is implemented to provide the data protection and integration service.

As the major module of WAPI, WAI[9] adopts port-based authentication architecture to authorize the credentials similar to 802.1x standard, including three components: the Authentication Supplicant Entity (ASUE), the Authentication Entity (AE), and the Authentication Service Entity (ASE). The process of the certificate authentication and key management in the WAPI can be illustrated in Fig. 3.3.

In the process of certificate authentication, AE first sends authentication activation packets to ASUE to active the entire authentication process. Once receiving the authentication activation from AE, ASUE verifies whether the activation packets meet ASUE's requirements. If so, ASUE will send an authentication request with its own certificate and an access request time to AE. Then, AE signs its own name on the ASUE's certificate, ASUE's access request time and its own certificate, and sends this information as the certificate authentication request to ASE. After the certificate request is successfully authenticated by ASE, AE will receive the certificate authentication

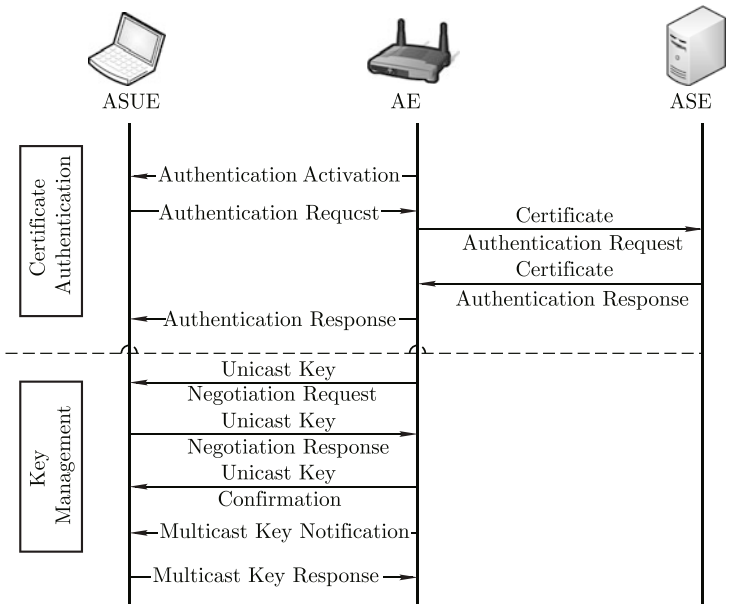

Fig. 3.3 Illustration of WAPI authentication process.

response from ASE and send it to ASUE. Finally, ASUE decides whether to access AE by checking the authentication response from ASE. From this Security in Wireless Local Area Networks architecture, we can see that WAPI supports the mutual authentication between ASUE (wireless clients) and AE (Access points).

In the process of key management, AE will first send a unicast key negotiation request including cryptography algorithms negotiation to ASUE. Once AE receives the agreement response of the negotiation request from ASUE, AE will send a unicast key confirmation to ASUE. After successfully building the agreement on the execution of the unicast key, AE will start the multicast key process, which utilizes the unicast session key for the encryption.

In short, as the first WLAN standard developed and owned by China itself, WAPI undoubtedly plays a very important role in the developments of the field of WLAN security in China.

3.4 WLAN Access Point Security

As one essential component in WLAN, access points, directly communicating with the end-users, need to be carefully deployed and protected. Thus, in this section, we mainly talk about security issues in the WLAN access points.

3.4.1 Rogue Access Points

As mentioned in Section 3.2.2, rogue access points are unauthorized access points that are deployed in the WLANs. The main purpose of deploying the rogue access points for the attackers is to get access of other users' resources. Specifically, the unauthorized clients can gain the open access to the WLAN through the rogue access points. In addition, the rogue access points can be utilized as honeypot access points to steal other users' credentials.

Existing rogue AP detection solutions can be mainly classified into two categories. The first category of the approaches monitors Radio Frequency (RF) airwaves and/or additional information gathered at routers/switches and then compares with a known authorized list. For example, AirDefense[19] scans RF from the Intranet APs to locate suspicious ones, and then compares specific "fingerprints" of the RF with an authorized list to verify. More specifically, for the scanning part, some studies such as[8,4,10] rely on sensors instead of sniffers to scan the RF; some studies like[20] propose a method to turn existing desktop computers into wireless sniffers to improve the efficiency. For the verification part, these studies verify MAC addresses, SSID, and/or location information of the AP by using an authorized list. However, these studies still have the risk of falsely claiming a normal neighbor AP as a rogue AP with a high probability. To solve this problem, they need to further verify whether such a rogue AP is indeed in the internal network.

The second category of approaches detects rogue access points by differentiating whether the clients come from wireless networks or wired networks. Essentially, if a client comes from a wireless network while it is not authorized to use wireless (comparing with an authorized list), the AP attached to this host is considered as a rogue AP. Some work such as[21,33,37,42,43] use statistical features (e.g., entropy, median, mean) on the traffic time (e.g., RTT) to distinguish the type of network. It is also possible to use the frequent rate adaptation in the wireless network to distinguish it with wired networks[25]. However, this line of work should solve the problem of falsely claiming an authorized wireless user who connects to Intranet with wireless networks. Thus, they may still need to further verify a wireless device is an authentic AP or not with some "fingerprints" from the authorized lists. To solve this problem, two hybrid studies[32,39] provide the technique to compare the fingerprints in the integrated systems.

3.4.2 Evil Twin Access Point

As one special type of rogue AP, an evil twin AP is essentially a phishing Wi-Fi access point (AP) that pretends to be a legitimate one (with the same SSID name). It is set up by an adversary, who can eavesdrop or modify wireless communications of users' Internet access. In the next paragraph, we

briefly introduce three representative works that are aiming to detect evil twin attacks.

In reference [31], Jana and Kasera utilize the fact that different APs usually have different clock skews to detect unauthorized wireless access points. This work utilizes the fingerprint technique, which still needs a white list of the authorized access points. In reference[28], Han et al. utilizes time interval information to detect rogue APs. Specifically, it calculates the round trip time between the user and the DNS server to independently determine whether an AP is legitimate or not without the assistance from the WLAN operators. Song et al.[38] proposes a user-side evil twin detection technique by differentiating one-hop and two-hop wireless channels from the user side. This work exploits fundamental communication structures and properties of evil twin attacks in wireless networks and designs active, statistical, and anomaly detection algorithms to identify evil twin APs.

3.5 Other WLAN Security Issues

Besides the security standards such as WEP, WPA, 802.1x, 802.11i and WAPI that have been discussed previously, other security mechanisms such as Wireless Firewalls, Wireless Virtual Private Network (VPN) and Wireless Intrusion Detection System (IDS) can also be utilized to enhance the security of WLANs.

- *Wireless Firewalls*: Like traditional network firewalls, a wireless firewall functions as a barrier between the private network and the Internet to prevent external attacks to the internal network. A wireless firewall can protect an internal host or server from insecure Internet traffic by filtering out suspicious packets.
- *Wireless VPN*: A virtual private network (VPN) utilizes a public telecommunication infrastructure, such as Internet, to provide secured remote communication for the users to their private organization network. Since WLAN uses unlicensed frequency bands and can be easily accessible to outsiders either accidentally or with malicious intent, wireless networking provides an important area for VPN deployment and maintenance[40].

Compared with the physical restriction on the deployments of wired VPNs, wireless VPNs can be applicable and deployed to any WLAN, as long as a high level of security is concerned. Although the standard of 802.11i can guarantee the same security requirements as the wireless VPNs, the vulnerabilities in the implementations of the 802.11i standard could still make it less trustworthy. Thus, in an environment requiring a high level of security, besides traditional protocol standards such as WEP, WPA and WPA2, wireless VPNs, based on the Internet Protocol Security (IPsec) protocol, can still function as another safeguard to protect the security in the WLAN. In addition, in the case of point-to-point wireless links it is easier and more economical

to deploy a network-to-network VPN than 802.11i-based defenses, including the RADIUS server and user credentials database, while using 802.11i with PSK and no 802.11x is not a good security solution for a high throughput network-to-network link[40].

- *Wireless IDS*: An intrusion detection system (IDS) is a device or software attempting to perform network intrusion detection and stop possible incidents/attacks by gathering and analyzing data. To protect WLAN security, IDSs have already been developed for the use on the WLAN, known as wireless IDSs. Similar to traditional IDSs, these wireless IDSs can recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WLANs by monitoring and analyzing network, user, and system activities. Also, like traditional signature based IDSs and anomaly-based IDSs, wireless IDSs can generate intrusion alters according to either the predefined signatures or the observed abnormal network behavior.

Wireless IDSs can be divided into centralized IDSs and decentralized IDSs. In a centralized wireless IDS, the central management system will combine and analyze all wireless data from each distributed individual sensor. In a decentralized wireless IDS, there are more than one device that both collect data and generate the intrusion alerts by analyzing the data.

3.6 Conclusion

In this chapter, we have discussed security issues and techniques in the Wireless Local Area Networks (WLAN). Essentially, we present a brief introduction of the WLAN background and the current state of WLAN security. Then, we provide some details on wireless security protocols and access point security. Finally, we also talk about other security mechanisms that can be used to enhance WLAN security including Wireless Firewalls, Wireless VPN, and Wireless IDS. As we can conclude, it is obvious that although WLANs, as a viable supplement to wired LAN, have been widely accepted in our real life, it is still in its infant stages as long as security is concerned.

References

[1] Airfart. http://airfart.sourceforge.net/.
[2] AirSnort. http://airsnort.shmoo.com/.
[3] Airtraf. http://airtraf.sourceforge.net/.
[4] Cisco Wireless LAN Solution Engine (WLSE). Available at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/. Accessed 10 November, 2011.
[5] Evil Twin Attack. Available at http://www.redoracle.com/index.php?option=com_remository&Itemid=82&func=fileinfo&id=59. Accessed 10 November, 2011.

[6] IEEE 802 Standards. Available at http://en.wikipedia.org/wiki/IEEE_802. Accessed 10 November, 2011.

[7] Kismet. http://www.kismetwireless.net/. Accessed 10 November, 2011.

[8] Rogue access point detection: Automatically detect and manage wireless threats to your network. http://www.proxim.com. Accessed 10 November, 2011.

[9] WAPI implementation plan. http://www.wapia.org/files/Guide. Accessed 10 November, 2011.

[10] Wavelink. http://www.wavelink.com. Accessed 10 November, 2011.

[11] Wellenreiter. http://www.kismetwireless.net/. Accessed 10 November, 2011.

[12] Wepcrack. http://wepcrack.sourceforge.net/. Accessed 10 November, 2011.

[13] Wep tools. http://www.redoracle.com/index.php?option=com_remository&Itemid=82&func=fileinfo&id=59. Accessed 10 November, 2011.

[14] Wireless LAN. http://en.wikipedia.org/wiki/Wireless_LAN. Accessed 10 November, 2011.

[15] WLAN Authentication and Privacy Infrastructure. http://en.wikipedia.org/wiki/WLAN_Authentication_and_Privacy_Infrastructure. Accessed 10 November, 2011.

[16] GB 15629.11-2003. Information technology telecommunications and information exchange between systems local and metropolitan area networks specific requirements part 11: Wireless Lan Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[17] GB 15629.11-2003-XG1-2006. Information technology telecommunications and information exchange between systems local and metropolitan area networks specific requirements part 11: Wireless Lan Medium Access Control (MAC) and Physical Layer (PHY) specifications amendment 1.

[18] SMAC 2.0 MAC Address Changer. http://www.klcconsulting.net/smac/. Accessed 10 November, 2011.

[19] AirDefense. Tired of Rogues? Solutions for Detecting and Eliminating Rogue Wireless Networks. White paper, http://wirelessnetworkchannel-asia.motorola.com/pdf/. Accessed 10 November, 2011.

[20] Bahl P, Chandra R, Padhye J, Ravindranath L, Singh M, Wolman A, Zill B (2006) Enhancing the security of corporate Wi-Fi networks using DAIR. In Proc. MobiSys'06.

[21] Baiamonte V, Papagiannaki K, Iannaccone G, Torino P (2007) Detecting 802.11 wireless hosts from remote passive observations. In Proc. IFIP/TC6 Networking.

[22] Beck M, Tews E (2009) Practical attacks against WEP and WPA. In Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec).

[23] Bittau A, Handley M, Lackey J (2006) The Final Nail in WEPs Coffin. In IEEE Symposium on Security and Privacy.

[24] Siemens Enterprise Communications. WLAN Security Today: Wireless more Secure than Wired. http://www.enterasys.com/company/literature/WLAN%20Security%20Today-Siemens%20whitepaper_EN.pdf. Accessed 10 November, 2011.

[25] Corbett C, Beyah R, Copeland J (2006) A passive approach to wireless NIC identification. In IEEE International Conference on Communications (ICC'06).

[26] Cui A, Stolfo S (2010) A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan. In Annual Computer Security Applications Conference (ACSAC'10).

[27] Fluhrer S, Mantin I, Shamir A (2001) Weaknesses in the Key Scheduling Algorithm of RC4. In Lecture Notes in Computer Science, 2259: 1C24.

[28] Han H, Sheng B, Tan C, Li Q, Lu S (2009) A Measurement Based Rogue AP DetectionScheme. In IEEE International Conference on Computer Communications (INFOCOM 2009).

[29] He C, Mitchel J (2005) Security Analysis and Improvements for IEEE 802.11i. In Proceedings of the Network and Distributed System Security Symposium (NDSS'05).

[30] Ilyas M, Ahson S (2005) Handbook of Wireless Local Area Networks: Applications, Technology, Security, and Standards (Internet and Communications). CRC Press.

[31] Jana S, Kasera S (2008) On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews. In The Annual International Conference on Mobile Computing and Networking (MobiCom08).

[32] Ma L, Teymorian A, Cheng X (2008) A hybrid rogue access point protection framework for commodity Wi-Fi networks. In Proc. IEEE INFOCOM 2008.

[33] Mano C, Blaich A, Liao Q, Jiang Y, Cieslak D, Salyers D, Striegel A (2008) RIPPS: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning. ACM Transactions on Information and System Security (TISSEC), 11(2): 1 – 23.

[34] Moen V, Raddum H, Hole K (2004) Weaknesses in the Temporal Key Hash of WPA. In Mobile Computing and Communications Review, pp. 76C83.

[35] Moskowitz R (2003) Weakness in Passphrase Choice in WPA Interface. http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html. Accessed 10 November, 2011.

[36] Pervaiz M, Cardei M, Wu J (2008) Security in Wireless Local Area Networks, Proceedings of Y. Xiao and Y. Pan (eds.). Security in Distributed and Networking Systems, World Scientific Publishing Co Inc.

[37] Shetty S, Song M, Ma L (2007) Rogue access point detection by analyzing network traffic characteristics. In IEEE Military Communications Conference (MILCOM'07).

[38] Song Y, Yang C, Gu G (2010) Who Is Peeping at Your Passwords at Starbucks? — To Catch an Evil Twin Access Point. In Proceedings of the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'10).

[39] Srilasak S, Wongthavarawat K, Phonphoem A (2008) Integrated Wireless Rogue Access Point Detection and Counterattack System. In International Conference on Information Security and Assurance, pp. 326 – 331.

[40] Vladimirov A, Gavrilenko K, Mikhailovsky A (2008) Wi-Foo: The Secrets of Wireless Hacking. Addison-Wesley Professional, Boston.

[41] Walker J (2005) 802.11 Security Series Part II: The Temporal Key Integrity Protocol (TKIP). http://jcbserver.uwaterloo.ca/cs436/handouts/miscellaneous/Intel_Wireless_2.pdf. Accessed 10 November, 2011.

[42] Wei W, Jaiswal S, Kurose J, Towsley D (2006) Identifying 802.11 traffic from passive measurements using iterative Bayesian inference. In Proc. IEEE INFOCOM'06.

[43] Wei W, Suh K, Wang B, Gu Y, Kurose J, Towsley D (2007) Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs. In Proceedings of the 7th ACM SIGCOMM conference on Internet measurement (IMC'07).

[44] Wexler J (2010) 2009 Wireless LAN State-of-the-Market Report. http://www.webtorials.com/content/2010/03/2009-wlan-sotm.html. Accessed 10 November, 2011.