Wireless Pers Commun (2016) 90:1261–1290
DOI 10.1007/s11277-016-3390-x

Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions

Bandar Alotaibi[1] · **Khaled Elleithy**[1]

Published online: 11 June 2016

Abstract Wireless Local Area Networks (WLANs) are increasingly integrated into our daily lives. Access Points (APs) are an integral part of the WLAN infrastructure, as they are responsible for coordinating wireless users and connecting them to the wired side of the network and, eventually, to the Internet. APs are deployed everywhere, from airports and shopping malls to coffee shops and hospitals, to provide Internet connectivity. One of the most serious security problems encountered by WLAN users is the existence of Rogue Access Points (RAPs). This article classifies existing solutions, identifies vulnerabilities, and suggests future directions for research into these RAPs. The ultimate objective is to classify existing detection techniques and find new RAP types that have not been classified by the research community. The literature typically categorizes Evil-twin, Unauthorized, Compromised, and Improperly Configured RAPs. Two other types have largely been abandoned by researchers, but can be classified as Denial of Service RAP attacks. These are deauthentication/disassociation attacks targeting wireless users, and the forging of the first message in a four-way handshake.

Keywords WLAN · Rogue Access Point · Evil-twin · Unauthorized AP · DoS attacks · Four-way handshake

Abbreviations

WLAN	Wireless Local Area Network
Wi-Fi	Wireless Fidelity (some resources indicate that it is just Wi-Fi)
DoS	Denial of Service
IP	Internet Protocol
SSID	Service Set Identifier
RTS	Request to Send

✉ Bandar Alotaibi
balotaib@my.bridgeport.edu

[1] Computer Science and Engineering Department, University of Bridgeport, 126 Park Ave, Bridgeport, CT 06604, USA

ATIM	Announcement Traffic Indication Message
IEEE	Institute of Electrical and Electronics Engineers
DNS	Domain Name System
MITM	Man-in-the-Middle
WPA-PSK	Wi-Fi Protected Access-Pre-Shared Key
WIDS	Wireless Intrusion Detection System
IV	Initialization Vector
EAP	Extensible Authentication Protocol
LEAP	Lightweight Extensible Authentication Protocol
TLS	Transport Layer Security
FAST	Flexible Authentication via Secure Tunneling
PEAP	Protected Extensible Authentication Protocol
VPN	Virtual Private Network
SVM	Support Vector Machine
RSSI	Received Signal Strength Indicator
ISP	Internet Service Provider
CA	Certification Authority
TSF	Timing Synchronization Function
ACK	Acknowledgment
CPU	Central Processing Unit
API	Application Programming Interface
3D	Three-Dimensional
GTK	Group Temporal Key
AP	Access Point
RAP	Rogue Access Point
IDS	Intrusion Detection System
MAC	Media Access Control
BSSID	Basic Service Set Identifier
CTS	Clear to Send
CF	Contention Free
DHCP	Dynamic Host Configuration Protocol
SSL	Secure Sockets Layer
iOS	iPhone Operating System (originally known as iPhone OS, but it can be used for iPad and iPod)
WEP	Wired Equivalent Privacy
WIPS	Wireless Intrusion Prevention System
ICV	Integrity Check Value
RADIUS	Remote Access Dial in User Services
MD5	Message Digest 5
TTLS	Tunneled Transport Layer Security
HTTP	Hypertext Transfer Protocol
DCF	Distributed Coordinated Function
RTT	Round Trip Time
TCP	Transmission Control Protocol
PLCP	Physical Layer Convergence Protocol
IANA	Internet Assigned Numbers Authority
SSH	Secure Shell
IBSS	Independent Basic Service Set

NAT	Network Address Translation
TOFU	Trust on First Use
NIC	Network Interface Controller
PTK	Pairwise Transient Key
PMK	Pairwise Master Key

1 Introduction

The widespread deployment of wireless infrastructure and the provision of portable devices are responsible for a surge in the popularity of Wireless Local Area Networks (WLANs) [1]. Internet usage has moved from stationary computers that are connected to the wired side of the network to mobile devices such as smartphones, laptops, and tablets, which use radio waves to connect to an Access Point (AP) and then to the Internet. People spend a large amount of time online, regardless of where they are. To connect to the Internet, users have to choose between two options. The first is to use a Wi-Fi network, in particular when connecting to the Internet from homes, offices, airports, shopping malls, and universities. The other, more costly option is to use mobile cellular networks. This second option has increased in popularity over the past decade. However, the influence of WLANs remains crucial, especially as Wi-Fi hotspots become ubiquitous. Most wireless users prefer WLANs because, unlike cellular networks, they are free to use [2]. APs are an integral part of WLANs, providing a coordinated point that manages workstations and connects users to the wired network [3]. One of the most common security problems faced by WLANs is the Rogue Access Point (RAP)[4–10], which is a fake AP that was not installed by the network administrator.

As APs have become cheaper, the ability to deploy them maliciously in WLANs has grown tremendously. In the literature, RAPs are classified into four categories: Evil-twin APs, Improperly Configured APs, Unauthorized APs, and Compromised APs [5, 11]. There are also RAP-based DoS attacks that are not classified by the research community. These are deauthentication/disassociation attacks and the forging of the first message in a four-way handshake (see Sect. 1.2 for a detailed explanation). It has been estimated that approximately 20 % of all APs in enterprise WLANs are in fact RAPs [12–14]. Some of the early RAP detection methods assumed that the RAP has been inserted by a naive user who wants to access the Internet from, for example, a conference room. Although this was initially true, today it is more likely that the person who has inserted the RAP is a skilled attacker that knows and can evade RAP countermeasures [12]. Current mobile devices contain an array of personal information, such as photos, passwords, business documents, and important emails. Therefore, connecting to RAPs is highly dangerous, because it could allow attackers to steal sensitive information. Thus, it is vital to secure WLANs and detect suspicious APs.

1.1 Overview of the 802.11 Standard

This subsection describes the 802.11 wireless standard at the abstract level. As the focal point of this survey is APs, we briefly explain the infrastructure mode. The frame types in the 802.11 standard fall into three categories: management, control, and data. Each type contains several sub-types, as shown in Table 1. Management frames allow WLAN devices to initiate and maintain communications. Control frames govern the wireless links,

Table 1 WLAN class 1, 2, and 3 frames

	Management	Control	Data
Class 1 frames	Beacon, Probe Request/Response	RTC, CTS, ACK	Frames with false ToDS
	Authentication, Deauthentication and ATIM	CF-END and CF-ACK	or FromDS
Class 2 frames	Association Request/Response, Disassociation		
	and Reassociation Request/Response		
Class 3 frames	Deauthentication	PS-Poll	All data frames

allowing some stations to access the medium while denying access to others. Data frames convey higher-layer data [15].

Connections are established using several management frame sub-types, as shown in Fig. 1. The first step is network discovery, which starts when the AP advertises its existence by broadcasting beacon frames to clients in the vicinity. Clients passively listen to the beacon frames or actively send probe requests to identify APs within range. After receiving a probe request, the AP sends a probe response frame that contains important information such as the supported rates and capabilities of the network. The second step involves the exchange of authentication and association messages. Authentication is the procedure of sending the identity of the station to the AP through the authentication request frame. Upon receiving the request, the AP either accepts or rejects the wireless user via an authentication response. In an open authentication environment, no identity checking takes place. The association request is sent by the station to enable the AP to allocate resources to the wireless user and to synchronize with the users NIC. The association response sent by the AP details the acceptance or rejection of the connection [16]. Subsequently, the AP and wireless user can exchange data. Establishing secure communication requires further steps after the association stage, such as the exchange of four-way handshake messages for mutual authentication (see Sect. 1.2.6) in WPA/WPA2-PSK or the provision of credentials

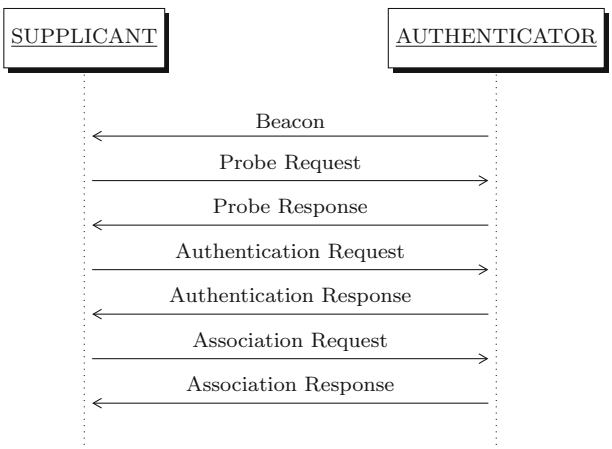

Fig. 1 Establishing a connection for open authentication

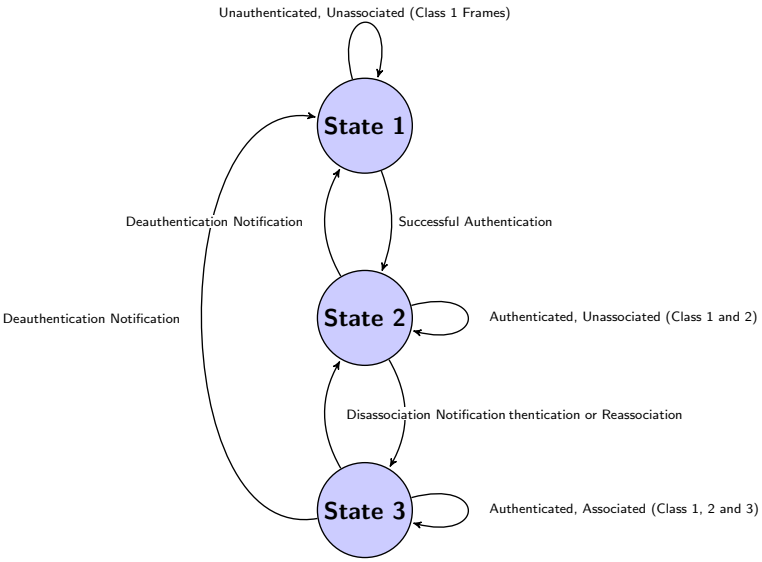

Fig. 2 Deauthentication and disassociation procedure

to the authentication server (i.e., RADIUS [17]) in the enterprise mode before the four-way handshake exchange [18].

The authentication/association and deauthentication/disassociation state diagram is shown in Fig. 2. In the first state, the station is neither authenticated nor associated. After the authentication exchange, the station becomes authenticated, but is not associated. Sending a deauthentication message at this stage causes the station to return to the first state, whereas exchanging association frames places the station in the third state, whereby the station is authenticated and associated and can exchange data. Sending a deauthentication frame pushes the station back to the first state, whereas sending a disassociation frame causes the station to return to the second state [19, 20]. To terminate an established connection, the AP disconnects one or all of the connected clients using the broadcast address by sending a deauthentication frame. Both the station and the AP can send a disassociation frame to end the association. For example, the wireless station can send a disassociation frame when the NIC is powering off, allowing the AP to remove the station from the association table and deallocate memory. Deauthentication/disassociation frames are not protected in 802.11i, but are encrypted in 802.11w [21] after the four-way handshake (i.e., exchanging the session keys (PTKs, GTKs)). However, there are some issues regarding the deployment of this standard, namely that millions of devices need to be changed or upgraded. Hence, few WLANs worldwide have implemented this standard. Thus, deauthentication/disassociation DoS attacks remain a problem in WLANs.

1.2 Taxonomy of RAPs

In the literature, RAPs are classified into four categories: Evil-twin, Improperly Configured, Unauthorized, and Compromised. Two more types that can also be classified as DoS attacks are RAP-based deauthentication/disassociation attacks and the forging of the first message in a four-way handshake. These latter two are classified as RAPs in this article, because the deauthentication/disassociation attacks can be sent on behalf of a legitimate AP to disconnect

wireless users. This is similar to the Evil-twin attack, because the attacker spoofs the MAC address of the legitimate AP to disconnect associated users. The forged message in a four-way handshake is sent by a hacker who masquerades as the genuine AP to disturb and block the four-way handshake message exchange between the wireless user and the AP.

1.2.1 Evil-twin

Sometimes referred to as Soft AP or Spoofed AP, we use the term Evil-twin to represent this type of attack. The Evil-twin AP uses a software-based AP installed on a portable device. Thus, a portable device with an external wireless card and a tool such as airbase-ng[1] are sufficient to set up this type of RAP. There are only two identifiers in the IEEE 802.11 standard that can authenticate APs to users. These are the SSID and MAC address (BSSID) of the AP [22]. As these identifiers can easily be spoofed, the AP can be fabricated by an outsider and remain undistinguishable by wireless users. Evil-twin APs come in two forms:

Coexistence: the legitimate AP and the Evil-twin coexist in the same location. The Evil-twin clones the SSID and MAC address of the legitimate AP [23], and increases its signal strength to force users to connect. It then relays packets through the legitimate AP.

Replacement: the Evil-twin shuts down the legitimate AP and replaces it. This form of RAP has its own Internet connection.

The first form uses two wireless cards, one built-in to the device and the other a plug-and-play wireless card. The built-in wireless card associates with the legitimate AP, while the other wireless card masquerades as the legitimate AP. Packets are then relayed from the Evil-twins plug-and-play wireless card to the built-in wireless card. The Evil-twin AP is set up by an adversary to listen to users traffic as they browse the Internet, and to launch several attacks on the victims devices [4, 24–26]. The IEEE 802.11 standard states that WLAN clients must connect to the AP that has the strongest signal. To lure users, the Evil-twin can move closer to the users or increase its signal strength to be stronger than the legitimate AP. The Evil-twin then waits for users to connect to it, or may send DoS attacks via deauthentication or disassociation frames on behalf of the legitimate AP to force users to disconnect from the legitimate AP. In practice, an Evil-twin configuration involves more steps to avoid IDSs, such as masquerading AP MAC address and SSID, establishing a DNS server to connect to the Internet, and establishing a DHCP server to automatically assign connected clients with valid IP addresses.

Once a user connects to the Evil-twin, their traffic is exposed to the adversary, who may launch several attacks such as interception, replaying, and traffic manipulation. This can also occur if encryption such as SSL is employed in the users device. The attacker can act as the Man-in-the-Middle using his AP [22]. To do so, the attacker can easily use tools such as SSLstrip[2] to decrypt the traffic and BurpProxy[3] to generate fake certificates. Because users trust their encryption method, most will accept the faked certificates [27, 28]. Therefore, Evil-twin APs can launch MITM attacks and decrypt encrypted traffic, modify this traffic, and hijack sessions. Evil-twin attacks are very dangerous because of their simplicity. Any mobile operating system such as iOS or Android can be used to create an Evil-twin. Thus, creating this attack using a smartphone does not necessarily attract

[1] A tool for attacking users and APs.

[2] An SSL stripping tool.

[3] An interception tool targeting web applications.

attention. Furthermore, easy-to-use tools such as airbase-ng and rfakeap[4] are readily available to help launch the attack.

The second form of Evil-twin attack replaces the legitimate AP, and uses the same Internet connection that the legitimate AP had been using. This type of Evil-twin is harder to detect than the first type, because it clones almost all of the characteristics of the legitimate AP. Additionally, timing approaches that depend on delay (see Sect. 4) cannot detect this type of Evil-twin.

1.2.2 Improperly Configured AP

This type of RAP is not placed by an adversary: it exists in WLANs because the AP is improperly configured. There are numerous situations where the AP can be misconfigured. An administrator who does not have a sufficient security background may choose insufficiently robust authentication or encryption settings. Another example occurs when the AP driver malfunctions or the whole device is worn out. In addition, the AP may become vulnerable after a software update (e.g., firmware with encryption enabled using WPA-PSK or WEP might cause the AP to resume without encryption) [5, 29]. This can open a backdoor to bypass the organizations authentication, allowing unauthorized users to share network resources. This is a hardware-based RAP that is plugged into a switch or router, and there is no malicious intent behind its existence.

1.2.3 Unauthorized AP

This type of RAP is installed by an employee or naive user without the network administrators permission. Although, this AP is not installed by the network administrator, it is considered part of the actual WLAN because it is connected to the wired side of the network, like the legitimate APs. Thus, the unauthorized AP receives and sends wireless traffic from the wireless users to the wired side of the network and vice versa. This RAP can be set up for purposes of convenience, especially in large organizations, to allow employees to gain access to network resources. Unauthorized APs can also be set up maliciously to create vulnerabilities in an organizations security, enabling outsiders to exploit these weaknesses. Thus, unauthorized users who use these RAPs share the medium with authorized users, eavesdrop the authorized users traffic, and launch attacks against the network resources [5, 29]. This is another hardware-based RAP.

1.2.4 Compromised AP

Security methods such as WPA-PSK and WEP use shared keys to secure the communication between the APs and the wireless users. If an adversary obtains the shared keys used by the APs, the AP becomes rogue [5, 29], allowing hackers to launch attacks and gain access to sensitive information. Hackers with no security background can use simple hacking software; Linux-based operating systems such as BackTrack[5] or Kali[6] provide multiple tools for hackers to crack the shared keys, such as Aircrack-ng.[7]

[4] A tool that sets up a fake AP.

[5] Linux-based distribution for ethical hacking.

[6] Another Linux distribution for ethical hacking and security auditing.

[7] A tool for cracking WEP and WPA-PSK keys.

1.2.5 RAP-Based Deauthentication/Disassociation

This survey focuses on the deauthentication/disassociation attacks that are launched by RAPs to target wireless users. The IEEE 802.11 standard states that deauthentication frames are a notification that cannot be rejected by the receiving wireless client. Thus, the hacker can masquerade as a legitimate AP, and send deauthentication frames on behalf of the AP to the wireless clients to terminate the connection. The attacker can launch a huge number of deauthentication frames to prevent the wireless users from maintaining their connection with the real AP or vice versa. There are three ways that a hacker can launch a deauthentication/disassociation attack:

1. The attacker can create forged deauthentication/disassociation frames on behalf of a connected user, and send the frames to the AP. When the AP receives these frames, it assumes that they were sent by a legitimate user who wants to disconnect from the WLAN. Hence, the AP disconnects the user. This type of attack is beyond the scope of this survey.
2. The attacker can generate forged deauthentication/disassociation frames on behalf of the AP, and send them to a single WLAN user. Once the frame is received, the user disconnects from the WLAN.
3. The attacker can forge deauthentication/disassociation frames on behalf of the AP, and send them to all connected users using the broadcast MAC address as a destination address. This attack is severe, because all associated WLAN users are disconnected when they receive the deauthentication/disassociation frame.

1.2.6 Forged First Message in a Four-Way Handshake

The purpose of the four-way handshake messages is to verify that the station is in possession of the pre-shared key. For simplicity, we now explain the four-way handshake in WPA2-PSK; this is similar to that in enterprise mode. The PSK in WPA-personal is also known as the PMK. The PTK is derived from PMK, and is installed into the MAC layer [30].

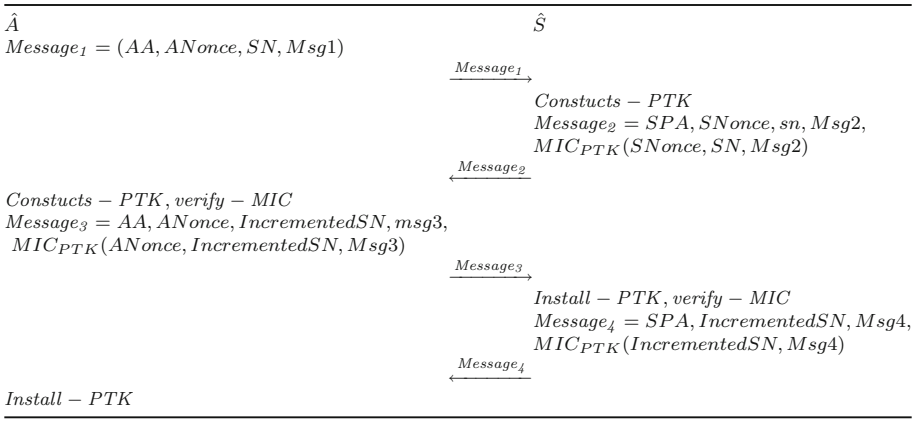

Fig. 3 Four-way handshake message exchange

The PTK is split into three keys. The first is known as the Key Confirmation Key (KCK), which is used to verify MIC during the four-way handshake. The other two keys (the Key Encryption Key (KEK) and Temporal Key (TK)) are created after the four-way handshake [16, 31], as shown in Fig. 3. Before sending the first message, the authenticator generates a nonce (known as ANonce, generated randomly by the AP) and sends it to the supplicant along with its MAC address, known as AA, the sequence number(sn) to prevent replay attacks, and the message number (i.e., in this case msg1). The supplicant generates a random number known as the SNonce, and has the ANonce and the PMK (i.e., entered by the wireless user when choosing the preferred AP from the AP list). Thus, the supplicant can construct the PTK. In the second message, the supplicant sends its own nonce, MAC address, sn, and message number (i.e., msg2) to the authenticator along with the related hash value (i.e., hashed using MIC), which are generated using the PTK that just has been computed at the supplicant device. The authenticator now has the three important components needed to compute the PTK, namely the ANonce, SNonce, and PMK (i.e., entered initially at the AP captive portal). Prior to sending the third message, the authenticator computes the PTK, verifies MIC, and sends a message including the hash values of ANonce, sn+1, and msg3 along with AA, ANonce, sn+1, and msg3 to the supplicant. The supplicant verifies their receipt by sending a confirmation to the authenticator using the same procedure.

The adversary can mimic the authenticator and transmit a forged first message to the supplicant. This occurs just after the second message has been sent by the supplicant, as the first message is not encrypted (see Fig. 3). The supplicant then generates a new PTK corresponding to the new nonces that have been generated according to the new received message. Thus, this vulnerability blocks the subsequent handshakes because of inconsistencies in the PTK at the authenticator and the supplicant. Smart attackers can determine the perfect time to send the forged first message by sniffing WLAN traffic, or may simply flood the WLAN with messages, causing a DoS [32, 33].

2 Classification of Existing Solutions

Existing countermeasures can be classified based on whether the technique protects against one or more RAPs, whether the technique is passive or active, and whether it requires protocol modification or special hardware. The following categories are identified to classify the existing countermeasures:

Operator versus Client-side In the operator option, the IDS is implemented on an AP or a router, and the AP tasks are divided between serving the traffic of the wireless users and detecting intrusions. The client-side option focuses on detecting RAPs. There are some challenges to developing a detection system on the client machine, such as:

1. Clients might be limited by the network settings or have fewer privileges than operators.
2. It is difficult for clients to gather WLAN traffic at the network gateway without the operators assistance.
3. Similarly, it is difficult for clients to have dedicated servers with which to detect RAPs.

Passive versus Active Passive methods simply observe RAPs through wireless traffic, whereas active approaches send test packets to the APs to examine how they react. The biggest problem with detecting RAPs is that they do not reply to active probing. This

absence of collaboration has led to passive detection becoming the more popular technique.

Techniques that require special hardware Some techniques require special hardware to perform detection methods, whereas others can simply use smartphones or laptops to perform the task.

Techniques that require protocol modification Some techniques require standards or protocols implemented by the APs to be modified or changed, either by adding more cryptography methods or additional identifiers.

Wireless versus Wired Wireless approaches detect the RAPs using wireless traffic only, whereas wired techniques detect the RAPs by analyzing the wireless traffic that has been relayed by the router/switch at the network backbone on the wired side. Hybrid approaches combine both wired and wireless approaches. Hackers can use various methods to evade the detection methods on the wired side of the network:

1. *The RAP can be hidden behind a legitimate AP*: As hotels, airports, universities, and other public WLANs have legitimate APs to which a hacker could connect, the hacker can provide access to friends or outsiders by connecting unauthorized APs to the legitimate AP. Several wired-side detection methods depend on the usage policy of the switch port; these methods detect the legitimate wireless traffic, and cannot detect an RAP connected to a legitimate AP.
2. *Modifying the pattern of the transmission*: Because wired-side detection methods depend on DCF statistics using wireless traffic, hackers can modify their traffic using traffic shaping methods to either add delay or reduce the delay to emulate wired traffic. Thus, an adversary that knows the Ethernet and WLAN speeds can add delay at the application layer to emulate wired-side traffic when the WLAN side is faster than the wired side, and vice versa.

Wireless approaches suffer from expensive sensor deployment. Hybrid techniques are generally good, but hackers can evade the hybrid methods through the wired side.

Techniques that detect all or some RAPs Most techniques focus on Evil-twin detection and indirectly detect RAP-based deauthentication/disassociation attacks. Some techniques detect Unauthorized APs, but the detection of Compromised APs is rare. There is no single technique that detects all RAP types.

The ideal method is one that can detect all RAP types, is passive, does not require protocol modification, and does not require specialized hardware (see Sect. 5). All existing techniques have one or more of these features, but none of them has all four. In the next two sections, the RAP prevention and detection methods are comprehensively surveyed to identify risks and clarify the restrictions of state-of-the-art detection approaches.

3 Available Security Countermeasures

In this section, we explain why available security countermeasures cannot protect against all RAP types. Some countermeasures are designed for WLANs, whereas the rest are adopted from the wired world. This section introduces the most widely used protocols in WLANs to help protect against rogue devices in general, and RAPs specifically.

WEP was developed to encrypt the data transmitted on WLANs. The encryption process in WEP starts by combining the 24-bit IV and the secret key that indicates the encryption/decryption key. In addition, the resulting key is used to produce the key sequence. Furthermore, the plaintext message and the ICV are XORed with the key sequence to produce

the cipher text. In the final step, the IV and the cipher text are concatenated. The reverse of the encryption process is the decryption process. There are two characteristic weaknesses with WEP: the IV is frequently reused, and the WEP secret key is not changed often enough. Hence, it is difficult to ensure the existence of two different key streams. Additionally, it is not difficult to attack WEP because it is possible to eavesdrop the IV that is transmitted. Thus, if the sender encrypts two messages using the same IV along with an original message, it is feasible to decrypt the encrypted messages using the XOR operation. The key can then be recovered once the attacker gathers the key streams [34]. Because WEP is not secure, it does not protect against all RAP types.

PSK is used to encrypt wireless traffic between the wireless user and the legitimate AP. One weakness of PSK is that the protocol does not allow any update or renewal property, so distributing the key in a secure manner is difficult. Some organizations distribute the key on a printed receipt, whereas others use easy-to-guess passwords, so it is easy to intercept the four-way handshake messages and perform a dictionary attack to obtain the key. Thus, network administrators must renew the PSK on the AP manually, and provide the key to all clients that participate in the network. Therefore, this procedure is time consuming and insecure, especially if the administrator chooses an easy-to-guess pass-phrase [35]. This method can protect against Compromised APs and Evil-twins if and only if the network administrator chooses a hard-to-guess password and distributes it in a secure manner.

WPA-Enterprise Mode (802.1x) IEEE 802.1x [36] was designed as an access control method to allow users to connect to the network. It also provides port security to prevent unauthorized access to network resources. IEEE 802.1x has three important components in a given wireless network: the supplicant, i.e., the wireless user that intends to join the wireless network, the authenticator, who is responsible for providing access, and the authentication server, which is responsible for making authentication decisions. IEEE 802.1x uses existing protocols to accomplish its objectives, such as EAP [37, 38] and RADIUS. EAP provides many methods, each having different properties that are suitable for a specific wireless network environment. The system administrator is responsible for choosing which EAP method is used in the wireless network that he/she administrates [39]. EAP uses challenge/response messages. The authenticator is responsible for asking the supplicant to provide more information before deciding which authentication method to use in the link control phase. The EAP authentication process consists of two important elements, requests and type fields. The authentication phase uses either success or failure messages. There are several EAP methods for different network environments, such as EAP-MD5, LEAP, EAP-TLS, EAP-TTLS, PEAP, and EAP-FAST. One of the most secure is EAP-TLS, which uses public key cryptography to provide certificates to the users. EAP-TLS provides certificates to both the client and the server, and supports mutual authentication and dynamic key derivation [40]. This method can protect against Evil-twin and Compromised APs, because it is hard to set up a fake authentication server that is protected by strong cryptographic methods. However, the method has to be set up by the administrator. This is difficult to implement, especially in Wi-Fi hotspots; this difficulty allows Evil-twin APs to continue to exist. Another drawback with this method is that the server certificate validation is optional, which may allow the authentication server to be faked by capturing the four-way handshake messages [41, 42].

Web-based Authentication is sometimes used in colleges, cafes, airports, malls, and hotels. In this type of authentication, the user is first directed to a captive portal that asks for credentials or a disclaimer. For instance, many college WLANs use software authentication systems to authenticate students or faculty members on the network. The systems belong to different vendors—either free systems or priority systems—so they are not

compatible with one another. In addition, authentication is not related to the network topology, so there is no knowledge of the networks structure. Thus, broadcasts that are sent over WLANs, such as DHCP broadcasts, could be leaked from DHCP requests prior to the authentication of a specific user on the network. This would enable an intruder to break into the network using DHCP requests. The authentication software employed in some colleges uses open WLAN, and the authentication procedure can be done using HTTP. A login webpage is used to force the user to enter their username and password to authenticate their identity. The authentication process depends on the firewall to redirect the HTTP requests to the login webpage and block all other requests. Once the user has provided the correct credentials, they are authenticated and authorized to access the network resources [43]. The problem with the open nature of WLANs and web-based authentication is that broadcasts such as DHCP frames can be seen by anyone in the network, even if they are not authenticated on the network or authorized to access the network resources. The broadcast frames can be seen by unauthorized users using tools such as Wireshark[8] or tcpdump[9]. This method cannot protect against all RAPs, because it is easy to clone the login webpage and capture users credentials using tools such as Airsnarf[10]. This method does not provide mutual authentication, whereby the user and the access point authenticate each other; it can authenticate the user, but not vice versa.

VPNs are used to connect to the Internet securely from unsecure environments. To implement a VPN, a tunnel is created over the IP. For example, OpenVPN is open-source software that uses SSL [44]. This method cannot protect against all types of RAP, because the security of VPNs is not satisfactory, especially for portable devices. There are several unsolved attacks that target SSL, such as certificate-based attacks. Thus, it is likely that the VPN session will be aborted because of sinking management packets, forcing the connection to return to the unsecure environment.

IEEE 802.11w amendment protects the management and control frames once the session key has been established after the key management exchange. Because the deauthentication and disassociation processes are protected, it is unfeasible to forge the deauthentication/disassociation frames. However, there are some issues regarding the deployment of this standard. Problems with upgrading the firmware and hardware mean that millions of WLAN devices must be changed to become compatible, so most WLANs do not currently implement the 802.11w standard.

4 Classification of Existing RAP Detection Approaches

Because the aforementioned countermeasures do not protect against all RAP types, several novel approaches have been proposed by researchers. Some existing approaches use fingerprint techniques to detect the RAP. A device fingerprint aims to stamp a target device using one or more characteristics via its wireless traffic. Fingerprinting can be used for network monitoring, identification, or IDSs. It is triggered either by actively sending traffic to a target device, or passively observing the traffic generated by the target device [45]. Fingerprinting uniquely identifies devices on a WLAN without using identifiers that can be easily spoofed, such as IP addresses and MAC addresses [46]. Some approaches require

[8] A network protocol analyzer.

[9] A command-line packet analyzer.

[10] A utility to set up RAPs.

standard modification, whereas others solve one type of problem. As most techniques focus on detecting Evil-twin APs, we split this section into six categories, two for Evil-twin AP solutions, one for Unauthorized AP solutions, one for deauthentication/disassociation attacks, and one for solutions that detect more than one RAP type. All forged first message approaches require protocol modifications. We do not consider these here, as this survey is focused on approaches that do not require protocol modifications.

4.1 Coexistence Approaches

This subsection introduces approaches that solve the Evil-twin Coexistence sub-type, as classified in Table 2. This sub-type seeks to insert an RAP into the WLAN simultaneously with the legitimate AP. In [4], a timing-based scheme was presented that detects RAPs that are injected through a Linux-based machine. In the attacking scenario, the RAP can change its identity by masquerading as the legitimate AP by spoofing the legitimate APs MAC address and SSID. The RAP then deceives users into connecting to it by increasing its signal strength, and then launches several attacks on the users machines. The scheme exploits the expected two hops that occur when the user connects to the DNS server.

The authors of [4] used RTT to determine whether or not the given AP is legitimate. The RAP is detected because it relays the traffic to the DNS server via the actual AP. Therefore, the delay results from the two hops that occur between the user and the RAP, instead of the permanent one-hop process. However, the proposed solution needs further investigation, because the authors focused on only one specific cause of the delay in a WLAN. There may be various reasons for such a delay, including (but not limited to) the WLANs exposure to interference and collisions. Thus, this scheme is neither accurate nor robust, especially in highly traffic-loaded WLANs. Additionally, the proposed technique is more likely to detect the hotspots AP as an RAP.

An approach called WiFiHop, in which test packets are actively sent to see if the RAP relays the packets on a different wireless channel, has been proposed [47]. The authors of [48] used SVM to train and validate the precise timing measurements related to the authentication procedure to distinguish fingerprints. This method achieved an accuracy rate of 86 %, but the validation considered only five APs. This technique also requires the use of another device to monitor the authentication sequences.

Kim et al. [49] simulated the launch of an RAP while the attackers device has more than one RSSI. Detection can be achieved using the deviation between the two APs received signal strength. However, this approach depends on the scenario in which the RAP relays traffic to the actual AP, which is not always the case. Bratus et al. [50] used an active behavioral fingerprinting method adopted from TCP/IP fingerprinting. This approach is implemented by network discovery and security auditing tools like Nmap[11], and applies an active request–response technique. This approach sends a request frame, and then waits for the response in order to determine how the devices react to fragmented or manipulated frames. This technique has the drawback of using active detection, which can be avoided by most attackers. In addition, this technique can interfere with regular WLAN traffic.

Nikbakhsh et al. [51] proposed a multi-step approach to detect RAPs. If two APs broadcast the same SSID and MAC address, the approach checks whether the IP addresses are the same, then compares the trace routes. It is unlikely that the same trace route will be found, because having the same IP addresses at the same time would cause an IP address conflict. Thus, the only possible situation is to have the same IP addresses and different

[11] Free security scanner for network exploration and hacking.

Table 2 Coexistence techniques

Technique	Source	Year	Accuracy	Passive/ active	No Protocol modification	Wire D/wire less/hybrid	Dedicated/ bundled	No special hardware	Dataset size
DNS server two hops	[4, 26]	2009, 2011	60 %	A	✔	L	D	✔	2
ETsniffer	[24, 25]	2010, 2012	TPR = 99 %, FPR = 1 %	A	✔	L	D	✔	NA
WiFihop	[47]	2011	TPR[a] = 98 %, FPR[b] = 0.1 %	A	✔	L	D	✔	NA
Authentication + SVM	[48]	2006	86 %	A	✔	L	D	✔	5
Duplicate RSSI	[49]	2012	97 %	P	✔	L	D	✔	NA
Active behavioral	[50]	2008	NA	A	✔	L	D	✔	5
Client-side	[51]	2012	NA	P	✔	D	D	✔	NA
Cipher types	[53]	2012	NA	P	✔	L	D	✔	NA
RAPiD	[55]	2010	NA	P	✔	D	D	✔	NA
Time Interval	[56]	2014	NA	P	✔	L	D	✔	2

[a] True Positive Rate

[b] False Positive Rate

trace routes, which is a result of IP spoofing. This approach cannot deal with such a condition, as it cannot determine which AP is authorized and which is unauthorized.

A second possibility is that there are different IP addresses. The method proposed by Nikbakhsh et al. then calculates the network IDs using different IP classes to compare the IP addresses. If the method finds that the network IDs are identical, the APs are definitely in the same WLAN, which is considered a result of load balancing in the WLAN. In this situation, large organizations use more than one AP to cover the whole WLAN. Thus, the IP addresses of the APs are different, but the network IDs are similar, so the proposed solution marks this situation as safe. Another possibility is that there are different network IDs and different IP addresses. In this case, the approach triggers the trace route for both APs to determine whether there is an extra hop, which would signify that the Evil-twin AP relays packets to the legitimate AP. The last possibility is that network IDs, IP addresses, and routes are different. In this situation, the attacker uses his AP to broadcast the same SSID as the legitimate AP. This situation cannot be handled by this approach, as it cannot determine which AP is legitimate. That is, the approach of Nikbakhsh et al. cannot protect against the Replacement sub-type, as it only detects the Evil-twins that relay packets to a legitimate AP.

Chumchu et al. [52] used the data rates and modulation types to differentiate between legitimate and rogue wireless devices. Important information from PLCP metadata is extracted to detect the rogue devices. The data rates and modulation types rely on a rate adaption algorithm, and are difficult to spoof because they belong to the physical layer. The problem with this approach is that it is limited to the small number of modulation types and data rates that can be used by the 802.11 standards. There is a high probability that hackers will use similar data rates and modulation types as one or more of the genuine wireless devices in the WLAN.

Chae et al. [53] used the authentication and cipher types of the AP to detect RAPs. Their method stores information on the authorized APs, such as SSID, authentication type, and cipher type, in a database. It then sniffs the beacon frames and compares the parameters with those in the database. If the information does not match that of the authorized APs, an alert is triggered. This approach is designed to be implemented on the client side for protection in airports or malls. However, it is not practical, because all Wi-Fi hotspots in airports and shopping malls are restricted to open authentication (i.e., no other authentication types are used in hotspots) and have only one cipher type.

Szongott et al. [54] combined parameters such as SSID, BSSID, supported authentication, key management, and encryption schemes to detect mobile Evil-twin APs. They also used cell tower information as an environment identifier. Finally, they used the location of the device, as determined by the Google Play services API or through Androids location API. If the user selects a WLAN that is not in the database, no warning message is needed. If the SSID is known, but the BSSID of this AP is not in the database, a warning message is triggered. In this situation, the user has two options. If the user trusts the AP, a profile of this AP is created in the database; otherwise, the connection process is dropped and no information is stored. The other parameters are used to determine the location of the mobile Evil-twin AP. This approach is similar to TOFU, a method used in contexts such as SSH that depend mainly on the user. This method can only detect mobile Evil-twin attacks. It cannot detect Evil-twin APs that share the Internet with existing legitimate APs, and cannot locate other devices such as laptops or iPhones, because it depends on applications that are related to Android.

Qu et al. [55] proposed an indirect RAP detection approach, known as RAPiD, which uses the Local Round Trip Time (LRTT) of TCP packets to measure the delay. This

approach is similar to several other approaches that assume any delay is a sign of RAPs. However, WLANs have two other main reasons for the delay: interference and collision. Kao et al. [56] proposed an approach based on the beacon time interval deviation. The approach takes advantage of the fact that the AP sends a beacon frame approximately every 100 ms, and the time interval between two consecutive beacon frames can be measured to identify suspicious activity. However, it is difficult to predict the time interval between two consecutive beacon frames. Additionally, this approach does not scale in real-life scenarios, because 802.11b, 802.11g, and 802.11n WLAN devices interfere with one another and Bluetooth and microwave ovens cause more interference and collisions in the frequency band. Collecting information from distributed sensors in large organizations would also be a problem, as the time interval would be different from sensor to sensor based on the distance to the AP.

4.2 Approaches that Handle all Evil-twin Sub-types

An overview of the approaches that solve both the coexistence and replacement Evil-twin sub-types is presented in Table 3. The authors of [57] combined ISP-based detection and timing-based detection to detect Evil-twin APs. A hotspots AP must have a gateway with a global IP address to provide Internet to wireless users. A block of IP addresses is given to the ISP by IANA[12], so the ISP provides a unique global IP address to customers who subscribe to this service. Information in each global IP address, such as the name of the organization, location, and assignment date, is publicly available on various websites. The proposed approach sends a request to one of these servers, and waits for the reply to obtain important information such as the source address of the AP, ISP information, and location. It was found that the hotspot APs that are connected to the same router share the same global IP address or the same ISP. The authors used the information obtained from the public servers to distinguish legitimate APs from Evil-twin APs. ISP-based detection cannot identify Evil-twin APs that share an Internet connection with one of the legitimate APs, as the Evil-twin AP uses the same Internet service, which cannot be differentiated from that of the legitimate AP. Thus, the authors developed another detection method called timing-based detection to detect Evil-twin APs that share the Internet with one legitimate AP. This approach uses active probing, which can add traffic to WLANs.

The work in [58–60] requires the modification of 802.11 standards or protocols. The authors of [58] introduced a protocol entitled “Secure Open Wireless Access, which adopts the well-known SSL protocol to distribute certificates. The SSID of a given access point is considered a unique string, and is associated with a certificate by a trusted CA. The association between the certificate and the unique string can be used to authenticate the AP operator. The authors of [59, 60] proposed an EAP-based authentication method, referred to as the Simple Wireless Authentication Technique (EAP-SWAT). This utilizes the SSH’s trust-on-first-use approach, whereby trust is certified for the first connection to the AP. Subsequent connections to the AP are ensured to be authenticated by the coexistence of the certificates. For deployment reasons, techniques that require standard or protocol modifications are not ideal solutions. It is impossible to deploy the protocols in [58–60] because it is difficult to change the drivers and firmware of the supplicants and APs.

Some researchers have focused on hardware fingerprinting to detect RAPs based on the characteristics that uniquely identify the WLAN device. The authors of [61, 62] proposed a clock skewing approach that extracts the TSF timestamp from beacon frames. In addition,

[12] The authority in charge of managing global IP addresses.

Table 3 All Evil-twin techniques

Technique	Source	Year	Accuracy	Passive/ active	No protocol modification	Wire D/WireLess/ Hybrid	Dedicated/ bundled	No special hardware	Dataset size
CETAD	[57]	2014	95 %[a]	A	✔	D	D	✔	3
SOWA	[58]	2011	NA	A		H	B		NA
EAP SWAT	[59, 60]	2008, 2010	NA	A		H	B		NA
Clock Skew	[61]	2010	90 %	P	✔	L	D	✔	41
Clock skew	[62]	2010	NA	P	✔	L	D	✔	2
Clock skew	[22]	2014	NA	P	✔	L	D	✔	388
Clock skew + temp	[63]	2014	TPR = 90 %, FPR = 10 %	P	✔	L	D	✔	12
Adjacent channel	[64]	2015	NA	A	✔	L	D	✔	60
Probe Request stimuli	[64]	2015	NA	A	✔	L	D	✔	60
Radio frequency	[65, 66]	2006, 2012	99 %	P	✔	L	D		130

[a] For timing-based approach, the average of two results 98 and 92 % is calculated to fit into our classification

the authors compared the beacon frame timestamp generated at the AP with the inter-arrival time of the frame at the user station. This technique is not robust because of variations in the WLAN medium that are susceptible to delay, especially in high-traffic WLANs.

The authors of [22, 63] applied the time skew method using TSF to differentiate between hardware- and the software-based APs. They only detect RAPs that are generated from airbase-ng-based RAP tools, and cannot detect RAPs that are generated by other tools. The authors of [64] used a method called active probing on adjacent channels, which, as the name implies, is an active technique. IEEE 802.11 g/n and some other existing technologies such as Bluetooth operate in the 2.4 GHz band for compatibility purposes. The protocols require channel separation of 16.25–22 MHz, but the problem is that the channel center frequencies can only be separated by 5 MHz, which causes adjacent channels to overlap. It is impossible for WLAN devices to receive a single frame that is not sent on the same operational channel on which this WLAN device operates. It was found that software-based APs treat these frames in a different way to hardware-based APs. Several probe requests were sent on the operating channel and adjacent channels of 30 hardware-based APs and several software-based APs to examine how probe request frames were treated. It was noticed that hardware-based APs send probe responses on the same operational channel, whereas software-based APs respond to both the operational channel and the adjacent channel.

The authors of [64] proposed another approach called Malformed Probe Request Stimuli. The Address 1 field is set to contain the destination MAC address (i.e., the MAC address or broadcast address of the AP). The Address 3 field is always set to the BSSID; therefore, it is only relevant to IBSSs such as ad hoc or mesh networks. Because the protocol in infrastructure mode states that the BSSID is the APs MAC address, the AP that receives a probe request should reply to Addresses 1 and 3, which includes the MAC address of the AP. However, the authors noticed that hardware-based APs do not check the Address 3 field of the probe request, unlike numerous software-based APs. This looks reasonable, because APs are designed to be in infrastructure mode and are not part of an IBSS or mesh network. These two approaches have similar drawbacks to other active probing techniques, namely the sharing of bandwidth with the WLAN devices, which causes interference and delay.

Wei et al. [65, 66] used ACK-pairs to distinguish whether traffic was being generated from the wired or wireless side. The authors used an algorithm known as iterative Bayesian inference to acquire a maximum likelihood approximation. Although this approach is effective, it cannot be deployed in real time, because it takes time to converge.

4.3 Unauthorized AP Countermeasures

A number of approaches focus on protecting against APs that have been inserted by insiders, as shown in Table 4. The authors of [67] proposed an active approach to the detection of unauthorized APs. Their approach has a verifier that is placed on the wired side of the network. This verifier sends test packets to the wireless side of the network. The APs that relay those test packets are detected as RAPs because they are on the wired side of the network and allow the relay of packets to the wireless side. Once an RAP has been detected, its IP address is returned to allow the network administrator to locate the RAP. The verifier was used to monitor the wired side of the network to avoid NAT private IP address problems. The verifier can monitor the active users on the wired side and send test packets to them. If a user who receives this packet is an AP, the packet is forwarded to the

Table 4 Unauthorized AP techniques

Technique	Source	Year	Passive/ active	No protocol modification	Wire D/wireless/ hybrid	Dedicated/ bundled	No special hardware
Unauthorized approach	[67]	2009	A	✔	D	D	✔
Shadow Honeypot	[11]	2015	P	✔	L	D	✔
Inter-packet Spacing	[68]	2004	P	✔	D	B	✔
RIPPS	[69]	2008	P	✔	D	B	✔
RTT approach	[70]	2007	P	✔	D	B	✔
Agent-based	[71]	2003	P	✔	L	D	✔

wireless side. If the AP uses the WPA or WEP mechanisms, the sniffer on the wireless side cannot reveal the payload of the sent packets. Thus, the authors used the sequence of predefined packet sizes, and employed an active technique to send test packets, although this added an overhead to the shared network medium.

The Shadow Honeypot approach [11] consists of three components: a filtering engine, anomaly detection sensors, and shadow honeypot code. The filtering engine is the first line of protection, responsible for purifying unauthorized wireless traces based on an authenticated list. The authenticated list contains the authorized AP MAC addresses. Any traffic sent from source MAC addresses other than the authorized ones is assumed to originate from an RAP. Traffic from authenticated users is bypassed by the detection engine. The traffic that goes through the detection engine is passed to the anomaly detection sensors, which examine the characteristics of the packets and pass legitimate packets to the shadow honeypot stage. The shadow honeypot stage uses popular signatures of worms and attacks and compares them with the network trace. This approach is not very accurate, and is not automated. The authors used different tools to analyze network traffic, an inefficient and time-consuming process. For instance, in the anomaly detection sensor stage, tools such as Wireshark and Ettercap[13] are needed to analyze the network trace and detect RAPs. Additionally, RAPs that have spoofed the MAC address of a legitimate AP have a high probability of passing the other two stages, especially if they send frames that cause a DoS attack. These frames have similar characteristics, and can bypass all of the anomaly detector sensors.

Beyah et al. [68] used the inter-packet spacing to determine whether traffic had been generated from a wired or wireless link. This approach is passive, so it does not add traffic to the WLAN, and can distinguish between wired and wireless traffic. It does not require protocol modification. This approach has a vital drawback, as inter-packet spacing can also be a load on a switch, which might cause this approach to be inaccurate. As the number of switches increase, the accuracy may become an issue. The authors of [69, 70] proposed using the RTT to distinguish between wired and wireless links. The RTT is the time that the TCP/IP session packet pair takes to travel from the router to the host.

An agent based approach has been proposed [71] whereby an agent equipped with a wireless card sniffs wireless frames and returns a packet to the analyzing engine containing information about new APs. The analyzing engine has an authorized list of legitimate APs, so the information corresponding to new APs is checked against the authorized APs to

[13] A comprehensive suite for MITM attacks.

determine suspicious nodes. This type of approach depends completely on the MAC addresses of the APs, which can easily be spoofed.

4.4 Deauthentication/Disassociation Countermeasures

The security standard of 802.11 series WLAN is IEEE 802.11i [72]. This was ratified in 2004, and provides data confidentiality, integrity, and mutual authentication in the MAC layer. It uses 802.1x for authentication and access control, and a four-way handshake for key management and distribution. However, there are some weaknesses in WLANs related to the fact that the management and control frames are unprotected. DoS attacks in WLANs can mainly be classified as deauthentication/disassociation attacks [73, 74] or four-way handshake memory/CPU DoS attacks [75].

The deauthentication and disassociation frames are management frames [76]. They can easily be forged by an adversary if IEEE 802.11w is not implemented, because management frames are not protected. An adversary can spoof the MAC address of a legitimate user, either a supplicant or an authenticator, and send either deauthentication or disassociation packets on behalf of that user to disassociate or deauthenticate the victim. More harmful attacks can be launched by broadcasting these frames on behalf of the authenticator to all the supplicants in the WLAN by setting the destination MAC address to the broadcast address [76, 77]. Thus, one deauthentication/disassociation frame disconnects all of the supplicants on the WLAN.

Table 5 lists several approaches to detect deauthentication and disassociation attacks launched by wireless users or the AP. Bellardo et al. [78] applied authentication to all of the management frames by modifying the authentication framework. This might help prevent the deauthentication attacks, but it necessitates an upgrade to the AP and WLAN users firmware. Authenticating each management frame acquires supplementary cost for the AP and the users, consuming the power resources of portable devices. The authors also proposed a delay to the deauthentication effect. If a deauthentication frame followed by a data frame is received from a victim, the deauthentication frame is discarded. However, delaying the management frames generates problems related to roaming.

Sequence number approaches [79–83] detect MAC address spoofing attacks, such as deauthentication attacks. These approaches assume that the legitimate wireless user generates a sequence of numbers, so it is hard for an adversary to manipulate the sequence to match the legitimate one. Because the sequence number counters at the legitimate wireless device are different from those of the adversary, a sequence number gap from the same MAC address confirms that spoofing is occurring. However, the detection systems can be traversed by injecting deauthentication frames after the sent frames from a specific user or AP. This can be done using an open-source driver or reverse engineering firmware, enabling adversaries to manipulate the sequence numbers on a per-frame basis. Additionally, some frames sent by certain wireless cards do not have any sequence numbers, which makes sequence number approaches inaccurate.

RSSI approaches [84–88] can be used to differentiate WLAN devices based on their location. The RSSI is the signal power of the frame, measured at the receiving wireless device. A number of factors play an integral role in measuring the RSSI, such as the transmission power, multi-path and absorption effects, and the distance between the two communicating parties. A wireless device does not ordinarily increase or decrease its transmission power, and so obvious changes in RSSI from the same MAC address are an indicator of MAC address spoofing. Because the distance between the adversary and the legitimate wireless device is significant, an adversary is more likely to be detected. One

Table 5 Deauthentication and disassociation techniques

Technique	Source	Year	Accuracy	Passive/ active	No protocol modification	Wire D/wireless/ Hybrid	Dedicated/ bundled	No special hardware
Sequence number	[79–81]	2004, 2005, 2006	FNR[a] = 0.029 %–0.036 %[b]	P	✔	L	D	✔
Sequence number	[82]	2003	NA	P	✔	L	D	✔
ANFIS	[83]	2010	FAR[c] = 0.00015	P	✔	L	D	✔
Signalprints	[84]	2006	95.6 %	P	✔	L	B	✔
SSFA	[85]	2006	NA	P	✔	L	D	✔
K-means	[86, 87]	2007, 2010	FPR = 0.0351 to 0.0957	P	✔	L	D	✔
GMM	[88]	2008	TPR = 98 %, FPR = 1 %	P	✔	L	D	✔
throughput + flood	[89]	2013	93 %–99 %[d]	P	✔	L	D	✔
Machine learning	[90]	2014	68 %–99 %[e]	P	✔	L	D	✔
Lightweight solution	[91]	2008	NA	A		H	B	

[a] False Negative Rate

[b] Based on the location of the monitor node

[c] False Alert Rate

[d] Based on the threshold value, as the threshold increases the accuracy increases

[e] Based on the used classifier

problem with these approaches is that a smart adversary will increase the transmission power to mimic the legitimate wireless device. Another problem is that it is hard to detect the attack, especially if the adversary is in close proximity to the legitimate wireless device.

The authors of [89, 90] assumed that deauthentication causes some degradation in throughput. Thus, they count the number of frames sent by a certain wireless client, and set a threshold value to detect an attack. Although this assumption might be true, it has some drawbacks. First, it is impossible to detect a single deauthentication attack. An attacker can do many disruptive things with only one frame, such as discovering hidden SSIDs or cracking WEP/WPA-PSK methods. Second, a legitimate wireless station may be marked as an attacker simply because it sends two or more frames, as some devices are designed to send more than one frame to leave a WLAN. Nguyen et al. [91] suggested that the AP and WLAN users employ a secret key to authenticate the deauthentication frames. However, this technique would require the firmware of the drivers and devices to be modified.

4.5 Countermeasures that Solve Multiple Attack Types

The approaches listed in Table 6 can protect against multiple RAP types. In [5, 29], a hybrid approach was proposed that works on the wired and wireless sides of the network. This approach includes several centralized and distributed tasks. A frame collector is used to capture frames and filter anomalies, allowing Evil-twin, Unauthorized, and Compromised RAPs to be detected. This approach has two main drawbacks: it uses active probing, and must be bundled with the router or the switch. It is difficult for the router or the switch to divide its work between serving the wireless users by carrying traffic and acting as an IDS.

Companies such as Air-Magnet [92] use wireless sniffing solutions. Sensors are deployed across the whole diameter of the network to gather physical and data link layer information, enabling RAPs to be detected in a distributed agent–server architecture [92, 93]. The collected information contains RF measurements, MAC addresses, signal strengths, and AP control frames. This approach is very expensive, because the analyzer system provided by Air-Magnet costs $3,000 [12, 92].

Vanjale et al. [94] proposed using the SSID, MAC address, and RSSI to detect RAPs. The authors created a profile containing these three parameters for each legitimate AP. This technique first checks the AP SSIDs. If it finds any duplication, then it considers the MAC addresses of the duplicate APs. If both are the same, this is considered a legitimate AP. If different MAC addresses are found, the RSSI is checked. If the difference in RSSIs is less than 10 dB, then the technique considers this AP legitimate. This approach is passive and does not require protocols or standard modifications, but it has some drawbacks. The first is that, in reality, it cannot detect Evil-twin APs, because these RAPs can mimic the same SSID and MAC address as one of the legitimate APs. This approach assumes that APs with the same SSID and MAC address are genuine; however, this assumption is misleading. A second drawback is that this approach detects a hotspots APs as RAPs, as they have the same SSID but different MAC addresses.

Sriram et al. [95] proposed a multi-agent solution that can detect Evil-twin and Unauthorized RAPs. This approach has two important components, namely a master agent and a slave agent. The master agent is used to regulate the authorization processes of the WLAN, while the slave agent is used by the master agent to identify active APs in the WLAN. The slave agent is connected to an AP to obtain important information such as SSID, vendor name, MAC address, and channel number. This information is sent to the

Table 6 Techniques that protect against multiple RAP types

Technique	Source	Year	Passive/ active	No protocol modification	Wire D/wireless/ hybrid	Dedicated/ bundled	No special hardware	Detect evil-twin, unauthorized, compromised
RAP	[5, 29]	2007, 2008	A	✔	H	B	✔	E, U, and C
Elimination	[94]	2014	P	✔	L	D	✔	E and U
Multi-agent	[95]	2010	P	✔	L	D	✔	E and U
DWSA	[96]	2004	A	✔	L	D	✔	E and U

master agent and compared with information on an authorized list. However, this approach depends on parameters that can be easily spoofed by many Evil-twin tools. Such approaches use an agent equipped with a wireless card to sniff wireless frames and return a packet containing information about new APs to the master agent. The master agent has an authorized list of legitimate APs, and checks the new AP against the authorized APs to determine suspicious nodes. This type of approach is heavily dependent on the AP MAC addresses, which are easy to spoof.

In [96], a Distributed Wireless Security Auditor (DWSA) was proposed. This approach uses both Linux and Windows-based implementations to provide network administrators with continuous wireless assessments. It also uses trusted wireless clients as distributed sensors to find anomalies throughout the WLAN. DWSA provides periodic security reports, and detects and locates RAPs using 3D trilateration. This approach can detect Evil-twins and Unauthorized RAPs.

Companies such as NetStumbler [97] use wireless packet analyzers on laptops or hand-held devices to detect RAPs. That is, IT personnel physically walk through the halls of an organization or university to search for RAPs. This technique is time-consuming and ineffective, because the scan is performed manually. Additionally, IT employees should upgrade the detection devices to be able to work on different frequencies. Furthermore, the scan can be evaded if the hacker simply unplugs the RAP as the detection is taking place.

Various techniques [98–101] use a scan from a central location to achieve enterprise-wide coverage. Several dedicated sensors are distributed with the help of one or more legitimate APs to scan beacon frames from surrounding areas. Information on the surrounding APs is sent to a central unit for further analysis under the prevailing security policy. The problem with these techniques is that each sensor only scans one frequency, and some sensors only cover one channel. Another problem with some techniques is that they detect neighboring APs as RAPs.

5 Road Map and Future Directions

The simplicity of configuring an RAP creates a real security threat to WLAN devices. There are several existing techniques that can detect RAPs, but they are inefficient and often inaccurate. Some techniques require the active addition of traffic to the WLAN, whereas other techniques require protocol modifications. The current techniques have several drawbacks, as listed in Table 7. Early wireless-side solutions detected Evil-twin APs by examining SSID and MAC addresses to differentiate legitimate (authorized) APs and locate the RAPs. The wired-side solutions locate RAPs using switch port mapping, but do not have an integral authorization method as they depend only on switch port policies. Furthermore, it is not possible to detect an RAP that is attached to a legitimate AP. The wired-side solutions must require authorization techniques other than the switch port policies.

The road map in Fig. 4 shows how the detection of RAPs has evolved from manual scanning by walking through halls to automated WIDS. Based on our survey, it is clear that future solutions should have numerous characteristics. A complete solution to the RAP problem should be able to detect all RAP types. A passive approach is preferable, as this will not increase the traffic on the WLAN. In addition, approaches that require protocol modifications or additional special hardware, besides sensors, should be avoided, because deploying modifications can be difficult, supplying new hardware is costly, and implementation may cause incompatibilities. An approach that is implemented on the AP is

Table 7 Strengths and weaknesses of existing techniques

Technique type	Strengths	Weaknesses
Unautomated wireless solutions	Passive	Can be evaded easily
	Minimal infrastructure is needed	Requires considerable effort and time
		Sensors must perform on every channel
Wired-active probing	Does not depend on wireless frequency	Active
		RAP might not respond to packets
		Only depends on switch port policies
Hybrid	Passive	Can be evaded from the wired side
	Can detect most RAP types	
Timing approaches	Passive	Necessitates samples on wired and wireless
	Does not depend on wireless frequency	Assumes wired link faster than wireless
		Could be evaded from insiders
Identification approaches	Passive	Could be evaded from insiders
	Does not depend on wireless frequency	
	No samples from wired and wireless	
	Link speed is not important	

disadvantageous, as it requires the detection task to be shared with the serving of wireless traffic. An ideal approach would allow complete coverage of a WLAN, including all possible channels and frequency bands. For robustness, a suitable approach should not rely on higher-layer protocols such as TCP ACKs, because this will delay detection and is ineffective against deauthentication/disassociation and forged first message attacks, which depend on management frames rather than higher-layer protocols. Finally, a well-built approach should not depend on easily spoofed identifiers such as MAC addresses or IP addresses.

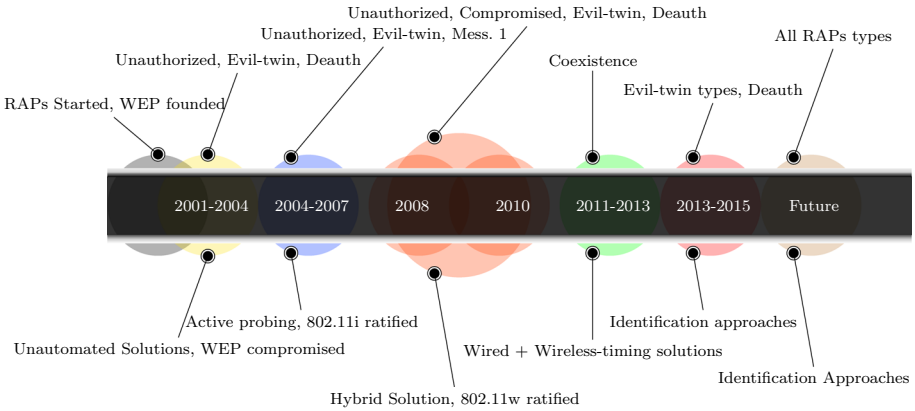

Fig. 4 Timeline of existing techniques

References

1. Wang, C., & Tai, T. (2010). Achieving time-based fairness for VoIP applications in IEEE 802.11 WLAN using a cross-layer approach. In *2010 IEEE 21st international symposium on personal indoor and mobile radio communications (PIMRC)* (pp. 1475–1480). IEEE.
2. Park, M. W., Choi, Y. H., Eom, J. H., & Chung, T. M. (2014). Dangerous Wi-Fi access point: Attacks to benign smartphone applications. *Personal and Ubiquitous Computing*, *18*(6), 1373–1386.
3. Carrano, R. C., Magalhaes, L., Saade, D. C. M., & Albuquerque, C. V. (2011). IEEE 802.11 s multihop MAC: A tutorial. *Communications Surveys & Tutorials, IEEE*, *13*(1), 52–67.
4. Han, H., Sheng, B., Tan, C. C., Li, Q., & Lu, S. (2011). A timing-based scheme for rogue AP detection. *Parallel and Distributed Systems, IEEE Transactions on*, *22*(11), 1912–1925.
5. Ma, L., Teymorian, A. Y., & Cheng, X. (2008). A hybrid rogue access point protection framework for commodity Wi-Fi networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE.
6. Alotaibi, B., & Elleithy, K. (2015). A passive fingerprint technique to detect fake access points. In *Wireless telecommunications symposium (WTS)*. IEEE.
7. Alotaibi, B., & Elleithy, K. (2015). An empirical fingerprint framework to detect Rogue Access Points. In *Systems, applications and technology conference (LISAT), 2015 IEEE Long Island* (pp. 1–7). IEEE.
8. 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* (pp. 365–378). ACM.
9. Yin, H., Chen, G., & Wang, J. (2007). Detecting protected layer-3 rogue APs. In *Broadband communications, networks and systems, 2007. Fourth International Conference on BROADNETS 2007* (pp. 449–458). IEEE.
10. Shetty, S., Song, M., & Ma, L. (2007). Rogue access point detection by analyzing network traffic characteristics. In *Military communications conference, 2007. MILCOM 2007. IEEE* (pp. 1–7). IEEE.
11. Agrawal, N., & Tapaswi, S. (2015). Wireless rogue access point detection using shadow honeynet. *Wireless Personal Communications*, *83*(1), 1–20.
12. Beyah, R., & Venkataraman, A. (2011). Rogue-access-point detection: Challenges, solutions, and future directions. *IEEE Security & Privacy*, *5*, 56–61.
13. Shivaraj, G., Song, M., & Shetty, S. (2008). A hidden Markov model based approach to detect rogue access points. In *Military communications conference, 2008. MILCOM 2008. IEEE* (pp. 1–7). IEEE.
14. Kim, A. S., Kong, H. J., Hong, S. C., Chung, S. H., & Hong, J. W. (2004). A flow-based method for abnormal network traffic detection. In *Network operations and management symposium, 2004. NOMS 2004. IEEE/IFIP* (Vol. 1, pp. 599–612). IEEE.
15. Bicakci, K., & Tavli, B. (2009). Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. *Computer Standards & Interfaces*, *31*(5), 931–941.
16. Li, X., Ma, J., & Shen, Y. (2012). An efficient WLAN initial authentication protocol. In *Proceedings of IEEE global communication conference (Globecom12)*.
17. Willens, S., Rubens, A. C., Rigney, C., & Simpson, W. A. (2000). Remote authentication dial in user service (RADIUS). RFC 2865, Internet Engineering Task Force, June 2000. http://www.ietf.org/rfc/rfc2865.txt?number=2865.
18. El Rifai, M., & Verma, P. K. (2014). An IEEE 802.11 quantum handshake using the three-stage protocol. In *2014 23rd international conference on computer communication and networks (ICCCN)* (pp. 1–6). IEEE.
19. Alipour, H., Al-Nashif, Y., Satam, P., & Hariri, S. (2015). Wireless anomaly detection based on IEEE 802.11 behavior analysis. In *IEEE transactions on information forensics and security*.
20. Alipour, H., Al-Nashif, Y., Satam, P., & Hariri, S. (2013). Wireless anomaly detection based on IEEE 802.11 behavior analysis. In *2013 international conference on computing, networking and communications (ICNC)* (pp. 369–373). IEEE.
21. IEEE Standard for Information Technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Protected Management Frames. IEEE Std. 802.11w-2009, September 2009. IEEE Std 802.11w-2009.
22. Lanze, F., Panchenko, A., Ponce-Alcaide, I., & Engel, T. (2014). Undesired relatives: protection mechanisms against the evil twin attack in IEEE 802.11. In *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks* (pp. 87–94). ACM.
23. Roth, V., Polak, W., Rieffel, E., & Turner, T. (2008). Simple and effective defense against evil twin access points. In *Proceedings of the first ACM conference on wireless network security* (pp. 220–235). ACM.

24. Yang, C., Song, Y., & Gu, G. (2012). Active user-side evil twin access point detection using statistical techniques. *Information Forensics and Security, IEEE Transactions on*, *7*(5), 1638–1651.
25. Song, Y., Yang, C., & Gu, G. (2010). Who is peeping at your passwords at Starbucks? To catch an evil twin access point. In *2010 IEEE/IFIP international conference on dependable systems and networks (DSN)* (pp. 323–332). IEEE.
26. Han, H., Sheng, B., Tan, C. C., Li, Q., & Lu, S. (2009). A measurement based rogue ap detection scheme. In *INFOCOM 2009, IEEE* (pp. 1593–1601). IEEE.
27. Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 581–590). ACM.
28. Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., & Cranor, L. F. (2009). Crying wolf: An empirical study of SSL warning effectiveness. In *USENIX security symposium* (pp. 399–416).
29. Ma, L., Teymorian, A. Y., Cheng, X., & Song, M. (2007). RAP: Protecting commodity wi-fi networks from rogue access points. In *The fourth international conference on heterogeneous networking for quality, reliability, security and robustness & workshops* (p. 21). ACM.
30. Raju, K. K., Vallikumari, V., & Raju, K. V. S. V. N. (2011). Modeling and analysis of IEEE 802.11 i wpa-psk authentication protocol. In *2011 3rd international conference on electronics computer technology (ICECT)* (Vol. 5, pp. 72–76). IEEE.
31. Li, X., Bao, F., Li, S., & Ma, J. (2014). FLAP: An efficient WLAN initial access authentication protocol. *Parallel and Distributed Systems, IEEE Transactions on*, *25*(2), 488–497.
32. He, C. (2005). Analysis of security protocols for wireless networks (Doctoral dissertation, Stanford University).
33. Alabdulatif, A., Ma, X., & Nolle, L. (2013). Analysing and attacking the 4-way handshake of IEEE 802.11 i standard. In *2013 8th International Conference for internet technology and secured transactions (ICITST)* (pp. 382–387). IEEE.
34. Wang, Y., Jin, Z., & Zhao, X. (2010). Practical defense against wep and WPA-PSK attack for WLAN. In *2010 6th international conference on wireless communications networking and mobile computing (WiCOM)* (pp. 1–4). IEEE.
35. Onno, S., Gelloz, R., Heen, O., & Neumann, C. (2012). User-based authentication for wireless home networks. In *2012 IEEE international conference on consumer electronics-Berlin (ICCE-Berlin)* (pp. 218–220). IEEE.
36. IEEE 802.1 Standard Working Group. IEEE standard for local and metropolitan area networks: port-based network access control. IEEE Std, 802.
37. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., & Levkowetz, H. (2004). Extensible authentication protocol (EAP) (No. RFC 3748).
38. Robyns, P., Bonn, B., Quax, P., & Lamotte, W. (2014). Short paper: exploiting WPA2-enterprise vendor implementation weaknesses through challenge response oracles. In *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks* (pp. 189–194). ACM.
39. Fan, C. I., Lin, Y. H., & Hsu, R. H. (2013). Complete EAP method: User efficient and forward secure authentication protocol for IEEE 802.11 wireless LANs. *IEEE Transactions on Parallel and Distributed Systems*, *24*(4), 672–680.
40. Ali, K. M., & Al-Khlifa, A. (2011, July). A Comparative Study of Authentication Methods for Wi-Fi Networks. In *2011 third international conference on computational intelligence, communication systems and networks (CICSyN)* (pp. 190–194). IEEE.
41. Marlinspike, M. M., Hulton, D., & Ray, M. (2012). Defeating PPTP VPNs and WPA2 Enterprise with MS-CHAPv2. *Defcon*.
42. Asokan, N., Niemi, V., & Nyberg, K. (2005). Man-in-the-middle in tunnelled authentication protocols. In *Security Protocols* (pp. 28–41). Springer Berlin Heidelberg.
43. Hassan, A., & Zhang, X. (2011). Bypassing web-based wireless authentication systems. In *Systems, applications and technology conference (LISAT), 2011 IEEE Long Island* (pp. 1–4). IEEE.
44. Pandurang, R. M., & Karia, D. C. (2015). Performance measurement of WEP and WPA2 on WLAN using OpenVPN. In *2015 international conference on nascent technologies in the engineering field (ICNTE)* (pp. 1–4). IEEE.
45. Neumann, C., Heen, O., & Onno, S. (2012). An empirical study of passive 802.11 device fingerprinting. In *2012 32nd international conference on Distributed computing systems workshops (ICDCSW)* (pp. 593–602). IEEE.
46. Radhakrishnan, S. V., Corbett, C., Baca, A., & Beyah, R. (2013). A passive technique for fingerprinting wireless devices with wired-side observations. In *2013 IEEE conference on communications and network security (CNS)* (pp. 305–313). IEEE.
47. Mnica, D., & Ribeiro, C. (2011). Wifihop-mitigating the evil twin attack through multi-hop detection. In *Computer securityESORICS 2011* (pp. 21–39). Springer Berlin Heidelberg.

48. Sieka, B. (2006). Active fingerprinting of 802.11 devices by timing analysis. In *Consumer communications and networking conference, 2006. CCNC 2006. 3rd IEEE* (Vol. 1, pp. 15–19). IEEE.
49. Kim, T., Park, H., Jung, H., & Lee, H. (2012). Online detection of fake access points using received signal strengths. In *2012 IEEE 75th vehicular technology conference (VTC Spring)* (pp. 1–5). IEEE.
50. Bratus, S., Cornelius, C., Kotz, D., & Peebles, D. (2008). Active behavioral fingerprinting of wireless devices. In *Proceedings of the first ACM conference on Wireless network security* (pp. 56–61). ACM.
51. Nikbakhsh, S., Manaf, A. B. A., Zamani, M., & Janbeglou, M. (2012). A novel approach for rogue access point detection on the client-side. In *2012 26th international conference on advanced information networking and applications workshops (WAINA)* (pp. 684–687). IEEE.
52. Chumchu, P., Saelim, T., & Sriklauy, C. (2011). A new MAC address spoofing detection algorithm using PLCP header. In *2011 international conference on information networking (ICOIN)* (pp. 48–53). IEEE.
53. Chae, S., Jung, H., Bae, I., & Jeong, K. (2012). A Scheme of Detection and Prevention Rogue AP using Comparison Security Condition of AP. In *2012 Universal Association of Computer and Electronics Engineers international conference on advances in computer science and electronics engineering* (pp. 302–306).
54. Szongott, C., Brenner, M., & Smith, M. (2015). METDS-A self-contained, context-based detection system for evil twin access points. In *Financial cryptography and data security* (pp. 370–386). Berlin: Springer.
55. Qu, G., & Nefcy, M. M. (2010). RAPiD: An indirect rogue access points detection system. In *2010 IEEE 29th international performance computing and communications conference (IPCCC)* (pp. 9–16). IEEE.
56. Kao, K. F., Chen, W. C., Chang, J. C., & Te Chu, H. (2014). An accurate fake access point detection method based on deviation of beacon time interval. In *2014 IEEE eighth international conference on software security and reliability-companion (SERE-C)* (pp. 1–2). IEEE.
57. Mustafa, H., & Xu, W. (2014). CETAD: Detecting evil twin access point attacks in wireless hotspots. In *2014 IEEE conference on communications and network security (CNS)* (pp. 238–246). IEEE.
58. Byrd, C., Cross, T., & Takahashi, T. (2011). In Black Hat-USA: Secure Open Wireless Networking.
59. Bauer, K., Gonzales, H., & McCoy, D. (2008). Mitigating evil twin attacks in 802.11. In *Performance, computing and communications conference, 2008. IPCCC 2008. IEEE International* (pp. 513–516). IEEE.
60. Gonzales, H., Bauer, K., Lindqvist, J., McCoy, D., & Sicker, D. (2010). Practical defenses for evil twin attacks in 802.11. In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE* (pp. 1–6). IEEE.
61. Arackaparambil, C., Bratus, S., Shubina, A., & Kotz, D. (2010). On the reliability of wireless fingerprinting using clock skews. In *Proceedings of the third ACM conference on Wireless network security* (pp. 169–174). ACM.
62. Jana, S., & Kasera, S. K. (2010). On fast and accurate detection of unauthorized wireless access points using clock skews. *Mobile Computing, IEEE Transactions on*, *9*(3), 449–462.
63. Lanze, F., Panchenko, A., Braatz, B., & Engel, T. (2014). Letting the puss in boots sweat: Detecting fake access points using dependency of clock skews on temperature. In *Proceedings of the 9th ACM symposium on Information, computer and communications security* (pp. 3–14). ACM.
64. Lanze, F., Panchenko, A., Ponce-Alcaide, I., & Engel, T. (2015). Hackers Toolbox: Detecting Software-Based 802.11 Evil Twin Access Points. In *12th annual IEEE consumer communications & networking conference*.
65. Wei, W., Jaiswal, S., Kurose, J. F., & Towsley, D. F. (2006). Identifying 802.11 Traffic from Passive Measurements Using Iterative Bayesian Inference. In *INFOCOM*.
66. Wei, W., Jaiswal, S., Kurose, J., Towsley, D., Suh, K., & Wang, B. (2012). Identifying 802.11 traffic from passive measurements using iterative bayesian inference. *IEEE/ACM Transactions on Networking (TON)*, *20*(2), 325-338.
67. Yan, B., Chen, G., Wang, J., & Yin, H. (2009). Robust detection of unauthorized wireless access points. *Mobile Networks and Applications*, *14*(4), 508–522.
68. Beyah, R., Kangude, S., Yu, G., Strickland, B., & Copeland, J. (2004). Rogue access point detection using temporal traffic characteristics. In *Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE* (Vol. 4, pp. 2271–2275). IEEE.
69. Mano, C. D., Blaich, A., Liao, Q., Jiang, Y., Cieslak, D. A., Salyers, D. C., et al. (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), 2.
70. Watkins, L., Beyah, R., & Corbett, C. (2007). A passive approach to rogue access point detection. In *Global telecommunications conference, 2007. GLOBECOM'07. IEEE* (pp. 355–360). IEEE.

71. Chirumamilla, M. K., & Ramamurthy, B. (2003). Agent based intrusion detection and response system for wireless LANs. In *IEEE international conference on communications, 2003. ICC'03* (Vol. 1, pp. 492–496). IEEE.
72. IEEE. (2004). IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE, Piscataway, USA.
73. Faria, D. B., & Cheriton, D. R. (2002). DoS and authentication in wireless public access networks. In *Proceedings of the 1st ACM workshop on Wireless security* (pp. 47–56). ACM.
74. Aslam, B., Akhlaq, M., & Khan, S. A. (2008). 802.11 disassociation DoS attack simulation using Verilog. *WSEAS Transactions on Communications, 7*, 198–206.
75. He, C., & Mitchell, J. C. (2004). Analysis of the 802.11 i 4-Way Handshake. In *Proceedings of the 3rd ACM workshop on Wireless security* (pp. 43–50). ACM.
76. Lockhart, A. (2005). Deauthentication Frame DoS.
77. Wang, L., & Srinivasan, B. (2010). Analysis and improvements over DoS attacks against IEEE 802.11 i standard. In *2010 Second International Conference on networks security wireless communications and trusted computing (NSWCTC)* (Vol. 2, pp. 109–113). IEEE.
78. Bellardo, J., & Savage, S. (2003). 802.11 Denial-of-service attacks: Real vulnerabilities and practical solutions. In *USENIX security* (pp. 15–28).
79. Guo, F., & Chiueh, T. C. (2006). Sequence number-based MAC address spoof detection. In *Recent Advances in Intrusion Detection* (pp. 309–329). Springer Berlin Heidelberg.
80. Xia, H., & Brustoloni, J. (2004). Detecting and blocking unauthorized access in Wi-Fi networks. In *Networking 2004* (pp. 795–806). Springer Berlin Heidelberg.
81. Anjum, F., Das, S., Gopalakrishnan, P., Kant, L., & Kim, B. (2005). Security in an insecure WLAN network. In *2005 international conference on wireless networks, communications and mobile computing* (Vol. 1, pp. 292–297). IEEE.
82. Wright, J. (2003). White Paper: Detecting wireless LAN MAC address spoofing.
83. Mar, J., Yeh, Y. C., & Hsiao, I. F. (2010). An ANFIS-IDS against deauthentication DOS attacks for a WLAN. In *2010 International symposium on information theory and its applications (ISITA)* (pp. 548–553). IEEE.
84. Faria, D. B., & Cheriton, D. R. (2006). Detecting identity-based attacks in wireless networks using signalprints. In *Proceedings of the 5th ACM workshop on Wireless security* (pp. 43–52). ACM.
85. Madory, D. (2006). New methods of spoof detection in 802.11 b wireless networking (Doctoral dissertation, Dartmouth College).
86. Chen, Y., Trappe, W., & Martin, R. P. (2007). Detecting and localizing wireless spoofing attacks. In *4th Annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks, 2007. SECON'07* (pp. 193–202). IEEE.
87. Chen, Y., Yang, J., Trappe, W., & Martin, R. P. (2010). Detecting and localizing identity-based attacks in wireless and sensor networks. *Vehicular Technology, IEEE Transactions on*, *59*(5), 2418–2434.
88. Sheng, Y., Tan, K., Chen, G., Kotz, D., & Campbell, A. (2008). Detecting 802.11 MAC layer spoofing using received signal strength. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE.
89. Agarwal, M., Biswas, S., & Nandi, S. (2013). Detection of de-authentication denial of service attack in 802.11 networks. In *India conference (INDICON), 2013 Annual IEEE* (pp. 1–6). IEEE.
90. Agarwal, M., Pasumarthi, D., Biswas, S., & Nandi, S. (2014). Machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization. *International Journal of Machine Learning and Cybernetics*, 1–17.
91. Nguyen, T. D., Nguyen, D. H., Tran, B. N., Vu, H., & Mittal, N. (2008). A lightweight solution for defending against deauthentication/disassociation attacks on 802.11 networks. In *ICCCN'08. Proceedings of 17th international conference on computer communications and networks, 2008* (pp. 1–6). IEEE.
92. Best Practices for Securing Your Wireless LAN (2004). *White paper, AirMagnet*.
93. Tired of Rogues: Solutions for Detecting and Eliminating Rogue Wireless Networks (2009). *White Paper, Air-Defense*.
94. Vanjale, S., & Mane, P. B. (2014). A novel approach for elimination of rogue access point in wireless network. In *India Conference (INDICON), 2014 Annual IEEE* (pp. 1–4). IEEE.
95. Sriram, V. S., Sahoo, G., & Agrawal, K. K. (2010). Detecting and eliminating Rogue Access Points in IEEE-802.11 WLAN-a multi-agent sourcing Methodology. In *Advance computing conference (IACC), 2010 IEEE 2nd international* (pp. 256–260). IEEE.
96. Branch, J. W., Petroni, N. L, Jr., Van Doorn, L., & Safford, D. (2004). Autonomic 802.11 wireless LAN security auditing. *IEEE Security & Privacy*, *3*, 56–65.
97. Netstumbler. www.netstumbler.com.

98. Wavelink. www.wavelink.com.
99. Air Defense. www.airdefense.net.
100. Bahl, P., Padhye, J., Ravindranath, L., Singh, M., Wolman, A., & Zill, B. (2005). DAIR: A framework for managing enterprise wireless networks using desktop infrastructure. HotNets.
101. Air Wave. www.airwave.com.

Bandar Alotaibi is a Ph.D. student in Computer Science and Engineering at University of Bridgeport. His research interests includes network security, mobile communications, computer forensics, wireless sensor networks and quantum computing. His Ph.D. dissertation focuses on distinguishing between the Rogue Access Points and the genuine Access Points in Wireless Local Networks using hard to spoof characteristics through fingerprinting techniques. Bandar received his Bachelor's of Science degree, with honors, in Computer Science-Information Security and Assurance emphasis from University of Findlay, and his Master's of Science degree in Information Security and Assurance from Robert Morris University.

Dr. Khaled Elleithy is the Associate Vice President for Graduate Studies and Research at the University of Bridgeport. He is a professor of Computer Science and Engineering. He has research interests in the areas of wireless sensor networks, mobile communications, network security, quantum computing, and formal approaches for design and verification. He has published more than three hundreds research papers in international journals and conferences in his areas of expertise. Dr. Elleithy has more than 25 years of teaching experience. His teaching evaluations are distinguished in all the universities he joined. He supervised hundreds of senior projects as well as MS theses. He supervised several Ph.D. students. He developed and introduced many new undergraduate/graduate courses. He also developed new teaching/research laboratories in his area of expertise. Dr. Elleithy is the editor or co-editor for 12 books by Springer. He is a member of technical program committees of many international conferences as recognition of his research qualifications. He served as a guest editor for several International Journals. He was the chairman for the International Conference on Industrial Electronics, Technology and Automation, IETA 2001, 19–21 December 2001, Cairo Egypt. Also, he is the General Chair of the 2005–2014 International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering virtual conferences.