Detecting Evil-twin Attacks in Smart Homes Using The Received Signal Strength Indicator

Zhanyong Tang[†], Yujie Zhao[†], Lei Yang[†], Shengde Qi[†], Dingyi Fang[†*]
Xiaojiang Chen[†], Xiaoqing Gong[†], Zheng Wang[‡]
[†]School of Information Science and Technology, Northwest University, Xi'an, 710127, P.R. China.
[‡]School of Computing and Communications, Lancaster University, UK.

ABSTRACT

Evil-twin is a common attack in WIFI environments, with which an attacker can set up a fake AP to steal sensitive information from the connected devices. The current approaches of detecting Evil-twin AP use some identities or fingerprints (such as SSIDs, MAC address and network traffic patterns) to verify the identify of the AP. However, such information can be easily obtained and faked by the attacker, leading to low detection rates.

This paper presents a novel Evil-Twin AP detection method based on the received signal strength indicator (RSSI). Our key insight is that the AP location rarely moves in a smart home environment where the RSSI of the genuine AP is relatively stable. Therefore, the RSSI can be used as the fingerprint of the genuine AP to detect fake APs. Our approach employs two strategies to detect a fake AP in two different scenarios where the genuine AP can be located on a single or multiple locations. Our approach uses the multipath effect of the WIFI signal to detect the identify of the connected AP. Compared to classical detection methods, our approach does not rely professional devices. Experimental results show that the single position detection approach achieves with an accuracy over 90% with little cost in delay time.

Keywords

Smart Homes; Evil-Twin Attack; RSSI; Detection

1. INTRODUCTION

Have you imaged that one day someone would open your intelligent door when you are outside, turn on your gas valve when you are sleeping and steal your bank count when you are surfing on the Internet? After the traditional internet and intelligent transportation internet, the attacker can put his claws to the Smart Homes Internet[1],It is not an exaggeration to say that these attacks are invading every corner of our lives with the rapid development of wireless communication technology, such as WIFI, 4G, GPS etc[2, 3].One of the most commonly attacks in the WIFI environment is referred to as the Evil Twin Attack which occurs when an adversary clones an AP with the same identity (or SSID) as an authentic AP.The bogus AP then exploits automatic access point selection techniques to trick a wireless client to connect to itself. Such fake APs are also known as Evil-Twin AP (Rouge AP or Fake AP)[4].An adversary can use an Evil-Twin AP as a platform to launch a variety of attacks, such as privacy and data theft. It is easily for the rogue AP to obtain information from the WIFI environment to compromise the security of the user. Smart Homes that rely on WIFI are also indispensable for suffering from Evil Twin Attacks. For instance, the Evil-Twin AP can hijack the DNS protocol and redirect the clients to a malicious server to steal the password of fingerprint lock or turning on the gas valve.

Because of the serious consequence, Evil-Twin AP detection has recently received much attention[5, 6].There are two widely used approaches in this domain. One is extracting unique traffic characteristics from the network flow[7, 8]. For example, to distinguish authorized WLAN hosts from unauthorized WLAN hosts connected to rogue access points by analyzing traffic characteristics, such as packet arrival time, request/response time of continuous ACK in TCP traffic. These methods are affected by the network's type, bandwidth and congestion. Purely relying on network traffics can result in poor detection performance because the detection algorithms can miss some rouge APs with high imperceptibility. The other approach, namely fingerprint identification detection methods, uses hard-ware features[9–16],to different the rogue APs from authentic APs. This is achieved by collecting key information of the authentic APs, such as firmware, chip, driver etc. Such an approach relies on the assumption that it is difficult for the attacker to build an AP with identical hardware information. However, building a fingerprint library is non-trivial. Moreover, extracting the fingerprints takes a long time, making such approaches infeasible when real-time is an essential requirement. Broadly speaking, the essence of Evil Twin detection is to find the as many differences between the rouge AP and the authentic AP as possible.

This paper introduces a novel method for detecting Evil-Twin APs, Our approach is based on the received signal strength indicator (RSSI). Our approach targets Smart Homes and exploits the fact the position of an AP is often fixed in a Smart Home environment. The main benefit of RSSI measurement based systems is that they do not require any addi-

*Corresponding author; Email: dyf@nwu.edu.cn

WOODSTOCK '97 El Paso, Texas USA

DOI: 10.475/123_4

tional sensor/actuator infrastructure but use already available communication parameters. By using RSSI, we can estimate the distance between the signal point and the receiving point [17–25].The work we are presenting relies only on received signal strength measurements from wireless radio access points to determine their possible position. In Smart Homes, The position of each AP is fixed and the RSSI signal is relatively stable, which is to great extent to meet the requirements of the detection factor not easy to imitate as previous refer. The challenge however is to identify the rouge APs in the case of that the intensity of the rouge AP is greater than that of the authentic AP. According to the 802.11 standard, when there are multiple APs existing nearby, a WLAN client will always choose the AP with the strongest signal to connect to[14, 26, 27].

Unlike past approaches, our detection factor is not easily to imitate as the the AP's position is stable in smart homes. Hence, in some cases, those APs who are not at predetermined position may have been forged. Our experimental results show that the proposed approach can effectively identify rouge APs. Our approach achieves on average a successful rate of 96% with less than 20s testing delay.

The main contributions of this paper are, (1) It is first the Evil-Twin attack detection system for Smart Homes, (2) It is also the first to demonstrate RSSI can be used as a means for detecting Evil-Twin Attacks in smart homes. Although our approach assumes the location of the AP is stable, the essential idea can be expanded to the other WIFI environments.

2. BACKGROUD

SSID and BSSID is always used to identify WIFI hot point since the protocol 802.11 does not define a strong sign to do it. In fact, both of them could be easily got by attacker, because the wireless network not only share the media but also cannot control the signal range. Although the access point is protected by password and sophisticated encryption, for an experienced attacker, it is not difficult to crack it during a short time. The original 802.11 security organization that try to solve these problems was the Wired Equivalent Privacy(WEP). In spite of having mechanisms to provide authentication, confidentiality and data integrity, WEP was found to be unsafe and trivially cracked after an attacker has gathered enough frames with the same Initialization Vector[28]. By actively accelerating the gather of frames, the latest WEP attack has been able to complete a breaking of WEP in under a minute[29]. WEP is increasingly being replaced by the Wi-Fi Protected Access(WPA). Nevertheless, to hold backward compatibility, WPA has not totally solved some security problems. Because control and management frames can be tricked and faked even with WPA enabled, wireless Local Area Networks(LANS) reserve impressionable to identity attacks and denial of service attacks[10].Once the attacker got the password, they will soon forge a same one called Evil-Twin AP (Rouge AP or Fake AP), is not easier recognized by user. Over the past few years, this kind of attack mainly exists in some public environments such as airports and cafes. However, as the development of the IoT, the attack value of private WIFI rises rapidly, and the attack develops towards the private WIFI in the Smart Home and other environments. Once the user connects the network to the Fake AP, the intruder can control the network environment of the user, and further, privacy sniffing, malicious data tampering and others advanced attack can be realized. The behavior of the intelligent device even can be controlled, for instance, opening or closing an intelligent lock, etc.

According to IEEE 802.11, when there is lots of APs around with the terminal, one with the strongest signal to be connected[14]. So the Fake AP is always be put at the nearest of attack target in order to be choose. This kind of attack can be called Fishing, which contains active Fishing and passive Fishing. Passive Fishing is namely that the Fake AP is just waiting for the connection from the terminal. This kind of attack cannot easily be found since it does not affect the Real AP, at the same time, the attack success rate is not high. Active Fishing means that to connect with the terminal, Fake AP cut of the connection between Real AP and the terminal by Evil-Twin Attack. Such attack can be carried out to precise attacks without affecting the other equipment except the target.

3. ATTACK SCENARIO AND ASSUMPTIONS

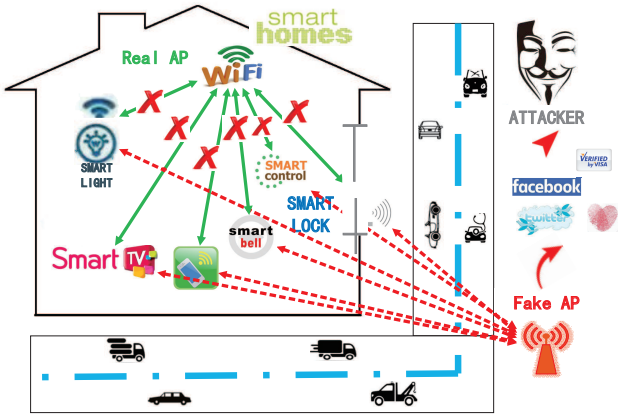


Figure 1: Examples scenarios in which the attacker can easily launch an Evil-Twin attack to steal information using a fake AP. This kind of attack typically happens when a hacker constructs a mock (but still functional) Wi-Fi access point (AP) right at the place where there ought to be an original and legitimate Access Point. The reason this works so well is that for a well-orchestrated attack, the illegitimate AP has stronger signals than the legitimate one and hence the unsuspecting users might log on to this mock-up connection and then use the internet while sharing all their precious data – all the way from their user IDs, passwords to credit/debit card information.

Attack scenarios.Figure 1 illustrates the scenarios where the Evil-Twin attack can be applied. Evil Twin are designed to look like real Wi-Fi hotspots. In those scenarios, the adversary is able to set a Fake AP to launch an Evil Twin attack from a laptop. Its signal might be stronger to the victim than the Real AP. Once disconnected from the legitimate Real AP, the tool then force offline computers and devices to automatically re-connect to the evil twin, allowing the hacker to intercept all the traffic to that device. When people in Smart Homes are using the Internet through an Evil Twin, they can unknowingly expose their passwords and other sensitive online data to hackers. According to the

Wi-Fi Alliance, a sophisticated Evil Twin can even control what websites appear when users access the Internet. That allows hackers to capture their passwords.

Assumptions.Our attacks require the adversary to set up the evil twin at a different location. We believe that the adversary maybe not set the Fake AP very close to the Smart Homes in order to avoid being caught. If a profile for the legitimate AP exists, the client device will automatically connect to the faked AP.

4. DRET OVERVIEW

DRET is a system that helps wireless home owner to discover and prevent Evil Access Points (AP) from attacking wireless users. The application can be run in regular intervals to protect your wireless network from Evil Twin attacks. By configuring the tool you can get notifications sent to you alarm signal whenever an evil access point is discovered. Additionally you can configure DRET to perform DoS on the legitimate wireless users to prevent them from connecting to the discovered evil AP in order to give the administrator more time to react. However, notice that the DoS will only be performed for evil APs which have the same SSID but different BSSID (AP's MAC address) or running on a different channel. This to avoid DoS your legitimate network

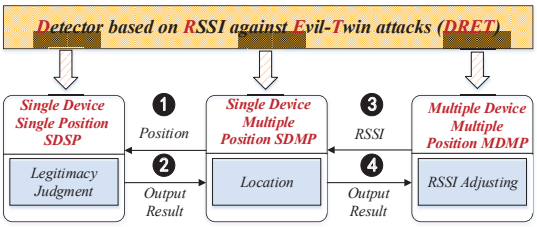


Figure 2: The overview of DRET System.DRET mainly consists of three parts (SDSP&SDMP&MDMP).

Following a common practice in FAKE AP detection, DRET will choose different modular depending on different circumstances. SDSP meet the simple scenario such as during night and when nobody is at home. However, SDSP is limited and the success rate is closely related to the Detector location. To addressing this limitation, SDMP is proposed, which locate the mobile phone firstly, the RSS fingerprint value is drawn to SDSP(❶), so the SDSP can determine the location of legitimacy(❷), the result return to SDMP. Sometimes many devices work in multi places, these devices need to use only one set of fingerprint data to check at the same time. MDMP will start, the RSSI is adjusted and then send to SDMP(❸), the result done by SDMP return to MDMP(❹).

5. PRELIMINARIES

In order to construct a real environment, the attacker will do anything to improve the Fake AP so that it has the same features a Real AP, including traffic characteristics and hardware fingerprint characteristics. However, the attacker cannot forge the position of the Real AP. In Smart Homes, the intuition underlying our design is that each Real AP has its fixed position, and the attacker cannot put the Fake AP exactly in the right place. Therefore, a new Smart Home Fake AP detected method based on RSSI is proposed in this paper.

Figure 3 is shown as the principle of Fake AP Detection based on RSSI. RAP and FAP are respectively represented Real AP and Fake AP. Detector receives the signal from each AP. D1 is the distance between the $Detector_1$ with the Real AP, and D1' is the distance between the $Detector_1$ with the Fake AP. If D1 is greater than D1', it means that the intensity of $Detector_1$ received from the Fake AP is stronger than the Real one. In general, when there exists multipath effect, Detector always choose the strongest signal in the homologous signals. So, undoubtedly, when the attacker turn on FAP_1, $Detector_1$ will choose it rather than the real RAP_1. But when the attacker turn off the FAP_1, The $Detector_1$ will choose RAP. According to the upper analysis, we can easily identify the Fake AP from the Real one by comparing the RSSI of them. In this scene, If $RSSI_1$' is greater than $RSSI_1$, it means that FAP_1 is Fake AP.

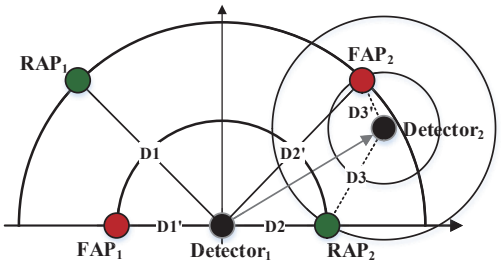


Figure 3: The figure shows two REAL APs(in green) and two FAKE APs(in red). The figure illustrates that the Detector(in black) how to recognize the FAP by using the differences of the RSSI that the APs locate differently.

However, there is another scene that the distance between the Real AP and detector is less than the Fake one's. In this condition, no matter open or shutdown the Fake AP, the detector would always choose the Real AP. So, we should try to build a scene like the previous one, namely, moving the detection's position to $Derector_2$, making D3' is greater than D3, then we can detect the Fake AP.

In free space, the path loss of signal propagation express signal attenuation, which is defined as the difference value between the effective radiated power and the received power. So the path loss in free space can be computed by the following formula.G_t and G_r separately express the antenna gain of the sender and the receiver.λ indicates the signal wave length, d is the distance between the sender and receiver.

$$PL(dB) = 10\log\frac{P_t}{P_r} = -10\log\left[\frac{G_t G_r \lambda^2}{(4\pi)^2 d^2}\right] (1)$$

Frequency of WIFI channel 1∼13 is from $2.412*10^9$ ∼ $2.472*10^9$. And there exists λ=c/f, c≈$3*10^8$m/s,so the value range of λ is 0.1214 ∼0.1244. We did some experiment to study what factors effecting the attenuation and the attenuation curve is shown as the Figure 4. In Figure a, both of the sender and receiver has unity-gain, and the channel is 1. In Figure b, both of the sender and receiver has unity-gain, and the channel is 13. In Figure c, the Antenna gain product of the sender and receiver is 100, and the channel is 13. From the Figure 4, we can find the following rules.

(1) From a and b, we can find that the effect of channel on attenuation is very small. (2) From b and c, we can find that antenna gain has a great influence on attenuation. (3) From a, b and c, we can find that the distance is the main factor to affect the attenuation, and the attenuation is less sensitive to the distance with the increase of distance.

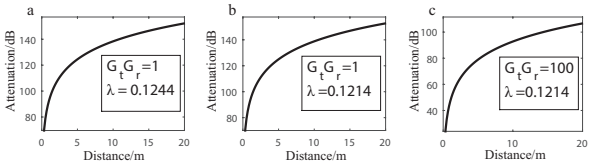


Figure 4: Signal attenuation curve

RSSI (Signal Strength Indicator Received) is the intensity of the received signal, its value can be calculated by the following formula:

RSSI = Transmit Power + Antenna gain - Path Loss

For a fixed transmitter and receiver, the Transmit Power and Antenna Gain are both constant, and the Path Loss is a function of the distance D, so RSSI can be expressed as RSSI=f(d). Then d will be d=f'(RSSI). Therefore, RSSI can be used directly to replace the distance for positioning.

In order to be simplify the calculation, we proposed Signal Space and Signal Distance. Signal Distance can be abbreviated as sd, then sd=|RSSI|. In Figure 5, the left are the physical space, and the right is the signal space. Both of them take AP as the reference point. Point a, b, c, d is the position of four mobile phones. In the physical space, the distance separately between a, c, d are equal, less than the distance between b and AP. But there are obstacles at the point a and d, where the attenuation of the black obstacle is higher than the gray obstacle, so $sd_a > sd_d > sd_c$, $sd_b > sd_c$. In general, the signal strength of straight line is the best when there is no obstacle, and wireless devices always give priority to the best signal when dealing with multipath effects. So, from the physical space to the signal space, the distance of their signal has some slight changes, which is shown as the right figure.

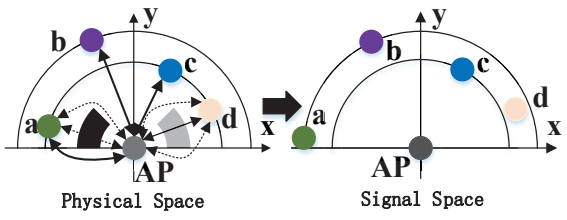


Figure 5: Physical Space convert to Signal Space

In order to verify that the RSSI can be used as the defection factor, we did an experiment. In normal circumstances, we build a fingerprint library by using the signal distance. Terminal MX3 is used as director to collect RSSI signal and the TL-WR882N is used as AP. The distance between them are 5m, and data collection rate is 2 times per second. We collected about 14000 of the total data, keeping surrounding environment is not changed during the process of collecting data, except that someone walked across. Its probability distribution histogram is shown as the following figure 6.

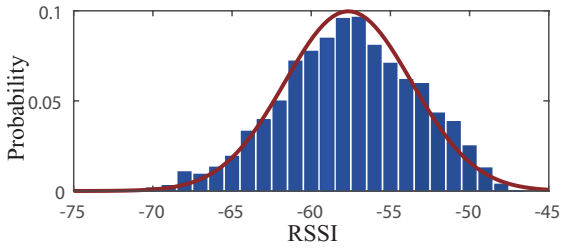


Figure 6: probability distribution histogram

By analyzing the experiment data, it is found that the measured value of the actual measurement is near to a stable value, and the probability distribution is approximately normal distribution. That means the RSSI can be used as the defection factor.

Actually, it seems that both of the Fake and Real AP is similar to the detector, which are difficult to be distinguished. According to multipath effect, the detector will select the one with the strongest signal to associate and compute the distance between the selected AP and it, which will be compared with the distance recorded in signal distance fingerprint database. If they are different, that means the AP should be forged. The mobile phone will be used as the detector. Depending on whether the mobile phone which be used as a detector in smart home moving or not, two different kinds of solution has been proposed in this paper, they are: a single fixed position detection and the multi-position collaborative detection.

6. AUTOMATED DETECTION ANALYSIS

6.1 *A SINGLE FIXED POSITION DETECTION*

Smart homes devices still need work under networking even there is no one at home, the detector is also. Therefore, we install the detector in a fixed position, and let it work 24 hours. Detector establish target AP RSSI fingerprint library in normal sense, which would be used as sample when detecting. Only the detected distance is within the error range of distances recorded in fingerprint database, it is considered as the fake AP, otherwise, it is true AP.

It is assumed that the deployment of hot spot and detector as shown in Figure 7. The position of fake AP and true AP are different, but the other features are same, such as network card hardware features, antenna gain, stability, etc.. A, B, and C are the positions of three detectors. The signal intensity of true AP and fake AP is the same in the position A (shown as Y2 axis). The signal intensity of true AP is stronger than ones of fake AP in the position B, and the opposite in position C.

In the security state, that is, where there not exits the fake AP, the RSSI and variance of signal intensity which separately received by three detectors at position A, B, C is shown in the following form.

Fake AP's working will lead to multipath effect. Therefore, it is assumed that PA,PB,PC is the probability of selecting true AP signal in A,B,C. Under ideal conditions, $0 <= P_C < P_A = 0.5 < P_B <= 1$, and the new Average and Variance is shown as the following form. Both of them wave in

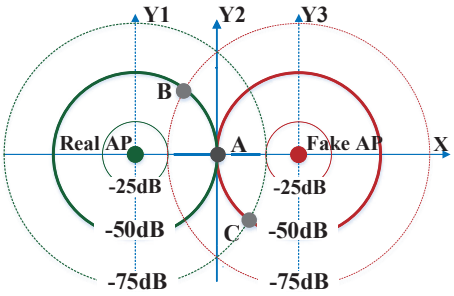


Figure 7: A single fixed position detection

Location	Average	Variance
A	μ_A=-50	σ_A
B	μ_B=-50	σ_B
C	μ_C=-75	σ_C

Table 1: FSSI and Variance in the security State

a certain range of fluctuation due to kinds of factors like the multipath effect, the external interference and etc.. It is assumed that the Average an Variance meeting the following conditions, μ-M<=μ<=μ+M,σ<=Σ .

Location	Average	Variance
A	μ'_A=μ_A=-50	σ'_A=σ_A
B	-75<μ'_B<-50	σ'_B>σ_B
C	-75<μ'_C<-50	σ'_C>σ_C

Table 2: FSSI and Variance when fake AP is working

From figure 7, we can see that when the detector in region C, it will select Fake AP since whose signal intensity is stronger than the Real AP's, which can be described with the formula like μ'>μ.When μ'>μ+M, we can say that there exists a Fake AP in the network. When the detector in region A,μ'=μ, that means we cannot distinguish the Real AP and the fake one. In region B, although the signal intensity of Real AP is higher than Fake AP, but the detector considers both of them is the same signal, the latter is still cannot be detected.

As analysis shows, detector and Real AP cannot be too close that will lead to high misdetection rate, so the best deployment location of detector is in region C where the signal is weak, far away from the Real AP and near the Fake AP.

6.2 *MULTI POSITION DETECTION*

Obviously, a single fixed position detection method can only solve part of the problem. In this part, multi position detection is proposed. Multi position detection relies on mobile phones, with it we can convert multi position to single fixed position detection. So, first what we need to do is determining the position of the mobile phone. The most well-known and high accuracy of the positioning method is GPS, while GPS devices have been known to not work very well indoors. In this paper, we use the WIFI signal for locating the position of mobile phone by Three point positioning method. With the popularity of WIFI, there are almost always more than three WIFI hotspots will be found when we are indoors.

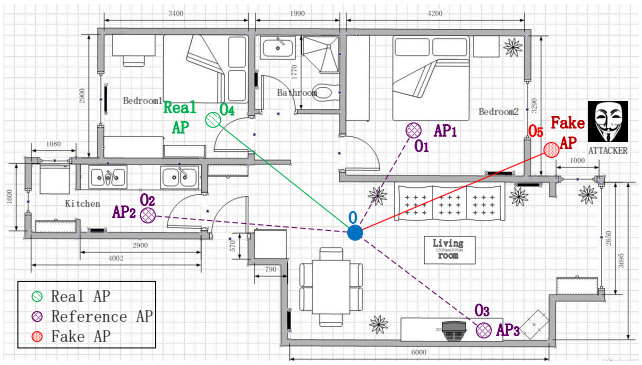


Figure 8: Multi position Detection transformation. The figure show that any three APs could be choosed as reference in the signal space. They are used to loacate the positions of the MobilePhone which is a detector in Smart Homes.

As shown in Figure 8, AP_1,AP_2 and AP_3 are three different APs, assuming their positions are known. O is the mobile phone's position. The original distance can be defined as sd which represents the distance between AP and mobile phone.sd_i=|OO_i|, i=1,2,3,4,5. So AP_1, AP_2 and AP_3 can locate the position of the mobile phone in the signal space. Then we can convert the Multi position detection to a Single fixed position detection.

There are two stages in Multi position cooperative detection: fingerprint gathering stage and detection stage. The first stage should be done in a safe state, we collect the RSSI information both of reference AP and target AP in many different positions, to build a fingerprint library. In the detection stage, using reference AP to locate the phone and the fingerprint data in a single fixed position detection, the program framework is shown in figure 8, we can locate the mobile phone's position by using reference AP, then using the method mentioned in the previous chapter to detect.

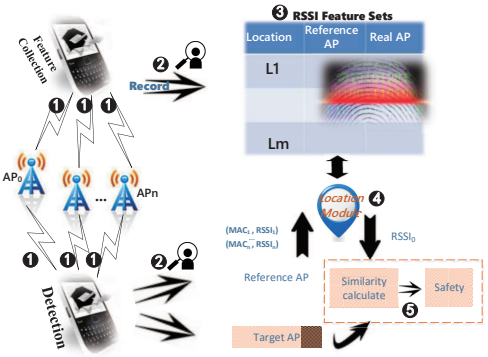


Figure 9: Multi position Detection framework

In Figure 9, AP_0 is the target AP,AP_2~AP_n are the candidate's reference AP, the whole process can be divided into the following 5 steps:

Step ❶: RSSI acquisition
Step ❷: Effective data selection
Step ❸: Establishment of fingerprint database

Step ❹: Mobile position determination
Step ❺: Validity judgment

6.2.1 *RSSI Acquisition*

In the experiment, the value of RSSI is collected by the interface (IOS: Android:android.net.WIFI. * (SystemConfiguration/CaptiveNetwork.h) in mobile phone .

6.2.2 *Effective Data Selection*

Effective RSSI Values Selection

It is a challenging job to choose the right RSSI values since the mobile phone are always moving. However the RSSI value we need should be waved in a small range, which is shown as the Figure 10. The data in two boxes are what we want, the others are generated by mobile phone when it is moving. In the condition that the distance between mobile phone and AP is 1m and there is no interference, which generating the data in the first box. Data in the second box is generated in the condition that the distance between mobile phone and AP is 4m and there are two source of interference. The other data is generated in the condition that someone take the mobile phone go around the house with the speed of 1.5m/s.

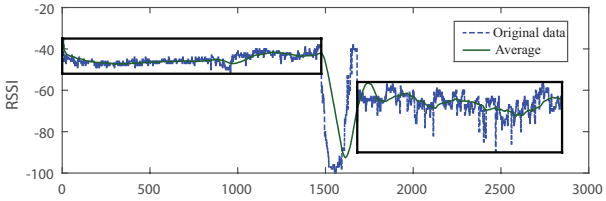


Figure 10: RSSI Sequence

In the first experiment, Variance increment method is used to judge whether the mobile phone is moving. It is assumed that the size of sliding window is 120. When the amount of data is less than the window, it is invalid data.

$$W_i = \{r_{i-ws+1}, r_{i-ws+2}...r_{i-1}, r_i\}\, i >= ws, r_i \in R$$

R is the whole RSSI sequence, r_i is the value of RSSI, ws is the window size.

The variance can be used to measure the deviation between the RSSI data and the mean value of the window. The variance of W_i is σ_i which express the data fluctuation of W_i. The greater the data fluctuation, the greater the variance.

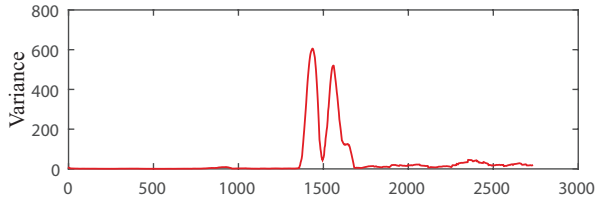


Figure 11: RSSI Sequence variance

As shown in Figure 11, the window size is 120, two peaks in the middle corresponding to the moving process, that is, it corresponds to the parts not in that two boxes in Figure 10. However, the cause of the big variance is not necessarily a person's movement, the stability of the signal will also affect it. Therefore, the slope of the variance curve is used to determine whether the current is moving. The variance increment k(i).

$$k(i) = \frac{d_{\sigma_i}}{d_i} = \frac{\sigma_i - \sigma_{i-1}}{i-(i-1)} = \sigma_i - \sigma_{i-1} (3)$$

In Formula 3,σ_i is the variance of W_i,σ_{i-1} is the variance of W_{i-1}.

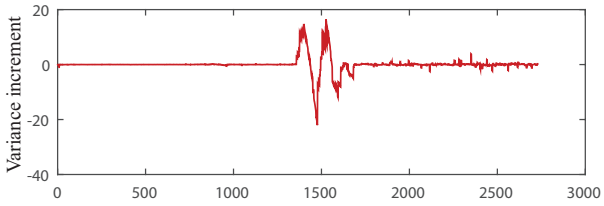


Figure 12: RSSI Sequence variance

The results of improved is shown in Figure 12. When k(i) is near to 0, it means that the original variance is stable in a certain range, that also means the mobile phone is not moving or moving in a small range. We set a threshold to detect whether the mobile phone is moving. If |k(i)|<=K, the mobile phone is considered to be stable, otherwise it means the position of mobile phone has changed.

Those sequence with a stable position has the following characteristics:

Start point:[|k(i)|<=K]-ws(+1)
End point:[|k(i)|>K]-ws/2

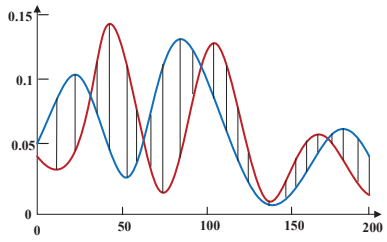
Effective reference AP selection

In order to improve the accuracy of multi position detection, it is needed to improve the accuracy of the location. Because of the complexity of the wireless signal transmission in the indoor environment, the AP signal is not stable. In the network environment, a position can be detected more than one AP. Therefore, Signal stability and the relevance with target AP are the two factors in choosing AP. Relevance here means that both the target AP and the reference AP moving with the mobile phone, that's why the fluctuations of the variance between the target AP and the reference AP should be consistent.

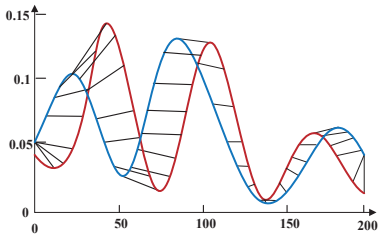
We use Dynamic (Time Warping DTW[30], dynamic time warping) algorithm to calculate the distance and determine the validity of the reference AP. DTW is a method that calculates an optimal match between two given sequences (e.g. time series) with certain restrictions. The sequences are "warped" non-linearly in the time dimension to determine a measure of their similarity independent of certain non-linear variations in the time dimension. This sequence alignment method is often used in time series classification.

As shown in Figure 13, picture on top calculate distance without using dynamic time but the below one uses, it can make calculation of the distance reaching the minimum distortion.

When selecting the effective reference AP, each AP is considered as the candidate reference AP. The large number of its variance increment is stored and the distance between its variance increment sequence and the target's. After getting the distance of all candidate reference APs and target



(a)



(b)

Figure 13: dynamic time warp (DTW)

APs, all candidate reference APs will be ordered by the distance. The smaller the distance, the better the effectiveness. Therefore, four candidate reference APs with the minimum distance will be choose as the reference APs to locate the mobile phone's position. In general, three points are enough for location. In order to prevent that one of the three reference APs is failure, so we choose four reference APs from the candidate lists.

6.2.3 *Establishment of Fingerprint Database*

The RSSI fingerprint Library (RSSI-MAP) is built by the RSSI sequence generated in previous section. RSSI-MAP is shown in Form3. R_J=($r_{1,J}$,$r_{2,J}$...$r_{L,J}$)represent the fingerprint information in RSSI-MAP. J is the position where the mobile phone is stayed for detecting. L is the number of candidate reference APs. r is the fingerprint information of AP, which can be described by triple like r($\overline{rssi}$,var,len). Items in triple represents the average, variance and length of RSSI sequence.

Location	Reference AP	Target AP
1	R_1=($r_{1,1}$,$r_{2,1}$...$r_{L,1}$)	R'_1=$r_{0,1}$
2	R_2=($r_{1,2}$,$r_{2,2}$...$r_{L,2}$)	R'_2=$r_{0,2}$
...	...	...
J	R_J=($r_{1,J}$,$r_{2,J}$...$r_{L,J}$)	R'_J=$r_{0,J}$

Table 3: structure of RSSI-MAP

6.2.4 *Mobile Position Determination*

R_T=($r_{1,T}$,$r_{2,T}$...$r_{L,T}$) represents RSSI fingerprinting information of the reference APs are detected at the position T.R'_T=$r'_{0,T}$ represents the RSSI fingerprinting information of the target AP is detected by the position T.Dist(R_T,R_J)is the distance between R_T and R_J.$\overline{rssi_{i,T}}$ is the average value of RSSI for reference AP,$\overline{rssi_{i,J}}$ is the average of the RSSI sequence for reference AP. j is the position where the distance between T and one in RSSI-MAP is the shortest. When there are more than three reference APs, we can locate the mobile phone.

$$Dist(R_T, R_J) = \sqrt{\sum_{i=1}^{L}(\overline{rssi_{i,T}} - \overline{rssi_{i,J}})^2} (4)$$

Dist(R_T,R_J) in Formula 4 depend on the number of L, in order to reduce the effect on $Dist_T$ that the number of reference AP are different in different position. The formula is improved as the following.

$$Dist_T = min\left[\frac{Dist(R_T, R_J)}{L}\right] (5)$$

When L is greater than or equal to 3, the fingerprint of the first three APs can be used to location by using Formula 4 and 5. When L is equal to 2, there will be more than one position and all of them have the same distance. Then we should choose the one who is the nearest one with the target AP. When L is equal to 1, in order to increase the accuracy of the positioning, the variance is used to measuring the similarity between position T and position J. From the previous section, the RSSI form one AP at the same position is approximate normal distribution, that is, the RSSI sequence is represented as follows:

$$P(rssi) = \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{(rssi-\mu)^2}{2\sigma^2}} (6)$$

In Formula 6,σ=var,μ=$\overline{rssi}$.

In the information theory, KL[31, 32] Kullback (Leibler - divergence) can be used to describe the difference between two probability distributions of Q and P,D_{KL}(P||Q) is the information loss caused by that Q is used to fit the true distribution P. So the distance between the T and the RSSI probability distribution can be calculated using the KL divergence. KL divergence is defined as the formula 7.

$$D_{KL}(P||Q) = \sum P(i) ln \frac{P(i)}{Q(i)} (7)$$

So, we can get formula 8 from formula 6 and formula 7.

$$Dist(R_T, R_J) = D_{KL}(R_T||R_J) =$$

$$\sum_{rssi=-100}^{0} \frac{P(rssi)}{2}\left[\frac{(rssi-\mu_1)^2}{\sigma_1^2} - \frac{(rssi-\mu_2)^2}{\sigma_2^2}\right] (8)$$

In the formula 8,σ_1=$var_{L,T}$, μ_1=$\overline{rssi_{L,T}}$

$$\sigma_2 = var_{L,J}, \mu_2 = \overline{rssi_{L,J}}$$

$$P(rssi) = \frac{1}{\sqrt{2\pi}\sigma_1} e^{\frac{(rssi-\mu_1)^2}{2\sigma_1^2}}$$

Then, according to the distance got by formula 8, the nearest neighbor algorithm is used to find the corresponding position in the J RSSI-MAP.

6.2.5 *Legitimacy Judgment*

max($\overline{rssi}$)represents the maximum mean of target RSSI at position J. It is can be easily query in RSSI-MAP when we find the position J. $\overline{rssi}$ is the mean value being detected. Then, there is $Diff_T$=$\overline{rssi}$-max($\overline{rssi}$).

If $Dist_T$<=M and $Diff_T$<=0, safe and there is no fake AP.

If $Dist_T$<=M and $Diff_T$>0, unsafe and there exits fake AP:

If $Dist_T$>M, fingerprint database should be updated. You can find the details in next section.

6.2.6 *Dynamic Update of Fingerprint Database*

The dynamic update of RSSI fingerprint database consists of two parts, one is the addition of the new fingerprint, and the other is the update of the existing fingerprint.

The new fingerprint should be added is because of various reasons in the training phase of the RSSI fingerprint database. It can't cover all the spatial sub regions of M, so it is necessary to improve the fingerprint database in the later stage.

The update of the existing fingerprint is caused by environmental changes such as survival status of reference AP, the correlation between the candidate reference AP and the target AP, the change of the reference AP's position and so on. At this point, we need to update the fingerprint information which has already exists in the fingerprint database in detection stage.

$$\left[R_J\left(r_{1,J}, r_{2,J}...r_{L,J}\right), R'_J\left(r_{0,J}\right)\right]$$

Assume there are four valid candidate reference AP, they are AP_1,AP_2,AP_3,AP_4, and the relationship or their effectiveness is as the following: E1>E2>E3>E4,then there is $Dist_T$=$Dist_T$(AP_1,AP_2,AP_3), The corresponding position is J.

When there is $Dist_T$>M

$$\begin{cases} Dist_{T3} = Dist_T\left(AP_1, AP_2, AP_4\right) \\ Dist_{T2} = Dist_T\left(AP_1, AP_3, AP_4\right) \\ Dist_{T1} = Dist_T\left(AP_2, AP_3, AP_4\right) \end{cases}$$

If $Dist_{Ti}$<=M, then we can use $r_{i,T}$ instead $r_{i,J}$ in the RSSI-MAP to update the existing fingerprint. If $Dist_{Ti}$>M, then put (R_T,R'_T) into the RSSI-MAP. If $Dist_{Ti}$<=M and $r_{i,t}$len>=$r_{i,j}$len, then we can use $r_{i,T}$ instead $r_{i,J}$ in the RSSI-MAP.

7. EVALUATION IN SPD AND MPD

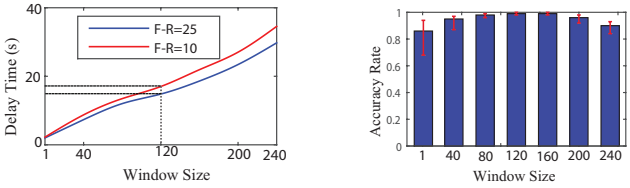
In order to verify the feasibility and effectiveness of the AP Evil-Twin detection method based on RSSI, we implement a number of experiments.

7.1 *Experiment and Assessment for Single Position Detection*

Discussion of Sliding Window Size

The previous section shows, the size of the sliding window affects the delay rate and false negative rate of detection. That means, the bigger the window, the higher the delay rate is, and the higher the false negative rate is. In order to find a suitable value for the size of sliding window, wo design a experiment like the following.

In order to verify the effect of window size on the delay, we set the mean difference respectively between the fake AP and the true RSSI is 25 and 10, that is, F-R=25 and F-R=10.The window size in turn is: 1, 40, 80, 120, 160, 200, 240. The safety threshold value for each round of detection is the maximum mean of RSSI in 30 minutes. There are 14 sets of experiment, each set of experiment will be done at 30 times, and the result is as showing in Figure 14. From the left figure we can see that when the difference of mean between true AP and fake AP is bigger, the delay rate is smaller. When the window size is 120, the average delay time is less than 20s.



(a) (b)

Figure 14: Effect of window size on delay and accuracy

To verify the effect of window size on accuracy, when it is in the condition that F-R=10, we set the windows size in turn: 1, 40, 80, 120, 160, 200, 240. After the test program running 10 minutes, open the fake AP and let it run for 3 minutes then close it for 3 minutes. Because it need a certain delay that the mean value is changed from abnormal status to normal status.

Due to the mean from abnormal status returned to normal needs a certain delay, so every 3 minutes spent after a delay time again wrong inspection or missed, it is assumed that the error detection. If there is wrong or missed detecting after delayed time, it is considered as the error status. This experiment is done 50 times, and the result is shown in the right of Figure 14. According to the experiment results, when the window size is 80, 120 and 160, the accuracy is more than 98%. If the windows size is too small or too bigger, the accuracy is lower since the false positive rate is higher.

Discussion of threshold value

In this experiment, we set the window size is 120 and the F-R is 25 or 10. Assume that the threshold value is Rmax, Rmax-2, Rmax+2, Rmax+4, Rmax+8. So there are 10 sets of experiment. In each experiment is be done as the following step 50 times. After the test program running 10 minutes, open the fake AP and let it run for 3 minutes then close it for 3 minutes. We can get the result of this experiment from Figure 15, when the security threshold value is Rmax, the accuracy is up to 96%. When the security threshold value is Rmax+2 , the accuracy of the condition that F-R=25 is up to 100%, and F-R=25 is 99%.

Discussion of distance

In this experiment, we set F-R=0,5,10,15,20, and the threshold value is Rmax. In each experiment is be done as the following step 50 times. After the test program running 10 minutes, open the fake AP and let it run for 3 minutes then close it for 3 minutes. We can get the result of this experiment from Figure 16. When F-R = 10, the accuracy is more than 96%, the missing rate is less than 3%.

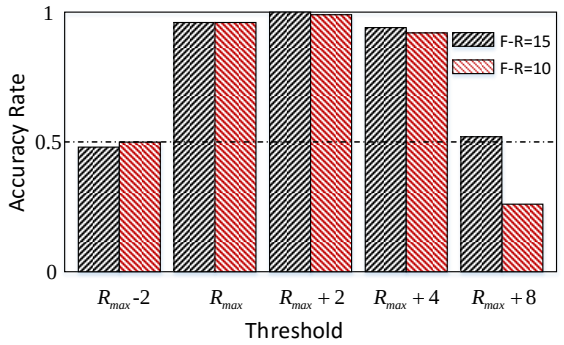


Figure 15: Effect of safety threshold on the accuracy of detection

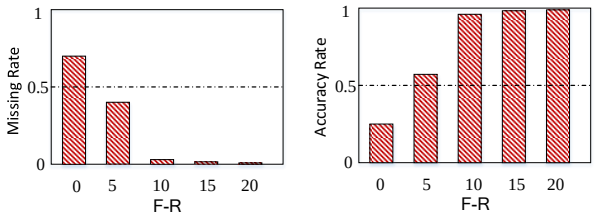


Figure 16: Effect of distance on the detection results

7.2 *Experiment and evaluation of multi position cooperative detection*

Validation of variance increment method

In this experiment, the window size is 120, and K is 4, then split the RSSI sequence using Variance increment method in the 6.2.1section. The result is shown as the Form 5. Dropping out the fragment whose length is shorter than 120, then we can get two effective RSSI sequence fragments (S_1 and S_10), the total length is 2598, the effective fragment length was 2605 in the original data sequence. So the accuracy is 99.7%.

Flag	Range	Length	Range	Mean
S_1	1-1422	1422	[-52,-35]	-45.15
S_2	1366-1431	66	[-44, -39]	-42.5
S_3	1424-1502	79	[-84, -38]	-50.04
S_4	1489-1560	72	[-100,-64]	-91.17
S_5	1507-1569	63	[-100,-87]	-95.95
S_6	1552-1620	69	[-100,-72]	-90.91
S_7	1609-1718	110	[-76, -38]	-56.54
S_8	1660-1726	67	[-75, -40]	-56.68
S_9	1669-1731	63	[-75, -40]	-59.95
S_10	1861-2848	1168	[-90, -56]	-66.37

Table 4: First time to split RSSI sequence

The validity of DTW algorithm

To verify that the DTW algorithm could be used to choose the valid AP, we open the detecting software which could find all the AP and getting their RSSI. Then we let the detecting software move with the speed of 1.5m, staying at three different locations and staying at each place for 15 minutes. At the end, there are 28 APs being found, including 1 target AP and 27 candidate reference AP. For each of 27 candidate reference AP, we use DTW algorithm to calculate the distance of variance increment sequence between target AP and it. Finally, we are successful to find four suitable reference AP.

The validity of localization algorithm

In a room with 100 square meters, we collect a set of data per 4 square meters. So there are 25 sets of data. In detecting stage, we stayed at every position for 5 minutes, then moving to another position with the speed of 1.5m/s. For the four suitable reference AP found in previous section, there are three kinds of conditions, that is, the first 4 AP should be considered as the reference AP, and the first 3, the first 2, respectively calculate their Euclidean distance. When there is only one reference AP, the accuracy of location is 62%. When there is two reference APs, the accuracy of location is 85%. When there is three reference APs, the accuracy of location is 90%.

The validity of Multi position cooperative detection

We play a role of an attack, simulating a fake AP in a notebook. And the experiment is done still in a room with 100 square meters, dividing it into 25 region. In each region, we collect data for every 30 minutes, and use the maximum mean of this region as the safety threshold. In detecting stage, we stayed at every position for 5 minutes, then moving to another position with the speed of 1.5m/s. Experiments were carried out for 200 times, 100 times is to open the fake AP, the other 100 times is to turn off the fake AP. When the fake AP is turned on, if there is any position detected by the fake AP, then the detection is successful, if all the positions are not detected by the fake AP, then the detection fails. Close the fake AP, if there is any position to detect the false AP, then the detection fails, if all the positions are not detected in the fake AP, then the detection successfully. When there is only one reference AP, the accuracy of location is 58%. When there is two reference APs, the accuracy of location is 80%. When there is three reference APs, the accuracy of location is 90%.

8. RELATED WORK

At present, most Evil-Twin detection method work for the public WIFI environment. They are two key approaches in this domain. One is based on hardware feature, the other is flow feature.

The hardware feature testing method utilizes the characteristic that different network card chips and different drives possess different fingerprint features to set up a fingerprint feature library and decide whether the Fake AP is existed or not through matching fingerprint data in the fingerprint feature library during testing. Bratus et al.[7] sends some SIMULATING frames which possess false formats but are not prohibited by a standard protocol. Although different network card chips or drives have different responses to various SIMULATING frames, the testing method is easy to be found by an intruder. Franklin et al.[9] characterize the drivers during the "active scanning period". This method is undefined in the IEEE 802.11 standard on the frequency and order of sending probe requests. Therefore, each manufacturer employs its own algorithm. This technique is that it cannot distinguish between two devices using the same network card and driver. So this technique may not be used for identifying individual devices. Loh et al.[10] fingerprint

client station, by surveying probe requests. Client station send probe requests in the light of characteristic periodic. The period itself is attached to slight variations. Far from being consistent, these variations can be clustered. With enough detection time, each cluster slowly derives, with a slope proportional to the time skew. This work is able to particularly identifying client station; however, the requires more than one hour of traffic and is only application to client stations. In a word, Franklin et al.[9] and Loh et al.[10] utilize the characteristic that different wireless network cards send different Probe Request frames with different periods during scanning to set up the fingerprint library. As the equipment only sends a small number of Probe Request during joining the network and the method can be valid when passive scanning is used, the expensive time overhead and the relatively bad real-time property are involved; Neumann et al.[11] utilizes the arrival time of inter-frame space to identify the wireless equipment, but the characteristic can be faked by the intruder and the testing method based on the characteristic can be bypassed. The testing methods for the hardware fingerprint feature of the equipment above mentioned cut both ways: various fake AP can be tested effectively and the cost of faking the hardware feature of the intruder is relatively high; but the cost of building the hardware feature fingerprint library is high, the time for extracting the hardware fingerprint is long, the testing real-time property is worse, and the expansibility is bad.

According to the flow feature testing method, the network flow feature is different when the fake AP is existent or nonexistent; so, whether Evil-Twin AP is existent or not can be tested. The method is excellent in extendibility, but also has some disadvantages. Beyah R et al. [12] utilizes the arrival time space of each data packet to build a flow feature library; as the method is influenced by flow shaping greatly, the practical operation and the applicability is not good; Wei W et al. [13] proposes that the arrival time of the ACK data packet in a TCP protocol can be used to set up the flow feature library; as the arrival time is influenced by TCP, the testing efficiency is limited; Sheng B et al. [14–16] proposes that data round trip time can be used to test whether the fake AP is existent or not, but the data round trip time is influenced by the network type, the band width and the state of congestion at the same time.

Besides, Xu et al. [33] puts forward the wireless fake AP attack in an in-vehicle network, meanwhile, gives the testing method based on RSSI. The method requires that all of the APs are equipped with GPS modules to report their own positions; a user judges whether the fake AP is existent or not through whether the measured RSSI is matched with the position or not. The method can effectively test the fake AP attack in the in-vehicle network, but is not suitable for indoor environment because the GPS signal is weakened, even shielded indoors.

9. CONCLUSIONS

This paper has presented a novel approach to detect fake APs in a smart home environment. Our approach uses RSSI as the fingerprint of the authentic AP to detect fake APs. We have proposed two methods to identity fake APs in two different scenarios where the genuine AP locates on a single, fixed or multiple positions. Our experimental results show that our approach can detect 90% of the fake APs with little extract overhead to the communication delay time.

10. ACKNOWLEDGMENTS

This work was supported in part by the National Natural Science Foundation of China (No. 61373177, and No. 61572402), the Key Project of Chinese Ministry of Education (No. 211181), the International Cooperation Foundation of Shaanxi Province, China ((No. 2013KW01-02, No. 2015KW-003 and No. 2016KW-034), the China Postdoctoral Science Foundation (grant No. 2012M521797), the Research Project of Shaanxi Province Department of Education (No. 15JK1734), and the Research Project of NWU, China (No. 14NW28), 14NW28), and the UK Engineering and Physical Sciences Research Council under grants EP/M01567X/1 (SANDeRs), EP/M015793/1 (DIVIDEND).

References

[1] Marie Chan, Daniel EstÍÍve, Christophe Escriba, and Eric Campo. A review of smart homesąłpresent state and future challenges. *Computer Methods and Programs in Biomedicine*, 91(1):55 – 81, 2008.

[2] Julius Schulz-Zander, Lalith Suresh, Nadi Sarrar, Anja Feldmann, Thomas Hühn, and Ruben Merz. Programmatic orchestration of wifi networks. In *2014 USENIX Annual Technical Conference (USENIX ATC 14)*, pages 347–358, Philadelphia, PA, June 2014. USENIX Association.

[3] Fabian Lanze, Andriy Panchenko, Ignacio Ponce-Alcaide, and Thomas Engel. 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*, Q2SWinet '14, pages 87–94, New York, NY, USA, 2014. ACM.

[4] D. A. Dai Zovi and S. A. Macaulay. Attacking automatic wireless network selection. In *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, pages 365–372, June 2005.

[5] J. Herzen, R. Merz, and P. Thiran. Distributed spectrum assignment for home wlans. In *INFOCOM, 2013 Proceedings IEEE*, pages 1573–1581, April 2013.

[6] O. Nakhila, E. Dondyk, M. F. Amjad, and C. Zou. Userside wi-fi evil twin attack detection using ssl/tcp protocols. In *Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE*, pages 239–244, Jan 2015.

[7] Sergey Bratus, Cory Cornelius, David Kotz, and Daniel Peebles. Active behavioral fingerprinting of wireless devices. In *Proceedings of the First ACM Conference on Wireless Network Security*, WiSec '08, pages 56–61, New York, NY, USA, 2008. ACM.

[8] Johnny Cache. Fingerprinting 802.11 implementations via statistical analysis of the duration field. *Uninformed. org*, 5, 2006.

[9] Damon McCoy, Jason Franklin, Jamie Van Randwyk, Douglas Sicker, and Parisa Tabriz. *Passive data-link layer 802.11 wireless device driver fingerprinting.* Jan 2006.

[10] Loh Chin Choong Desmond, Cho Chia Yuan, Tan Chung Pheng, and Ri Seng Lee. Identifying unique devices through wireless fingerprinting. In *ACM Conference on Wireless Network Security, WISEC 2008, Alexandria, Va, Usa, March 31 - April*, pages 46–55, 2008.

[11] C. Neumann, O. Heen, and S. Onno. An empirical study of passive 802.11 device fingerprinting. In *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*, pages 593–602, June 2012.

[12] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland. Rogue access point detection using temporal traffic characteristics. In *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, volume 4, pages 2271–2275 Vol.4, Nov 2004.

[13] Wei Wei, Kyoungwon Suh, Bing Wang, Yu Gu, Jim Kurose, and Don Towsley. 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, pages 365–378, New York, NY, USA, 2007. ACM.

[14] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu. A timing-based scheme for rogue ap detection. *IEEE Transactions on Parallel and Distributed Systems*, 22(11):1912–1925, Nov 2011.

[15] Chad D. Mano, Andrew Blaich, Qi Liao, Yingxin Jiang, David A. Cieslak, David C. Salyers, and Aaron Striegel. Ripps: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning. *ACM Trans. Inf. Syst. Secur.*, 11(2):2:1–2:23, May 2008.

[16] G. Qu and M. N. Michael. Rapid: An indirect rogue access points detection system. In *Performance Computing and Communications Conference (IPCCC), 2010 IEEE 29th International*, pages 9–16, Dec 2010.

[17] KSAP Levis. Rssi is under appreciated. In *Proceedings of the Third Workshop on Embedded Networked Sensors, Cambridge, MA, USA*, volume 3031, page 239242, 2006.

[18] David Kotz, Calvin Newport, Robert S. Gray, Jason Liu, Yougu Yuan, and Chip Elliott. Experimental evaluation of wireless simulation assumptions. In *Proceedings of the 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, MSWiM '04, pages 78–82, New York, NY, USA, 2004. ACM.

[19] N. Patwari, A. O. Hero, M. Perkins, N. S. Correal, and R. J. O'Dea. Relative location estimation in wireless sensor networks. *IEEE Transactions on Signal Processing*, 51(8):2137–2148, Aug 2003.

[20] Manikanta Kotaru, Kiran Joshi, Dinesh Bharadia, and Sachin Katti. Spotfi: Decimeter level localization using wifi. *SIGCOMM Comput. Commun. Rev.*, 45(4):269–282, August 2015.

[21] K. Wu, Jiang Xiao, Youwen Yi, Min Gao, and L. M. Ni. Fila: Fine-grained indoor localization. In *INFOCOM, 2012 Proceedings IEEE*, pages 2210–2218, March 2012.

[22] Anshul Rai, Krishna Kant Chintalapudi, Venkata N. Padmanabhan, and Rijurekha Sen. Zee: Zero-effort crowdsourcing for indoor localization. In *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, Mobicom '12, pages 293–304, New York, NY, USA, 2012. ACM.

[23] Hongbo Liu, Yu Gan, Jie Yang, Simon Sidhom, Yan Wang, Yingying Chen, and Fan Ye. Push the limit of wifi based localization for smartphones. In *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, Mobicom '12, pages 305–316, New York, NY, USA, 2012. ACM.

[24] Souvik Sen, Jeongkeun Lee, Kyu-Han Kim, and Paul Congdon. Avoiding multipath to revive inbuilding wifi localization. In *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '13, pages 249–262, New York, NY, USA, 2013. ACM.

[25] Julius Schulz-Zander, Carlos Mayer, Bogdan Ciobotaru, Stefan Schmid, Anja Feldmann, and Roberto Riggio. Programming the home and enterprise wifi with opensdwn. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, pages 117–118, New York, NY, USA, 2015. ACM.

[26] S. D. Hermann, M. Emmelmann, O. Belaifa, and A. Wolisz. Investigation of ieee 802.11k-based access point coverage area and neighbor discovery. In *Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on*, pages 949–954, Oct 2007.

[27] Damon McCoy, Jason Franklin, Jamie Van Randwyk, Douglas Sicker, and Parisa Tabriz. *Passive data-link layer 802.11 wireless device driver fingerprinting.* Jan 2006.

[28] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting mobile communications: the insecurity of 802.11. In *International Conference on Mobile Computing and NETWORKING*, pages 180–189, 2001.

[29] Erik Tews, Ralf Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit wep in less than 60 seconds. In *Information Security Applications, International Workshop, Wisa 2007, Jeju Island, Korea, August 27-29, 2007, Revised Selected Papers*, pages 188–202, 2007.

[30] Jue Wang and Dina Katabi. Dude, where's my card?: Rfid positioning that works with multipath and non-line of sight. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, SIGCOMM '13, pages 51–62, New York, NY, USA, 2013. ACM.

[31] R. A. Leibler S. Kullback. On information and sufficiency. *The Annals of Mathematical Statistics*, 22(1):79–86, 1951.

[32] Solomon Kullback. Letter to the editor: the kullback-leibler distance. 1987.

[33] H. Han, F. Xu, C. C. Tan, Y. Zhang, and Q. Li. Defending against vehicular rogue aps. In *INFOCOM, 2011 Proceedings IEEE*, pages 1665–1673, April 2011.