PEDR: A Novel Evil Twin Attack Detection Scheme Based on Phase Error Drift Range

Jiahui Zhang[1], Qian Lu[1,2], Ruobing Jiang[1(✉)], and Haipeng Qu[1]

[1] Department of Computer Science and Technology, Ocean University of China, Qingdao, China
{izjh,luqian}@stu.ouc.edu.cn, {jrb,quhaipeng}@ouc.edu.cn
[2] College of Computer Science and Technology, Qingdao University, Qingdao, China

Abstract. In recent years, wireless local area networks (WLANs) have become one of the important ways to access the Internet. However, the openness of WLANs makes them vulnerable to the threat of the evil twin attack (ETA). Existing effective ETA detection solutions usually rely on physical fingerprints. Especially fingerprints made by information extracted from channel state information (CSI) are more reliable. However, demonstrated by our experiment, the fingerprint of the state-of-the-art ETA detection scheme, which is based on phase error extracted from CSI, is not stable enough, and it results in a large number of false negative results in some cases. In this paper, we present a novel ETA detection scheme, called PEDR, which uses range fingerprint extracted from CSI to identify the evil twin (ET). Inspired by the significant observation that the phase error will drift over time, the concept of drift range fingerprints is proposed and exploited to improve ETA detection accuracy in real-world attack scenarios. Range fingerprints are not affected by drift in phase error and can be uniquely identified. The proposed range fingerprint is implemented and extensive performance evaluation experiments are conducted in the large-scale experiment with 27 devices. The experimental results demonstrate that the detection rate of PEDR is close to 99% and the false negative data is only 1.11%. It is worth mentioning that PEDR is outstanding in the scenario with similar device fingerprints.

Keywords: Evil twin attack · Rogue access point detection · WLAN security · Wi-Fi security · Channel state information

1 Introduction

In recent years, wireless local area networks (WLANs) are rapidly gaining popularity due to the widespread development of wireless network technology and the explosive growth of portable devices. Compared with wired networks, WLAN is more flexible and easier to be installed and expanded, so many wireless access

N. Park et al. (Eds.): SecureComm 2020, LNICST 336, pp. 188–207, 2020.
https://doi.org/10.1007/978-3-030-63095-9_10

points (APs) are deployed in various places such as homes, campuses, hotels, fast food restaurants, airports and shopping centers. As the core device of WLAN, AP provides an effective connection between wired networks and WLANs. Users can access the network freely through APs. Therefore, WLANs provide users with great convenience to access the network and become an integral part of life.

However, the openness and convenience of WLANs bring enormous security risks to wireless users [1]. The ETA is the most prominent one. The ET, also known as the phishing AP, refers to a fraudulent AP established by an attacker. ET tricks wireless users through mimicking the Service Set Identity (SSID) and MAC address (BSSID) of a legitimate AP, as shown in Fig. 1. According to the IEEE 802.11 standard, the client operating system usually selects the AP with the same SSID based on Received Signal Strength Indicator (RSSI). The attacker will exploit this weakness to induce the user to connect to ET by using various means. For example, the attacker can conduct the denial-of-service attack against the legitimate AP or provide a stronger RSSI than the legitimate AP.

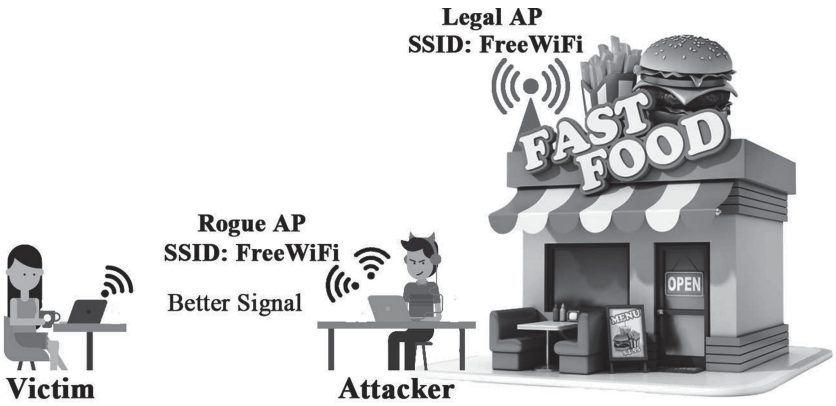


Fig. 1. Illustration of ETA attack scene. The attacker establishes ET by imitating the parameters of the legitimate AP. ET attracts users by providing stronger RSSI.

Once a user has inadvertently connected to an ET, she will face serious consequences such as sensitive information leakage, traffic hijacking and other malicious attacks. For example, the attacker can snoop on the sensitive personal information of the victim, such as photos, emails, various login passwords and bank card information, according to the packets sent to ET by the user. The attacker can also manipulate DNS server/communication, launch a DNS spoofing attack [2], hijack the victim to visit the malicious website [3], and cause direct economic loss to the victim. Moreover, the victim connected to ET may suffer SSL Strip Attacks [4], which strip the SSL layer from the original HTTPS connection and force the victim's data to be sent in plain text format. Thus encryption function is deprived.

Because ETA poses a significant threat to wireless users, researchers have done much work on the ETA detection. Based on whether it can be deployed independently on the client and provide real-time detection for wireless users, the existing detection schemes can be divided into two types in this paper: admin-based and client-based. Specifically, although admin-based detection schemes defend ETA to a certain extent, they all require additional hardware equipments or higher permissions to achieve detection. It means that independent real-time detection cannot be provided by admin-based detection schemes. For example, Brik et al. [5] and Nguyen et al. [6] proposed schemes based on radio frequency fingerprint (RFF); In the study [7], researchers determined the target AP's legitimacy according to its network access method which is judged by the wireless traffic flowing through the gateway. On the other hand, some researchers proposed client-based detection schemes. For example, Arackaparambi et al. [8] detected ETA by using inter-packet arrival time (IAT) and clock skew. Lu et al. [9] used the forwarding behavior of ET. ETA can be determined by comparing the 802.11 data frames sent by target APs to users. The state-of-the-art research [10] proposed a detection scheme based on the non-linear phase errors extracted from CSI. Although these schemes can provide users with independent security detection, there are still many limitations in terms of detection rate and attack model.

In this paper, we innovatively use the phase error drift range as the physical device fingerprint for ETA detection on the basis of the study [10]. Specifically, Liu et al. [10] discovered that the non-linear phase error in CSI can be used as the device fingerprint. However, a large number of experimental results confirm that the phase errors have drift phenomenon. Drift phenomenon may cause fingerprints of different devices to overlap each other, and result in failure of Liu's method [10]. In addition, we found that the phase error drift range always remains relatively stable in the time dimension. Based on this observation, PEDR uses the drift range of phase errors as the wireless device fingerprints. In our scheme, the phase error drift range, instead of the phase errors, is used as the device fingerprint, which overcomes the shortcomings of false positives and false negatives due to drift phenomenon. At the same time, PEDR is deployed on the user client, and it can provide users with real-time detection without additional hardware equipments or protocol modification.

In summary, we make the following contributions to the field of WLAN security in our paper:

- Through a large number of experimental observations, we find that the non-linear phase errors extracted from the CSI have drift phenomenon. In other words, if only the phase error is used as the fingerprint, the wireless device cannot be uniquely identified.
- Based on the phase error drift phenomenon, we innovatively use the phase error drift range as the physical fingerprint of the device to identify the ETA. A new detection scheme PEDR deployed on the client is proposed. Compared with admin-based solutions, PEDR can better meet the needs of users, and does not require any additional overhead on wireless devices.

– Extensive simulation experiments are performed with 27 devices. The experimental results prove that the detection rate of ETA by PEDR was close to 99%. Especially for devices with similar phase errors, the detection effect of PEDR is more noticeable than Liu's method [10].

The rest of the paper is organized as follows: Sect. 2 introduces the work related EAT detection. Section 3 briefly introduces the background of CSI and the empirical research of PEDR. Section 4 details the modules of PEDR. In Sect. 5, we demonstrate the feasibility of fingerprints and perform a performance evaluation of PEDR. Finally, we summarize the paper in Sect. 6.

2 Related Work

Due to the great perniciousness of ETA, researchers in the field of wireless network security have conducted extensive research on ETA detection, and they proposed several solutions. A large amount of existing work is usually classified based on the detection model, additional hardware and advanced permissions requirements, etc. [11]. In this paper, whether the detection scheme can provide users with real-time efficient and independent detection is used as the classification standard. We accordingly divide existing detection schemes into two categories: admin-based and client-based.

2.1 Admin-Based ETA Detection Schemes

In the admin-based ETA detection schemes, higher permissions, additional hardware equipments, or protocol modification are required to achieve the ETA detection. In other words, it is difficult for users to conduct real-time ETA detection independently by using admin-based schemes, because most admin-based solutions require information that is hard for ordinary users to collect.

Gonzales et al. proposed a scheme to defend ETA by modifying the existing protocol, called Simple Wireless Authentication Technique (EAP-SWAT) [12,13], which is an extension of the Extensible Authentication Protocol (EAP). EAP-SWAT leverages SSH's Trust On First Use (TOFU) security model. Specifically, if the security of the first connection with the AP can be assured, TOFU can ensure that subsequent connections to this AP will not be spoofed. In addition, researchers in the study [14] also proposed a method that required protocol modification, Secure Open Wireless Access (SOWA). SOWA binds the SSID of the AP with a digital certificate to verify the operator of the AP and determines whether the target AP is legitimate. The solution proposed by Kumar et al. [15] uses a connection count table established between each client and AP to assist users in ETA detection. The connection counts of both parties will increase while the client and the AP are successfully connected. By comparing the values in both tables, the counts of successful connections between each client and AP are confirmed to prevent wireless users from accessing the ET. Unfortunately, this solution has many flaws. For example, both the AP and probe response frame must be adjusted, and

the client operating system also needs to be modified to establish a counter. The above solutions could defend ETA to a certain extent, but all need to modify the existing protocol, driver, or firmware. Therefore, all of the above solutions are difficult to be implemented easily.

Some researchers [5,6,16] proposed RFF-based methods to identify ETA. By monitoring Radio Frequency (RF) waves, the hardware defects in the network card can be obtained. RFF can be acquired by combining hardware defects and other information such as the SSID and RSSI of the device. In short, the researchers utilize the physical characteristics obtained from the radio signal to identify the ETA. The scheme based on RFF can resist the influence of mobility, noise, and hardware aging, and it achieves a very high detection rate in the experimental scenario. However, the detection in a real scenario requires special wireless sensors to continuously monitor the RF signal sent by the AP. Obviously, this kind of schemes is difficult to be deployed on a large scale.

Wei et al. [7] proposed the method of using the network traffic passing through the gateway to detect ETA, and similar schemes were also proposed in studies [17–22]. Specifically, two parameters, the fraction of TCP flows and the degree of belief that a TCP flow traverses a WLAN inside the network, can be calculated by the iterative Bayesian inference algorithm; they can be used to determine whether client traffic comes from wireless or wired connection according to the difference of network protocol. Unfortunately, capturing the wireless traffic flowing through the gateway requires advanced permissions that ordinary users cannot obtain. In addition, the algorithm used in the study requires a certain amount of time to converge. Therefore, it is difficult to provide users with real-time security detection.

2.2 Client-Based ETA Detection Schemes

The second type of detection scheme is client-based detection schemes which can be independently deployed on the client. Compared with admin-based solutions, it can provide users with real-time ETA detection. However, the existing client-based solutions still have limitations in several aspects, such as detection rates, detection efficiency [23] and detection scenarios, etc.

Jana et al. [24] first used clock skew as the unique fingerprint for ETA detection. Clock skew is calculated by the timing synchronization function timestamp extracted from the beacon frame. Arackaparambil et al. [8] improved the above work and proposed a more accurate detection. It can be achieved by comparing the beacon frame timestamp generated by the AP with the IAT of the client packets. The IAT is extracted from the Radiotap header and represents the difference between the arrival times of two sequential frames. Song et al. [25,26] believed that additional propagation delays will be introduced due to the wireless connection between ET and legitimate APs. The user can determine whether the client is directly connected to the legitimate AP by using the IAT. Neumann et al. [27] evaluated a variety of network parameters and concluded that using IAT as a signature to identify the ETA is ideal. Although the above methods are effective, the

IAT lacks robustness and will change due to various factors [28], such as the fluctuation of wireless signals and the increase of wireless traffic. Therefore, the detection rates are difficult to satisfy users. In addition, the diversity of attack models will directly cause the failure of the detection.

Alotaibi et al. proposed a method that uses Radiotap length (PLL) as the fingerprint in the study [29]. ETA can be detected by comparing the PLL extracted from the target AP with the legitimate device fingerprint in the fingerprint library. Although this method has a high detection rate and does not require additional equipments, unfortunately, collecting information about all legitimate APs results in a huge amount of work and the scheme is only valid for ETs built by soft APs.

The application of CSI has gradually matured in recent years [30]. As physical layer information, CSI has been widely used in localization and action recognition. Therefore some researchers have begun to use CSI for ETA detection. For example, Liu et al. [31] proposed that the ETA detection can be implemented by using the amplitude information in CSI. Specifically, this solution combines the amplitude and the position information as a device fingerprint to detect ETA. However, multiple monitors are required to collect wireless packets in the scheme. In addition, the scheme requires that the detection terminal equipment must be static, which is impractical in a real scenario. Hua [32] used the carrier frequency offset (CFO) estimated from CSI as the device fingerprint to realize the ETA detection. CFO is based on the instability of the oscillator drift caused by the crystal imperfection. Compared with directly using CSI, CFO is not affected by the environment and remains stable with time. Although the scheme based on CFO achieves successful detection, it is difficult to meet the condition that the equipment needs to be stationary during the detection process, which will lead to unsatisfactory detection results. Zhuo et al. [33] first proposed the existence of non-negligible non-linear phase errors in CSI, and they pointed out that non-linear phase errors are caused by I/Q imbalance. Based on the above achievements, Liu et al. [10] used non-linear phase errors as fingerprints for ETA detection. The phase error is not affected by temperature, physical location, and it can play a good effect on some attack scenarios. However, according to our experiments and observations, the detection scheme will produce false negative results in scenarios where the phase errors of the equipments are similar. The specific content will be detailed in Sect. 3.

3 Empirical Study

In this section, the basic knowledge of CSI is first introduced, and the experiment in the study [10] is reproduced. We describe the phenomenon, phase errors drift, found in the experimental results, and further observe the characteristics of the phase error drift phenomenon.

3.1 Background

CSI is the channel attribute of wireless communication links. It describes the attenuation characteristics of wireless signals on each propagation path. The attenuation characteristics combine multiple effects such as delay, ambient scattering, amplitude attenuation and phase offset. Besides, CSI includes the amplitude and phase information of each subcarrier in the frequency domain space. The amplitude and phase contain the inherent properties of the wireless communication devices. Therefore, CSI is widely used in the fields of localization, identification, and environmental perception.

In the study [10], the non-linear phase errors were proposed as a fingerprint of the hardware device to detect ETA. Non-linear phase errors are caused by the I/Q imbalance and oscillator defects. Liu et al. derived the Eq. (1) for calculating the non-linear phase error E. The equation is as follows:

$$E = \Phi - (2\pi\lambda \cdot K + Z^*), \tag{1}$$

where Φ is the phases of subcarriers measured at the receiver. The parameter K contains subcarrier index. Z^* includes the true phase and a constant. The parameter λ is also a constant and will change across sampled CSIs. It is related to frame detection delay (FDD), sampling frequency offset (SFO) and time of flight (TOF) which affect the phase error. In order to obtain a stable fingerprint, the author used special λ which makes the phase errors of the subcarrier -28 and 28 equal to 0 to remove the effects of FDD, SFO and TOF.

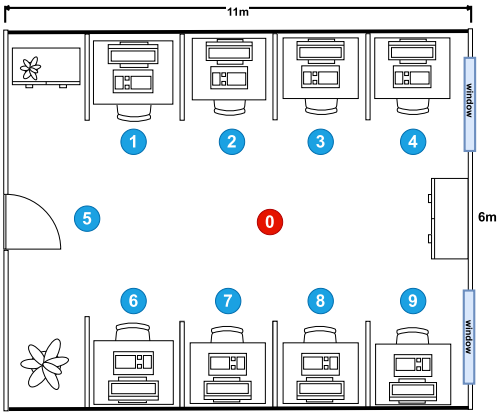


Fig. 2. Experiment scene: 1–9 are the positions of the target devices; 0 is the position of the detection terminal.

3.2 Setup

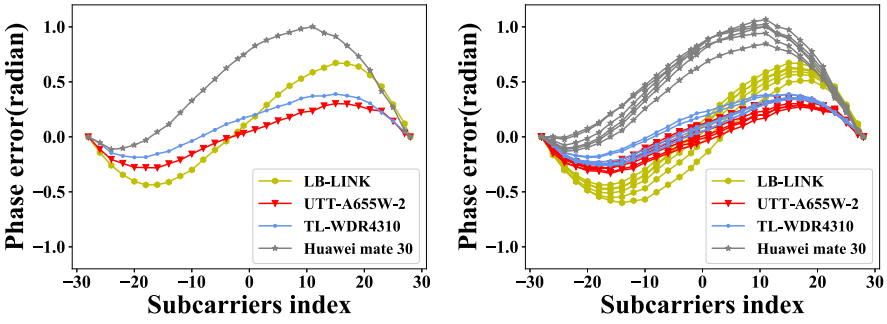
In order to reproduce the experiment, the same experimental scenario was set up according to the study [10]. The detection terminal of the experiment was

a Thinkpad SL410 equipped with Intel 5300 NIC and it ran Ubuntu 12.04 LTS system. The Linux 802.11n CSI Tool was installed to collect CSI. We selected four different wireless devices and placed them in positions 1–4 in Fig. 2. The laptop was placed in position 0 as the detection terminal to connect target devices and collect the CSI information. In order to collect CSI, the detection terminal first sent ICMP messages to the wireless AP and estimated the CSI based on the response frame. The shortest interval of ICMP messages in the experimental scenario of study [10] was 5 ms, and the collection time was 10 s. Therefore, in the verification experiment, we used the same sending interval and collecting time. That is, about 200 frames containing CSI were collected every second. For each wireless AP, a total of 10 groups of data were collected, the interval between each group was 30 s. Each group of data collection took 10 s, and a total of 2000 packets containing CSI information were collected.

3.3 Observation

According to the method mentioned by Liu et al. in the study [10], the expected experimental results are shown in Fig. 3a. The abscissa represents the subcarrier index, and the ordinate represents the value of phase error. Each hardware device has an invariable and unique phase error fingerprint. Unfortunately, from the results of the reproduction experiment, we can observe the following phenomenon which is obviously different from the expected experimental results.

Phase Error Drift Phenomenon (PEDP): PEDP refers to the phenomenon that the phase errors will change to some extent at different times. In other words, the phase error curve will drift instead of staying fixed. This phenomenon will have many effects. For example, devices with similar phase errors will overlap due to PEDP, which will lead to the failure of detection based on phase errors.

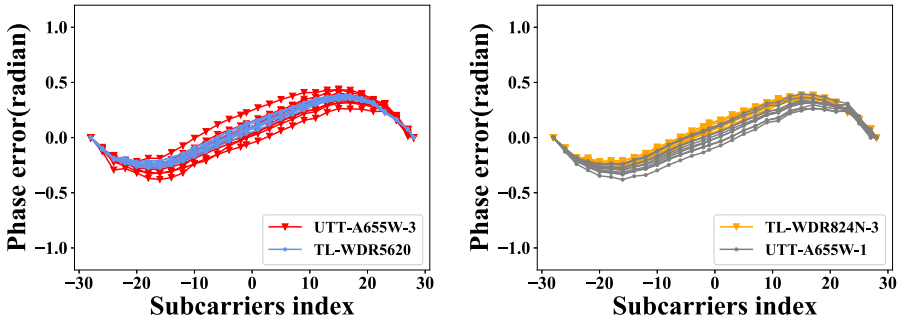


(a) Experimental result obtained by a single collection according to Liu et al.'s method.

(b) Experimental result obtained by multiple collections according to Liu et al.'s method.

Fig. 3. Expected experimental results and actual experimental results.

The common occurrence of PEDP in hardware devices will lead to the failure of detection work based on phase error. Figure 3b depicts the phase errors of four devices. Apparently, all devices produced PEDP with intervals of only 30 s. In addition, it can be clearly observed that the fingerprints of UTT-A655W-2 and TL-WDR4310 partially overlap due to PEDP. In small-scale experiments with only four wireless AP devices, there are two devices that have phase errors overlapping because of the PEDP. Then, the overlapping phenomenon could not be ignored in large-scale experiments. Therefore, in order to verify the universality of overlapping phenomenon caused by the PEDP, we expanded the scale of the experiment to 27 devices. Table 1 shows the specific types and quantities of devices. The experimental results show that the overlapping phenomenon is common in AP equipment. In addition to the overlapping phenomenon of phase errors that occurred in the above equipment, we also found the other two groups of AP equipment also have similar overlapping phenomenon, as shown in Fig. 4a and b. Therefore, attackers can make use of the phenomenon that overlap caused by PEDP to deceive detection. If an attacker deliberately chooses a device with a fingerprint similar to a legitimate AP, Liu's method will generate a lot of false negatives, which will lead to a failure of detection.



(a) Case 1 of phase error overlap. (b) Case 2 of phase error overlap.

Fig. 4. Devices with similar phase errors overlap due to PEDP.

In summary, although the scheme based on phase error will achieve a high detection rate when the phase errors between ET and the legitimate device are significantly different, it could produce non-negligible false negatives when the target device and the legitimate device have similar phase errors. In short, due to the instability of the phase error caused by PEDP, the fingerprints will overlap. The overlap phenomenon provides an opportunity for attackers to cause the failure of the Liu's method. At the same time, we found that the drift of the phase error is regular, and the phase error of each device drifts within a unique range. Therefore, we consider that using the drift range of phase errors as the fingerprint will achieve higher accuracy detection.

4 Proposed Approach

A novel ETA detection system PEDR is proposed, which is used to detect the legitimacy of target APs. PEDR uses the drift range of the phase errors as the fingerprint, it overcomes the shortcoming of false negatives caused by PEDP. In this section, we will introduce the components of the PEDR system and the process of detecting the target device.

4.1 Overview of PEDR

The PEDR we proposed is a novel and effective ETA detection scheme. As shown in Fig. 5, PEDR is divided into two parts: the fingerprint library establishment and the legitimacy detection.

Fingerprint Library Establishment: This module is responsible for establishing a legitimate fingerprint library. The legitimate fingerprint library is used for verification and comparison with the fingerprint of target AP during the legitimacy detection process. For each legitimate AP device, fingerprint can be obtained by collecting and processing enough CSI data. The fingerprint is divided into two parts: function expressions and distribution area. The function expressions represent the upper and lower boundaries of the phase error drift range; the distribution area is used to represent the area of the phase error drift. Both are regarded as the fingerprint and added to the legitimate fingerprint database.

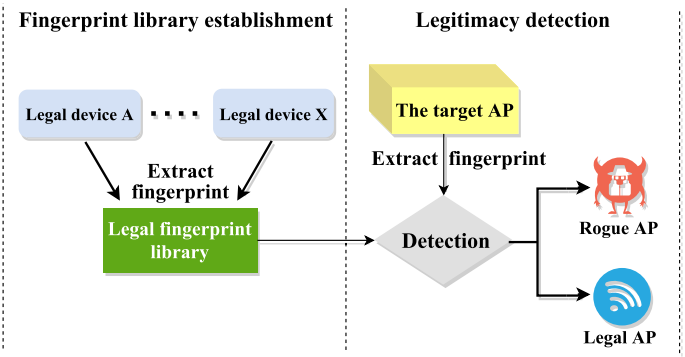


Fig. 5. The overview of PEDR.

Legitimacy Detection: This module is the core part of the PEDR system which is responsible for the legitimacy detection of target APs. The detection terminal collects CSI data by connecting to the target AP and the fingerprint can be made by phase errors extracted from the CSI data. Based on the SSID and MAC of the target AP, the corresponding legitimate fingerprint is extracted from the legitimate fingerprint database, and it will be used to check the legitimacy of the target AP.

Algorithm 1. Generating the device's fingerprint

Require: $Info_{LAP}$: the SSID, MAC and phase error set of legitimate AP;
Ensure: FP_i: Legitimate device fingerprint;
1: Calculating the max and min phase error values from $Info_{LAP}$ on each subcarrier;
2: Getting new functions by separately fitting the max and min values with $AX^3 + BX^2 + CX + D$;
3: $FP_i['F_{max}\ ']= \alpha X^3 + \beta X^2 + \gamma X + \theta$;
4: $FP_i['F_{min}\ ']= \alpha' X^3 + \beta' X^2 + \gamma' X + \theta'$;
5: Calculating the distribution area S by the definite integral;
6: $FP_i['S']=$ The value of the distribution area S;
7: Output FP_i;

4.2 Fingerprint Library Establishment

Before the legitimacy detection, each legitimate device needs to be constructed a unique fingerprint to establish the legitimate fingerprint database. PEDR uses the drift range of phase errors as the device fingerprint. The feasibility of the fingerprint is verified in Sect. 5.

For each experimental device, in order to make a fingerprint based on phase error drift range, the maximum range of phase error drift must be obtained. Therefore, the detection terminal needs to collect a sufficient amount of CSI data and estimates the phase error from it. The bound functions (F_{max}, F_{min}) of the drift range are obtained by fitting the extrema of phase errors on each subcarrier with the function $AX^3 + BX^2 + CX + D$. PEDR uses the functions obtained by the fitting technique to represent the drift range of the phase error, which is more intuitive. In addition, the phase error distribution area S on the phase error graph is determined by the definite integral method. The fitting functions (F_{max}, F_{min}) and the distribution area S are stored in the dictionary FP_i as the fingerprint of the device. The construction algorithm of FP_i is shown in Algorithm 1, and the data structure of FP_i is shown as Eq. (2). Finally, fingerprints of all legitimate APs are collected to establish the legitimate fingerprint library.

Compared with the phase error-based scheme, PEDR overcomes the defect of false negatives caused by PEDP. The result of the verification experiment in Sect. 5 further determined the feasibility using the phase error drift range as the fingerprint.

$$\begin{aligned} FP_i = \{&SSID : XXXX, \\ &MAC : XX : XX : XX : XX : XX : XX, \\ &F_{max} : \alpha X^3 + \beta X^2 + \gamma X + \theta, \\ &F_{min} : \alpha' X^3 + \beta' X^2 + \gamma' X + \theta', \\ &S : 0.00\} \end{aligned} \tag{2}$$

4.3 Legitimacy Detection

The core of legitimacy detection is to compare the target AP fingerprint with the corresponding legitimate fingerprint. The fingerprint of the target AP needs to be made before comparing it with the legitimate fingerprint. When the detection terminal is connected to the target AP, it sends ICMP messages with an interval of 5 ms to the target AP for 10 s. Each time the target AP returns response packets, the detection terminal collects a group of CSI data. The collected data is used to make the fingerprint FP' of the target AP, that is, the upper and lower bound fitting functions (F'_{max}, F'_{min}) and the distribution area S'. The legitimate fingerprint FP_i is extracted from the legitimate fingerprint library according to the SSID and MAC address of the target AP. The first step in comparison verification is determining the difference between two fingerprints based on the number of intersections between the upper and lower bounds of the target AP and the legitimate AP.

On the one hand, if there are three intersections between F_{max} and F'_{max} (or F_{min} and F'_{min}), the two fingerprints are in a cross relationship, as shown in Fig. 6a. PEDR considers that the target AP fingerprint is different from the legitimate AP fingerprint. That is, the target AP is an illegitimate AP. Specifically, since phase errors of subcarriers 28 and −28 are both 0, there are at least two intersections between the boundary functions. Therefore, if there is a third intersection between F_{max} and F'_{max} (or F_{min} and F'_{min}) in the range of subcarriers −28 to 28, it means that the boundaries in the fingerprints crosse each other, and the two fingerprints are clearly different. The target AP is considered an ET.

On the other hand, if there is no third intersection, it means that the target AP fingerprint and the legitimate fingerprint are contained, separated, or partially overlapped, as shown in Fig. 6b, c, d, e and f. The legitimacy of the target AP needs to be further judged. We define the values of $F_{max}(0)$, $F'_{max}(0)$, $F_{min}(0)$, and $F'_{min}(0)$ as the zero value of boundaries, and $F_{max}(0) - F'_{max}(0)$, $F_{min}(0) - F'_{min}(0)$ are respectively defined as the upper and lower bound zero point difference values D_{up}, D_{bot}. Based on this, the specific positional relationship between the two fingerprints can be distinguished. If the result of $D_{up} \times D_{bot}$ is positive, it means that the fingerprints are partially overlapped or separated, and the target device is judged as an ET. Otherwise, the D_{up} is used for further judgment. If $D_{up} < 0$, it means that the upper and lower bounds of the target AP are outside the range of the legitimate fingerprint, as shown in Fig. 6c. The target AP fingerprint contains the legitimate fingerprint, and the device is illegitimate. If $D_{up} > 0$, it means that all phase errors of the target AP are within the range of legitimate fingerprint. In other words, the legitimate fingerprint contains the target fingerprint, but there may be some differences in the fingerprint distribution range, as shown in Fig. 6b and f. Therefore, the phase error distribution area S is used to distinguish the fingerprint distribution of the two devices. At this moment, the threshold TSV is introduced. If the absolute value of the difference between S' and S is less than TSV, PEDR considers that the two fingerprints are coincident and the target AP is legitimate. Otherwise, the

Algorithm 2. Detecting the legitimacy of target AP

Require: $Info_{TAP}$: the SSID, MAC and fingerprint of target AP;
$Dict_{LF}$: the dictionary stored legitimate devices's fingerprints;
Ensure: The legitimacy of the target AP;
1: Extracting Legitimate fingerprint FP from $Dict_{LF}$ based on the SSID and MAC of target AP;
2: Seeking the intersection number N_{max} of F_{max} and F'_{max} on the subcarriers -28 to 28;
3: Seeking the intersection number N_{min} of F_{min} and F'_{min} on the subcarriers -28 to 28;
4: **if** $(N_{max} = 3)$ **or** $(N_{min} = 3)$ **then**
5: Triggering a rogue AP alarm;
6: **Return** rogue AP is detected;
7: **else**
8: calculating $F_{max}(0), F_{min}(0), F'_{max}(0), F'_{min}(0)$;
9: calculating $D_{up} = F_{max}(0) - F'_{max}(0)$, $D_{bot} = F_{min}(0) - F'_{min}(0)$;
10: **if** $(D_{up} \times D_{bot} < 0)$ **and** $(D_{up} > 0)$ **and** $(|S - S'| < S_{TSV})$ **then**
11: **Return** the target AP is legitimate;
12: **else**
13: Triggering a rogue AP alarm;
14: **Return** rogue AP is detected;
15: **end if**
16: **end if**

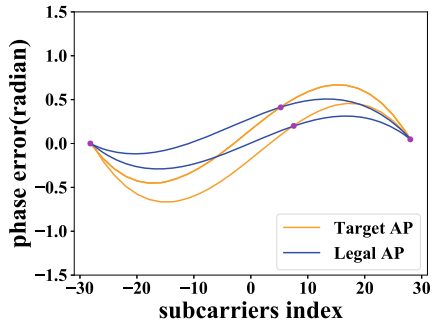
fingerprints are considered included, and the target AP is determined to be an ET. The threshold TSV will be discussed in detail in the verification experiment. The process of verifying legitimately is shown in Algorithm 2.

5 Evaluation

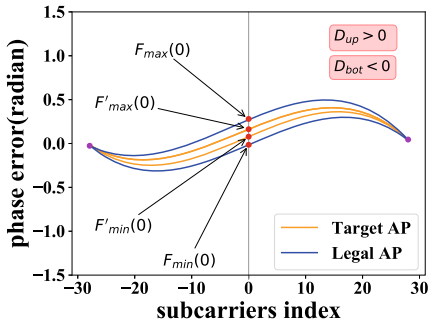
In this section, the experimental setup and experimental environment are first described. Then, it is verified that the drift range of phase errors remains relatively stable, so using phase error drift range as the fingerprint is feasible. Finally, the performance evaluation of PEDR was performed in a simulated scenario. We compared the PEDR system with the existing physical fingerprint detection method, and further explained the rationality and superiority of the fingerprint based on phase error drift range.

5.1 Setup

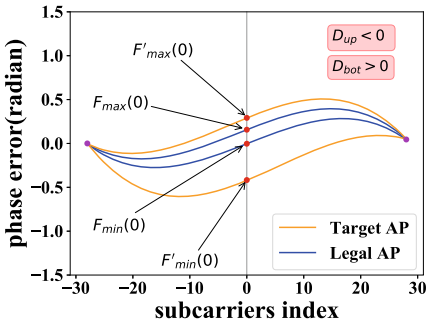
Hardware Implementation: In the experiment, the detection terminal uses the laptop Thinkpad SL410 equipped with Intel 5300 NIC, and the CPU is Intel T6670. It runs Ubuntu 12.04 LTS system. There are 27 devices to be detected, such as wireless routers that can release hotspots, laptops which can turn on soft APs and smartphones. Table 1 shows the specific types and quantities of devices. The validity of fingerprints based on the phase error drift range can be



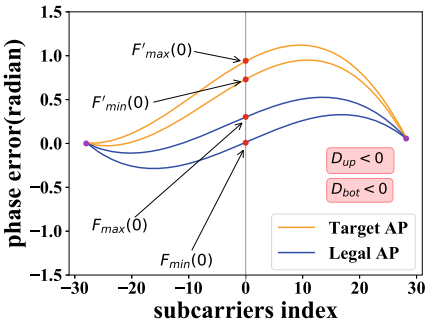
(a) Fingerprints cross each other.



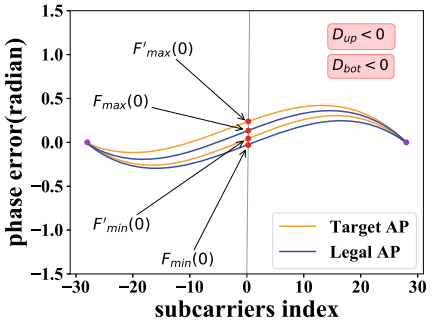
(b) The target fingerprint is contained.



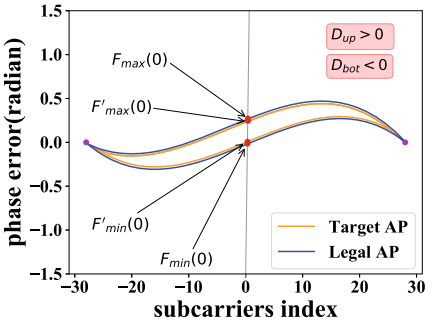
(c) The legitimate fingerprint is contained.



(d) Fingerprints are separated from each other.



(e) Fingerprints partially overlap.



(f) Fingerprint coincidence.

Fig. 6. Position relationship of PEDR fingerprint.

more scientifically explained by using different types of devices as target APs. In addition, experiment results verify that device fingerprints of the same model are also different, which means that attackers cannot use the devices with same model to circumvent PEDR.

Table 1. Type and quantity of device.

Device	Quantity	Device	Quantity
TL-WDR5620	2	UTT-A655W	3
Laptop with AR9588	1	Laptop with AR9580	1
TL-WR824N	4	Huawei mate 30	4
TL-WDR4310	2	Samsung	1
LB-LINK	2	Device with openwrt and AR9531	2
Others	5		

Software Implementation: In terms of software, the kernel of the detection terminal laptop is changed to Linux 4.2.0, and the Linux 802.11n CSI Tool is installed on the detection terminal to collect CSI data under the 802.11n wireless network. In particular, Hostapd is installed in the detected laptop, it can help the laptop to turn on the soft AP.

The experiments are scheduled in the laboratory which is a typical office environment with the size of 11 m × 6 m, and contains desks and other furniture. As shown in Fig. 2, the position of the serial number 1–9 is used to place the target equipment, and the detection equipment is placed in the position 0. Obviously, the target devices in different positions can provide different CSI information, which is more helpful to verify the validity of the fingerprint.

5.2 Verification

In this section, experiments in a real network environment have confirmed that the phase errors drift in a relatively stable range. At the same time, the experimental results show that the difference in fingerprints of different devices is obvious and using the phase error range as the device fingerprint can be uniquely identified. Therefore, the feasibility of using phase error drift range as the fingerprint can be explained.

Fingerprint Feasibility: In order to verify the feasibility of using the phase error drift range as the fingerprint, it must be investigated whether the device fingerprint can remain relatively stable. By studying the change of the phase error distribution area of the device over a period of time, the stability of the device fingerprint can be judged. We randomly selected 4 different types of APs and successively placed them in the same place (e.g., position 1 in Fig. 2). For each AP device, data collection was performed daily, and 10 groups of data were collected each time for 15 consecutive days. When collecting each set of data, the detection terminal needed to connect to the target AP. Considering the packet loss rate and network conditions, we set the sending interval to 5 ms. That is, the detection terminal sent the ICMP messages with the interval of 5 ms to the target AP for 10 s. When the target AP returned response packets, the CSI information was collected and processed to obtain the drift range of the phase errors over

time. In order to intuitively display the variation of fingerprints, we plotted the change of the phase error distribution area within 15 days, and evaluated the stability of the phase error drift range on the time dimension. Figure 7 shows the curve of the phase error distribution area of the four devices at different time periods. Obviously, the phase error distribution area of the 4 devices can remain stable in the time dimension, and we can design the legitimacy detection threshold TSV accordingly. The experimental results prove that the phase error drift range remains relatively stable in time.

According to our experimental results, the phase error drift range fingerprint is relatively stable, and the fingerprints are significantly different between different devices. Therefore, fingerprints based on the phase error drift range are feasible.

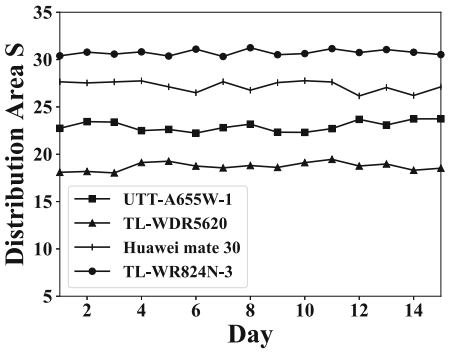


Fig. 7. Variation of phase error distribution area of four devices.

Efficiency: We conducted extensive experiments on the PEDR system, and evaluated both the detection rate and the false negative rate. Besides, we compared PEDR with the latest Liu's method to illustrate the superiority of the fingerprint based on phase error drift range.

The ETA scenario was simulated, and the two parameters, detection rate and false negative rate, were introduced to evaluate the system performance. The detection rate indicates the probability that the detection system can successfully detect the ET in the attack scenario. The false negative rate refers to the probability that ET is not found. In the experiment, 9 devices were randomly selected from 27 experimental devices as illegitimate devices to simulate ETA. In the simulation experiment scenario, the PEDR and Liu's method were used for detection respectively, and the experimental results of the two were compared. During the experiment, the detection terminal extracted CSI information from each target device and made fingerprints to detect its legitimacy. In order to ensure the accuracy and rationality of the experiment, we performed a legitimacy detection experiment 10 times a day for 10 days, and took the average value of the attack detection rate measured multiple times a day for statistics. The

results of PEDR and Liu's method are shown in Figs. 8 and 9 respectively. Due to the existence of devices with similar phase errors in the experiment, the phase errors of these devices have overlapped each other due to PEDP. Liu 's method which based on phase error is difficult to distinguish such target devices, and it is easy to generate false negative results. Therefore, the false negative rate of Liu's method is as high as 15.56%, while the attack detection rate is only maintained at about 84.44%. Compared with Liu's method based on phase error, PEDR uses the phase error drift range as the fingerprint. Although it takes a certain amount of time to collect fingerprints, it overcomes the defect of false negative results caused by phase errors drift with time and can achieve more accurate detection. After 10 days of the simulation experiment. The detection rate of PEDR is still stable and as high as 98.89%, and only a few cases have a false negative rate of 1.11%.

The experimental results prove that the PEDR system can implement the legitimacy detection more successfully. Especially when the devices with only slight differences in phase errors, PEDR can also achieve high-precision detection. We believe that the detection environment and target devices will be more complicated in actual scenarios, and the probability of devices with similar phase errors will increase significantly. PEDR has a higher detection rate, which can effectively detect ETA and protect the safety of the device.

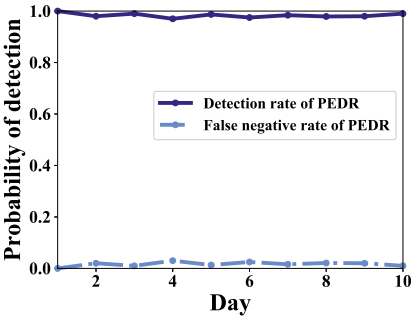


Fig. 8. Detection rate and false negative rate of PEDR.

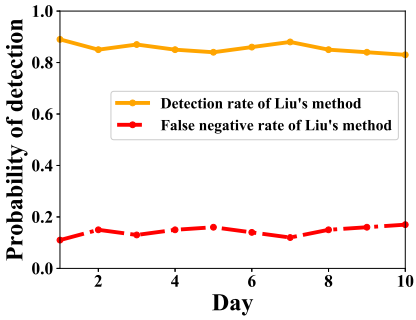


Fig. 9. Detection rate and false negative rate of Liu's method.

6 Conclusion

Validated by our experiments, the phase error drift phenomenon, i.e. PEDP, is widespread in wireless devices, which may cause the failure of detection scheme based on phase errors. In order to achieve higher precision ETA detection, we proposed the legitimacy detection scheme PEDR based on the phase error drift range. Because the phase error drift range remains stable in the time dimension, PEDR can effectively detect ETA. Especially for devices with similar phase

errors, the detection effect of PEDR is outstanding. Therefore, attackers cannot use the equipment with the same model to avoid detection, which improves the security between the AP and client devices. In addition, PEDR is based on the user client and does not require additional hardware equipment, which makes it more lightweight and practical. Compared with the active detection scheme, it is not easy for attackers to find and deceive during the entire detection process. We have conducted extensive experiments and proved that the fingerprint based on the phase error drift range is more effective and reliable than the fingerprint only based on phase error for detecting ETA. In the future, we plan to improve the efficiency of legitimacy detection and on the premise of ensuring the detection rate.

Acknowledgment. The work is partly Supported by China Postdoctoral Science Foundation (Grant No. 2019M652475) and the Fundamental Research Funds for the Central Universities (Grant No. 201813021).

References

1. Lu, Q., Jiang, R., Ouyang, Y., et al.: BiRe: a client-side bi-directional SYN reflection mechanism against multi-model evil twin attacks. Comput. Secur. **88**, 101618 (2020)
2. van Rijswijk-Deij, R., Sperotto, A., Pras, A.: DNSSEC and its potential for DDoS attacks: a comprehensive measurement study. In: Proceedings of the 2014 Conference on Internet Measurement Conference, pp. 449–460 (2014)
3. Lu, Q., Qu, H., Ouyang, Y., et al.: SLFAT: client-side evil twin detection approach based on arrival time of special length frames. Secur. Communi. Netw. **2019** (2019)
4. Marlinspike, M.: More tricks for defeating SSL in practice. Black Hat USA (2009)
5. Brik, V., Banerjee, S., Gruteser, M., et al.: Wireless device identification with radiometric signatures. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, pp. 116–127 (2008)
6. Nguyen, N.T., Zheng, G., Han, Z., et al.: Device fingerprinting to enhance wireless security using nonparametric Bayesian method. In: 2011 Proceedings IEEE INFOCOM, pp. 1404–1412. IEEE (2011)
7. Wei, W., Jaiswal, S., Kurose, J.F., et al.: Identifying 802.11 traffic from passive measurements using iterative Bayesian inference. In: INFOCOM (2006)
8. Arackaparambil, C., Bratus, S., Shubina, A., et al.: On the reliability of wireless fingerprinting using clock skews. In: Proceedings of the Third ACM Conference on Wireless Network Security, pp. 169–174 (2010)
9. Lu, Q., Qu, H., Zhuang, Y., et al.: A passive client-based approach to detect evil twin attacks. In: 2017 IEEE Trustcom/BigDataSE/ICESS, pp. 233–239. IEEE (2017)
10. Liu, P., Yang, P., Song, W.Z., et al.: Real-time identification of rogue WiFi connections using environment-independent physical features. In: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, pp. 109–198. IEEE (2019)
11. Agarwal, M., Biswas, S., Nandi, S.: An efficient scheme to detect evil twin rogue access point attack in 802.11 Wi-Fi networks. Int. J. Wirel. Inf. Netw. **25**(2), 130–145 (2018)

12. Bauer, K., Gonzales, H., McCoy, D.: Mitigating evil twin attacks in 802.11. In: 2008 IEEE International Performance, Computing and Communications Conference, pp. 513–516. IEEE (2008)
13. Gonzales, H., Bauer, K., Lindqvist, J., et al.: Practical defenses for evil twin attacks in 802.11. In: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, pp. 1–6. IEEE (2010)
14. Byrd, C., Cross, T., Takahashi, T.: Secure open wireless networking. Black Hat (2015)
15. Kumar, A., Paul, P.: Security analysis and implementation of a simple method for prevention and detection against Evil Twin attack in IEEE 802.11 wireless LAN. In: 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), pp. 176–181. IEEE (2016)
16. Bahl, P., Chandra, R., Padhye, J., et al.: Enhancing the security of corporate Wi-Fi networks using DAIR. In: Proceedings of the 4th International Conference on Mobile Systems, Applications and Services, pp. 1–14 (2006)
17. Wei, W., Wang, B., Zhang, C., et al.: Classification of access network types: ethernet wireless LAN, ADSL, cable modem or dialup? In: Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 2, pp. 1060–1071. IEEE (2005)
18. Wei, W., Suh, K., Wang, B., et al.: 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 (2007)
19. Yin, H., Chen, G., Wang, J.: Detecting protected layer-3 rogue APs. In: 2007 Fourth International Conference on Broadband Communications, Networks and Systems (BROADNETS'07), pp. 449–458. IEEE (2007)
20. Shetty, S., Song, M., Ma, L.: Rogue access point detection by analyzing network traffic characteristics. In: MILCOM 2007-IEEE Military Communications Conference, pp. 1–7. IEEE (2007)
21. Baiamonte, V., Papagiannaki, K., Iannaccone, G.: Detecting 802.11 wireless hosts from remote passive observations. In: Akyildiz, I.F., Sivakumar, R., Ekici, E., Oliveira, J.C., McNair, J. (eds.) NETWORKING 2007. LNCS, vol. 4479, pp. 356–367. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72606-7_31
22. Watkins, L., Beyah, R., Corbett, C.: A passive approach to rogue access point detection. In: IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference, pp. 355–360. IEEE (2007)
23. Xia, H., Li, L., Cheng, X., et al.: Modeling and analysis botnet propagation in social Internet of Things. IEEE Internet Things J. **7**, 7470–7481 (2020)
24. Jana, S., Kasera, S.K.: On fast and accurate detection of unauthorized wireless access points using clock skews. IEEE Trans. Mob. Comput. **9**(3), 449–462 (2009)
25. Song, Y., Yang, C., Gu, G.: Who is peeping at your passwords at Starbucks?-To catch an evil twin access point. In: 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), pp. 323–332. IEEE (2010)
26. Yang, C., Song, Y., Gu, G.: Active user-side evil twin access point detection using statistical techniques. IEEE Trans. Inf. Forensics Secur. **7**(5), 1638–1651 (2012)
27. Neumann, C., Heen, O., Onno, S.: An empirical study of passive 802.11 device fingerprinting. In: 2012 32nd International Conference on Distributed Computing Systems Workshops, pp. 593–602. IEEE (2012)
28. Xia, H., Zhang, R., et al.: Two-stage game design of payoff decision-making scheme for crowdsourcing dilemma. IEEE/ACM Trans. Netw. (2020)
29. Alotaibi, B., Elleithy, K.: A passive fingerprint technique to detect fake access points. In: Wireless Telecommunications Symposium (WTS), pp. 1–8. IEEE (2015)

30. Xia, H., Li, L., Cheng, X., et al.: A dynamic virus propagation model based on social attributes in city IoTs. IEEE Internet Things J. **7**, 8036–8048 (2020)
31. Liu, H., Wang, Y., Liu, J., et al.: Practical user authentication leveraging channel state information (CSI). In: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, pp. 389–400 (2014)
32. Hua, J., Sun, H., Shen, Z., et al.: Accurate and efficient wireless device fingerprinting using channel state information. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications, pp. 1700–1708. IEEE (2018)
33. Zhuo, Y., Zhu, H., Xue, H., et al.: Perceiving accurate CSI phases with commodity WiFi devices. In: IEEE INFOCOM 2017-IEEE Conference on Computer Communications, pp. 1–9. IEEE (2017)