Detecting Rogue Access Points Using Client-agnostic Wireless Fingerprints

YUXIANG LIN, College of Computer Science, Zhejiang University, China & Alibaba Group, China
YI GAO, BINGJI LI, and WEI DONG, College of Computer Science, Zhejiang University, China

The broadcast nature of wireless media makes WLANs easily attacked by *rogue* **Access Points (APs)**. Rogue AP attacks can potentially cause severe privacy leakage and financial loss. Hardware fingerprinting is the state-of-the-art technology to detect rogue APs since an attacker would find it difficult to set up a rogue AP with specific hardware fingerprints. However, existing hardware fingerprints not only depend on the AP but also depend on the client, significantly limiting their application scenarios. In this work, we investigate two novel **client-agnostic** fingerprints, which can be extracted using commercial off-the-shelf WiFi devices, to detect rogue APs. One is the *power amplifier non-linearity fingerprint* and the other is the *frame interval distribution fingerprint*. These two fingerprints remain consistent over time and space for the same AP but vary across different APs even with the same brand, model, and firmware. We use the fingerprint similarity between the candidate AP and the authorized AP for device authentication in typical indoor environments. We have also proposed a threshold-improved authentication scheme to improve the robustness of our system in dynamic environments. Our schemes can be implemented without modifying the infrastructural APs and can work well with new clients without rebuilding the fingerprint database. We evaluate our scheme in both in-lab and field scenarios, by analyzing 18 million WiFi packets. Results show that our scheme achieves an overall 96.55% positive detection rate and a 4.31% false alarm rate. Moreover, the threshold-improved authentication scheme can further reduce the false alarm rate by 13.0%-44.8% for dynamic environments.

CCS Concepts: • **Networks** → **Mobile and wireless security;**

Additional Key Words and Phrases: Rogue AP detection, node authentication, client-agnostic fingerprint

ACM Reference format:
Yuxiang Lin, Yi Gao, Bingji Li, and Wei Dong. 2022. Detecting Rogue Access Points Using Client-agnostic Wireless Fingerprints. *ACM Trans. Sensor Netw.* 19, 1, Article 14 (December 2022), 25 pages.
https://doi.org/10.1145/3536423

A preliminary version of this article appears in *Proceedings of the 18th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom 2020).* This work is supported by NSFC under grant no. 62072396 and 61872437, Zhejiang Provincial Natural Science Foundation for Distinguished Young Scholars under grant no. LR19F020001, the Fundamental Research Funds for the Central Universities, and Alibaba-Zhejiang University Joint Institute of Frontier Technologies.

Authors' addresses: Y. Lin, College of Computer Science, Zhejiang University, 38 Zheda Rd, Hangzhou, Zhejiang, 310027, China & Alibaba Group, 969 West Wen Yi Road, Hangzhou, Zhejiang, 311121, China; email: linyx@zju.edu.cn; Y. Gao (corresponding authors), B. Li, and W. Dong (corresponding authors), College of Computer Science, Zhejiang University, 38 Zheda Rd, Hangzhou, Zhejiang, 310027, China; emails: {gaoyi, lbj123kst, dongw}@zju.edu.cn.

1550-4859/2022/12-ART14 $15.00
https://doi.org/10.1145/3536423

1 INTRODUCTION

While WiFi has become highly prevalent, attacks using rogue **Access Points (APs)** are posing a more severe threat to user privacy and financial safety [1, 2]. An adversary can set up rogue APs having the same identifiers (MAC address, **Basic Service Set IDentifier (BSSID),** and **Service Set IDentifier (SSID)**) as the authorized AP, and thus fool a wireless client in the WiFi network to access the internet through the rogue AP. Then the adversary can launch various attacks such as DoS, data theft, or Man-In-The-Middle attack [3]. It has been estimated that almost 20% of corporations have rogue APs in their networks [4]. Therefore, being able to detect rogue APs is an essential technology for modern wireless networks.

Existing cryptography-based authentication techniques can provide strong authentication above the link layer, but cannot address the rogue AP problem [5]. Specifically, as the current AP selection mechanisms are based on signal strength, the attacker could place a rogue AP with a higher transmission power and always let clients pass the authentication to cheat users. To make it worse, in public places such as airports and shopping malls, there is even no cryptography-based authentication due to its key management and distribution overhead [6, 7]. Therefore, location-based fingerprinting technique [8–11] has been proposed in the literature. The basic principle of location-based fingerprinting is that some low layer features (e.g., Received Signal Strength, or **Channel State Information** [10] **(CSI)**) of WiFi signals present spatial properties due to the complex multipath effects. An adversary half-wavelength away from the legitimate user will incur quite different features when receiving the same WiFi signal [7]. However, when using location-based fingerprinting, even the legitimate client and AP can only be authenticated at a pair of specific locations, significantly limiting its application scenarios. Several recent approaches try to use hardware fingerprints to address the rogue AP detection problem. State-of-the-art approaches [12, 13] extract phase-related characteristics of off-the-shelf wireless devices from CSI as their hardware fingerprints. These phase features are essential signatures of the NIC, however, they are related to not only the AP, but also the client (e.g., oscillator frequencies and compensation errors of the phase correctors at the client). As a result, every time we use a new client to authenticate the APs, it is inevitable to manually rebuild the fingerprint database, which limits the applicability of phase-based approaches.

In this paper, we aim to extract **client-agnostic** hardware fingerprints which are only determined by the AP, to achieve accurate and robust rogue AP detection. We investigate and extract two novel wireless device fingerprints: **Power Amplifier (PA)** non-linearity fingerprint and **Frame Interval Distribution (FID)** fingerprint. (1) The PA non-linearity fingerprint is attributed to the power amplifier imperfections and will introduce a specific time-varying amplitude offset to the CSI measurements. In order to obtain this fingerprint within wireless signals, we propose a novel extraction approach based on CSI amplitude vibration. Further, we also propose several methods to mitigate the amplitude interference caused by other factors like variable-gain amplifier resolution error. The details of PA non-linearity fingerprint extraction are shown in Section 3. (2) The FID fingerprint is attributed to the imperfect oscillator for generating timestamps, and exhibits a unique time offset pattern when generating response frames. We analyze the patterns of different APs and extract the FID fingerprints in the form of histograms to preserve the diversity of fingerprints. The details of FID fingerprint extraction are shown in Section 4.

In the authentication process, we calculate the fingerprint similarity between candidate and authorized APs using absolute distance (for the PA non-linearity fingerprint) and **Earth Mover's Distance (EMD)** [14] (for the FID fingerprint). We then propose a two-step AP authentication scheme with fixed thresholds to detect rogue AP. Besides, we have analyzed that the PA non-linearity fingerprint may be affected by dynamics in the environment. Therefore, we also propose a threshold-improved authentication scheme to improve the rogue AP detection performance in dynamic environments such as coffee shops and airports. In this scheme, we will adaptively relax the threshold of the PA non-linearity fingerprint, or simply not use this fingerprint for authentication according to the dynamics in the environment.

These two fingerprints are fairly consistent over time and space, and vary across devices even with the same brand, model, and firmware version. These two fingerprints can be extracted from wireless signals using **Commercial Off-The-Shelf (COTS)** WiFi devices, without using specialized devices. More importantly, these fingerprints are caused by the AP hardware imperfections and do not depend on the client. Therefore, a new client can authenticate an AP using its fingerprints in the database, significantly reducing the fingerprint collection overhead.

We implement and evaluate the proposed rogue AP detection method extensively, using 20 APs and 5 clients at six different locations and five different times. In total, 9,000 samples are collected for performance evaluation, where each sample includes the fingerprints of 2,000 WiFi packets. Results show that our system achieves an overall 96.55% positive detection rate and a 4.31% false alarm rate. Moreover, comparing to the threshold-fixed scheme, our threshold-improved scheme can reduce the false alarm rate by 13.0%-44.8% in dynamic environments.

The contributions of our work are summarized as follows.

(1) We extract a novel AP-related fingerprint called PA non-linearity, and explain the detailed sources of the fingerprint. Experiments show that PA non-linearity fingerprint is consistent over time, locations, and clients.

(2) We propose another AP-related FID fingerprint and represent it in the form of a frequency histogram. Combined with the PA non-linearity fingerprint, our scheme can achieve a better rogue AP detection rate.

(3) We implement our system on COTS wireless clients and conduct experiments in different scenarios during normal day hours. Results show that our system can achieve high positive detection rates and low false alarm rates in both indoor and dynamic environments. Moreover, our scheme can work well using new clients without rebuilding the fingerprint database.

The rest of the paper is organized as follows. Section 2 reviews the related work of device authentication. We introduce PA non-linearity fingerprint and FID fingerprint in detail in Sections 3 and 4, respectively. In Section 5, we present the device authentication process in both typical indoor environments and dynamic environments. We implement and evaluate our rogue AP detection scheme in Section 6, and finally, Section 7 concludes this paper.

2 RELATED WORK

2.1 Cryptography-based Approaches

Existing cryptography-based authentication techniques such as 802.11i [15] can provide strong mutual authentication between wireless clients and the APs. However, an adversary can still spoof the 802.11 **Management Frames (MFs)** since they have not been protected by any security measures [5]. Further, security schemes such as WPA2 encryption and 802.1X authentication are susceptible to attacks launched through a rogue AP. Specifically, the adversary just needs to employ the same security measure as the authorized AP but always lets clients pass the authentication. Therefore, existing cryptography-based approaches mainly focus on providing a secure channel among legitimate APs and clients, but fail to defend rogue AP attacks.

2.2 Location-based Approaches

Location-based authentication schemes [3, 9, 10, 16–18] are proposed to use the signal shape similarity of either **Received Signal Strength (RSS)** or CSI to conduct user authentication. The signal shape is naturally random and location-dependent due to the complex multipath transmission of wireless signals, and is hard to spoof unless the adversary is within a distance of half-wavelength. Demirbas et al. [16] use RSS to detect Sybil attack in wireless sensor networks. In [3, 10], the proposed methods achieve accurate user authentication based on the high CSI similarity of legitimate users. However, these location-based fingerprints can only work when AP and client are placed at a pair of fixed locations. Although the APs could have been deployed in advance in public places, it is difficult, if not impossible, to build the fingerprint database for every possible client location. As a result, the location-based authentication schemes are not suitable for rogue AP detection in many application scenarios.

2.3 Hardware-based Fingerprinting Approaches

Hardware-based fingerprinting schemes [1, 12, 19] have been proposed since the fundamental physical properties of wireless devices cannot be manipulated easily and remain fairly consistent over time but vary significantly across devices. Kohno et al. [20] and Jana et al. [1] attempt to extract clock skews from various system timestamps, which are tagged by hardware, to detect rogue AP. However, clock skew is possible to spoof by modifying the device driver of a rogue AP [3]. In this work, the PA non-linearity fingerprint is contributed to the hardware imperfection of PA and is represented using multiple values, each of which corresponds to a TX antenna. The FID fingerprint is contributed to the imperfection of oscillator and is represented using finer-grained histograms of clock offsets. As a result, both fingerprints are hard to spoof.

Recent works have tried to extract **Radio Frequency (RF)**-based hardware fingerprints from wireless signals. Nguyen et al. [21] extract radio-metrics such as amplitude, frequency and phase to detect spoofing. Brik et al. [22] employ a set of radiometric features, like frequency error, magnitude error, sync correlation and I/Q offset, to conduct device authentication. However, these works require specialized wireless devices such as USRP2. There is also some work using the CSI frames reported by COTS wireless devices to extract RF fingerprints. Hua et al. [12] employ the **Carrier Frequency Offset (CFO)** for device fingerprinting since CFO is due to the carrier oscillator drift in the WiFi network card. Liu et al. [13] propose a phase error fingerprint, which is due to the I/Q imbalance and imperfect oscillator of the NIC. However, both the extracted CFO and phase errors are client-related fingerprints, which can be affected by oscillator frequencies of different client devices. Moreover, these phase-based fingerprints can be further influenced by different compensation errors of CFO correctors in these clients. When authenticating the same AP with a new client, the fingerprint database needs to be rebuilt. Although it may be more secure for the fingerprint to be client-related, this property makes these fingerprints unable to authenticate APs that have already been deployed in public places such as airports and train stations. In these scenarios, users need to spend a lot of time to build the fingerprint database and need the cooperation of administrators. However, due to the large population and variable clients, the above requirements usually cannot be satisfied in practice.

In this work, the two extracted features are both independent of the clients, making our method applicable for more rogue AP detection scenarios.

3 PA NON-LINEARITY FINGERPRINT

There are several requirements of an effective hardware fingerprint for rogue AP detection.

(1) The fingerprint extraction should be lightweight without introducing high computation overhead at AP and client sides.

(2) The fingerprint can be extracted using COTS devices. This requirement is essential since otherwise the proposed scheme is hard to apply in current WiFi infrastructure.

(3) The fingerprint should be stable in different scenarios. Whether collected at different times, locations, or clients, the fingerprint should remain consistent with the same AP.

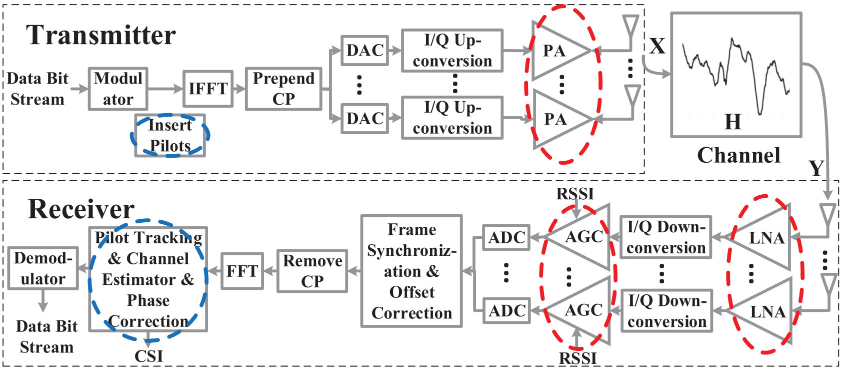


Fig. 1. A block diagram of the 802.11n. The components in blue circles are related to CSI estimation. The amplifiers in red circles are designed for amplitude compensation.

In this section, we first introduce the 802.11n framework and the hardware components related to this fingerprint. We then describe what the PA non-linearity fingerprint is and how to extract it from CSI in detail.

3.1 The 802.11n Preliminaries

The block diagram of the 802.11n framework is shown in Figure 1. At the transmitter, the data bit stream is first modulated and mapped onto a number of subcarriers. Next, pilot bits are inserted into each subcarrier. These pilot bits will be used for CSI estimation at the receiver side. Then, after **Inverse Fast Fourier transform (IFFT)** and adding **Cyclic Prefix (CP)**, each OFDM symbol is transmitted via multiple transmit antenna chains. In each transmit antenna chain, the signal is converted from digital to analog with a DAC, followed by an I/Q up-converter to RF and a PA. These amplifiers, as well as those at the receiver side, are designed to compensate the signal amplitude attenuation and meet power requirements of the devices. Note that the hardware imperfections of these PAs are the source of the PA non-linearity fingerprint which we will describe in the next subsection in detail. Then the signal travels across the channel that characterizes signal attenuation, distortion and rotation and finally arrives at the receiver.

A **Multiple Input Multiple Output (MIMO)** receiver has multiple receive antenna chains, and each antenna chain includes an antenna, a **Low-Noise Amplifier (LNA)**, an I/Q down converter, an **Automatic Gain Control (AGC)**, and an ADC [23]. In this paper, we focus on the AGC and the LNA which adjust the amplitude of the WiFi signals. The main control module of AGC is also an amplifier, **Variable-Gain Amplifier (VGA)**, which is designed to maintain a desired and stable signal power for the receiver. The signal will then be synchronized in both time and frequency. At the same time, a phase offset corrector will compensate the CFO. As mentioned earlier, Hua et al. [12] use the fractional CFO as a fingerprint. However, the fractional CFO is related to not only the oscillator frequency but also the compensation error of the CFO corrector. Therefore, the CFO-based fingerprint is dependent on the client, limiting its application scenarios. After CP removal and FFT, the CSI is estimated using the pilot bits [24]. Finally, the transmitted data bit stream is received by the receiver after demodulation.

3.2 Extracting PA Non-Linearity Fingerprint

CSI and Measured CSI. CSI characterizes the **Channel Frequency Response (CFR)** of the wireless channel at the granularity of subcarrier level. CFR $H(f,t) = |H(f,t)|e^{j\theta(f,t)}$ represents the time-varying wireless spatial channel on a subcarrier index f at time t, where $|H(f,t)|$ and

$e^{j\theta(f,t)}$ represent the attenuation and the phase shift of the signal, respectively. Let $X(f,t)$ and $Y(f,t)$ represent the transmitted and received signal before and after the wireless transmission, as shown in Figure 1. $H(f,t)$ can be expressed as:

$$Y(f,t) = H(f,t) \times X(f,t). \tag{1}$$

Here, $H(f,t)$ is the actual CSI of the wireless channel.

However, as described in the previous sub-section, the *measured* CSI is obtained at the receiver side using the pilot bits in each packet. There is a clear difference between the actual CSI and the measured CSI, i.e., the amplitude adjustments by amplifiers. The measured CSI amplitude $|\hat{H}(f,t)|$ are the sum of the gains of the amplifiers and the propagation fading $|H(f,t)|$, which can be formulated as follows in dB [25]:

$$|\hat{H}(f,t)| = |H(f,t)| + G_{PA}(t) + G_{LNA} + G_{VGA}(t) + n, \tag{2}$$

where n is the noise term, G_{PA}, G_{LNA}, G_{VGA} are the power gain of PA, LNA, and VGA, respectively. Since hardware imperfections of the PA are the source of the PA non-linearity fingerprint, our goal is to isolate $G_{PA}(t)$ from $|\hat{H}(f,t)|$, i.e., removing the impact of G_{LNA}, G_{VGA}, and $|H(f,t)|$.

In Equation (2), G_{VGA} is a *known* variable since it is extracted by WiFi NICs at a packet-level granularity. In our experiments, we install the CSI tool [26] in devices equipped with Intel 5300 NICs to obtain the measured CSI values and the detailed VGA value. Although some other native WiFi NICs do not yet report the VGA values to the upper layer, these values can be extracted by modified firmware released by manufacturers or researchers [27]. Further, in order to average out the impact of noise n, we take frequency-based weighted average [28] of the reported CSI at 30 subcarriers. Then, Equation (2) becomes the following.

$$\overline{G_{PA}(t)} = \overline{|\hat{H}(t)|} - \overline{|H(t)|} - \overline{G_{LNA}} - \overline{G_{VGA}(t)}, \tag{3}$$

where the over-line means weighted average at subcarriers. The remaining items are $\overline{G_{LNA}}$ and the actual channel fading $\overline{|H(t)|}$, i.e., the actual CSI amplitude. It is difficult, if not impossible, to obtain these two values using COTS WiFi devices. Therefore, directly calculating $\overline{G_{PA}(t)}$ as the fingerprint is not feasible. In the following, we will first describe more details about PA non-linearity, and then describe how to calculate the PA non-linearity fingerprint.

PA Non-linearity. In a commodity WiFi NIC, the hardware imperfections of a PA cause its non-linear behavior when amplifying the input signal close to saturation [23]. To achieve maximum power efficiency, the PAs in commercial APs operate close to their saturation points, leading to nonlinear distortion [29]. This distortion will be further exaggerated due to the high peak-to-average power ratio of the input signal [29, 30]. The 802.11n OFDM system is especially sensitive to the PA non-linearity since it uses high order modulation and has high dynamic waveforms [23]. This non-linearity can be modeled via the Rapp PA model [31].

$$A_{out} = \frac{A_{in}}{\left(1 + A_{in}^{2\delta}\right)^{1/2\delta}}, \tag{4}$$

where A_{in} and A_{out} are the input and output signal amplitudes, respectively. δ is the non-linear coefficient that controls smoothness of the model. The coefficient δ is a positive parameter and $\delta \to \infty$ represents the ideally linearized model. δ typically varies from 2 to 4 in modern WiFi hardware [32]. For example, $\delta = 3$ is typically adopted for high power amplifiers while $\delta = 2$ is a typical value for moderate cost PAs.

This non-linear coefficient δ captures the PA hardware imperfections and remains fairly consistent over time but varies significantly across devices. Although directly calculating $\overline{G_{PA}(t)}$

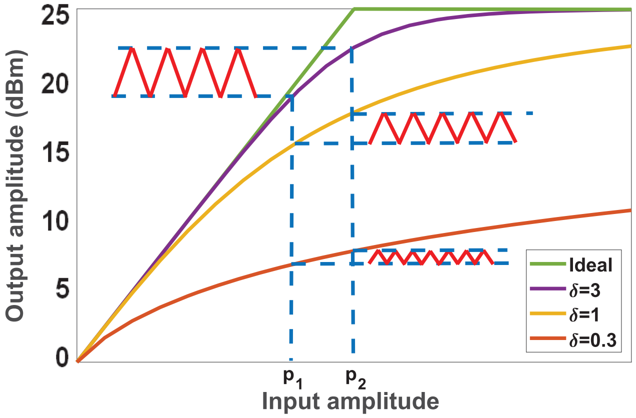


Fig. 2. PA non-linearity of several APs with different non-linear coefficients δ's. The same vibration of the input amplitude causes different vibrations of the output amplitude, depending on δ. Referring to [23], the typical transmitted power at full saturation is 25 dBm when $\delta = 3$.

as the fingerprint is not feasible, we found that the vibration of $\overline{G_{PA}(t)}$ is closely related to the non-linear coefficient δ and can be extracted as the PA non-linearity fingerprint.

Figure 2 shows the PA distortion between the input amplitude and output amplitude at the transmitter with different non-linear coefficients δ's. As seen, different non-linear distortions are applied to the amplitude of the signal when the output amplitude is close to saturation. The input power will adjust to make the output amplitude reach a specified value. However, due to hardware imperfections, the input power will vibrate around the ideal power (e.g., between p_1 and p_2 in Figure 2) to meet the desired output amplitude. As shown in Figure 2, even the same change of input amplitude can cause very different output amplitude vibrations (red waves in the figure), which depend on the non-linear coefficients δ's of internal PAs. On the other hand, the input vibration ranges of different PAs can also vary due to their different no-linear behaviors close to saturation, leading to greater differences in output amplitude vibrations. As a result, the output amplitude vibration is attributed to the PA non-linearity (i.e., δ) and can quantitatively reflect its impact. To the best of our knowledge, the vibration and the PA non-linearity are both hard to be manipulated through software with COTS APs. Therefore, the vibration of G_{PA} is also a good hardware fingerprint to characterize the PA non-linearity.

Extracting the PA Non-linearity Fingerprint. So far, instead of directly using $\overline{G_{PA}(t)}$ as the fingerprint, we use its vibration, i.e., its standard deviation $\sigma(\overline{G_{PA}})$, as the fingerprint. In the 802.11n framework, the gain factor of each amplifier is determined by the device manufacturer. The actual amplitude gains of amplifiers (i.e., $\overline{G_{PA}}$, $\overline{G_{LNA}}$, and $\overline{G_{VGA}}$) are only related to the input amplitude, and should be independent from each other and the channel state. As a result, the variables in Equation (3) are independent. To calculate $\sigma(\overline{G_{PA}})$, we take variance of both sides of Equation (3) as follows.

$$\sigma^2(\overline{G_{PA}}) = \sigma^2(\overline{|\hat{H}|}) - \sigma^2(\overline{|H|}) - \sigma^2(\overline{G_{LNA}}) - \sigma^2(\overline{G_{VGA}}). \tag{5}$$

Since G_{LNA} is usually a constant and does not change over time, $\sigma^2(\overline{G_{LNA}})$ is zero. $\hat{H}$ is the measured CSI.

In typical NICs, both the real and imaginary components of each CSI value are quantized into 8 bits [23]. To quantify the impact of CSI quantization, we evaluate the quantitative error between the quantized 8-bit depth CSI amplitudes and the absolute CSI amplitudes (16-bit) that are extracted

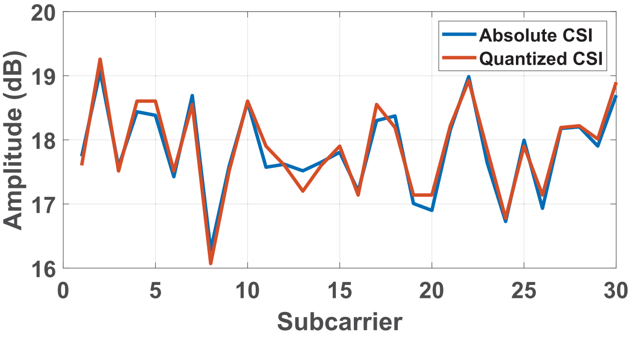


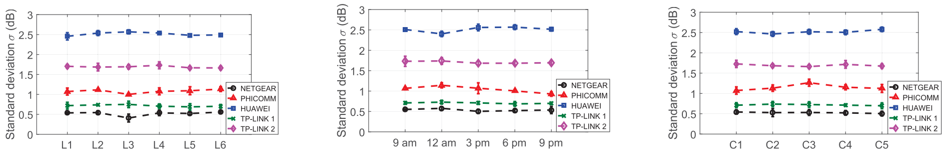
Fig. 3. Quantitative error between the quantized 8-bit depth CSI amplitudes and the absolute CSI amplitudes.

using a dedicated device USRP N210 [33] with XCVR2450 daughter boards. Figure 3 shows a comparison example of these two CSI amplitudes on 30 subcarriers. The unsmooth CSI amplitudes are due to the presence of the researcher when collecting the CSI measurements. Different subcarriers experience frequency-selective fading and will not be equally affected by the multipath introduced by nearby objects [34]. Results show that the 8-bit depth CSI quantization will only introduce an average quantitative error of 0.17 dB. Compared to the amplitude variation introduced by the input power vibration (dB level as shown in Figure 2), the quantization variation is negligible. Combined with the weighted average CSI measurements in Equation (3), the quantization process will not introduce great CSI measurement errors and affect the fingerprint accuracy. It is also worth noting that the absolute CSI amplitudes can be lost in modern NICs. However, this phenomenon will not affect the PA non-linearity fingerprint since we use the vibration of CSI amplitudes (i.e., $\sigma^2(\overline{|\hat{H}|})$ in Equation (5)) to extract the fingerprint, which is independent of the absolute CSI amplitudes after quantization.

Given that G_{VGA} is a known variable, the only remaining item is $\sigma^2(\overline{|H|})$ which is the variance of the actual CSI amplitude. Note that the actual CSI represents the multipath wireless channel of the physical environment. Existing technologies have proved that using WiFi signals is sufficient to detect physical environment changes like moving transceivers or adjacent human activities [35]. Therefore, we extract the CSI measurements when there are no significant changes of the adjacent physical environment for rogue AP detection, where $\sigma^2(\overline{|H|})$ is also close to zero. We need fewer than 50 CSI measurements to calculate the standard deviation and the required fingerprint extraction time is fairly short. For a sampling rate of 100Hz, this process only takes half a second, which can be easily satisfied and detected in the daily use of typical indoor scenarios (e.g., lab, meeting room). However, in dynamic environments with large numbers of walking people (e.g., railway stations), it may be difficult and takes a long time to detect such a stable environment. To improve the robustness of rogue AP detection, we will relax the detection threshold of this fingerprint. The detailed authentication scheme in dynamic environments will be shown in Section 5.2. In summary, the PA non-linearity fingerprint proposed in this paper is given as:

$$\sigma^2(\overline{G_{PA}}) = \sigma^2(\overline{|\hat{H}|}) - \sigma^2(\overline{G_{VGA}}). \tag{6}$$

In modern wireless systems, MIMO is a typical configuration in COTS APs. As shown in Figure 1, there are multiple antennas in the transmitter and each is connected with a PA. MIMO can help further improve the robustness of the PA non-linearity fingerprint. Specifically, we can get CSI



(a) At different locations

(b) At different times in one day

(c) At different clients

Fig. 4. PA non-linearity fingerprints σ's (with 95% confidence intervals) of five different APs. σ's of the same AP are consistent across (a) locations, (b) time, and (c) clients.

measurements of each TX/RX antenna pair[1] and obtain multiple PA non-linearity fingerprints. Supposing there are N TX antennas and M RX antennas, we can obtain $N \times M$ $\sigma(\overline{G_{PA}})$'s in total. For each TX antenna, its M PA non-linearity fingerprints (obtained at the M RX antennas) are similar because they all correspond to a specific PA. Therefore, for each TX antenna, we average the M fingerprints to refine its fingerprint. Finally, N different PA non-linearity fingerprints can be extracted for AP authentication.

3.3 Fingerprint Validation

To validate the effectiveness of this fingerprint, we conduct experiments with five different APs (i.e., a NETGEAR JR6100, a PHICOMM K2, a HUAWEI E5885Ls, and two TP-LINK WDR6300). We moved the client to six different locations in both indoor and outdoor scenarios. The surrounding environments (e.g., furniture, walls, etc.) are different among these locations. Client and APs are placed 1-5 m away and 1m above the ground. We perform the same experiments 50 times for each AP at each location. Figure 4(a) plots the averaged PA non-linearity fingerprints σ's at different locations. To make the figure more clear, we only show the fingerprints of the first PA (embedded in the first antenna) for each AP. As seen, σ of the same AP remains fairly consistent when client location changes. However, σ varies across different APs even with the same model, and thus can be employed for AP authentication.

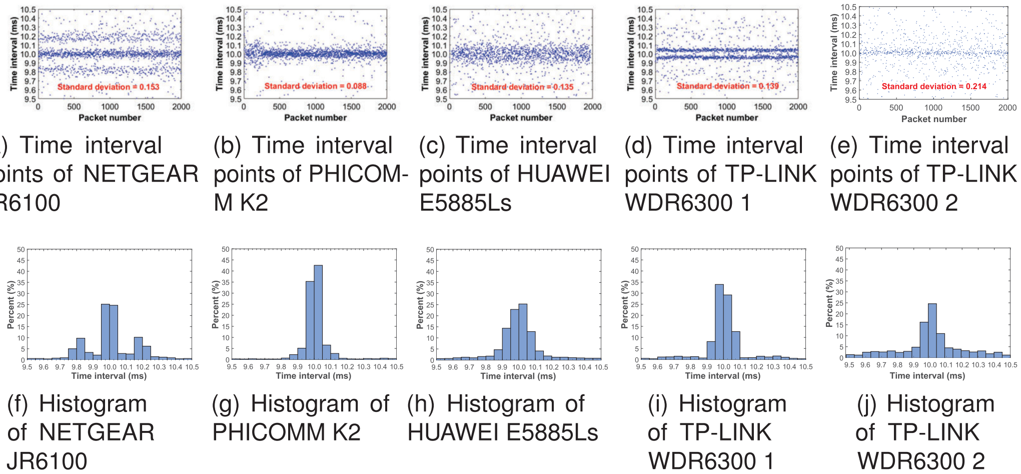
To further validate the time stability of the extracted fingerprint, the experiments were also conducted at five different times in one day. Figure 4(b) plots the averaged σ's of the five APs at different times. The averaged σ's are rather stable across different times and their variations can be neglected compared with the differences between APs.

To validate the extracted fingerprint is only related to AP, we have conducted the same experiments with four more clients (i.e., mini-PCs equipped with different Intel 5300 NICs). The validation results are shown in Figure 4(c). As can be seen, the PA non-linearity fingerprints σ's extracted from different clients are approximate with the same AP. Take a closer look at Figure 4, the PA non-linearity fingerprint of an AP remains stable over time, space, and different clients.

4 FID FINGERPRINT EXTRACTION

In this section, we extract another AP-related fingerprint called **Frame Interval Distribution (FID)**. Specifically, a client sends ICMP packets to an AP with a fixed inter-packet interval (e.g., 10 ms), and records the timestamps of *response* packets. The NIC's oscillator of the AP is responsible for generating 8-byte timestamps to the response packets [26]. Theoretically, the time interval of response packets should be the same as the sending packets. However, the exact frequency of crystal in the oscillator will shift slightly due to the limited mechanical accuracy of the crystal cutting process [1]. Even two crystals using the same cutting process will have

[1] This is supported by commodity WiFi cards such as Intel 5300.



(a) Time interval points of NETGEAR JR6100 (b) Time interval points of PHICOMM K2 (c) Time interval points of HUAWEI E5885Ls (d) Time interval points of TP-LINK WDR6300 1 (e) Time interval points of TP-LINK WDR6300 2

(f) Histogram of NETGEAR JR6100 (g) Histogram of PHICOMM K2 (h) Histogram of HUAWEI E5885Ls (i) Histogram of TP-LINK WDR6300 1 (j) Histogram of TP-LINK WDR6300 2

Fig. 5. Distributions and histograms (i.e., FID fingerprints) of the time intervals Δt's of different APs.

different frequencies. Due to the unique frequency offset of oscillator, the time interval of response packets will drift at the granularity of sub-millisecond, leading to a unique time offset pattern. This frequency offset is determined by oscillator hardware and cannot easily be manipulated by software [1]. FID characterizes the distribution of the time interval of every two consecutive response packets.

FID can be a hardware fingerprint for rogue AP detection because it satisfies all the three requirements mentioned in Section 3, i.e., lightweight, stable, and supporting COTS devices. Since obtaining FID only requires subtracting a number of timestamps, it satisfies the lightweight requirement. The timestamps of ICMP response packets can be obtained from the CSI data of each packet. Each CSI frame contains an MIMO control field, which reports its TSF timestamp T [36]. To obtain the FID, we calculate the time interval $\Delta t_i = T_{i+1} - T_i$ of each pair of consecutive packets, where T_i is the TSF timestamp of the i-th packet. Therefore, the third requirement is also satisfied. In the following, we focus on the second requirement, i.e., the fingerprint should be stable. Concretely, the fingerprint should *only* depend on AP hardware, and be stable under changes of other aspects, e.g., different firmware, clients, and environments.

FID is AP dependent. We first show that FID is hardware dependent and varies significantly across devices. Figure 5(a-e) plot the time interval distributions, as well as their standard deviations, of five APs. As seen, although the distributions are quite distinct, their standard deviations cannot capture these differences. Therefore, in this paper, we use the histograms of these distributions (shown in Figure 5(f-j)) as the FID fingerprint. Another advantage of using histograms as fingerprints is that histogram values are independent of the absolute packet rate. In current implementation, we set the time range of a histogram as 1ms and the number of bins as 20. In order to conduct AP authentication using this fingerprint, we need to define the distance between two histograms. We adopt **Earth Mover's Distance (EMD)** [14], which is a cross-bin similarity metric, to calculate the distance between two histograms. EMD is analogous to the minimal effort to transform one histogram into another one. For example, the EMD between Figures 5(f) and 5(g) is 0.783. Experimental results in Figure 5 show that FID is dependent on AP.

FID is stable under different clients, firmware, and environments. We use a NETGEAR JR6100 AP to validate the stability of FID fingerprint in different situations. We first compare the histograms extracted with *different clients* in Figure 6(a) and (b). The similar histograms

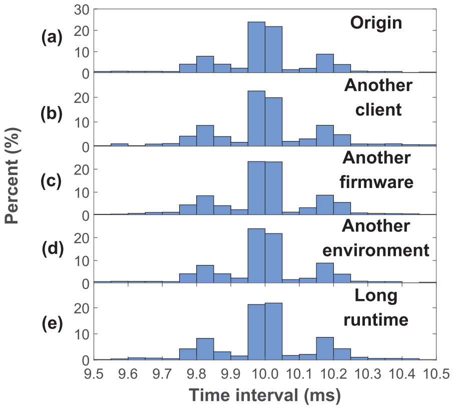


Fig. 6. FID fingerprints (in the form of histograms) of NETGEAR JR6100 in different situations.

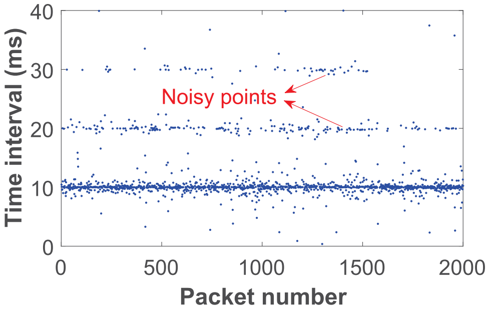


Fig. 7. Time interval distribution of NETGEAR JR6100 with heavy traffic.

(EMD is 0.094) indicate that the FID fingerprint is independent of the client. Next, we show the histogram extracted with the same AP using a *different firmware version* in Figure 6(c). We use firmware versions V1.0.1.14 and V1.0.0.10 in Figures 6(a) and 6(c), respectively. As seen, different firmware versions will also generate histograms with a similar shape (EMD is 0.108). Therefore, the FID fingerprint is independent of the firmware of wireless routers. We observe that although different wireless channel conditions will introduce random and variable delays to the time interval distribution, the FID fingerprint is seldom affected and can be easily captured. To validate this, we plot the histogram extracted *in another environment* in Figure 6(d). Network conditions (including traffic, interference, etc.) are different in Figure 6(a) and (d). Figure 6(a) is in a meeting room with little wireless traffic and Figure 6(d) is in a lab with heavy traffic during daily life. The introduced noisy points shown in Figure 7 can be divided into two parts: noisy points at a higher granularity and scattered around. For noisy points at a higher granularity, these points are due to packet loss and retransmission in bad wireless channel conditions and can be easily filtered out using a simple threshold-based point filter. In our experiments, we reserve the time intervals within the range of [9.5, 10.5] to filter out the influence of these points. Then we can use these reserved intervals to extract the FID fingerprint. For noisy points scattered around the target points, they should have random time interval values, which are attributed to software delays caused by wireless channel contention, uncertain packet sending and receiving delay, etc. However, as shown in Figure 7, these points are relatively sparsely distributed in modern wireless networks, and will not introduce a significant impact on the shape of APs histogram and thus the FID fingerprint. Other environmental factors, such as temperature, humidity and light intensity, have also been considered in the experiments since they may impact the hardware (e.g., oscillator) [20] and further the FID. The comparison result indicates that the FID fingerprint will not be greatly influenced (EMD is 0.090) in different environments. Finally, we show the histogram extracted *after long system runtime* (running for a month) in Figure 6(e). The similar histogram shape between Figure 6(a) and (e) (EMD is 0.112) shows that the FID fingerprint remains stable after the AP has been running for a long time. This also indicates that the FID fingerprint will not be significantly affected by the changing software details as the AP runs. In summary, the above experiments show that the FID fingerprint of an AP remains stable under different firmware, clients, environments, and system runtime. As a result, the FID fingerprint is attributed to the interior hardware imperfection of the AP's oscillator when generating timestamps for ICMP packets.

5 DEVICE AUTHENTICATION

Once a client connects to a pre-deployed AP, the authentication process will be triggered. The client will extract the two fingerprints of the candidate AP and estimate their similarity with the legitimate fingerprints. The fingerprints of the legitimate AP should be collected by the manufacturer or administrator when the AP is first deployed. In our experiments, we have observed that for a specific AP, the two fingerprints are closely distributed around their means with slight random errors even when they are extracted in different scenarios. To deal with the slight randomness of fingerprints, we expect that there are K pre-stored fingerprint profiles for **each** authorized AP in the fingerprint database. Each profile includes a PA non-linearity fingerprint and an FID fingerprint. We need to compare the fingerprint profile extracted from the candidate AP with the K fingerprint profiles of the corresponding legitimate AP for device authentication. In the following, we provide two device authentication schemes: a threshold-fixed authentication scheme for typical indoor environments with relatively stable mobility and a threshold-improved authentication scheme for dynamic environments.

5.1 Threshold-Fixed Authentication Scheme

For typical indoor environments, we propose a two-step AP authentication scheme with fixed thresholds to detect rogue AP. Before introducing the concrete algorithm, we introduce the following notations:

- $P_{aut} = \{P_{1,1}, \ldots, P_{1,N}, P_{2,1}, \ldots, P_{2,N}, \ldots, P_{K,1}, \ldots, P_{K,N}\}$ is the K pre-stored PA non-linearity fingerprints, where N is AP's antenna number. Each element $P_{k,n}$ denotes the k-th PA non-linearity fingerprint at the n-th antenna in an MIMO system.
- $F_{aut} = \{F_{1,1}, \ldots, F_{1,B}, F_{2,1}, \ldots, F_{2,B}, \ldots, F_{K,1}, \ldots, F_{K,B}\}$ is the K pre-stored FID fingerprints, where B is the number of bins in the histogram. $F_{k,b}$ denotes the histogram value at the b-th bin in the k-th FID fingerprint. For simplicity, we use F_k to denote the k-th FID fingerprint (i.e., the k-th histogram).
- P_{mean} denotes the mean value of the pre-stored PA non-linearity fingerprints. $P_{mean,n}$ denotes the mean value at the n-th antenna.
- F_{mean} denotes the mean histogram of the pre-stored FID fingerprints. $F_{mean,b}$ denotes the mean histogram value at the b-th bin.
- T_{PA} and T_{FID} denote the threshold set for PA non-linearity and FID fingerprints, respectively. $T_{PA,n}$ denotes the threshold at the n-th antenna. Theoretically, T_{PA} and T_{FID} characterize the slight randomness of the two fingerprints in the fingerprint database.
- D_{PA} denotes the absolute distance between the extracted and pre-stored PA non-linearity fingerprints. $D_{PA,n}$ denotes the absolute distance at the n-th antenna.
- D_{FID} denotes the EMD between the extracted and pre-stored FID fingerprints.
- $PA_{can} = \{PA_1, \ldots, PA_N\}$ denotes the PA non-linearity fingerprints extracted from the candidate AP at its N antennas.
- $FID_{can} = \{FID_1, \ldots, FID_B\}$ denotes the extracted FID fingerprint (i.e., a histogram with B bins).

Algorithm 1 shows the pseudocode of our algorithm. The first step is PA non-linearity fingerprint matching. We first compute the mean value P_{mean} of K fingerprints in the database. In order to cope with the increasing fingerprint database in the future and eliminate the effect of random errors, we adaptively set the threshold T_{PA} to the greatest value difference between P_{mean} and the K PA non-linearity fingerprints. Next, we calculate the absolute distance D_{PA} between the extracted PA non-linearity fingerprint of the candidate AP and P_{mean}. We determine whether

ALGORITHM 1: Threshold-fixed Authentication Algorithm

```
Input: Fingerprint profiles of the authorized AP: $P_{aut}$ and $F_{aut}$, Candidate fingerprints: $PA_{can}$ and $FID_{can}$
Output: Rogue AP flag: $True$ or $False$
for each antenna $n \in [1, N]$ do
    $P_{mean,n} = \sum_{i=1}^{K} P_{i,n}/K$
    $T_{PA,n} = max_{k \in [1,K]}(|P_{k,n} - P_{mean,n}|)$
    $D_{PA,n} = |PA_n - P_{mean,n}|$
    if $D_{PA,n} > T_{PA,n}$ then
        return $True$
for each bin $b \in [1, B]$ do
    $F_{mean,b} = \sum_{i=1}^{K} F_{i,b}/K$
Let $F_{mean}$ denote the constructed mean histogram;
$T_{FID} = max_{k \in [1,K]}(EMD(F_k, F_{mean}))$, where $EMD()$ is the EMD calculation formula.
$D_{FID} = EMD(FID_{can}, F_{mean})$
if $D_{FID} > T_{FID}$ then
    return $True$
return $False$
```

the candidate AP is legitimate by comparing D_{PA} to the threshold T_{PA}. When $D_{PA} \leq T_{PA}$, the candidate AP can be considered as an authorized device. As a COTS AP usually supports MIMO, it can contain N PA non-linearity fingerprints. Each fingerprint corresponds to a PA embedded in a TX antenna. Only when all N PA non-linearity fingerprints match, the candidate AP can be considered as an authorized device.

The second step is FID fingerprint matching. Similarly, we first compute the mean value of each bin of K histograms in the database and construct a new mean histogram. We also adaptively set the threshold T_{FID} to the greatest EMD between the mean histogram and the K histograms. Next, we calculate the EMD D_{FID} between the extracted histogram of the candidate AP and the mean histogram. When $D_{FID} \leq T_{FID}$, the candidate AP can be considered as an authorized device.

As a rogue AP detection scheme, the positive detection rate is desired to be as high as possible since misidentifying a rogue AP as an authorized one can lead to serious problems. To increase the positive detection rate, the candidate AP is considered legitimate (i.e., not a rogue AP) only when *both* fingerprints match the fingerprint profiles of the authorized AP.

5.2 Threshold-Improved Authentication Scheme

In dynamic environments, the above device authentication scheme with fixed thresholds may not work well. This is because the PA non-linearity fingerprint is related to the variance of the actual CSI amplitude (shown in Equation 5). Therefore, its performance will be greatly affected in a dynamic environment with objects continuously moving around (evaluated in Figure 13). As rogue APs may be deployed in dynamic environments such as supermarkets or airports, it is important to improve the robustness of our authentication algorithm with dynamics in the environment.

For dynamic environments, we further propose a threshold-improved authentication scheme to improve the rogue AP detection performance. The key idea of the algorithm is that we should appropriately relax the threshold for the PA non-linearity fingerprint in different dynamic environments. Moreover, when the environment is extremely dynamic (e.g., subway stations), we should consider using only the FID fingerprint for AP authentication. This is because the FID fingerprint will be hardly affected by dynamics. Indoor dynamics can only introduce meter-level path changes, leading to microsecond-level time offsets. Such offsets will have a negligible impact on the frame intervals (see Section 6.5).

ALGORITHM 2: Threshold-improved Authentication Algorithm

```
Input: Fingerprint profiles of the authorized AP: $P_{aut}$ and $F_{aut}$, Candidate fingerprints: $PA_{can,S}$ and $FID_{can}$
Output: Rogue AP flag: $True$ or $False$
 1: for each antenna $n \in [1, N]$ do
 2:     $\mu_{PA,n} = \frac{\sum_{i=1}^{S} PA_{i,n}}{S}$
 3:     $\sigma_{PA,n} = \sqrt{\frac{1}{S}\sum_{i=1}^{S}(PA_{i,n} - \mu_{PA,n})^2}$
 4:     $P_{mean,n} = \sum_{i=1}^{K} P_{i,n}/K$
 5:     $T_{PA,n} = max_{k \in [1,K]}(|P_{k,n} - P_{mean,n}|)$
 6:     if $\frac{\sigma_{PA,n}}{T_{PA,n}} > T_{dynamic}$ then
 7:         $continue$
 8:     else
 9:         $T_{PA,n,new} = \sqrt{T_{PA,n}^2 + \sigma_{PA,n}^2}$
10:         $D_{PA,n} = |PA_n - P_{mean,n}|$
11:         if $D_{PA,n} > T_{PA,n,new}$ then
12:             return $True$
13: for each bin $b \in [1, B]$ do
14:     $F_{mean,b} = \sum_{i=1}^{K} F_{i,b}/K$
15: Let $F_{mean}$ denote the constructed mean histogram;
16: $T_{FID} = max_{k \in [1,K]}(EMD(F_k, F_{mean}))$
17: $D_{FID} = EMD(FID_{can}, F_{mean})$
18: if $D_{FID} > T_{FID}$ then
19:     return $True$
20: return $False$
```

We first add the following notations:

- $PA_{can,S} = \{PA_{1,1}, \ldots, PA_{1,N}, PA_{2,1}, \ldots, PA_{2,N}, \ldots, PA_{S,1}, \ldots, PA_{S,N}\}$ denotes the PA non-linearity fingerprints extracted from the past S packets of the candidate AP at its N antennas. Each element $PA_{s,n}$ denotes the PA non-linearity fingerprint at the n-th antenna extracted from the s-th packet in the past.
- μ_{PA} and σ_{PA} denote the mean value and the standard deviation of the past S PA non-linearity fingerprints, respectively. $\mu_{PA,n}$ and $\sigma_{PA,n}$ denote the mean value and the standard deviation at the n-th antenna, respectively.
- $T_{dynamic}$ denotes the threshold set for the ratio between σ_{PA} and T_{PA}. If the ratio is greater than $T_{dynamic}$, we consider the current authentication process is in an extremely dynamic environment.

Algorithm 2 shows the pseudocode of the threshold-improved authentication algorithm. As seen, the major improvement of the threshold-improved authentication algorithm is that it can adaptively increase the threshold of the PA non-linearity fingerprint T_{PA} in different dynamic environments. Specifically, for each antenna n, we first get the standard deviation of the past S PA non-linearity fingerprints $\sigma_{PA,n}$, and calculate the initial value of $T_{PA,n}$ (line 2-5). There is a tradeoff in determining the number of past packets S. A larger S will improve the estimation accuracy of standard deviation, but may also reduce the overall accuracy due to the introduction of outdated data. It is worth noting that there is often out-of-date data due to the phased movement of people or other objects in dynamic environments. We empirically set $S = 50$ in our experiments, which means we calculate current $\sigma_{PA,n}$ using the packets collected in the past half a second. Then we

Table 1. Detailed Information of the Experimental APs

AP No.	Brand & model	Firmware Ver.	Place
AP_1	NETGEAR JR6100	V1.0.1.14	Lab & Meeting room & Lobby
AP_2	PHICOMM K2	V22.5.11.14	
AP_3	HUAWEI E5885Ls	V21.187.61.00.233	
AP_4	XIAOMI R3	V2.26.11	
AP_5-AP_6	TP-LINK WDR6300	V9.0	
AP_7-AP_{12}	H3C MSR20-20	Unknown but identical	Teaching building
AP_{13}-AP_{18}	H3C MSR20-20	Unknown but identical	Supermarket
AP_{19}-AP_{24}	Unknown	Unknown	Subway station

identify whether the authentication process is in an extremely dynamic environment by comparing the current fingerprint variation $\sigma_{PA,n}$ with the normal randomness of legitimate PA non-linearity fingerprint $T_{PA,n}$. If $\sigma_{PA,n}$ is much larger than $T_{PA,n}$ (i.e., the ratio of these two values is greater than a predefined threshold $T_{dynamic}$), we consider that the n-th antenna is greatly affected by dynamics nearby and will not be used for authentication (line 6-7). Based on empirical experiments, we set $T_{dynamic} = 3$. Otherwise, we will update $T_{PA,n}$ to $T_{PA,n,new}$, which is the square root of the squared sum of current $\sigma_{PA,n}$ and the initial $T_{PA,n}$. We can directly combine $\sigma_{PA,n}$ and $T_{PA,n}$ to get the improved threshold $T_{PA,n,new}$ since these two values are independent of each other. We then calculate D_{PA}. If $D_{PA} > T_{PA}$, the candidate AP is identified as a rogue AP (line 8-12). The following FID fingerprint matching process is the same as Algorithm 1 since the FID fingerprint will not be significantly affected by dynamic environments.

6 EVALUATION

In this section, we first introduce the experimental settings and then evaluate our scheme in both lab and field scenarios under different conditions. We compare our method with a state-of-the-art rogue AP detection approach [12]. Finally, we evaluate the system overhead on both client and AP sides.

6.1 Experimental Setup

6.1.1 Implementation. The two fingerprints can be extracted with COTS wireless devices such as laptops and desktops equipped with wireless NICs. In our experiments, we employ the **HummingBoard (HMB)** Pro mini-PC [37] (1.2GHz ARM Cortex-A9 processor and 1GB RAM) equipped with an Intel 5300 NIC [26] to collect fingerprints of testing devices. We use HMB for wireless signal collection because it is lightweight and easy to be deployed in different environments. Our system can be hosted on any Wi-Fi channel in the 2.4GHz and 5GHz bands since the two fingerprints are independent of the carrier frequency. We conduct our experiments in a commonly used 2.4GHz band with a 20MHz bandwidth. HMB works as the client and sends ICMP packets to an AP at a frequency of 100Hz. The HMB client collects fingerprints for 20 seconds in each experiment, in which there are in total 2,000 CSI frames. From each experiment, we can extract a fingerprint profile which consists of a PA non-linearity fingerprint and an FID fingerprint.

6.1.2 Methodology. We conduct our experiments with COTS APs during normal day hours when people may walk around. Table 1 shows the detailed information of all APs used in our experiments. AP_1 to AP_6 are laboratory routers and their firmware versions are fixed. Note that AP_5 and AP_6 share the same brand, model, and firmware version. The first six APs are deployed in three different scenarios including a laboratory (3m × 9m), a lobby (6m × 9m), and a meeting room (5m × 8m). AP_7 to AP_{12} are deployed in a five-floor teaching building (50m × 45m). These

APs are part of the wireless network service of the campus and also share the same brand, model, and firmware version. We use the MAC address to distinguish these pre-deployed APs. AP_5 to AP_{12} are used to evaluate the performance of our rogue AP detection scheme when the attacker sets up a rogue AP with the same model as the authorized AP. During the evaluation, AP_1 to AP_6 are only connected with one client at a time while AP_7 to AP_{12} are likely to be connected with other existing wireless devices. Since AP_1 to AP_{12} are deployed in typical indoor scenarios with limited numbers of people and low mobility, we can easily detect a static environment and extract the corresponding fingerprints during authentication. Therefore, the **threshold-fixed authentication algorithm** (i.e., Algorithm 1) can work well in these scenarios and is used by default to detect rogue APs in our experiments. To further evaluate the **threshold-improved authentication algorithm** (i.e., Algorithm 2), we also collected CSI data in two more dynamic environments. Specifically, AP_{13} to AP_{18} are pre-deployed in a supermarket on campus. AP_{19} to AP_{24} are pre-deployed in a subway station in Hangzhou. Detailed fingerprint performance of different dynamic environments will be evaluated in Section 6.5.

In each scenario, we collect the CSI frames at five different times, i.e., 9 AM, 12 AM, 3 PM, 6 PM, and 9 PM. To validate that the extracted fingerprints are independent of the client, we conduct the same experiments with five HMB clients equipped with different Intel 5300 NICs. We repeat 10 times in each case to mitigate random errors. As such, each scenario contains 1,500 (=6 APs × 5 times × 5 clients × 10 repeated experiments) fingerprint profiles. In total, we have manually collected 9,000 fingerprint profiles in the six scenarios.

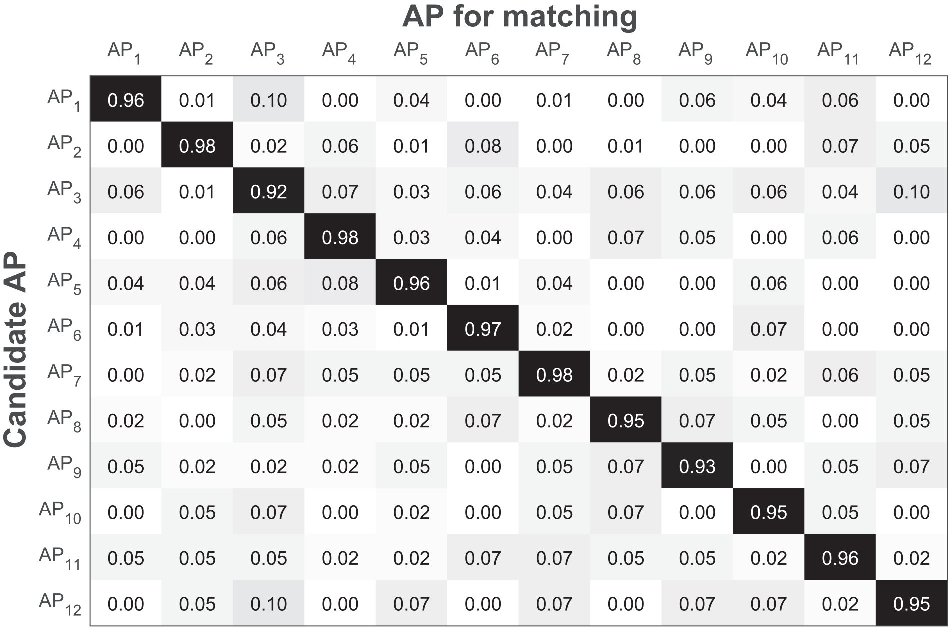
In our evaluation, we mainly focus on the rogue AP detection accuracy and use performance metrics including the **Positive Detection Rate (PDR**, successfully detects a rogue AP) and the **False Alarm Rate (FAR**, misidentifies an authorized AP as a rogue AP) for evaluation.

6.2 Overall Performance

To evaluate the performance of our rogue AP detection scheme in typical indoor scenarios, we use the 6,000 fingerprint profiles collected by AP_1 to AP_{12} for analysis. We randomly select 30% of the profiles of each AP as the whitelist (with a size of 1,800 profiles) and the other profiles as the validation set (with a size of 4,200 profiles). Each fingerprint profile in the validation set will be compared with the profiles of all 12 APs in the whitelist. We have conducted profile matching on 4,200 × 12 pairs of profiles. A match indicates that the compared two fingerprint profiles pass our device authentication process and are considered belonging to the same AP.

Figure 8 shows the overall profile matching rate matrix for rogue AP detection. Each element of the i-th row and j-th column in the matrix indicates the average matching rate between the AP_i's profiles in the validation set and the AP_j's profiles in the whitelist. It is better when the matching rates on the diagonal are close to one and the others are close to zero. Results show the following. (1) When comparing the fingerprint profiles of the same AP, which simulate the legitimate communication, the matching rates of the 12 APs are close to 1. (2) When comparing between different APs, which simulate the rogue AP attack, the matching rates are all close to 0. Looking at the 3rd row and the 3rd column, the matching results related to AP_3 (i.e., HUAWEI E5885Ls, a portable router without antenna) are relatively worse. (3) It is more likely to mismatch the profiles of AP_3 with other APs. This is because the CSI of AP_3 is relatively more changeable, and thus the two fingerprints are more unstable. (4) As AP_5 and AP_6 are two identical APs, the matching results between AP_5 and AP_6 indicate that our scheme can work well even with the same brand, model, and firmware version.

Figure 9 shows the authentication performance with individual fingerprints and their combination. Results show that our scheme achieves an overall PDR of 96.55% and an average FAR of 4.31%. We see that with the PA non-linearity fingerprint alone and the FID fingerprint alone, the



	AP_1	AP_2	AP_3	AP_4	AP_5	AP_6	AP_7	AP_8	AP_9	AP_{10}	AP_{11}	AP_{12}
AP_1	0.96	0.01	0.10	0.00	0.04	0.00	0.01	0.00	0.06	0.04	0.06	0.00
AP_2	0.00	0.98	0.02	0.06	0.01	0.08	0.00	0.01	0.00	0.00	0.07	0.05
AP_3	0.06	0.01	0.92	0.07	0.03	0.06	0.04	0.06	0.06	0.06	0.04	0.10
AP_4	0.00	0.00	0.06	0.98	0.03	0.04	0.00	0.07	0.05	0.00	0.06	0.00
AP_5	0.04	0.04	0.06	0.08	0.96	0.01	0.04	0.00	0.00	0.06	0.00	0.00
AP_6	0.01	0.03	0.04	0.03	0.01	0.97	0.02	0.00	0.00	0.07	0.00	0.00
AP_7	0.00	0.02	0.07	0.05	0.05	0.05	0.98	0.02	0.05	0.02	0.06	0.05
AP_8	0.02	0.00	0.05	0.02	0.02	0.07	0.02	0.95	0.07	0.05	0.00	0.05
AP_9	0.05	0.02	0.02	0.02	0.05	0.00	0.05	0.07	0.93	0.00	0.05	0.07
AP_{10}	0.00	0.05	0.07	0.00	0.02	0.00	0.05	0.07	0.00	0.95	0.05	0.00
AP_{11}	0.05	0.05	0.05	0.02	0.02	0.07	0.07	0.05	0.05	0.02	0.96	0.02
AP_{12}	0.00	0.05	0.10	0.00	0.07	0.00	0.07	0.00	0.07	0.07	0.02	0.95

Fig. 8. Overall profile matching rate matrix of our rogue AP detection scheme.

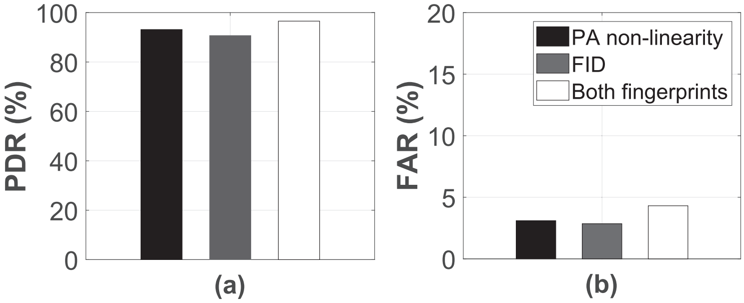


Fig. 9. Rogue AP detection performance in terms of (a) PDR and (b) FAR using individual fingerprints and both the two fingerprints.

accuracy of our scheme can exceed 93% and 90%, respectively. Results show that the probability for two APs to share the same PA and FID fingerprints is very small even with the same model. Hence, the attacker has to buy numerous APs and analyze their fingerprints to deploy a rogue AP, which is *time-consuming* and *costly*. Combining the two fingerprints, our scheme is able to achieve a high rogue AP detection rate at the cost of a slightly higher FAR. The raised false alarms are due to the unexpected CSI variance, which is below the moving threshold but will still affect the two fingerprints. Due to our two-step device authentication scheme, interference of either fingerprint can lead to a false rogue AP detection alarm. We leave integrating a more robust static environment detection technology as future work.

6.3 Comparison Study

In the following, we compare our rogue AP detection scheme with one state-of-the-art rogue AP detection approach [12], which employs CFO as its device fingerprint. The CFO-based approach

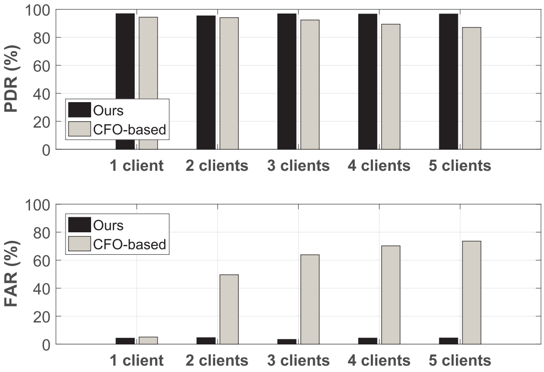


Fig. 10. PDR and FAR comparison between our scheme and the CFO-based approach with different numbers of clients in the validation set.

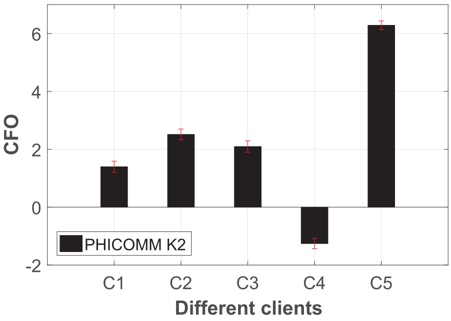


Fig. 11. CFOs of a PHICOMM K2 AP extracted with different clients. The error bars are the 95% confidence intervals.

Table 2. Fingerprint Characteristic Comparison

Fingerprint	Fingerprint value range	Variation range
PA non-linearity	0.04-2.86	0.01-0.13
CFO [12]	1.44-3.57	0.04-0.18

extracts a fractional CFO fingerprint with a slope estimation process, and conducts a threshold-based fingerprint matching for rogue AP detection.

Compared to the CFO-based hardware fingerprint shown in [12], the difference of PA non-linearity fingerprint between different APs is more significant. Table 2 shows the detailed value range and variation range of PA non-linearity fingerprint and the CFO-based fingerprint reported in [12]. As seen, our PA non-linearity fingerprints have a larger margin and better stability. Furthermore, the FID fingerprint is more distinguishable between different APs since it is represented using finer-grained histograms. Therefore, our proposed fingerprints are supposed to achieve a better rogue AP detection accuracy.

We also evaluate whether our scheme works well for different clients, **i.e., client-agnostic**, using different numbers (i.e., 1 to 5) of clients. To conduct the comparison experiments, we employ 30% of the profiles of the first client as the common whitelist. We first employ the remaining 70% of the profiles of the first client as the validation set for performance comparison when only using one client. Then in each iteration, we add the profiles of another client into the validation set.

Figure 10 shows the comparison results between our scheme and the CFO-based approach with different numbers of clients. We can observe the following. (1) Compared to CFO-based approach, our scheme improves the PDR by 5.5% and reduces the FAR significantly by 91.9% on average. With only the first client, our scheme still performs better than CFO-based approach due to the effectiveness of our two fingerprints. (2) For our scheme, PDR and FAR are well kept at a good level with different numbers of clients since our fingerprints remain consistent across clients. (3) For CFO-based approach, FAR increases significantly when using more clients to authenticate the AP. FARs reach up to around 1/2, 2/3, 3/4, 4/5 with 2, 3, 4, 5 clients, respectively. This is because CFOs of the authorized AP can still vary across different clients. Figure 11 shows that a commercial AP can have significantly different CFOs (A positive CFO means the estimated slope is less than 90° while a negative CFO means the slope is greater than 90°) with different clients. These differences in CFO values lead to a high FAR when conducting AP authentication. Moreover, the extracted

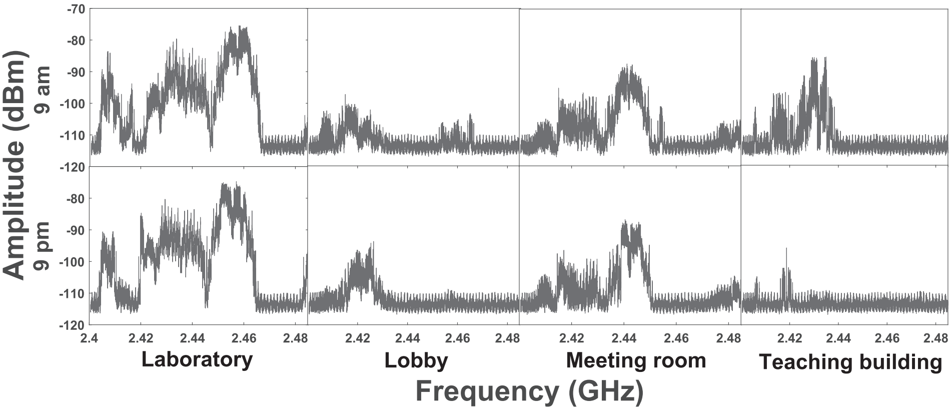


Fig. 12. Spectrums of different wireless environments when collecting the CSI frames. X-axis is the four experimental scenarios and Y-axis is the two experimental times.

Table 3. Rogue AP Detection Performance in Different Locations and Times

Scenario	Time1 (9 am)		Time2 (9 pm)	
	PDR	FAR	PDR	FAR
Laboratory	96.28%	4.34%	96.20%	4.50%
Lobby	97.05%	3.19%	97.17%	3.03%
Meeting room	97.03%	3.23%	96.91%	3.65%
Teaching building	95.31%	5.31%	95.99%	5.23%

CFOs of rogue APs will also change with clients and could coincidentally match the profiles of the authorized AP, leading to a relatively lower PDR. As a result, our scheme achieves a high rogue AP detection accuracy and low false alarm rate with various clients while the CFO-based approach can only achieve a good performance with a specific client.

6.4 Impact of Wireless Environments

Wireless environments can influence both the two extracted fingerprints. We employ a USRP N210 to conduct spectrum sensing during normal day hours (at 9 AM and 9 PM) in the four experiment locations. The spectrums are reported in the 2.4GHz frequency band. Figure 12 shows the frequency spectrums when collecting the CSI frames at different times and locations. As can be seen, the wireless environment patterns are pretty different across different scenarios. For example, there is reasonable wireless energy in the laboratory most of the time. The wireless energy in the lobby and meeting room are relatively lower and stable. For the teaching building, wireless energy is high in the daytime and is relatively low in the night. Besides the wireless condition, other environmental factors, such as furniture location and crowd movement, have also changed in these scenarios.

We show the rogue AP detection performance in the above scenarios in Table 3. Results show that the rogue AP detection rates in all scenarios exceed 95.3% and the FARs are below 5.4%. The performance in the lobby is relatively better because its wireless environment is relatively less complicated than the other three scenarios and the corresponding fingerprints are more stable. The teaching building achieves the worst performance due to its highest wireless noise. In addition, there are more people walking around in the building during normal day hours, which could

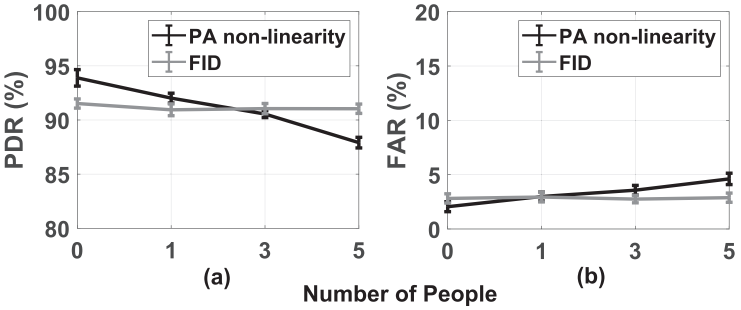


Fig. 13. (a) PDR and (b) FAR of each fingerprint in different simulated dynamic environments.

impact the accuracy of the fingerprints. However, the performance in the teaching building is still acceptable.

6.5 Impact of Different Dynamic Environments

Effectiveness of Each Fingerprint. To evaluate the impact of dynamic environments on the two fingerprints, we asked different numbers (i.e., 0, 1, 3, 5) of volunteers to walk around the test AP in a lab to simulate different dynamic environments. Zero means the lab is in a static environment. We have conducted multiple rounds of experiments in each dynamic setting. Figure 13(a) and (b) show the average PDR and FAR (with 95% confidence intervals) of each fingerprint in these environments. Results show that the PA non-linearity fingerprint has a relatively higher PDR and lower FAR than the FID fingerprint when the environment is relatively static (i.e., in the lab environment). However, even with the static environment detection approach and carefully designed thresholds, the performance of the PA non-linearity fingerprint will decrease in a more dynamic environment. On the contrary, both the PDR and FAR of the FID fingerprint will not be significantly affected by dynamic environments. This is because the changing wireless paths indoors caused by dynamics will only introduce microsecond-level time interval changes and will have a negligible impact on the frame interval offset pattern (at the millisecond level). To enhance the robustness of authentication, we have proposed a threshold-improved scheme to adaptively increase the threshold of the PA non-linearity fingerprint T_{PA} when the AP needs to be placed in more dynamic environments. In the following, we will evaluate the performance improvement of this scheme.

Effectiveness of the Threshold-improved Authentication Scheme. Compared with our previous work [38], the major improvement of this work is the threshold-improved authentication scheme. To evaluate how our threshold-improved authentication scheme deals with dynamic environments, we compare the authentication performance in four scenarios with increasing dynamics: **Static Lab (SL)**, **Teaching Building (TB)**, **SuperMarket (SM)**, and **Subway Station (SS)**. Figure 14 shows the PDR and FAR (with 95% confidence intervals) of the threshold-fixed scheme (i.e., Algorithm 1) and the threshold-improved scheme (i.e., Algorithm 2) in different dynamic environments. Results show the following. (1) The FAR of the threshold-fixed scheme will increase with more dynamics in the environment since the extracted PA non-linearity fingerprint is more likely to mismatch the profiles. On the contrary, the threshold-improved authentication scheme can significantly reduce the FAR by 13.0%-44.8% at the cost of reducing the PDR by 0.3%-1.3% in different dynamic environments. (2) The authentication performance of both schemes will decrease in a more dynamic environment. However, in the threshold-improved scheme, the lower bound of PDR is close to the PDR of FID fingerprint alone, and the upper bound of FAR is close to the FAR of FID fingerprint alone. This is because we will only use the FID fingerprint

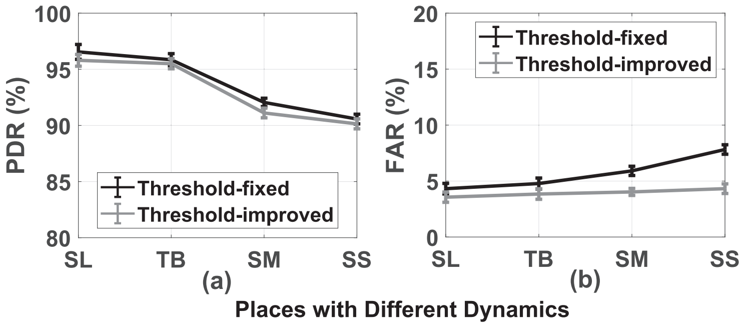


Fig. 14. (a) PDR and (b) FAR comparison between the threshold-fixed scheme and the threshold-improved scheme in different real-world dynamic environments.

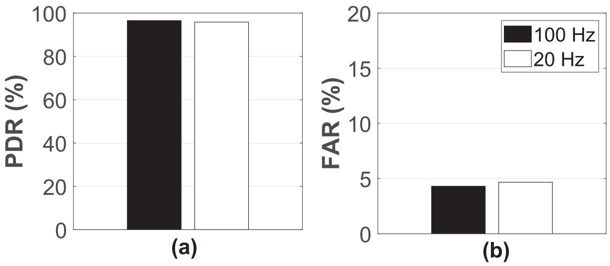


Fig. 15. (a) PDR and (b) FAR comparison with different packet rates.

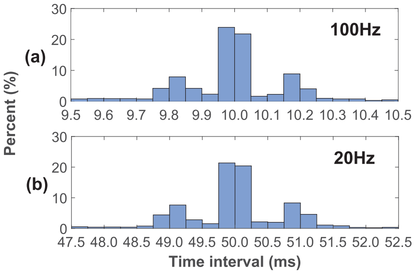


Fig. 16. FID fingerprints of NETGEAR JR6100 with different packet rates.

for authentication in extremely dynamic environments with the threshold-improved scheme. (3) In all environments, the threshold-improved scheme will achieve a relatively lower PDR due to the introduction of measurement noise of the past *S* PA non-linearity fingerprints. This noise will unexpectedly raise the threshold when updating the threshold and cannot be ignored especially for static environments. In summary, it is better to use the threshold-improved authentication scheme in dynamic environments and use the threshold-fixed scheme in relatively static environments. Users can determine to use one of these two schemes based on the dynamics of the places where the candidate AP is deployed.

6.6 Impact of Packet Rate

We also compare the authentication performance when collecting fingerprints at two different packet rates: 100Hz and 20Hz. Figure 15 shows that our scheme achieves consistent authentication performance with different packet rates. This is due to the following three reasons: (1) Our scheme does not need to use many packets to extract fingerprints. Instead, our scheme can achieve AP authentication with only one fingerprint profile extracted from a small number of packets. (2) The PA non-linearity fingerprint is attributed to the PA and will not be affected by different packet rates. (3) As shown in Figure 16, although the absolute frame interval will be affected by the packet rate, the interval distribution (i.e., the FID fingerprint) will not be significantly affected by different packet rates.

6.7 System Overhead

Table 4 shows the system overhead of the two proposed authentication schemes.

Table 4. Authentication Overhead

Scheme	Memory (KB/per AP)	Time (ms)	Throughput (Kbps)
Threshold-fixed	0.82-0.90	41	50
Threshold-improved	0.82-0.90	553	50

6.7.1 Overhead of the Threshold-Fixed Authentication Scheme. **Client Overhead.** Each fingerprint profile consists of 21-23 floats (including 1-3 σ's of the corresponding 1-3 antennas in common APs and 20 bin values) and we pre-store 10 fingerprint profiles for each authorized AP. For an authorized AP, the memory cost is 0.82-0.90KB. Therefore, the total memory cost of the frequency-used APs for an individual user is usually acceptable. For example, since there are around 3,000 APs in the campus WLAN, the local fingerprint database for a user takes less than 2.7MB. For large-scale rogue AP detection, a global fingerprint database can be established on a cloud server via crowdsourcing. One can upload/download his/her local fingerprint database based on his/her location. To evaluate the time cost of our system, we first randomly generate 1,000 fingerprint profiles and store the profiles in a client device. Then we conduct the proposed rogue AP detection scheme, including fingerprint extraction and device authentication. The overall processing time only takes 41 milliseconds on a laptop with an Intel Core i7-6500U CPU. As a result, even if the mobile devices are moving, our system requires users to hold the devices only for a short time to complete the authentication and will not significantly affect user experience.

AP Overhead. Since each ICMP packet is 64 bytes, the overhead of CSI collection process (at a sampling rate of 100Hz) is around 50Kbps, which can be further reduced by decreasing the sampling rate (e.g., to 20Hz). As an 802.11n network supports a data rate of more than 300Mbps [23], such low overhead is negligible for commercial APs. In addition, since users only need to send a small number of ICMP packets for authentication once when connecting to the AP, the AP will hardly suffer from denial of service attacks even in large public WiFi networks. To evaluate the overhead at the AP side, we collect CSI frames for 20 seconds using a lab AP which is also connected by a wired user and three wireless users. All the four devices were placed as normal use and transmitting a 10GB file. We measure the throughput of the four co-existing users for one minute. The CSI collection starts at the 20th second and stops at the 40th second. Note that there may be other users that have already connected to the AP and share the networks in the lab. The network speed can also be limited by the commercial AP and operator. Therefore, the measured throughput in our experiments is relatively low for an 802.11n system. Results in Figure 17 show that the throughput is relatively stable during CSI collection, which indicates that CSI collection will not introduce a noticeable impact on the throughput of these clients.

6.7.2 Overhead of the Threshold-Improved Authentication Scheme. **Client Overhead.** The memory cost of an authorized AP is still 0.82-0.90KB since the threshold-improved authentication scheme will not change the pre-stored fingerprint profiles. However, since we need to use the past S packets to help update the threshold of PA non-linearity fingerprint in this scheme, the time cost will certainly increase. We evaluate the time cost of this scheme using the same experimental setup mentioned above. Results show that the overall authentication process takes 553 ms, including 500 ms for packet collection, and 53 ms for fingerprint extraction and authentication. Such a short authentication time will still not significantly affect the user experience.

AP Overhead. If the sampling rate remains unchanged, the throughput overhead of the threshold-improved authentication scheme will be the same as that of the threshold-fixed AP authentication scheme.

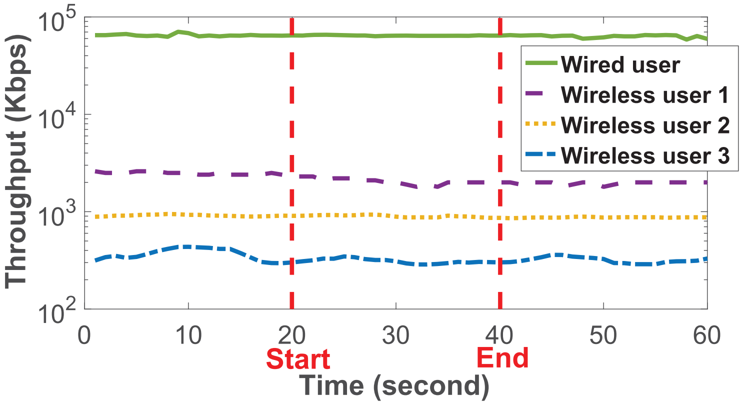


Fig. 17. Throughput of 4 co-existing AP users. One is a wired user and the others are wireless users. We collect the CSI frames from 20 to 40 seconds.

6.8 Practical Issue

There are some advantages and limitations of our rogue AP detection approach. The proposed two fingerprints are hard to be manipulated through software methods since they are caused by hardware imperfection. However, among the huge number of APs on the market, there may still exist APs that have similar fingerprints due to the relatively limited resolution of the two proposed fingerprints. In practice, when an attacker tries to find an AP with similar fingerprints, it is labor-intensive and costly to extract these fingerprints and find such a rare AP. Integrating more radiometric features [22] can further increase the difficulty of such imitation and is worth future investigation.

7 CONCLUSION

In this paper, we propose two novel hardware fingerprints of AP: PA non-linearity fingerprint and FID fingerprint. We have first investigated the sources of these fingerprints in detail. Next, we carefully extract the fingerprints from the CSI frames, which are reported via the NIC drivers of COTS wireless devices. We have conducted validation experiments to show the consistency of these fingerprints over time, space, and different clients. We then utilize the similarity of the two fingerprints between the candidate AP and the authorized AP for AP authentication in typical indoor environments. We also propose a threshold-improved scheme to improve the authentication performance in dynamic environments. We have conducted experiments in lab and field scenarios. Experimental results show that our scheme achieves an accurate rogue AP detection rate without introducing much overhead in both static and dynamic environments. Besides, our scheme is more robust since it can work well with different clients without rebuilding the fingerprint database. For the future work, we will pay more attention to radiometric features that can be extracted from COTS wireless devices to further improve the authentication robustness.

REFERENCES

[1] Suman Jana and Sneha K. Kasera. 2010. On fast and accurate detection of unauthorized wireless access points using clock skews. *IEEE Transactions on Mobile Computing* 9, 3 (2010), 449–462.

[2] Philip N. Ballai. 2006. System and method for detection of a rogue wireless access point in a wireless communication network. (June 27 2006). US Patent 7,068,999.

[3] Zhiping Jiang, Jizhong Zhao, Xiang-Yang Li, Jinsong Han, and Wei Xi. 2013. Rejecting the attack: Source authentication for Wi-Fi management frames using CSI information. In *INFOCOM 2013-IEEE Conference on Computer Communications, IEEE.* 2544–2552.

[4] Raheem Beyah and Aravind Venkataraman. 2011. Rogue-access-point detection: Challenges, solutions, and future directions. *IEEE Security & Privacy* 9, 5 (2011), 56–61.

[5] W. A. Arbaugh, N. Shankar, J. Wang, and K. Zhang. 2001. Your 802.11 network has no clothes. *IEEE Wireless Communications* 9, 6 (2001), 44–51.

[6] Christoph Neumann, Olivier Heen, and Stéphane Onno. 2012. An empirical study of passive 802.11 device fingerprinting. In *Distributed Computing Systems Workshops (ICDCSW'12), 32nd International Conference on.* IEEE, 593–602.

[7] Wei Xi, Chen Qian, Jinsong Han, Kun Zhao, Sheng Zhong, Xiang Yang Li, and Jizhong Zhao. 2016. Instant and robust authentication and key agreement among mobile devices. In *Proc. of ACM SIGSAC Conference on Computer and Communications Security.* 616–627.

[8] Jie Yang, Yingying Chen, W. Trappe, and J. Cheng. 2009. Determining the number of attackers and localizing multiple adversaries in wireless spoofing attacks. In *INFOCOM 2009-IEEE Conference on Computer Communications, IEEE.* 666–674.

[9] Suhas Mathur, Robert Miller, Alexander Varshavsky, Wade Trappe, and Narayan Mandayam. 2011. Proximate: Proximity-based secure pairing using ambient wireless signals. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services.* ACM, 211–224.

[10] Hongbo Liu, Yan Wang, Jian Liu, Jie Yang, and Yingying Chen. 2014. Practical user authentication leveraging channel state information (CSI). In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security.* ACM, 389–400.

[11] Jie Xiong and Kyle Jamieson. 2013. SecureArray: Improving WiFi security with fine-grained physical-layer information. In *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking.* ACM, 441–452.

[12] Jingyu Hua, Hongyi Sun, Zhenyu Shen, Zhiyun Qian, and Sheng Zhong. 2018. Accurate and efficient wireless device fingerprinting using channel state information. In *INFOCOM 2018-IEEE Conference on Computer Communications, IEEE.*

[13] Pengfei Liu, Panlong Yang, Wen-Zhan Song, Yubo Yan, and Xiang-Yang Li. 2019. Real-time identification of rogue WiFi connections using environment-independent physical features. In *INFOCOM 2019-IEEE Conference on Computer Communications, IEEE.*

[14] Yossi Rubner, Carlo Tomasi, and Leonidas J. Guibas. 2000. The Earth Mover's Distance as a metric for image retrieval. *International Journal of Computer Vision* 40, 2 (2000), 99–121.

[15] William A. Arbaugh et al. 2003. *Real 802.11 Security: Wi-Fi Protected Access and 802.11 i.* Addison-Wesley Longman Publishing Co., Inc.

[16] Murat Demirbas and Youngwhan Song. 2006. An RSSI-based scheme for Sybil attack detection in wireless sensor networks. In *Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks.* IEEE Computer Society, 564–570.

[17] Zang Li, Wenyuan Xu, Rob Miller, and Wade Trappe. 2006. Securing wireless systems via lower layer enforcements. In *Proceedings of the 5th ACM Workshop on Wireless Security.* ACM, 33–42.

[18] Ibrahim Ethem Bagci, Utz Roedig, Ivan Martinovic, Matthias Schulz, and Matthias Hollick. 2015. Using channel state information for tamper detection in the Internet of Things. In *Proceedings of the 31st Annual Computer Security Applications Conference.* ACM, 131–140.

[19] Adam C. Polak, Sepideh Dolatshahi, and Dennis L. Goeckel. 2011. Identifying wireless users via transmitter imperfections. *IEEE Journal on Selected Areas in Communications* 29, 7 (2011), 1469–1479.

[20] T. Kohno, A. Broido, and K. Claffy. 2005. Remote physical device fingerprinting. In *Proc. of IEEE Symposium on Security and Privacy.* 211–225.

[21] Nam Tuan Nguyen, Guanbo Zheng, Zhu Han, and Rong Zheng. 2011. Device fingerprinting to enhance wireless security using nonparametric Bayesian method. In *INFOCOM 2011-IEEE Conference on Computer Communications, IEEE.* 1404–1412.

[22] Vladimir Brik, Suman Banerjee, Marco Gruteser, and Sangho Oh. 2008. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking.* ACM, 116–127.

[23] Eldad Perahia and Robert Stacey. 2013. *Next Generation Wireless LANs: 802.11n and 802.11ac.* Cambridge University Press.

[24] Asaf Tzur, Ofer Amrani, and Avishai Wool. 2015. Direction finding of rogue Wi-Fi access points using an off-the-shelf MIMO OFDM receiver. *Physical Communication* 17, C (2015), 149–164.

[25] Eldad Perahia and Robert Stacey. 2008. *Next Generation Wireless LANs.* Cambridge University Press. 473–477 pages.

[26] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. 2011. Tool release: Gathering 802.11n traces with channel state information. *ACM SIGCOMM CCR* 41, 1 (Jan. 2011), 53.

[27] Yaxiong Xie, Zhenjiang Li, and Mo Li. 2015. Precise power delay profiling with commodity WiFi. In *Proc. of ACM MobiCom*. 53–64.

[28] Kaishun Wu, Jiang Xiao, Youwen Yi, Min Gao, and Lionel M. Ni. 2012. FILA: Fine-grained indoor localization. In *INFOCOM 2012-IEEE Conference on Computer Communications, IEEE*. 2210–2218.

[29] Praveen Kumar Singya, Nagendra Kumar, and Vimal Bhatia. 2017. Mitigating NLD for wireless networks: Effect of nonlinear power amplifiers on future wireless communication networks. *IEEE Microwave Magazine* 18, 5 (2017), 73–90.

[30] N. Maletić, M. Čabarkapa, and N. Nešković. 2017. Performance of fixed-gain amplify-and-forward nonlinear relaying with hardware impairments. *International Journal of Communication Systems* 30, 6 (2017), e3102.

[31] Christoph Rapp. 1991. Effects of HPA-nonlinearity on a 4-DPSK/OFDM-signal for a digital sound broadcasting signal. *ESASP* 332 (1991), 179–184.

[32] Hideki Ochiai. 2013. An analysis of band-limited communication systems from amplifier efficiency and distortion perspective. *IEEE Transactions on Communications* 61, 4 (2013), 1460–1472. http://dx.doi.org/10.1109/TCOMM.2013.020413.120384

[33] Ettus Inc. USRP N210. https://www.ettus.com/all-products/un210-kit/. ([n. d.]).

[34] Ju Wang, Jie Xiong, Hongbo Jiang, Kyle Jamieson, Xiaojiang Chen, Dingyi Fang, and Chen Wang. 2018. Low human-effort, device-free localization with fine-grained subcarrier information. *IEEE Transactions on Mobile Computing* 17, 11 (2018), 2550–2563. http://dx.doi.org/10.1109/TMC.2018.2812746

[35] Wei Wang, Alex X. Liu, Muhammad Shahzad, Kang Ling, and Sanglu Lu. 2015. Understanding and modeling of WiFi signal based human activity recognition. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 65–76.

[36] 2009. *IEEE 802.11n-2009-Amendment 5: Enhancements for Higher Throughput.* IEEE-SA.

[37] SolidRun. 2014. HummingBoard Pro. http://wiki.solid-run.com/doku.php?id=products:imx6:hummingboard.

[38] Y. Lin, Y. Gao, B. Li, and W. Dong. 2020. Accurate and robust rogue access point detection with client-agnostic wireless fingerprinting. In *2020 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. 1–10. http://dx.doi.org/10.1109/PerCom45495.2020.9127375

Received 22 December 2020; revised 29 April 2022; accepted 2 May 2022