2020 IEEE International Conference on Pervasive Computing and Communications (PerCom)

Accurate and Robust Rogue Access Point Detection with Client-Agnostic Wireless Fingerprinting

Yuxiang Lin, Yi Gao, Bingji Li, Wei Dong
College of Computer Science, Zhejiang University, China
Alibaba-Zhejiang University Joint Institute of Frontier Technologies
Email:{*linyx, gaoyi, lbj123kst, dongw*}@*zju.edu.cn*

***Abstract*—The broadcast nature of wireless medium makes WLANs easily be attacked by *rogue* Access Points (APs). Rogue AP attacks can potentially cause severe privacy leakage and financial lost. 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 applicable 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. Our scheme 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 12 million WiFi packets. Results shows that our scheme achieves an overall 96.55% positive detection rate and a 4.31% false alarm rate.**

I. Introduction

While WiFi has become highly prevalent, attacks using rogue Access Points (APs) are posing a severer threat to user privacy and finical 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 fools a wireless client in the WiFi network into accessing 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 link layer, but cannot address the rogue AP problem [5]. Specifically, as the current AP selection mechanisms are based on the signal strength, the attacker could place a rogue AP with a higher transmission power and always lets clients pass the authentication. 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], [9], [10], [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 of the signals [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. While 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. Details about this fingerprint extraction are included in Section III. 2) The FID fingerprint is attributed to the imperfect working stack to handle and response to the ICMP packets, and reveals 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. 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]

978-1-7281-4657-7/20/$31.00 ©2020 IEEE

(for the FID fingerprint).

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 does not depend on the client. Therefore, a new client can authenticate an AP using the fingerprints extracted by another client, significantly reducing the fingerprints collection overhead.

We implement and evaluate the proposed rogue AP detection method extensively, using 12 APs and 5 clients at four different locations and five different times. In total, 6,000 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.

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 achieves a high positive detection rate and low false alarm rate. Moreover, our scheme can work well using new clients without rebuilding the fingerprint database.

II. Related Work

A. 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.

B. Location-based Approaches

Location-based authentication schemes [16], [10], [9], [3], [17], [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 [10] and [3], 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.

C. Hardware-based Fingerprinting Approaches

Hardware-based fingerprinting schemes [1], [19], [12] 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 screw is possible to spoof by modifying the device driver of a rogue AP [3]. In this work, the two proposed fingerprints are contributed to the hardware imperfection of the working stacks in different APs, and thus 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 error 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. In this work, the two extracted features are both independent to the clients, making our method applicable for more rogue AP detection scenarios.

III. 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 with no hardware modifications using COTS devices. This requirement is essential

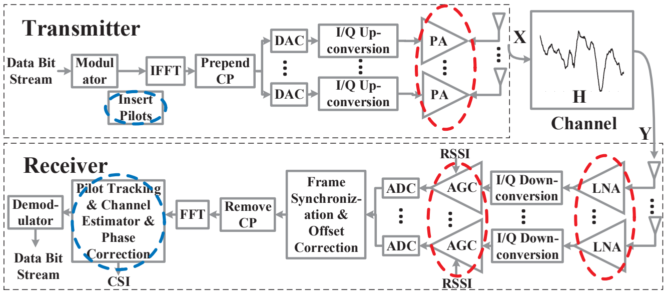


Fig. 1: **A block diagram of the 802.11n. The components in blue circles are related to CSI estimation. The amplifiers in red circles are designed for amplitude compensation.**

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.

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.

A. The 802.11n Preliminaries

The block diagram of the 802.11n framework is shown in Fig. 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 sub-section 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 to 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.

B. 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 Fig. 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 reported from WiFi NICs to upper layer, at a packet-level granularity. Further, in order to average out the impact of noise n, we take frequency-based weighted average [26] 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 the 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 at saturation. This non-linearity can be modeled via the Rapp PA model [27].

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

where A_{in} and A_{out} are the input and output signal amplitudes, respectively. δ is the non-linear coefficient. This non-linear coefficient δ captures the PA hardware imperfections

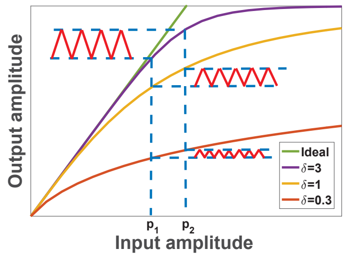


Fig. 2: **PA non-linearity of several APs with different non-linear coefficients δ's. The same vibration of the input amplitude causes different vibrations of the output amplitude, depending on δ.**

and remains fairly consistent over time but varies significantly across devices [27]. Although directly calculating $\overline{G_{PA}(t)}$ 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.

Fig. 2 shows the PA distortion between the input amplitude and output amplitude at the transmitter with different non-linear coefficient δ's. As seen, different non-linear distortions are applied to the amplitude of the signal when the output amplitude is at full saturation which is usually the case in modern APs. The input power will adjust to make the output amplitude reaches a specified value. However, due to hardware imperfections, the input power will vibrate (e.g., between p_1 and p_2 in Fig. 2) to meet the desired output amplitude. As shown in the figure, the same change of input amplitude can cause very different output amplitude variations on different APs. 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 order to calculate it, we take variance of both two 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. Therefore, given that G_{VGA} is a known variable and $\hat{H}$ is the measured CSI, 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 [28]. 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. The required extraction time is fairly short (41ms shown in Section VI-E) and can easily be satisfied in daily use. Detailed fingerprint performance of different dynamic environments will be evaluated in Section VI. 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 Fig. 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 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.

C. *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 at 6 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 5m away and 1m above the ground. We perform the same experiments 50 times for each AP at each location. Fig. 3(a) plots the averaged PA non-linearity fingerprints σ's at different locations. To make the figure clearer, 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.

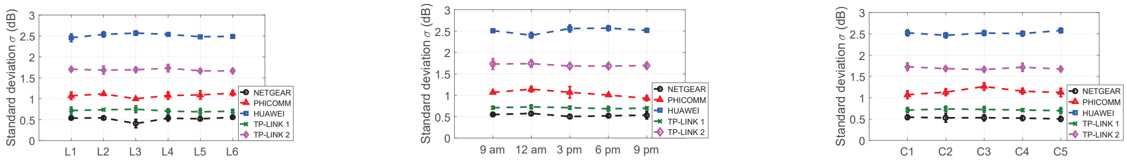
To further validate the time stability of the extracted fingerprint, the experiments were also conducted at 5 different times in one day. Fig. 3(b) plots the averaged σ's of the five APs at different times. The averaged σ's are rather stable across different times and their variations can be neglected compared with the differences between APs.

To validate the extracted fingerprint is only related to AP, we have conducted the same experiments with 4 more clients (i.e. mini-PCs equipped with different Intel 5300 NICs). The validation results are shown in Fig. 3(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 Fig. 3, the PA non-linearity fingerprint of an AP remains stable over time, space and different clients.

IV. FID Fingerprint Extraction

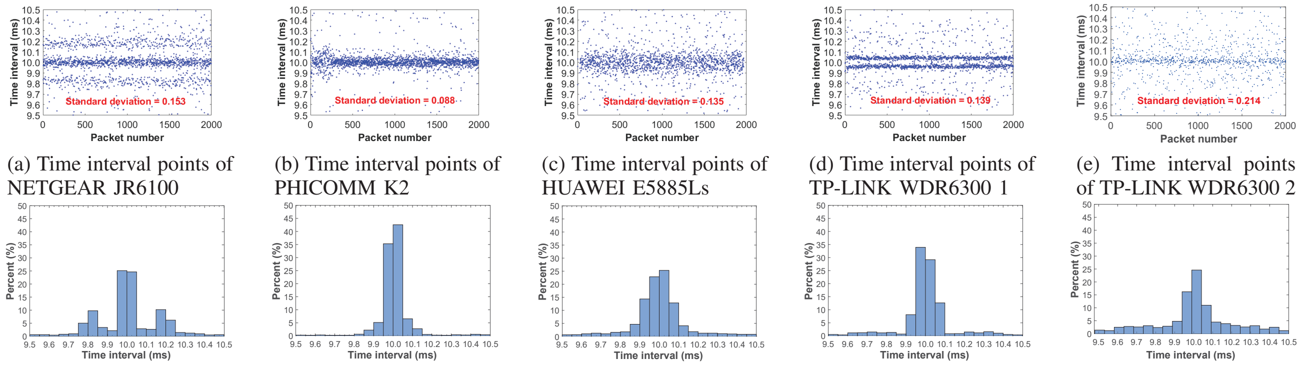
In this section, we extract another AP-related fingerprint called Frame Interval Distribution (FID). Specifically, a client sends ICMP packets to an AP with a fixed inter-packet interval (e.g., 10ms), and records the timestamps of the *response*

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



(a) At different locations (b) At different times in one day (c) At different clients

Fig. 3: **PA non-linearity fingerprints σ's (with 95% confidence intervals) of three different APs. σ's of the same AP are consistent across (a) locations, (b) time, and (c) clients.**



(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. 4: **Distributions and histograms of the time intervals Δt's of different APs.**

packets. Then FID is 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 III, 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 [29]. 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, different clients, or different environments.

FID is AP dependent. We first show that FID is hardware dependent and varies significantly across devices. Fig. 4(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 Fig. 4(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 Fig. 4(f) and Fig. 4(g) is 0.783. Experimental results in Fig. 4 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 under different firmware, clients, and environments in Fig. 5. We first compare the histograms extracted with *different clients* in Fig. 5(a) and (b). The similar histograms (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 Fig. 5(c). 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 then plot the histogram extracted *in another environment* in Fig. 5(d). Network conditions (including traffic, interference, etc.) are different in Fig. 5(a) and (d). Fig. 5(a) is in a meeting room with little wireless traffic and Fig. 5(d) is in a lab with heavy traffic during daily life. We have found that network conditions will introduce noisy points at a higher granularity (i.e. tens of milliseconds shown in Fig. 6) due to wireless back-off mechanisms. While FID is a sub-millisecond feature (shown in Fig. 4), it is easy to filter out these noisy points and extract the actual 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. As a result, the FID fingerprint is attributed to the interior hardware imperfection of the working stack for responding

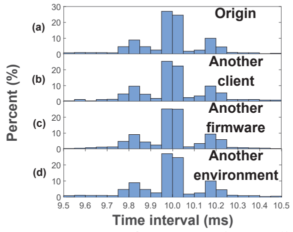


Fig. 5: **FID fingerprints (in the form of histograms) of NETGEAR JR6100 in different situations.**

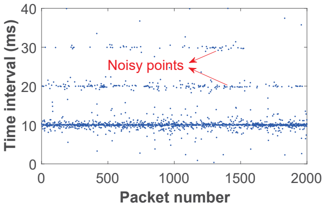


Fig. 6: **Time interval distribution of NETGEAR JR6100 with heavy traffic.**

ICMP packets.

V. Device Authentication

In this section, we introduce how a client estimates the similarity of the two fingerprints for AP authentication when connecting to a candidate AP.

Suppose that there are K pre-stored fingerprint profiles (should be extracted in various scenarios) for **each** authorized AP in the fingerprint database. Each profile includes a PA non-linearity fingerprint and an FID fingerprint. For rogue AP detection, we only need to compare the fingerprint profile extracted from the candidate AP with the K fingerprint profiles of the corresponding authorized AP. Real-world implementation in Section III and Section IV has empirically shown that for a specific AP, the two fingerprints are closely distributed around their means expect for some random error even when they are extracted in different scenarios. To deal with the slight randomness of the features and enhance the robustness of rogue AP detection, we develop a two-step AP authentication algorithm.

Before introducing the concrete algorithm, we introduce the following notations:

- $P_{aut} = \{P_{1,1}, ..., P_{1,N}, P_{2,1}, ..., P_{2,N}, ..., P_{K,1}, ..., P_{K,N}\}$ 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.
- $F_{aut} = \{F_{1,1}, ..., F_{1,B}, F_{2,1}, ..., F_{2,B}, ..., F_{K,1}, ..., F_{K,B}\}$ 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).
- σ_{mean} denotes the mean value of the pre-stored PA non-linearity fingerprints. $\sigma_{mean,n}$ denotes the mean value at the n-th antenna.
- FID_{mean} denotes the mean histogram of the pre-stored FID fingerprints. $FID_{mean,b}$ 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.
- 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.

Algorithm 1 Device Authentication Algorithm

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

- D_{FID} denotes the EMD between the extracted and pre-stored FID fingerprints.
- $P_{can} = \{PA_1, ..., PA_N\}$ denotes the PA non-linearity fingerprints extracted from the candidate AP at its N antennas.
- $F_{can} = \{FID_1, ..., FID_B\}$ 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 σ_{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 error, we adaptively set the threshold T_{PA} to the greatest value difference between σ_{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 σ_{mean}. We determine whether 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 an 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 misidentify 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.

TABLE I: **Detailed information of the experimental APs.**

AP No.	Brand & model	Firmware Ver.
AP_1	NETGEAR JR6100	V1.0.1.14
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

VI. Evaluation

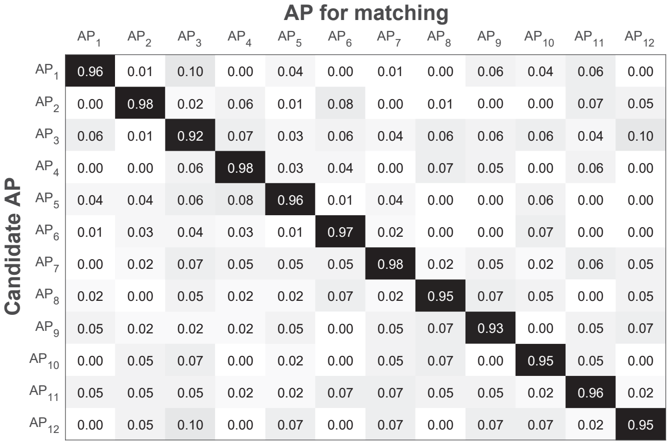
In this section, we first introduce the experimental settings and then evaluate our scheme in both lab and field scenarios under different conditions. We compare our method with a state-of-the-art approach in [12]. Finally, we evaluate the system overhead on both client and AP sides.

A. Experimental Setup

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 [30] (1.2GHz ARM Cortex-A9 processor and 1GB RAM) equipped with an Intel 5300 NIC [31] 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.

2) Methodology: Table I shows the detail information of APs used in our experiments. AP_1 to AP_6 are laboratory routers and their firmware version are fixed. Note that AP_5 and AP_6 share the same brand, model, and firmware version. We manually deploy the first six APs 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 pre-deployed in a five-floor teaching building (50m × 45m), which 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 set 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.

In each scenario, we collected the CSI frames at five different times, i.e., 9 AM, 12 AM, 3 PM, 6 PM and 9 PM, during normal day hours when people may walk around. To validate that the extracted fingerprints are independent with the client, we conducted the same experiments with five HMB clients equipped with different Intel 5300 NICs. We repeated 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 collected 6,000 fingerprint profiles in the four scenarios, where each sample includes 2,000 CSI frames.



	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. 7: **Overall profile matching rate matrix of our rogue AP detection scheme.**

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

B. Overall Performance

To evaluate the performance of our rogue AP detection scheme, we randomly select 30% 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 $4,200 \times 12$ pairs of profiles. A match indicates that the compared two fingerprint profiles pass our device authentication process and considered belonging to the same AP.

Fig. 7 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. It is more likely to mismatch the profiles of AP_3 with other APs. This is because the CSI is relatively more changeable and thus the two fingerprints of AP_3 are more unstable. As AP_5 and AP_6 are two identical APs, the matching results between AP_5

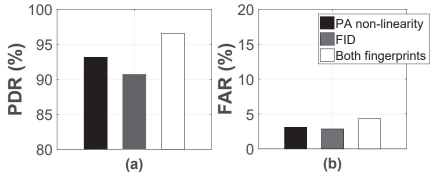


Fig. 8: **Rogue AP detection performance in terms of (a) PDR and (b) FAR using individual fingerprints and both the two fingerprints.**

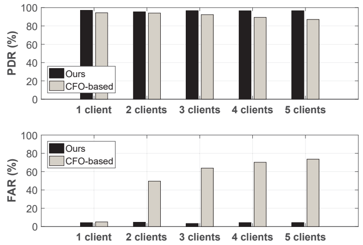


Fig. 9: **PDR and FAR comparison between our scheme and the CFO-based approach with different number of clients in the validation set.**

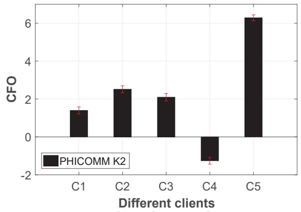


Fig. 10: **CFOs of a PHICOMM K2 AP extracted with different clients. The error bars are the 95% confidence intervals.**

and AP_6 indicate that our scheme can work well even with the same brand, model, and firmware version.

Fig. 8 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, 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 an accurate 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.

C. Impact of Clients

To evaluate whether our scheme works well for different clients, **i.e., client-agnostic**, we evaluate the PDR and FAR using different number (i.e., 1 to 5) of clients. In this part, we also compare our rogue AP detection scheme with a state-of-the-art approach [12], which employs CFO as its device fingerprint. The CFO-based approach extracts a fractional CFO fingerprint with a slope estimation process, and conducts a threshold-based fingerprint matching for rogue AP detection. To conduct the comparison experiments, we employ 30% profiles of the first client as the common whitelist. We first employ the remaining 70% profiles of the first client as the validation set for performance comparison when only using one client. Then we add the profiles of another client into the validation set in each iteration.

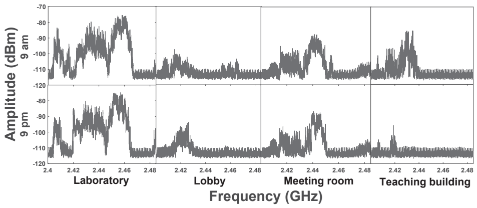


Fig. 11: **Spectrums of different wireless environments when collecting the CSI frames. X-axis is the four experimental scenarios and Y-axis is the two experimental times.**

Fig. 9 shows the comparison results between our scheme and the CFO-based approach with different number 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 number 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. Fig. 10 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 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.

D. Impact of Environments

Different 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. Fig. 11 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 lobby and meeting room are relatively lower and stable. For the teaching building, the 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 II. Results show that the rogue AP detection

TABLE II: **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%

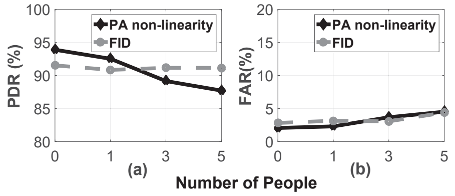


Fig. 12: **Fingerprint performance in different dynamic environments.**

rates in all scenarios exceed 95.3% and the FARs are below 5.4%. The performance in lobby is relatively better because the lobby is relatively less complicated than the other three scenarios and its 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 impact the accuracy of the fingerprints. However, the performance in the teaching building is still acceptable.

Different Dynamic Environments. To further evaluate the impact of dynamic environments on the two fingerprints, we asked different number (i.e., 1, 3, 5) of volunteers to walk around the test AP in a lab to simulate different dynamic environments. Fig. 12(a) and (b) show the PDR and FAR of each fingerprint in these environments. Zero means the lab is empty and in a static environment. Results show that the PA non-linearity fingerprint has a relatively higher PDR and lower FAR than the FID fingerprint when only a few people walk around. However, even with the dynamic environment detection approach and the adaptive fingerprint thresholds, the performance of the PA non-linearity fingerprint will decrease in a more dynamic environment. On the contrary, the performance of the FID fingerprint is relatively stable across different dynamic environments. As a result, to enhance the robustness of authentication, we could manually increase the threshold of the PA non-linearity fingerprint T_{PA} when the AP needs to be placed in more dynamic environments such as airports and coffee shops.

E. System Overhead

Client Overhead. Each fingerprint profile consists of 21-23 floats (including 1-3 σ's and 20 bin values) and we prestore 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.

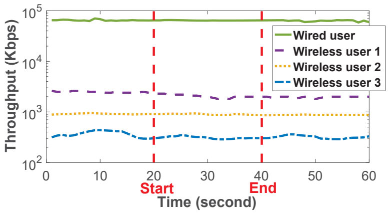


Fig. 13: **Throughput of 4 co-existing AP users. One is a wired user and the others are wireless users. We collect the CSI frames from 20 to 40 seconds.**

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 is negligible for an 802.11n system. 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 20th second and stops at 40th second. Results in Fig. 13 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.

VII. 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. 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. Besides, our scheme is more robust since it can work well with different clients without rebuilding the fingerprint database.

Acknowledgment: This work is supported by the National Key R&D Program of China under Grant No. 2019YFB1600700, the National Science Foundation of China (No. 61772465 and No. 61872437), Zhejiang Provincial Natural Science Foundation for Distinguished Young Scholars under No. LR19F020001. Yi Gao and Wei Dong are corresponding authors.

References

[1] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 449–462, 2010.

[2] P. N. Ballai, "System and method for detection of a rogue wireless access point in a wireless communication network," Jun. 27 2006, uS Patent 7,068,999.

[3] Z. Jiang, J. Zhao, X.-Y. Li, J. Han, and W. Xi, "Rejecting the attack: Source authentication for wi-fi management frames using csi information," in *INFOCOM 2013-IEEE Conference on Computer Communications, IEEE*, 2013, pp. 2544–2552.

[4] R. Beyah and A. Venkataraman, "Rogue-access-point detection: Challenges, solutions, and future directions," *IEEE Security & Privacy*, vol. 9, no. 5, pp. 56–61, 2011.

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

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

[7] W. Xi, C. Qian, J. Han, K. Zhao, S. Zhong, X. Y. Li, and J. Zhao, "Instant and robust authentication and key agreement among mobile devices," in *Proc. of ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 616–627.

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

[9] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proceedings of the 9th international conference on Mobile systems, applications, and services*. ACM, 2011, pp. 211–224.

[10] H. Liu, Y. Wang, J. Liu, J. Yang, and Y. Chen, "Practical user authentication leveraging channel state information (csi)," in *Proceedings of the 9th ACM symposium on Information, computer and communications security*. ACM, 2014, pp. 389–400.

[11] J. Xiong and K. Jamieson, "Securearray: Improving wifi security with fine-grained physical-layer information," in *Proceedings of the 19th annual international conference on Mobile computing & networking*. ACM, 2013, pp. 441–452.

[12] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, "Accurate and efficient wireless device fingerprinting using channel state information," in *INFOCOM 2018-IEEE Conference on Computer Communications, IEEE*, 2018.

[13] P. Liu, P. Yang, W.-Z. Song, Y. Yan, and X.-Y. Li, "Real-time identification of rogue wifi connections using environment-independent physical features," in *INFOCOM 2019-IEEE Conference on Computer Communications, IEEE*, 2019.

[14] Y. Rubner, C. Tomasi, and L. J. Guibas, "The earth mover's distance as a metric for image retrieval," *International journal of computer vision*, vol. 40, no. 2, pp. 99–121, 2000.

[15] W. A. Arbaugh *et al.*, *Real 802.11 security: Wi-Fi protected access and 802.11 i*. Addison-Wesley Longman Publishing Co., Inc., 2003.

[16] M. Demirbas and Y. Song, "An rssi-based scheme for sybil attack detection in wireless sensor networks," in *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*. IEEE Computer Society, 2006, pp. 564–570.

[17] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM workshop on Wireless security*. ACM, 2006, pp. 33–42.

[18] I. E. Bagci, U. Roedig, I. Martinovic, M. Schulz, and M. Hollick, "Using channel state information for tamper detection in the internet of things," in *Proceedings of the 31st Annual Computer Security Applications Conference*. ACM, 2015, pp. 131–140.

[19] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE Journal on selected areas in communications*, vol. 29, no. 7, pp. 1469–1479, 2011.

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

[21] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric bayesian method," in *INFOCOM 2011-IEEE Conference on Computer Communications, IEEE*, 2011, pp. 1404–1412.

[22] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008, pp. 116–127.

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

[24] A. Tzur, O. Amrani, and A. Wool, "Direction finding of rogue wi-fi access points using an off-the-shelf mimocofdm receiver," *Physical Communication*, vol. 17, no. C, pp. 149–164, 2015.

[25] EldadPerahia and RobertStacey, *Next generation wireless LANs*. Cambridge University Press, 2008.

[26] K. Wu, J. Xiao, Y. Yi, M. Gao, and L. M. Ni, "Fila: Fine-grained indoor localization," in *INFOCOM 2012-IEEE Conference on Computer Communications, IEEE*, 2012, pp. 2210–2218.

[27] A. Stephens, *IEEE 802.11 TGn Comparison Criteria*. IEEE 802.11-03/814r31, 2004.

[28] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Understanding and modeling of wifi signal based human activity recognition," in *Proceedings of the 21st annual international conference on mobile computing and networking*. ACM, 2015, pp. 65–76.

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

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

[31] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11n traces with channel state information," *ACM SIGCOMM CCR*, vol. 41, no. 1, p. 53, Jan. 2011.