SecurePilot: Improving Wireless Security of Single-Antenna IoT Devices

Huangxun Chen, Qianyi Huang, Chenyu Huang, Chenchen Liu, Tony Xiao Han, and Qian Zhang, *Fellow, IEEE*

***Abstract*—With the arrival of the Internet-of-Things era, IoT devices and the services built on them make our lives more convenient and also raise public concerns on their vulnerability to attacks. Recent literature advocates physical-layer solutions to help IoT devices detect attacks instead of using sophisticated cryptographic methods. However, there is still no satisfying solutions for IoT devices with single antenna and sparse traffic. Thus, we introduce SecurePilot to fill this gap. SecurePilot is an unsupervised and plug-and-play solution which works without an attacker's knowledge in advance. It leverages the strengths of two orthogonal physical-layer information, propagation signatures and device signatures embedded in pilot signals to enable effective attack detection. It could work on single-antenna IoT devices with sparse traffic and also work compatibly with communication protocols. The experimental results show that SecurePilot can successfully detect 99.6% of attacks, triggering false alarms on 3.1% of legitimate traffic in a typical office environment.**

***Index Terms*—Single antenna IoT, wireless security, pilot signal, multipath channel, radio imperfection**

I. Introduction

Recently, IoT devices have been widely deployed as one of the most important building blocks in smart homes, intelligent factories and even smart cities to support numerous applications [1], [2]. In daily residential and office space, we have witnessed the increasing adoption of IoT devices, such as Amazon Ring doorbell [3], Google Nest thermostat [4], Philip smart bulbs [5], various smart locks [6], [7], smart speakers [8], [9] and health trackers [10], [11], which transmit many critical and private data using WiFi. Despite the convenience, IoT devices are particularly vulnerable to malicious attacks. As shown in Fig. 1, when an IoT device and an IoT Access Point (AP) interact with each other, an attacker may impersonate as a legitimate device to send packets to disturb their transmission, *e.g.*, make them disassociated and launch man-in-the-middle attack. Such attacks have been successfully launched to some commercial products, like Amazon's Ring Video Doorbell [12] and KeyWe Smart Lock [13]. In these real attacks, the attacker infers the key command of the transmission and inject it opportunistically to defraud the doorbell of home wifi-password or fool the smart lock to unlock the door. Thus, it presses for an effective and plug-and-play (*i.e.*, not require any training phase or prior knowledge of attackers.) approach to find out the attack during transmission to help trigger further protective actions.

Many existing works [14], [15], [16], [17] advocate using physical-layer propagation signatures to secure a wireless system against such attacks. An attacker is highly unlikely located at the exact same place as a legitimate device (IoT or IoT AP). Thus, when an attack occurs, an IoT receiver could observe a noticeable abnormal deviation in the feature space of physical-layer propagation signatures as shown in Fig. 1. It is worth mentioning that the feature space could be high-dimensional though Fig. 1 only presents single dimension for convenient illustration. Compared with some advanced cryptographic protocols, physical-layer solutions are generally more affordable for IoT devices with minimalist designs. However, we believe further efforts can be made to advance this direction. SecureArray [14] extracts sensitive angle-of-arrival (AoA) signatures using multiple half-wavelength separated antennas, which can not work on IoT devices with small form-factor and single antenna. SNAP [17] leverages the signal behavior in a transmitting antenna's near-field region to securely paring IoT devices, which can not work when two devices are not in proximity. In addition, the frequency (*i.e.*, number per second) of exchanged packets in many typical IoT networks, such as smart building and supply chain tracking are below 5Hz (*i.e.*, sparse traffic) for power saving [18]. Thus, it may not be ideal for them to adopt channel state information (CSI) signatures that need to be averaged over multiple consecutive Wi-Fi packets (*e.g.*, around 45 in [15]). We prefer physical-layer signatures whose effectiveness and robustness do not heavily rely on the number of available Wi-Fi packets. For the compatibility with communication (*e.g.*, Wi-Fi), the backscatter-assisted solution [16] is not suitable since its requires transmitting sinusoidal waves. Many device identification schemes [19], [20], [21], [22], [23], [24] generally register devices' signatures in the training stage for future classification/matching. However, detecting attacks in Fig. 1 prefers an unsupervised and plug-and-play solution which works without an attacker's knowledge in advance.

To fill this gap, this paper introduces *SecurePilot* for IoT devices with single antennas and sparse traffic. The ultimate

This work was partially supported by the RGC under Contract CERG 16204418, 16203719, 16204820, R8015 and the Guangdong Natural Science Foundation No. 2017A030312008. (*Corresponding author: Qian Zhang.*)

Huangxun Chen is previously with Department of Computer Science and Engineering, Hong Kong University of Science and Technology, and now with Huawei Theory Lab, Hong Kong, China (Email: hchenay@connect.ust.hk, chen.huangxun@huawei.com).

Qianyi Huang is with the Institute of Future Networks, Southern University of Science and Technology, Shenzhen 518055, China, and also with the Network Communication Research Center, Peng Cheng Laboratory, Shenzhen 518066, China (Email: huangqy@sustc.edu.cn).

Chenyu Huang and Qian Zhang are with Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong, China (Email: chuangak@connect.ust.hk, qianzh@cse.ust.hk).

Chenchen Liu and Tony Xiao Han are with Huawei 2012 Labs, Shenzhen, China (Email: liuchenchen1@huawei.com, tony.hanxiao@huawei.com).

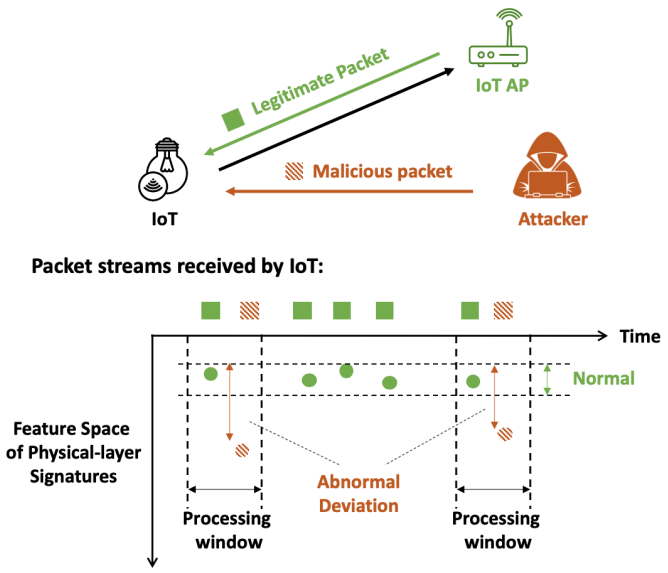

Fig. 1. Attack detection based on physical-layer signatures.

goal of our system is to help them find out attacks during transmission as in Fig. 1 without the need of multiple antennas, dense traffic and the violation of WiFi transmission. SecurePilot leverages the physical-layer signatures embedded in pilot signals to achieve its goal. Specifically, partial sub-carriers in each Wi-Fi symbol are populated with predefined modulated symbols, denoted as pilot signals in Fig. 3. Pilot-based signatures are compatible with WiFi transmission, and also more feasible for single-antenna IoT devices than AoA-based ones. Compared with CSI, they also carry propagation signatures and have advantages in temporal domain to help relax the requirements of dense traffic, because given one WiFi packet with multiple symbols, we can only obtain one CSI sample but multiple samples of pilot signals.

Despite above benefits, it is challenging to extract robust pilot-based signatures for attack detection due to deficiency of pilot signals on frequency domain. Pilot signals only capture propagation signatures of a few sub-carriers rather than the whole channel (Fig. 3). To address this challenge, we observe that another dimension information, device-specific signatures incorporated in pilot signals can be leveraged to reinforce pilot-based signatures. Just as no two devices are located at the exact same location, no two ones have the exact same manufacturing imperfections. Through our derivation, a pair of symmetric pilot signals carries the effects of such imperfections. However, the limited pairs of pilot signals along frequency domain make it still challenging to figure out effective signatures covering the superposition effect of both channel propagation and device imperfection. To overcome this challenge, we observe the cyclical varying symbol patterns of same pair of pilot signals along time domain and leverage this property to extract both propagation and device-specific signatures simultaneously from pilot signals of single packet for attack detection. The former is location- and time-specific, since the wireless channels are generally uncorrelated beyond the distance over a half-wavelength of carrier frequency and changing out of coherence time, while the latter is transceiver-specific, because even two radios of the same type can experience different manufacturing imperfections. Our method not only compensates deficiency of pilot signals in frequency domain, but also places more burden on attackers by making forging signatures more difficult.

Contributions The contributions of this paper are threefold: Firstly, we propose an effective scheme for IoT devices to detect attacks with single-antenna, sparse traffic, compatibility with original WiFi communication. Secondly, we provide an efficient method to extract robust pilot-based signatures, which combines strengths of both channel propagation and device signatures embedded in pilot signals to make it harder to attack. Thirdly, we evaluate our system under various compound factors. Our results show that the proposed system can detect 99.6% of attack attempts, while triggering false alarms on 3.1% of legitimate traffic in a typical office environment.

II. System Design

In this section, we first introduce the threat model addressed in this work (Section II-A). Next, we give an overview of the system workflow (Section II-B). Then we illustrate the technical details on pilot signal extraction (Section II-C) and propagation and device signatures extraction from pilot signals of single packet for comparison (Section II-D), which is the key step to detect attack during transmission. Finally in Section II-E, we present an experiment to intuitively demonstrate the benefits of compound signatures in attack detection.

A. Threat Model

In our threat model, similar to previous works [16], [14], it is assumed that an attacker has some priori knowledges of the protocols and legitimate devices, such as SSID, MAC address, secret credentials, carrier frequency, coding scheme, and *etc*. The attack may sniff traffic to get basic information of legitimate devices (e.g., device type) and further infer more from the Internet or the source like [25]. Thus, it can assemble packets following the well-known Wi-Fi protocol or copy one legitimate device's identity but include fake command/data to fool the other. It is assumed that attacker will not blindly launch attacks, because that will dramatically increase its exposure risk and also not efficient since IoT devices may not listen packets at most time (*i.e.*, sleep mode) to save energy. It is assumed that the attacker takes a smarter move to first act as a sniffer to get window of opportunity, once a wake-up IoT/IoT AP sends initial packet(s) to invite another device for link establishment and communication, the attacker grasps this opportunity to send its malicious packet. If the attack succeeds, it may cause unauthorized access to the IoT AP or rejection of the legitimate IoT during link establishment, or makes IoT's data delivered wrongly or stolen by the attacker during data sharing. It is assumed that IoT devices are equipped with single-antenna and they does not have priori knowledge of the attackers.

B. System Workflow and Overview

The workflow of SecurePilot is demostrated in Fig. 2. The receiver will maintain a sliding processing window and initiate pilot-based signature extraction and comparison between two packets within the window. Based on the threat model in Section II-A, IoT initially receives one or a few legitimate packets. If the system detects the difference between two signature profiles to be within normal range, then IoT continues the normal transmission. Otherwise, if the system detects abnormal deviation between two profiles, then an potential attack is detected and proper actions should be executed like further examining or packet dropping. Next, we will introduce the detailed operations in the modules of pilot signal extraction, signature extraction and comparison respectively.

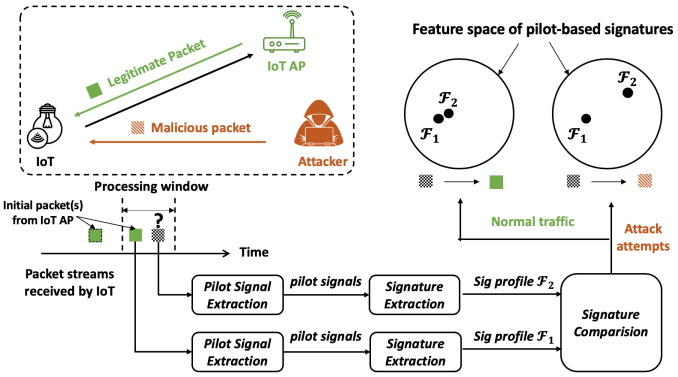

Fig. 2. System workflow of SecurePilot.

C. Pilot Signal Extraction

The first processing module of the system is to extract pilot signals from a WiFi packet. The Wi-Fi physical layer [26] builds upon the orthogonal frequency division multiplexing (OFDM) technique, where a wide bandwidth (*e.g.*, 20MHz) is divided into multiple (*e.g.*, 64) orthogonal sub-carriers, each of which supports a constellation symbol with many bits per symbol. Given modulated symbols $S_k(k = -32, ..., -1, 0, 1, ..., 31)$ transmitted on sub-carriers and a 20MHz sampling rate, a baseband OFDM waveform in Wi-Fi is constructed as an inverse Fourier transform of S_k.

$$r(t) = \frac{1}{N} \sum_{k} S_k exp(j2\pi k \Delta_F t), 0 \leq t < T \qquad (1)$$

where Δ_F (=312.5 kHz) is the sub-carrier frequency spacing; T (=3.2μs) is the inverse Fourier transform symbol period with $\Delta_F = 1/T$, and N (=64) is the number of samples in the inverse Fourier transform. Among 64 sub-carriers in WiFi (802.11n), besides data sub-carriers and non-populated sub-carriers, four sub-carriers are used as pilot signals for phase and frequency tracking and training [27]. Numbering the sub-carrier locations as -32, -31, ..., -1, 0, 1, ..., 31, the pilot sub-carriers are located in $-21, -7, 7$ and 21 sub-carriers (Fig. 3). Pilot signals are inserted in all symbols of L-SIG, H-SIG and Data fields in Fig. 3, which means one WiFi packet has multiple samples of pilot signals.

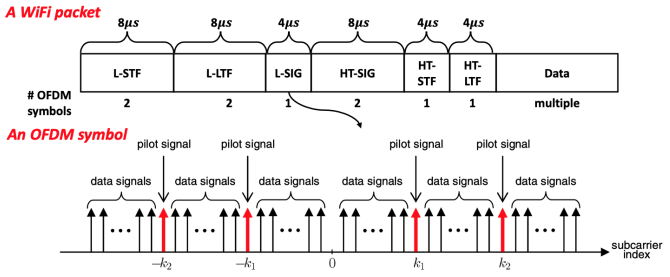

Fig. 3. Frame structure of a WiFi packet and pilot signals in a WiFi OFDM symbol ($k_1 = 7, k_2 = 21$).

Therefore, the module of pilot signal extraction reuses partial functions of packet reception, including down conversion, low-pass filter (LPF), Analog-to-Digital conversion (A/D) and FFT operation. Unlike the normal reception which conducts equalization to decode data signals afterwards, we extract unequalized pilot signals and feeds them into the next module.

D. Pilot-based Signatures Extraction and Comparison

As in Fig. 2, effective and robust signatures are critical to attack detection. Thus, this section will cover the technical details on extracting pilot-based signatures from a WiFi packet.

1) Signatures embedded in pilot signals: Pilot-based signatures extracted by our method carry the superposition effects of both manufacture imperfections and channel propagation.

In terms of manufacture imperfections, most Wi-Fi network interface cards (NICs) adopt direct conversion radio architecture [28] as shown in Fig. 4, where quadrature/complex mixers are used to up-convert the signal to Radio Frequency (RF) for transmission, and down-convert it to baseband for reception. It provides benefits for current consumption, size, radio performance and inherently allows a great degree of channel bandwidth flexibility, but also suffers from inevitable I/Q imbalance [29], one type of manufacture imperfections.

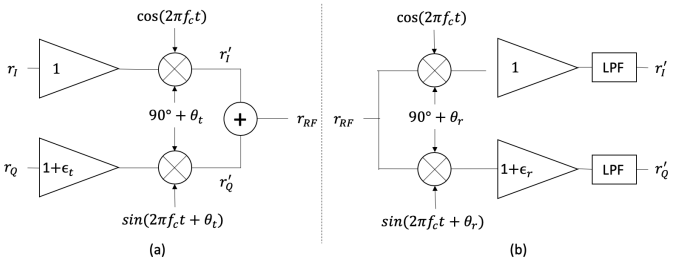

Fig. 4. Direct-conversion radio: I/Q imbalances in transmission (sub-fig (a)) and reception (sub-fig (b)).

In an ideal radio, I and Q branches have the same gain with $\frac{\pi}{2}$ phase difference. However, quadrature mixers in direct conversion radios are impaired by gain mismatch (ϵ) and phase mismatch (θ) of I and Q branches. To simplify the following analysis, this paper adopts an I/Q imbalance model where the effects of both gain and phase imbalances are on the Q branch. As shown in Fig. 4, the ideal signal $r(t) = r_I(t) + jr_Q(t)$,

$r_I(t)$ and $r_Q(t)$ denote the real and imaginary parts of the ideal baseband signals without I/Q imbalance respectively.

$$\begin{aligned} r_I(t) &= r_{RF}(t) \cdot cos(2\pi f_c t) \\ r_Q(t) &= r_{RF}(t) \cdot sin(2\pi f_c t) \end{aligned} \tag{2}$$

where f_c is the carrier frequency. Then the signal impaired by I/Q imbalance is $r'(t) = r'_I(t) + jr'_Q(t)$, where

$$\begin{aligned} r'_I(t) &= r_{RF}(t) \cdot cos(2\pi f_c t) \\ &= r_I(t) \\ r'_Q(t) &= r_{RF}(t) \cdot (1+\epsilon) \cdot sin(2\pi f_c t + \theta) \\ &= (1+\epsilon)cos(\theta) \cdot r_Q(t) + (1+\epsilon)sin(\theta) \cdot r_I(t) \end{aligned} \tag{3}$$

From the perspective of communication, I/Q imbalances will cause channel estimation errors and disturb demodulation. Considerable works have estimated and compensated them to improve communication [30], [31]. From the perspective of security, I/Q imbalances are a kind of unique manufacturing imperfection, which are varied across different radios even those of the same type. Such device signatures may fluctuate due to temperature and device aging. However, this does not affect their effectiveness on attack detection in Fig. 2, because our system detects attacks by observing signature deviation within processing window, *i.e.*, it does not compare signatures of recent packets with a stored template long before.

To show the effect of this imperfection on pilot signals, we rearrange Equation 3 as follows:

$$\begin{aligned} r'(t) &= r'_I(t) + jr'_Q(t) \\ &= r_I(t) + j[(1+\epsilon)cos(\theta) \cdot r_Q(t) + (1+\epsilon)sin(\theta) \cdot r_I(t)] \\ &= \alpha(r_I(t) + jr_Q(t)) + \beta(r_I(t) - jr_Q(t)) \\ &= \alpha r(t) + \beta r^*(t) \end{aligned} \tag{4}$$

where

$$\begin{aligned} \alpha &= \frac{1}{2}[1 + (1+\epsilon)(cos(\theta) - jsin(\theta))] \\ \beta &= \frac{1}{2}[1 - (1+\epsilon)(cos(\theta) + jsin(\theta))] \end{aligned} \tag{5}$$

It is noticed that I/Q imbalance (ϵ and θ) generates an extra image signal $r^*(t)$, which is the complex conjugate of the original signal $r(t)$. Considering an OFDM-modulated WiFi baseband signal $r(t)$:

$$\begin{aligned} r'(n) &= \alpha r(n) + \beta r^*(n) \\ &= \frac{\alpha}{N} \sum_{k=-N/2}^{k=N/2-1} S_k e^{j2\pi kn/N} + \frac{\beta}{N} \sum_{k=-N/2}^{k=N/2-1} S_k^* e^{-j2\pi kn/N} \end{aligned} \tag{6}$$

By taking the N-point discrete Fourier transform (DFT) of above equation, the signal in the frequency domain is:

$$R'(k,n) = \alpha S(k,n) + \beta S^*(-k,n) \tag{7}$$

where $R'(k,n)$ and $S(k,n)$ denote the distorted symbol and original one at the k-th sub-carrier of the n-th OFDM symbol, and α and β denote the device signatures stemming from radio's I/Q imbalance (gain and phase imbalances ϵ and θ).

From Equation 7, it is noted that I/Q imbalance in WiFi causes the crosstalk phenomenon between symmetrical sub-carriers, where symbol on sub-carrier k leaks into mirror sub-carrier $-k$ and vice versa. Since pilot signals are located in symmetrical sub-carriers (see Fig 3), we can extract device-specific signatures from mirror pilot signals.

Given a pair of transceivers, the transmitted signals will be distorted by transmitter's I/Q imbalance (α_t, β_t), wireless channel H and receiver's I/Q imbalance (α_r, β_r) successively. Based on Equation 7, the signal transmitted by the I/Q imbalanced transmitter is:

$$X(k,n) = \alpha_t S(k,n) + \beta_t S^*(-k,n) \tag{8}$$

Then, given channel response at k-th sub-carrier H_k,

$$\begin{aligned} Y(k,n) &= H_k X(k,n) \\ &= H_k[\alpha_t S(k,n) + \beta_t S^*(-k,n)] \end{aligned} \tag{9}$$

Finally, the received signal at I/Q imbalanced receiver is:

$$R'(k,n) = \alpha_r Y(k,n) + \beta_r Y^*(-k,n) \tag{10}$$

Substituting Equation 9 into Equation 10, we have:

$$R'(k,n) = C_1^k \cdot S(k,n) + C_2^k \cdot S^*(-k,n) \tag{11}$$

where

$$\begin{aligned} C_1^k &= \alpha_r H_k \alpha_t + \beta_r H_{-k}^* \beta_t^* \\ C_2^k &= \alpha_r H_k \beta_t + \beta_r H_{-k}^* \alpha_t^* \end{aligned} \tag{12}$$

As shown in Equation 5, α and β are functions of I/Q imbalance parameters, gain and phase imbalance ϵ and θ, which represent device-specific signatures. And channel response H represents the propagation signatures. Thus, Equation 12 shows (C_1^k, C_2^k) contain the effects from both device and propagation signatures. It is worth mentioning that the transmitter's device signatures (α_t, β_t) matter more than the receiver's ones (α_r, β_r) in attack detection in Fig. 2.

2) Signature extraction and comparison: If we can obtain two independent equations with the form as Equation 11, compound physical-layer signatures (C_1^k, C_2^k) can be solved out and utilized in attack detection. An intuitive thought is to leverage two pairs of pilot signals along the frequency domain (see Fig. 3), the estimated channel responses H from CSI and the pre-measured I/Q imbalances of the receiver (α_r, β_r) to solve the following equation set:

$$\begin{cases} R'(k_{p1},n) = C_1^{k_{p1}} \cdot S(k_{p1},n) + C_2^{k_{p1}} \cdot S^*(-k_{p1},n) \\ R'(k_{p2},n) = C_1^{k_{p2}} \cdot S(k_{p2},n) + C_2^{k_{p2}} \cdot S^*(-k_{p2},n) \end{cases} \tag{13}$$

where $k_{p1} \in \{7, -7\}$ and $k_{p2} \in \{21, -21\}$

However, this method has fundamental flaws because I/Q imbalance parameters are frequency-dependent [32]. Compared with pilot sub-carriers in DVB-T only having 4kHz frequency spacing [33], the pilot sub-carriers in the Wi-Fi protocol are separated with larger spacing (14*312.5kHz = 4375kHz). Thus, Equation 12 should be revised as:

$$\begin{aligned} C_1^k &= \alpha_r^k H_k \alpha_t^k + \beta_r^k H_{-k}^* (\beta_t^k)^* \\ C_2^k &= \alpha_r^k H_k \beta_t^k + \beta_r^k H_{-k}^* (\alpha_t^k)^* \end{aligned} \tag{14}$$

Therefore, it is infeasible to solve Equation 13. Instead of using pilot pairs along the frequency domain, we resort to

pilot pairs of contiguous WiFi OFDM symbols along the time domain. Specifically, the equation set used to figure out the compound signatures is as follows:

$$\begin{cases} R'(k_p,n) = C_1^{k_p}\cdot S(k_p,n) + C_2^{k_p}\cdot S^*(-k_p,n) \\ R'(k_p,n+1) = C_1^{k_p}\cdot S(k_p,n+1) + C_2^{k_p}\cdot S^*(-k_p,n+1) \end{cases} \tag{15}$$

where $k_p \in \{7,-7,21,-21\}$.

If we define a matrix A as follows:

$$A = \begin{bmatrix} S(k_p,n) & S^*(-k_p,n) \\ S(k_p,n+1) & S^*(-k_p,n+1) \end{bmatrix} \tag{16}$$

A full-rank matrix A is the precondition of solving $(C_1^{k_p}, C_2^{k_p})$ from Equation 15, *i.e.*, $rank(A) = 2$. According to WiFi standard [27], the modulated signals inserted at the positions of pilot signals for single-antenna devices are:

$$S_n^{-21,-7,7,21} = \{\Psi_{n\oplus 4}, \Psi_{(n+1)\oplus 4}, \Psi_{(n+2)\oplus 4}, \Psi_{(n+3)\oplus 4}\} \tag{17}$$

where $n \oplus a$ indicates symbol number n modulo integer a, and the pattern Ψ_n is $\{\Psi_0 = 1, \Psi_1 = 1, \Psi_2 = 1, \Psi_3 = -1\}$. Thus, the pattern is cyclically shifted from symbol to symbol (Table I) due to the modulo indexing operation of $\Psi_{n\oplus 4}$. Thus, we can have a full-rank matrix A.

TABLE I
PILOT SIGNALS ACROSS WIFI OFDM SYMBOLS.

$S(k_p,n)$ k_p \ n	0	1	2	3	4	...
-21	1	1	1	-1	1	...
-7	1	1	-1	1	1	...
7	1	-1	1	1	1	...
21	-1	1	1	1	-1	...

Based on Equation 15, the module of signature extraction derives the compound signatures as follows:

$$\begin{bmatrix} C_1^{k_p} \\ C_2^{k_p} \end{bmatrix} = A^{-1} \begin{bmatrix} R'(k_p,n) \\ R'(k_p,n+1) \end{bmatrix} \tag{18}$$

where $k_p \in \{7,-7,21,-21\}$. Then, the signature profiles are constructed as follows for comparison.

$$\mathcal{F} = \{(|C_1^{k_p}|, |C_2^{k_p}|)\}, k_p \in \{7,-7,21,-21\} \tag{19}$$

Equation 15 requires pilot signals from at least two contiguous symbols to extract signatures. A Wi-Fi packet generally has several symbols depending on the amount of transmitted data and the modulation type. Thus, the compound signatures of a packet can be obtained by averaging multiple ones extracted from every two contiguous OFDM symbols that satisfy full-rank requirement of matrix A.

In terms of signature comparison, to detect attack in plug-and-play manner, for two contiguous packets in the processing window, we extract pilot-based signatures respectively from them, *i.e.*, we obtain two signature profiles $\mathcal{F}_1$ and $\mathcal{F}_2$. Based on our evaluation, the differences between profiles of different transmitters are evident in Euclidean space. Thus, we adopt the Euclidean distance to quantify their distinction as in Equation 20. When the estimated distance $\mathcal{D}(\mathcal{F}_1,\mathcal{F}_2)$ is larger than a threshold η, an potential attack is detected; otherwise, they are regarded as normal traffic. The detailed discussion about threshold determination is elaborated in Section III-B1.

$$\begin{aligned} \mathcal{D}(\mathcal{F}_1,\mathcal{F}_2) = sqrt(\sum_{k_p}\{(|(C_1^{k_p})_{\mathcal{F}1}| - |(C_1^{k_p})_{\mathcal{F}2}|)^2 \\ + (|(C_2^{k_p})_{\mathcal{F}1}| - |(C_2^{k_p})_{\mathcal{F}2}|)^2\}) \end{aligned} \tag{20}$$

E. Demonstrating Benefits of Compound Signatures

The key advantage of our system is combining two orthogonal dimensions of information from pilot signals of single packet, location- and time-specific propagation signatures and transceiver-specific ones to provide effective attack detection for IoT devices with single antenna and sparse traffic.

To demonstrate its benefits intuitively, we set up a stringent attack scenario. We run our system on a single-antenna receiver to collect packets from two other devices within wireless coherence time. One device acts as a legitimate user and the other acts as an attacker. Besides, their antennas are within 1cm distance and they have the same type Wi-Fi radios. Within wireless coherence time, two devices take turns to send packets to the receiver. CSI amplitudes/phases of collected packets in Fig. 5 shows that the propagation signatures of the attacker's packets are almost the same as those from legitimate device. However, the extracted pilot-based signatures in the rightmost of Fig. 5 still exhibit evident differences between two different transceivers with the assistance from transceiver-specific signatures.

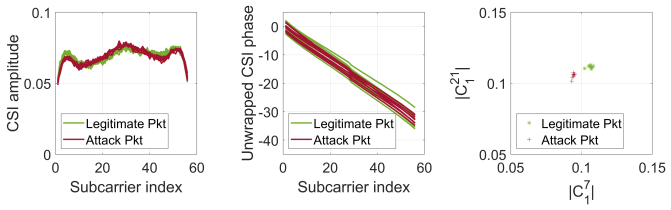

Fig. 5. From left to right: CSI amplitudes profiles, CSI phases profiles and partial pilot-based signatures profiles of the received packets respectively.

III. EVALUATION

We first describe our experimental settings, then evaluate the system performance in different situations respectively. Finally, we analyze the system latency.

A. Experimental Setting

The ultimate goal of our system is to help IoT detect attacks during transmission without the need of multiple antennas, dense traffic and the violation of WiFi transmission. To achieve this goal, it is critical to detect whether two packets (expected to be sent by the same transmitter) within coherent time are sent from different transmitters or not. Therefore, our evaluation focuses on quantifying our system's performance on this key capability.

In the evaluation, we implement the proposed system on a laptop using Matlab. A single-antenna radio front end implemented on Rice WARP v3.0 platform [34] sends the received WiFi signals back to Matlab for processing.

Eight pairs of Wi-Fi radios operating in the 2.4GHz band are involved in experiments and each pair of them contains two Wi-Fi radios of the same type, *i.e.*, they are manufactured by the same vendor and all their factory parameters including antenna gain and sensitivity are the same. It is worth mentioning that our goal is not to classify these 16 (8 pairs) devices. Instead, we use each pair of them to mimic stringent attack scenarios: attacker use the same type radio as legitimate device. For each pair, when one of them acts as the legitimate device, the other will act as the attacker. We adopt this setting to impose stringent attacks to challenge our system.

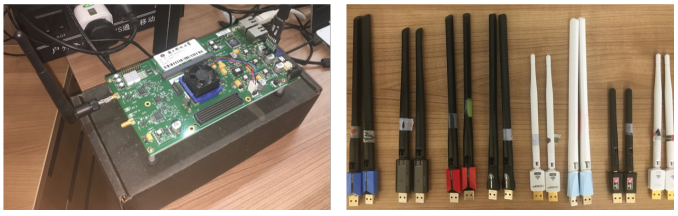

Fig. 6. **Left sub-figure**: Radio front end of the prototype on Rice WARP 3.0. **Right sub-figure:** Eight pairs of Wi-Fi radios operating in 2.4GHz band act as the legitimate devices and active attackers.

In the experiments, we let a pair of legitimate device and attacker send packets to the receiver equipped with our proposed system, covering the cases of both normal traffic and attack attempts in Fig. 7 with various compound factors (including different Tx-Rx distances, attack distances, packet intervals, packet durations and radio types). The receiver runs the proposed system to detect attack attempts.

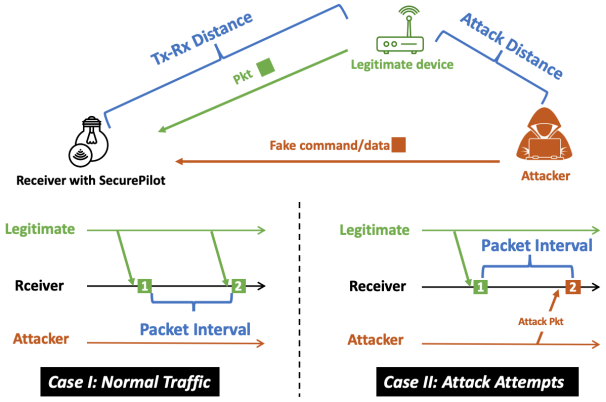

Fig. 7. Cases and compound factors in the evaluation.

For static experiments (*i.e.*, the devices did not move), we deploy the legitimate devices at 20 randomly chosen positions in a 27×6.5 meters typical office environment as shown in Fig. 8. The tested positions (blue squares in Fig 8) include both the line-of-sight (LOS) and non-line-of-sight (NLOS) cases, and also cover the positions behind or near wood cabinet, plastic water dispenser, mental machine cases, leather sofa, concrete wall and people who are typing in the office to make our evaluation more comprehensive and realistic.

In terms of location of attackers, it is well-known that location correlation is one of important properties of wireless propagation channels, *i.e.*, the propagation characteristics

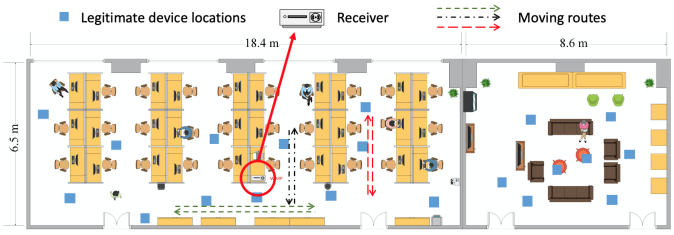

Fig. 8. Floor plan of our evaluation environment.

are generally uncorrelated beyond the distance over a half-wavelength of the carrier frequency [35]. Thus, to test the system robustness, we randomly deploy attackers at a specific distance with respect to legitimate devices, which varies from two and a half meters down to around five centimeters. It is worth mentioning that 'attack distance' is different from 'Tx-Rx distance'. As blue squares shown in Fig. 8, the distance between Tx and Rx are up to 15.5 meters in NLOS cases. 'Attack distance' refers to the distance between legitimate device and attacker (see Fig. 7), which varies from 5 centimeters to 2 meters in our evaluation. Besides, the intervals fall in the range from 2 milliseconds to 2 seconds for every two consecutive Wi-Fi packets for signature extraction and comparison.

We conduct evaluation in a functioning office and run the experiments in both daytime and nighttime. Beside the deployed devices, the wireless environment of our evaluation site has three other APs and tens of clients communicating.

For dynamic experiments, we evaluate two cases, one of them has a volunteer walking and doing activities nearby deliberately, and the other has both the legitimate device and the attacker moving at the same time. Other settings are similar to those in static experiments.

We adopt the following metrics to evaluate the performance:

- True Positive (TP): An attack attempt is identified correctly. (Detected attack)
- False Negative (FN): An attack attempt is identified as normal traffic. (Missed attack)
- False Positive (FP): A normal traffic is identified as attack attempt. (False alarm)
- True Negative (TN): A normal traffic is identified correctly. (Normal traffic)
- Attack Detection Rate = $\frac{TP}{TP+FN}$: ratio of detected attacks among all attacks.
- Attack Miss Rate = $\frac{FN}{TP+FN}$: ratio of missed attacks among all attacks.
- False Alarm Rate = $\frac{FP}{FP+TN}$: ratio of false alarm among all normal traffic.
- Legitimate Detection Rate = $\frac{TN}{FP+TN}$: ratio of detected normal traffic among all normal traffic.

B. Experiments in Relatively Static Environment

In this section, we present the system performance in a typical office environment when devices are static. We evaluate the system with different combinations of Wi-Fi radio types, device locations, distances between attackers and legitimate devices and time intervals between collected Wi-Fi packets.

1) Overall performance and threshold determination: The distance $\mathcal{D}$ between signature profiles (Fig. 2) should be compared with an appropriate threshold η to reject attack attempts and accept normal traffic. To determine the best threshold, we examine the attack detection rate and legitimate detection rate for various choices of threshold η. The results averaging across different radio types, Tx-Rx distances, attack distances and packet intervals are shown in Fig. 9. It is obvious that the attack detection rate increases when the threshold η decreases, while the legitimate detection rate has the opposite trend. That is because when threshold η decreases, the bound to be identified as normal traffic tightens. Thus, more attack attempts are excluded, resulting in high attack detection rate. However, when threshold η becomes smaller, some legitimate traffic may also be mis-recognized as attacks, resulting in low legitimate detection rate. When $\eta = 0.045$, SecurePilot achieves 97.6% attack detection rate and 97.2% legitimate detection rate, *i.e.*, triggering false alarm on 2.8% of legitimate traffic. We argue that such system has less tolerance to attack detection than false alarm. Thus, we choose to trade a little false alarm for higher attack detection rate by setting a stricter threshold $\eta = 0.04$, where SecurePilot achieves 99.6% attack detection rate at a false alarm rate as 3.1%. We evaluate with threshold $\eta = 0.04$ in the remainder of our evaluation.

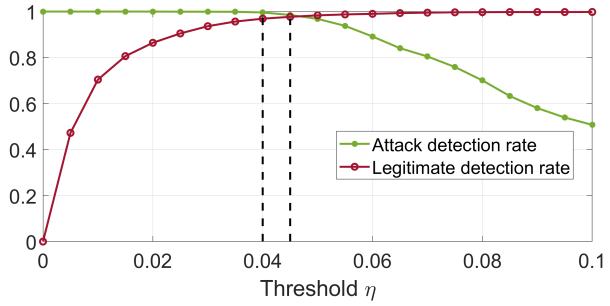

Fig. 9. System performance w.r.t various threshold η.

2) Impact of distance between attacker and legitimate device: Usually, the attacker will be far way from the legitimate device to reduce exposure risk. However, it is still possible that the attacker can be closer when smart devices become smaller and even miniature. Thus, to demonstrate the system capability on handling the cases where the attackers are close to legitimate users, we evaluate the performance with respect to different attack distances between them. In particular, we move an attacker from around two and a half meters to five centimeters away from a legitimate user to evaluate the system performance. The results are shown in Fig 10, which are averaged across different radio types, Tx-Rx distances and packet intervals. It is noticed that we achieve almost 100% attack detection rate under different attack distances, even for closer ones, 5cm and 10cm, which validates the system effectiveness in attack detection for IoT devices. However, when the attack distances become smaller, the false alarm rates also become higher since the distinction on propagation signatures, a part of pilot-based signatures, become smaller. However, they are still lower than 5% false alarm rate, which is acceptable for most IoT devices.

3) Impact of inter-packet time: The channel is dynamic between any particular antenna pair in both amplitude and phase. Our pilot-based signatures incorporate the propagation signatures, so that the channel stability has effects on the signature stability. Therefore, we present the performance results for different packet intervals, averaging across multiple radio types, Tx-Rx distances and attack distances.

Fig. 11 shows that in a typical working office environment when the devices are static, with the packet intervals from two millisecond to two second, SecurePilot still achieves good performance on attack detection, but obviously with an increasing false alarm rate. The reason that attack detection rates are not affected by the large packet intervals is that the signatures of malicious packets do not change to be similar to the legitimate ones as time goes. However, with packet interval increases, the legitimate ones will have larger signature distances due to channel instability so that some will be mis-regarded as attack attempts, resulting in higher false alarm rate.

4) Impact of packet duration (number of WiFi OFDM symbols): As mentioned before, the final signatures of a packet as in Equation 19 can be obtained by averaging multiple ones extracted from every two consecutive WiFi OFDM symbols, since a packet generally includes several symbols. Considering some IoT devices may only send small amount of data at a time, *i.e.*, small number of symbols in a packet, we naturally ask that does the number of OFDM symbols in a packet have effects on the system performance. Therefore, we evaluate the system performance with respect to the number of OFDM symbols. As shown in Fig. 12, the increase of symbol number can help reduce false alarm rate a bit, because averaging may rule out more noises and provide more stable signatures. But even with two symbols, the false alarm rate is within 5%, which is acceptable for the most daily IoT devices. Thus, even the packet carries little data, our system can utilize pilots from two consecutive OFDM symbols in L-SIG and H-SIG fields (Fig. 3) to extract signatures for attack detection.

5) Impact of packet signal-noise ratio (SNR): Considering in real scenarios, some IoT devices may experience low SNR due to long distance away transmitter or obstacles. We naturally wonder whether the proposed system still has a good performance on the noise-corrupted received signals. Therefore, our data collection covers both the short/long-range and LOS/NLOS cases. We evaluate the system performance with respect to the signal-noise ratio (SNR) of collected packets. We calculate SNR of a packet based on estimated error vector magnitude (EVM) between received symbols and constellation symbols [36]. As shown in Fig. 13, the increase of SNR level can help reduce false alarm rate and improve attack detection rate, because high SNR level helps extracting more stable signatures. But even in low-SNR cases, the attack detection rate is above 95% and the false alarm rate is only a little bit above 5%.

C. Experiments in Dynamic Environment

Coherence time is another important properties of wireless propagation channels. Wireless coherence time (T_c) refers to

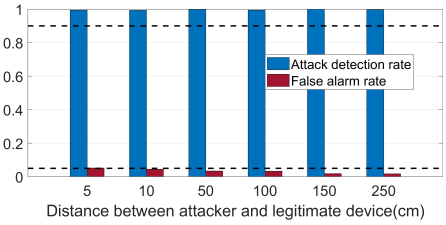

Fig. 10. Different attack distances.

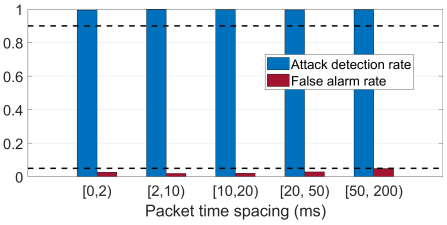

Fig. 11. Different packet intervals.

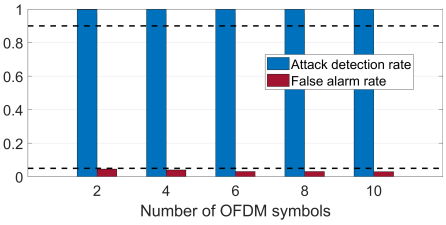

Fig. 12. Different symbol numbers.

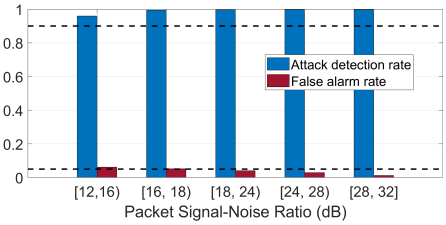

Fig. 13. Different SNR levels.

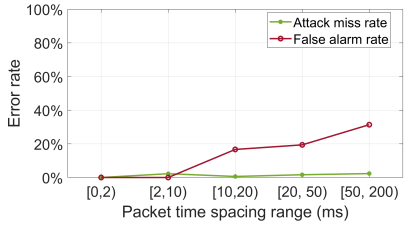

Fig. 14. People walking around.

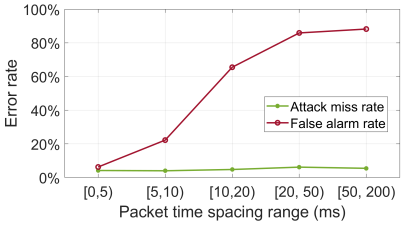

Fig. 15. Moving devices.

the time duration over which the wireless channel can be considered unchanging with high likelihood. It is determined by the carrier wavelength λ (m) and maximum object velocity v (m/s) in the environment as $T_c = \frac{9\lambda}{16\pi v}$ [14]. Given a normal walking speed $1.5m/s$ and 2.4 GHz band, $T_c = 14.3ms$. Thus, in this section, we set up two dynamic environments to evaluate the system performance.

1) People waking around: In the first case, we deliberately ask a volunteer to walk and do some activities (*i.e.*, playing on smartphones, waving hands) along the routes as shown in Fig. 8, which cover the cases including walking close around the devices, approaching the receiver and going across the channel between transceivers. We evaluate the system performance with respect to different packet intervals. As shown in Fig. 14, compared with the results in static experiments, when there are substantial movements nearby, the wireless coherent time become much shorter. Thus, to achieve both low attack miss rate and false alarm rate, the packet interval is better to be within ten milliseconds. Similar to Fig. 11, the false alarm rate is rising with the increasing packet interval. In the experiments of Fig. 11, people in the office are sitting and typing, *i.e.*, tiny movements. While in this part, the volunteer performs substantial movements on purpose around the devices during data collection. Thus, false alarm rates in Fig. 14 increase more sharply compared with those in Fig. 11.

2) Moving devices: In the second case, we evaluate a more challenging case where both attacker and legitimate device are moving at the same time. We place both devices on a platform with wheels and keep their antennas separated by 50 centimeters. We ask a volunteer to push/pull them along the routes shown in Fig. 8. These routes cover both LOS and NLOS cases since the working stations and people will block the direct transmission paths for some portions of routes. We evaluate the system performance with respect to different packet intervals. The results are shown in Fig. 15. Compared with Fig. 14, the wireless coherence time becomes much shorter, *i.e.*, 5 milliseconds for moving devices. The possible reason is that walking people around may pose effects on only one or two propagation paths, but a moving device experience dramatical changes of each propagation path, which pushes the allowed packet interval down to 5 milliseconds.

To sum up, in the dynamic environment, the wireless coherence time becomes shorter as expected in theory. Therefore, the allowed packet interval becomes shorter accordingly. However, considering short packets (microsecond-level duration) and low duty cycle of IoT devices, a millisecond-level packet interval is sufficient for most scenarios.

D. System Latency

A real-time system may prefer low-latency schemes. In our current implementation, the components of latency are analyzed as follows:

1) T_1 denotes time for packet detection and sample recording by receiver. When two symbols in L-SIG/H-SIG fields (Fig. 3) are utilized for pilot extraction, $T_1 = 24\mu s$.
2) T_2 denotes the time for transferring samples to Matlab. if we transmit time-domain samples of two symbols, there are 160 samples (20MHz $\times$ $4\mu s$ $\times$ 2) transferred at the rate of 1Mbps supported by WARP platform. Thus, T_2 =(160 samples) $\times$ (32 bits/sample) / (1 Mbit/s) = $5.12ms$. If the FFT operations are conducted to extract frequency-domain pilot signals on hardware level, then there are only 8 samples (4 pilot sub-carriers $\times$ 2 symbols) to be transferred, and T_2 =(8 samples) $\times$ (32 bits/sample) / (1 Mbit/s) = $256\mu s$
3) T_3 denotes the time for compute the signatures and make the comparison. For our current Matlab implementation with an Intel Core i7, 2.0GHz CPU and 8GB RAM, the processing time is around $2ms$.

Therefore, the total latency from the start of an examined packet is less than $8ms$, which will be improved when partial processing can be implemented on hardware level to reduce transfer cost for samples.

IV. Related Work

A. Physical-layer Propagation Signatures

In recent years, physical-layer propagation signatures have been extensively exploited to secure wireless systems against attacks. CSITE [15] uses Channel State Information(CSI) measurements averaged in time over around 45 packets to form a signature. Its performance is relevant to the traffic intensity of the legitimate user, Patwari *et al.* [37] and Zhang *et al.* [38] measure channel impulse response as temporal propagation signatures to identify the link between a pair of legitimate transceivers. SecureArray [14] constructs the highly sensitive angle-of-arrival (AoA) signature to secure Wi-Fi against attacks, which relies on multiple half-wavelength separated antennas, which does not fit for IoT devices with small form-factor and single antenna. ShieldScatter [16] resorts to nearby backscatters to help single-antenna devices extract multi-path propagation signatures. But it transmits sinusoidal waves and controls the tags to reflect them, which is not compatible with existing WiFi transmission. Physical-layer propagation signatures also play a critical role in proximity detection. Many existing works [39], [40], [41], [17], [42] use propagation signatures to securely pair two wireless devices in proximity (within half-wavelength of carrier frequency in general). However, they do not aim to protect the devices separated beyond a certain distance against attacks. In summary, the physical-layer propagation signatures are location-specific. If the attacker has chances to be located near the legitimate device (*e.g.*, using miniature attack devices), it is difficult to distinguish them only relying on propagation signatures.

B. Physical-layer Device Signatures

A large body of literatures have explored the device signatures for device identification. PARADIS [43] extracts minute transmitter-specific imperfections that are acquired at manufacture from the wireless signals and applies machine-learning tools to achieve NIC identification with 99% accuracy. Kohno *et al.* [20] and Suman *et al.* [19] exploit small, microscopic deviations in device hardware, clock skews for client fingerprinting. Hua *et al.* [21] derive the Carrier Frequency Offsets (CFOs) of wireless devices from CSI of tens of consecutive Wi-Fi packets as their hardware fingerprints. Liu *et al.* [22] extract the nonlinear phase errors of different subcarriers from CSI as device signatures for identification. Most works on device identification generally register devices' signatures in training stage for future classification/matching [23], [24]. However, different from device identification, our work focuses on attack detection. Thus, we propose an unsupervised and plug-and-play solution with no need for priori knowledge of attackers, since we detect attacks by observing abnormal signature deviation within the processing window. In addition, it is beneficial to combine the strengths of orthogonal signatures, both location- and time-specific propagation ones and device-specific ones to place more burden on attackers.

V. Discussion

A. Integrating with CSI

SecurePilot extracts signatures within one packet, where one CSI can also be extracted from the preamble (*i.e.*, L-LTF/HT-LTF in Fig. 3). In theory, propagation signatures carried in preamble can be included to enhance the system. However, we then need to balance the weight between signatures from preamble and pilot signals, which complicates the system unnecessarily given pilot-based signatures have achieved satisfying performance. It is also worth mentioning that we can not extract compound signatures from preamble as those from pilot signals. Because unlike cyclically shifted pattern in pilots signals (Table I), the symbols in preamble part are repeated (*i.e.*, exactly the same) so that it fails to satisfy the full-rank requirement. Thus, the current design does not include CSI.

B. Forge the Legitimate Device's Compound Signature

There are a few possible schemes that the attacker may employ to crack the system.

1. The attacker has a chance to be located near to the legitimate device, and has prior knowledge of the Wi-Fi radio type of the legitimate device. Our experimental results in Fig. 5 have demonstrated that our system can handle such attack due to the help from unique devices signatures that vary across different Wi-Fi radios even of the same type.

2. The attacker obtains the legitimate device's compound signatures, and then use an advanced radio platform to mimic the device's signature at a different location in order not to be discovered. We argue that this is difficult to be realized. The attacker firstly needs to be at the exact same position as the receiver to collect the legitimate device's signature. Besides, the radio difference between attacker and receiver also affects collected signatures since I/Q imbalances of reception side also manifest themselves into signatures.

Even we assume this signature can somehow be obtained, it is still challenging for the attacker to mimic it. To mimic the part of propagation signature, the attacker may exploit the method in [44] to emulate multipath propagations. To mimic the part of device signatures, we need to assume the attacker is equipped with advanced software-defined radios (SDRs) so that it can independently manipulate each pilot signal to mimic the legitimate device's signature. However, it is still impractical because I/Q imbalances are inevitable in direct-conversion radios, even for advanced SDRs like WARP and USRP. Therefore, when the attacker tires to manipulate symbol S_k on pilot sub-carrier k to forge α^k and β^k, I/Q imbalances of its own radio will manifest this manipulation into the results of α^{-k} and β^{-k}. The need to craft pilot signals that match all signatures in Equation 19 places quite a burden on the attacker. Moreover, in Wi-Fi protocols, signals on pilot sub-carriers are generally used for phase and frequency tracking [27], *i.e.*, helping demodulate data sub-carriers. Thus, such manipulation may affect the data reception of attack packet, *i.e.*, the attacker may fail to deliver fake command/data.

In summary, our system places heavy burden on the attacker to forge the legitimate device's signatures.

C. Compatibility with Various Antenna Capability

In this work, we emphasize the single-antenna capability of the receiver side since attack detection is conducted by the receiver. However, our proposed system can be easily extended to apply on multiple-antenna IoT devices. As shown in Section II, our physical-layer signature is derived from pilot signals of a Wi-Fi packet received from an antenna. If there are multiple antennas, we can obtain signatures for each antenna and expand the signature profiles $\mathcal{F}$ (Equation 19) accordingly for attack detection. The use of multiple antennas enhances signatures and will place more burden on the attackers to forge them. It is worth mentioning that our system does not have requirements on the transmitter side. In common practice, the antennas used for a link are negotiated and fixed between the transmitter and the receiver. Thus, the transmitter can use either single antenna or multiple antennas. To sum up, our proposed system can work compatibly on cases of different antenna capabilities of both transmitter and receiver side.

D. System Overhead

Our system provides a plug-and-play method to detect attacks by mapping received packets to pilot-based signature space and observing abnormal signature deviation. Thus, it can be called by upper-layer protocols to help find out attacks. In every calling, it introduces little overhead in terms of both hardware and software by reusing partial functions of original packet reception and processing pilot signals with low latency. The upper-layer protocol can flexibly balance the total overhead and security level by adjusting the calling frequency. For example, one of the most common threat to link establishment process is malicious deauthentication frame [45]. In this case, the association protocol may choose to call our system to help verify the received deauthentication frames for security.

VI. Conclusion

This work provides an plug-and-play attack detection system for IoT devices without the need of multiple antennas, dense traffic and the violation of WiFi transmission, and also with no need of priori knowledge of attackers. The proposed system extracts two orthogonal physical-layer information from pilot signals of single packet, combining strengths of both propagation and device signatures to detect attacks effectively and make forging signatures more difficult for attackers. The experimental results show that our system can successfully detect 99.6% attack attempts, only triggering false alarms on 3.1% of legitimate traffic in a typical office environment.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] D. Kumar, K. Shen, B. Case, D. Garg, G. Alperovich, D. Kuznetsov, R. Gupta, and Z. Durumeric, "All things considered: an analysis of iot devices on home networks," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 2019, pp. 1169–1185.

[3] Amazon ring doorbell. [Online]. Available: https://ring.com/

[4] Google nest thermostat. [Online]. Available: https://nest.com/

[5] Philip smart wi-fi bulbs. [Online]. Available: https://www.androidpolice.com/2019/08/09/philips-unveils-a-new-range-of-wi-fi-bulbs-that-forgo-the-hue-bridge/

[6] Samsung shp-dp609 wifi iot smart lock. [Online]. Available: https://www.samsungdigitallife.com/samsung-digital-door-locks/

[7] Keymitt smart lock and wi-fi hub. [Online]. Available: https://www.keymitt.com/

[8] Amazon echo smart speaker. [Online]. Available: https://www.amazon.com/all-new-Echo/dp/B07PBGN2WX

[9] Apple homepod smart speaker. [Online]. Available: https://www.apple.com/hk/en/homepod/

[10] Fitbit aria 2 smart scales. [Online]. Available: https://www.fitbit.com/eu/shop/aria2

[11] Apple watch. [Online]. Available: https://www.apple.com/apple-watch-series-5/

[12] Amazon's ring video doorbell lets attackers steal your wi-fi password. [Online]. Available: https://thehackernews.com/2019/11/ring-doorbell-wifi-password.html

[13] Smart lock has a security vulnerability that leaves homes open for attacks. [Online]. Available: https://www.cnet.com/home/security/smart-lock-has-a-security-vulnerability-that-leaves-homes-open-for-attacks/

[14] 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.

[15] 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 *2013 Proceedings IEEE INFOCOM*. IEEE, 2013, pp. 2544–2552.

[16] Z. Luo, W. Wang, J. Qu, T. Jiang, and Q. Zhang, "Shieldscatter: Improving iot security with backscatter assistance," in *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*. ACM, 2018, pp. 185–198.

[17] T. J. Pierson, T. Peters, R. Peterson, and D. Kotz, "Proximity detection with single-antenna iot devices," in *Proceedings of the 25th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '19. ACM, 2019.

[18] A. Pekar, J. Mocnej, W. K. Seah, and I. Zolotova, "Application domain-based overview of iot network traffic characteristics," *ACM Computing Surveys (CSUR)*, vol. 53, no. 4, pp. 1–33, 2020.

[19] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," in *International Conference on Mobile Computing and Networking*, 2008.

[20] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 2, pp. 93–108, 2005.

[21] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, "Accurate and efficient wireless device fingerprinting using channel state information," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 1700–1708.

[22] 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 *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 190–198.

[23] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, "Deep learning convolutional neural networks for radio identification," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 146–152, 2018.

[24] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu, and Y. Yan, "Design of a hybrid rf fingerprint extraction and device classification scheme," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 349–360, 2018.

[25] Hacker leaks passwords for more than 500,000 servers, routers, and iot devices. [Online]. Available: https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/

[26] I. S. Association *et al.*, "Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements, part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications," *IEEE Std*, vol. 802, p. 2793, 2012.

[27] P. Eldad and S. Robert, "Next generation wireless lans:'throughput, robustness, and reliability in 802.1 in," *Cambridge Univ. Press*, 2008.

[28] B. Razavi, "Design considerations for direct-conversion receivers," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 44, no. 6, pp. 428–435, 1997.

[29] L. Smaini, *RF Analog Impairments Modeling for Communication Systems Simulation*. Wiley Online Library, 2012.

[30] A. Tarighat, R. Bagheri, and A. H. Sayed, "Compensation schemes and performance analysis of iq imbalances in ofdm receivers," *IEEE Transactions on Signal Processing*, vol. 53, no. 8, pp. 3257–3268, 2005.
[31] K.-Y. Sung and C.-c. Chao, "Estimation and compensation of i/q imbalance in ofdm direct-conversion receivers," *IEEE Journal of Selected Topics in Signal Processing*, vol. 3, no. 3, pp. 438–453, 2009.
[32] Y. Zou, M. Valkama, and M. Renfors, "Pilot-based compensation of frequency-selective i/q imbalances in direct-conversion ofdm transmitters," in *2008 IEEE 68th Vehicular Technology Conference*. IEEE, 2008, pp. 1–5.
[33] E. ETSI, "Digital video broadcasting (dvb); framing structure, channel coding and modulation for digital terrestrial television," *ETSI EN*, vol. 300, no. 744, p. V1, 2004.
[34] Warp project. [Online]. Available: http://warpproject.org
[35] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" in *2013 Proceedings IEEE INFOCOM*. IEEE, 2013, pp. 200–204.
[36] R. A. Shafik, M. S. Rahman, and A. R. Islam, "On the extended relationships among evm, ber and snr as performance metrics," in *2006 International Conference on Electrical and Computer Engineering*. IEEE, 2006, pp. 408–411.
[37] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. ACM, 2007, pp. 111–122.
[38] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008, pp. 26–37.
[39] 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.
[40] N. Ghose, L. Lazos, and M. Li, "Sfire: Secret-free-in-band trust establishment for cots wireless devices," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 1529–1537.
[41] T. J. Pierson, X. Liang, R. Peterson, and D. Kotz, "Wanda: securely introducing mobile devices," in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 2016, pp. 1–9.
[42] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, "Proximity based iot device authentication," in *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*. IEEE, 2017, pp. 1–9.
[43] 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.
[44] S. Fang, Y. Liu, W. Shen, and H. Zhu, "Where are you from?: confusing location distinction using virtual multipath camouflage," in *Proceedings of the 20th annual international conference on Mobile computing and networking*. ACM, 2014, pp. 225–236.
[45] M. Eian and S. F. Mjølsnes, "A formal analysis of ieee 802.11 w deadlock vulnerabilities," in *2012 Proceedings IEEE INFOCOM*. IEEE, 2012, pp. 918–926.

Huangxun Chen received her Ph.D. degree in Computer Science and Engineering from the Hong Kong University of Science and Technology in 2020, supervised by Prof. Qian Zhang. During her Ph.D. study, she worked on topics in the intersection of intelligent IoT sensing and security. She received her B.S. degree in Computer Science and Technology from Shanghai Jiaotong University in 2015. She is currently a Researcher with Theory Lab of 2012 Labs, Huawei, Hong Kong.

Qianyi Huang received the bachelor's degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in July 2013 and the Ph.D. degree from the Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong, in November 2018. She is a Research Assistant Professor with the Southern University of Science and Technology, Shenzhen, China. She is also affiliated with Peng Cheng Laboratory. Her research interests lie in mobile computing, Internet of Things, and security.

Chenyu Huang received the B.S. degree in computer science from Wuhan University, Wuhan, China, in 2015, and the Ph.D. degree from Hong Kong University of Science and Technology, Hong Kong, in 2020. He is currently a Postdoctoral Researcher with Hong Kong University of Science and Technology. His research interests include mobile computing, IoT security, and blockchain.

Chenchen Liu received the B.E. degree from Tsinghua University in 2011 and the M.Phil. degree from the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology in 2013. He is currently a Research Engineer with Huawei Technologies Corporation Ltd., Shenzhen, China.

Tony Xiao Han (Member, IEEE) received the B.E. degree in electrical engineering from Sichuan University, in 2008, and the Ph.D. degree in communication engineering from Zhejiang University, Hangzhou, China, in 2013. He was a Postdoctoral Research Fellow with the National University of Singapore from 2013 to 2014. He then joined Huawei Technologies, Shenzhen, where he is currently a Principal Engineer with the 2012 Lab, Central Research Institute. His research interests include wireless communications, integrated sensing and communication, standardization in IEEE 802.11, and 3GPP. He served as the Chair of IEEE 802.11 WLAN Sensing Topic Interest Group, and he is currently the Chair of IEEE 802.11 WLAN Sensing Study Group.

Qian Zhang (Fellow, IEEE) received the B.S., M.S., and Ph.D. degrees in computer science from Wuhan University, Wuhan, China, in 1994, 1996, and 1999, respectively. She was with Microsoft Research Asia, Beijing, China, in July 1999, where she was the Research Manager with the Wireless and Networking Group. In September 2005, she joined Hong Kong University of Science and Technology, Hong Kong, where she is a Full Professor with the Department of Computer Science and Engineering. She has published about 300 refereed papers in international leading journals and key conferences in the areas of wireless/Internet multimedia networking, wireless communications and networking, wireless sensor networks, and overlay networking. Prof. Zhang has received the MIT TR100 (MIT Technology Review) World's Top Young Innovator Award and the Best Asia–Pacific Young Researcher Award elected by the IEEE Communication Society in 2004. She is a Fellow of IEEE for his contribution to the mobility and spectrum management of wireless networks and mobile communications