IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

SPECIAL SECTION ON ARTIFICIAL INTELLIGENCE
FOR PHYSICAL-LAYER WIRELESS COMMUNICATIONS

Received July 23, 2019, accepted July 31, 2019, date of publication August 5, 2019, date of current version August 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2933242

Location-Invariant Physical Layer Identification Approach for WiFi Devices

GUYUE LI [1], JIABAO YU [2], YUEXIU XING [2], AND AIQUN HU [1]
[1] School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China
[2] School of Information Science and Engineering, Southeast University, Nanjing 210096, China

Corresponding author: Guyue Li (h.derrouz@ieee.org)

This work was supported in part by the National Natural Science Foundation of China under Grant 61801115 and Grant 61571110, in part by the Campus France PHC Cai Yuanpei 2019 project under Grant 44016XA, in part by the China Scholarship Council, and in part by the Purple Mountain Laboratory Network and Communication Security and the Joint Laboratory for Mobile Key Management, State Key Laboratory of Cryptology, School of Cyber Science and Engineering, Southeast University.

ABSTRACT Recently, Radio Frequency Fingerprinting (RFF) becomes a promising technique which augments existing multifactor authentication schemes at the device level to counter forgery and related threats. As RFF leverages the discriminable hardware imperfections reflected in Radio Frequency (RF) signals for device identification, it has a good property of scalability, accuracy, energy-efficiency and tamper resistance. However, its identification accuracy might be compromised when the locations of training and testing are different, which is a more realistic assumption in practical scenarios. To address this issue, we study the location-invariant RFF feature extraction and identification method for WiFi Network Interface Cards (NICs). Firstly, we present an RFF feature extraction approach named Differential Phase of Pilots (DPoP). To further address the low-dimensional feature space problem, we propose another novel RFF extraction approach named Amplitude of Quotient (AoQ). AoQ exploits the fact that the RFFs of two Long Training Sequences (LTSs) in WiFi frames exhibit semi-steady characteristics and two LTSs in the same frame have similar channel frequency responses. Next, we use Euclidean distance and Deep Neural Network (DNN) for AoQ authentication and identification, respectively. Experimental results verify the effectiveness of our proposed AoQ method among 55 WiFi NICs of 5 models. The identification accuracy is higher than 95% and the Equal Error Rate (EER) is around 4% when SNR is higher than 40 dB.

INDEX TERMS Wireless communications, physical layer security, radio frequency fingerprint, device identification, 802.11n OFDM.

I. INTRODUCTION

Due to the ease of deployment, WiFi has become a pervasive communication medium in connecting various wireless devices in Local Area Networks (LANs) and the Internet of Things (IoT). Unfortunately, the exposed security problems have been increasingly serious because of the openness of radio transmission. For example, insecure authentication protocols, implementation attacks, side channel attacks, impersonation and the replay attack. Since these attacks may happen in and below data link layer, soft-identifiers using passwords, Service Set Identifier (SSID) and/or MAC/IP addresses are prone to be spoofed. Therefore, it is significant to find an efficient method to identify and prevent rogue WiFi connections.

Recently, Physical Layer Security (PLS) becomes a promising paradigm for safeguarding the air interface in 5G-and-beyond networks [1]–[4]. PLS exploits the inherent features of devices and wireless channels to authenticate users and encrypt the communication data [5]. As one of the PLS technologies, Radio Frequency Fingerprinting (RFF) is adopted herein as a way to augment existing multifactor authentication schemes at the device level to counter forgery and related threats [6]–[9]. RFF identifies a transmitter through discriminating features (also called patterns) extracted from its intrinsic physical properties [10]. These device-specific features, such as transient phase, modulation error, timing error, frequency offset and power perturbation, are resulted from the joint effects of hardware imperfections. These imperfections are originated from analogous components including digital-to-analog converters, band-pass filters, frequency mixers, and power amplifiers, etc.

The associate editor coordinating the review of this manuscript and approving it for publication was Guan Gui.

Different features may have different granularities in device identification giving rise to trade-offs in false positive and false negative rates. Once features are extracted, the next step is to develop identification algorithms that utilize these features for device identification [11]. In general, an RFF based device identification system includes two phases, i.e., training and identification [12]. At the training phase, the receiver will first acquire signals, extract features, and save them as a template library for reference from the legitimate devices. During the identification stage, the receiver will obtain signals from the target devices, compare the same type of features with the legitimate ones in the library, and classify the devices based on the similarity between these features. Due to the characters of scalability, accuracy, energy efficiency and tamper resistance, RFF has been widely studied for device authentication in the IoT networks [13]–[16]. Many RFF prototypes have been reported among various IoT systems, including UWB [17], GSM [18], 802.16 WiMax [19], LTE [20], WiFi [21], ZigBee [22], [23], LoRa [24], Bluetooth [25], [26], RFID [27], wireless audio communications [28], USRP [29] and so on.

Despite the significant advancement of RFF, there are still many major challenges in using it at a practical level. One of the biggest challenges is the change of locations. Effective RFF features should be stable in the presence of environmental changes and node mobility. In contrast, location dependent features such as the popular Radio Signal Strength (RSS) and Channel State Information (CSI) cannot be used on their own as fingerprints since they are susceptible to location changes. Most previously published studies have focused on idealized scenarios where locations are unchanging between training and validation. However, their identification accuracy might be compromised when the locations of training and validation are different, which is a more realistic assumption in practical scenarios. For example, Peng *et al.* propose a hybrid RFF extraction and device identification scheme for 54 Zigbee devices working with the IEEE 802.15.4 protocol [30]. Their experimental results show that the performance losses due to channel variations are not severe, with 4% to 9% loss in terms of identification accuracy. The reason is that the chip rate for IEEE 802.15.4 is only 1 M/s for each In-phase / Quadrature (I/Q) channel, and hence in one chip period, the Radio Frequency (RF) signal can travel for a distance of $\frac{3\times10^8}{1\times10^6} = 300\ m$. In most of the experimental scenarios, the distinctions between different paths are only approximately tens of meters. So the RF signal coming from the line-of-sight path is very similar to the signals from the other paths. Therefore, the combination of those signals is similar to multiplying the RF signal from the line-of-sight path by a factor. However, for 802.11n WiFi signals whose symbol rate is 20 M/s, the negative effect of the multipath channel becomes a discriminating factor, when the classifier is trained with the raw samples. Multipath fading might attenuate the RF signal strength severely in one location and strengthen it in another location. Therefore many traditional RFF methods tend to be inapplicable in these scenarios. In [29], large amounts of experiment results of WiFi devices demonstrate that the wireless channel affects the distribution of complex symbols captured by the receiver in a non-negligible manner. Therefore, we believe that it is important to overcome wireless channel effects and explore those RFF features which are consistent and constant to location conditions.

To address these challenges, some RFF extraction algorithms have been proposed. Brik *et al.* examine the steady state signal of IEEE 802.11 cards transmitted through a wireless channel and extract some time-averaged features [31]. The frequency offset error between the transmitter and receiver dominates the discriminatory performance of their solution. However, the system is constrained by the low-dimensional feature space and thus it is not applicable to the identification for a large number of devices. Kunal *et al.* propose a new RFF system named ORACLE [29], which needs to be trained only once. It can easily identify radios even if the experienced channel changes or radios are moved to different locations. However, since they use artificial impairments to enable robust identification, the attacker could use the equivalent perturbations of the transmitted constellations to achieve a similar effect. Under the assumption that the nonlinearity parameter set of an emitter is unique, Ming *et al.* provide a robust identification by first using alternative degrees of nonlinearities associated with symbol amplitudes for initial estimation, and then iteratively estimating the channel coefficients and distorted transmit symbols to overcome the Inter Symbol Interference (ISI) effect [32]. In [33], Adam *et al.* also study the nonlinear characteristics of power amplifiers which are modeled with Volterra series representations. However, they only consider an Additive White Gaussian Noise (AWGN) channel instead of a multipath channel. Another work [21] alleviates channel effects by implementing channel estimation and deconvolution and identifying the deconvoluted signals. They only match the carrier frequency offset and the nonlinear terms. This is because all the other linear parts are highly related to the transmitted data and the environment. To improve the identification accuracy, these methods often need an additional anechoic chamber to obtain pure RFF features in the training phase. In addition, a transfer learning method is proposed in [34] for the identification of devices with changing bandwidth. It is also applied to the removal of the bias introduced by RF receivers through the use of one golden reference [35]. The core idea of [34] and [35] is to know the change of environment with the aid of a known reference device. This idea can also be used to address the changing location issue. However, the performance bottleneck of the transfer learning method lies in providing exactly the same environment of the target device for the reference device.

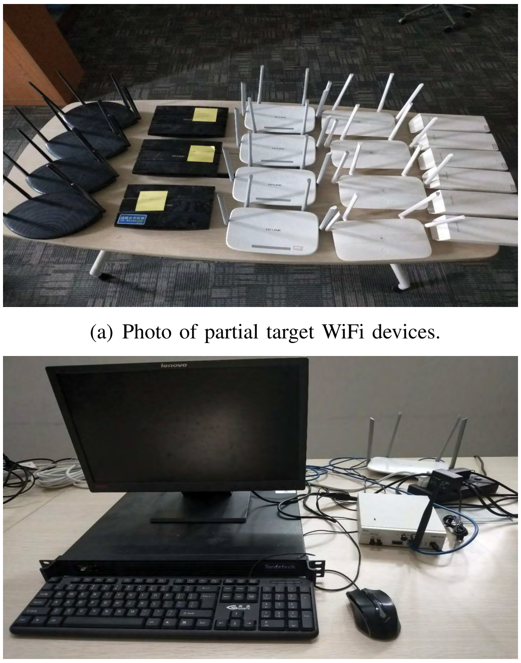
On the whole, it is still missing how to extract channel robust RFF features for 802.11n devices in practical scenarios. Under the assumption that the wireless channel keeps constant during the coherence time, this paper introduces two location-invariant RFF feature extraction methods using pilots and Long Training Sequences (LTSs) in the IEEE

802.11n beacon frame preamble, respectively. The main contributions of this paper are listed as follows:

- We present an RFF feature extraction approach named Differential Phase of Pilots (DPoP). By building the phase model, we find that the received phase is affected by sub-carriers, symbols and locations. Next, we demonstrate that the phase difference between two adjacent received pilots is robust to locations as it mainly consists of frequency offset.
- We propose another novel RFF extraction approach named Amplitude of Quotient (AoQ). Exploiting the fact that two LTSs in the same frame have similar channel frequency responses, we demonstrate that AoQ is invariant to spatial variations and multipath channels so that it can be applied in reality. Compared with those deep learning based approaches, our model teases apart RFF and channel effects in the received signals rather than a blind use of machine learning. Therefore, our model is more explainable and efficient.
- We further improve the approach by collecting AoQs from multiple locations to constitute a robust AoQ feature. The improved AoQ approach can address the noise amplification issue which is caused by the division operator. Furthermore, as AoQ is a comprehensive feature, it has the potential to identify the IoT devices that are indistinguishable in any low-dimensional feature space.
- We verify the effectiveness of the proposed approaches on 55 commercial WiFi Network Interface Cards (NICs) spanning 5 different models, including one set of 15 cards and other sets of 10 cards each (from reputable manufacturers). Experimental results show that both DPoP and AoQ are robust to location variations, but DPoP is restricted to a single dimension and thus can hardly distinguish a large number of devices. The identification accuracy is higher than 95% and the Equal Error Rate (EER) is around 4% when SNR is higher than 40 dB.

The material in this paper has been partially submitted at IEEE SiPS 2019. In our previous work, we have investigated the AoQ approach in theory and use the Euclidean distance for device authentication. Experiment results show that AoQ achieves low EER. In this paper, we considerably extend and complement this work by additionally providing another location-invariant approach based on DPoP as a reference. To further improve the accuracy, we add a two-layer Deep Neural Network (DNN) for identification. Furthermore, we conduct more experiments to verify the effectiveness of our proposed approaches.

The rest of the paper is organized as follows. Section II introduces the experimental setup, structure of IEEE 802.11n frame and the process of signal acquiring. In Section III and Section IV, we present the models and algorithms of two proposed RFF feature extraction approaches, respectively. The device identification methods are described in Section IV-C. Section V presents our implementation and experimental results. We finally conclude our work in Section VI.


(a) Photo of partial target WiFi devices.

(b) Photo of the USRP receiver platform and PC.

FIGURE 1. Experimental platform. (a) Photo of partial target WiFi devices. (b) Photo of the USRP receiver platform and PC.

II. EXPERIMENTAL SYSTEM AND SIGNAL ACQUIRING

WiFi has become a pervasive communication medium in connecting various wireless devices in LAN and IoT due to the ease of deployment. The WiFi protocol includes various physical layer technologies, such as IEEE 802.11a/b/ac/g/n and the mixed ones. High Rate/ Direct Sequence Spread Spectrum (HR/DSSS) is used for IEEE 802.11b and Orthogonal Frequency Division Multiplexing (OFDM) is used for IEEE 802.11n. In this paper, we focus on IEEE 802.11n devices with the OFDM modulation.

A. EXPERIMENTAL SETUP

The experimental system is shown in Fig. 1, which works at 2.4/5.8 GHz Industrial, Scientific and Medical (ISM) band. We aim to classify 55 WiFi NICs of 5 different models from 3 manufacturers. We implemented our work on a Ubuntu-16.04-amd64 PC with an Intel Core i7-4790 CPU @ 3.60 GHz processor, and this PC is connected to an Ettus USRP transceiver to form an identification server.

A USRP platform with a UBX daughterboard is used as the receiver for capturing RF signals with a sampling rate of $f_s = 20\ MHz$. The captured baseband signals are transferred to a PC and processed off-line. The details of the target WiFi NICs and the information of the collected data set are listed in Table 1, where N_d and N_f represent the number of devices and the number of collected frames for each device, respectively. 16,384 signals from each device were captured and stored by the receiver, resulting in a data set of 901,120 received signals in total. The signals were measured from 4 different locations

TABLE 1. Information of experimental data set.

NICs	Manufacturer	N_d	N_f	File size
WDR-5620	TP-LINK	15	16,384	60.62KB
WDR-5660	TP-LINK	10	16,384	60.62KB
CPE-500	TP-LINK	10	16,384	71.25KB
WS-5100	Hua Wei	10	16,384	88.12KB
MI-3A	Xiao Mi	10	16,384	76.25KB
SUM	/	55	901,120	60.06GB

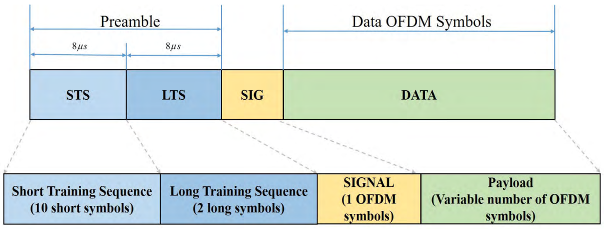

Preamble
Data OFDM Symbols
8μs
8μs
STS
LTS
SIG
DATA
Short Training Sequence (10 short symbols)
Long Training Sequence (2 long symbols)
SIGNAL (1 OFDM symbols)
Payload (Variable number of OFDM symbols)

FIGURE 2. IEEE 802.11 OFDM frame format.

in a 5 m × 8 m room. The distance between the receiver and the target devices was approximately 4 meters.

B. IEEE 802.11 OFDM FRAME

In this paper, we only consider the IEEE 802.11 legacy OFDM standard with 20 MHz channel spacing. According to the standard, 52 of 64 non-zero sub-carriers are used for symbol modulation. Starting from the origin of Direct Current (DC), 26 pairs of sub-carriers are selected from two-axis. They are numbered by $-26 \sim -1$ and $1 \sim 26$. The frequency difference between two continuous sub-carriers equals to 312.5 kHz. Among them, four sub-carriers numbered

$$\mathbf{K}_{pilot} = [-21, -7, 7, 21], \tag{1}$$

are specifically designed for pilot transmission. The pilots are pseudo-random binary sequences modulated by Binary Phase Shift Keying (BPSK).

Fig. 2 shows the frame structure of the IEEE 802.11n OFDM standard. Each 802.11 RF frame contains three parts, i.e., preamble, SIGNAL and data. The preamble consists of two training sequences, i.e., 10 Short Training Sequences (STSs) and 2 LTSs, each with a duration of 8 μs. To reduce the Inter-Symbol Interference (ISI), there is a part of Guard Interval (GI) in the LTS part, besides the two long symbols. The length of GI is half that of a long symbol. Since the GI is not used in our approaches, we do not show it explicitly in Fig. 2. The STS is primarily used for frame synchronization, Automatic Gain Control (AGC), and coarse frequency offset estimation. STS uses 12 OFDM sub-carriers which are symmetric to the DC. The sequence number is given by

$$\mathbf{K}_{short} = [-24, \quad -20, \quad -16, \quad -12, \quad -8, \quad -4, \quad 4, \quad 8, \quad 12, \quad 16, \quad 20, \quad 24]. \tag{2}$$

For each sub-carrier, the STS is BPSK modulated with the amplitude of $\sqrt{\frac{13}{3}}$. The modulated phases are

$$\varphi_{short} = [\frac{\pi}{4}, \quad \frac{-3\pi}{4}, \quad \frac{\pi}{4}, \quad \frac{-3\pi}{4}, \quad \frac{-3\pi}{4}, \quad \frac{\pi}{4}, \quad \frac{-3\pi}{4}, \quad \frac{-3\pi}{4}, \quad \frac{\pi}{4}, \quad \frac{\pi}{4}, \quad \frac{\pi}{4}, \quad \frac{\pi}{4}]. \tag{3}$$

The LTS is mainly used for channel estimation, fine frequency and symbol timing offset estimation. LTS uses the whole 52 sub-carriers and in each sub-carrier, it is BPSK modulated with phases of π or $-\pi$. The sequence number is denoted by

$$K_{long} = [-26, -25, \cdots, -1, 1, 2, \cdots, 26]. \tag{4}$$

C. SIGNAL ACQUIRING

The RFF identification system contains three main parts: RFF feature extraction, RFF library establishment, and legitimacy testing. We assume that there is a set of legitimate devices to initialize the RFF library. Firstly, an RFF library of legitimate devices should be established after authentication. Secondly, when a rogue WiFi device tries to connect with the other one, our system must detect and reject it accurately. In this subsection, we briefly introduce the signal acquiring technologies which are the preliminaries for RFF feature extraction.

1) COARSE SYNCHRONIZATION

STS has significant spectrum characteristics and thus can be used to find the coarse position of the frame header quickly. Denote $x(n)$ as the received baseband data measured by the RF front end and slice $x(n)$ into M_B data blocks, then the m_B-th block is defined as

$$\mathbf{X}_{m_B} = [x(m_B N - N + 1), x(m_B N - N + 2), \cdots, x(m_B N)], \tag{5}$$

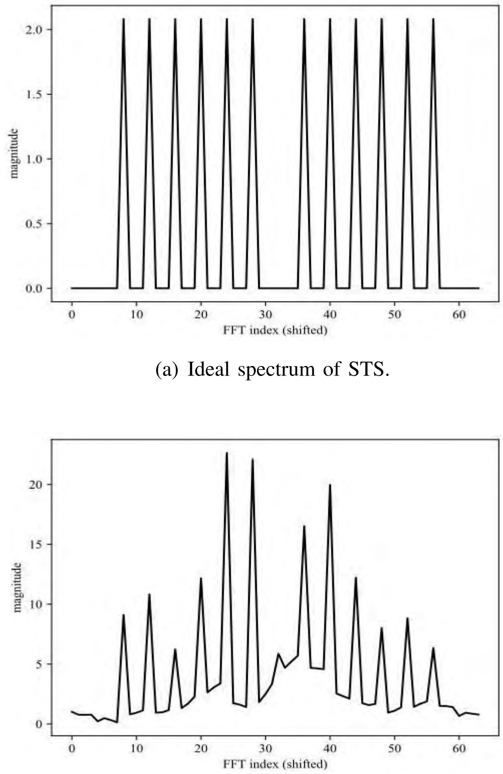
where $m_B = 1, 2, \cdots, M_B$ is the block number and $N = 64$ is the number of sub-carriers. Transforming $\mathbf{X}_{m_B}$ from the time domain to the frequency domain, we get

$$\mathbf{Y}_{m_B}(k) = \sum_{i=0}^{N-1} \mathbf{X}_{m_B}(i)\, e^{-j\frac{2\pi}{N}ki}, \quad k = 0, 1, \ldots N-1. \tag{6}$$

Fig. 3(a) and Fig. 3(b) are the spectrums of an ideal and real received STS, respectively. These spectrums are calculated by using the Discrete Fourier Transform (DFT) transform defined in (6) for ideal and real received STSs, respectively. Define ξ_{m_B} as the ratio of the sub-carrier power in STS and that of all sub-carriers,

$$\xi_{m_B} = \frac{\sum\limits_{i \text{ in } \mathbf{K}_{short}} \left|\mathbf{X}_{m_B}(i)\right|^2}{\sum\limits_{i=0}^{N-1} \left|\mathbf{X}_{m_B}(i)\right|^2}. \tag{7}$$

When $\xi_{m_B} > \xi_{th}$, the data block $\mathbf{X}_{m_B}$ is considered as an STS symbol. The threshold ξ_{th} is an empirical value and the value of ξ_{m_B} provides an efficient criterion for coarse synchronization with precision N.



(a) Ideal spectrum of STS.

(b) Real spectrum of STS.

FIGURE 3. **Spectrums of STS in coarse synchronization. (a) Ideal spectrum of STS. (b) Real spectrum of STS.**

2) FINE SYNCHRONIZATION

Next, we further conduct a fine synchronization with locally stored ideal preamble signals. The correlation coefficients between the received and ideal symbols are

$$C_{short}(m) = \sum_{i=1}^{L_{short}} p^{*}_{short}(i)x(m+i), \tag{8}$$

and

$$C_{long}(n) = \sum_{i=1}^{L_{long}} p^{*}_{long}(i)x(n+i), \tag{9}$$

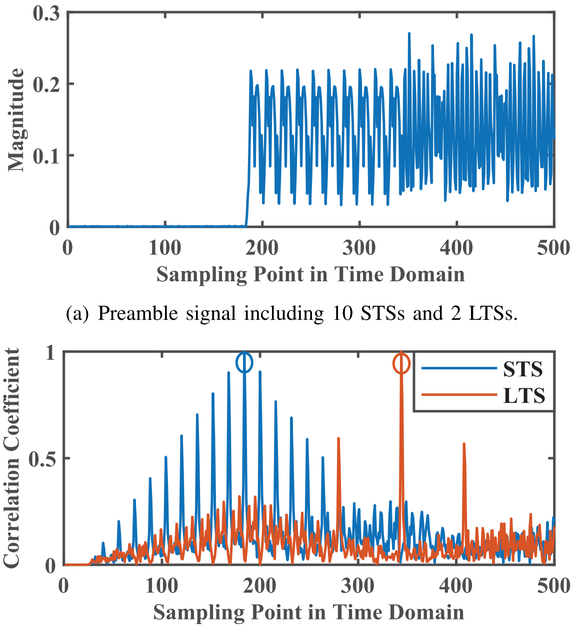
respectively. p_{short} and p_{long} are the ideal STS and LTS signals in the time domain. Superscript $(\cdot)^*$ denotes the conjugate. $L_{short} = 16 \times 10 = 160$ and $L_{long} = 32 + 64 \times 2 = 160$ are the sampling numbers of STS and LTS, respectively. Define the Correlation Coefficient Ratio (CCR) of STS and LTS as

$$\xi_{short}(m) = \frac{|C_{short}(m)|^2}{\sum_{i=m-L_{short}}^{m+L_{short}} |C_{short}(i)|^2}. \tag{10}$$

and

$$\xi_{long}(n) = \frac{|C_{long}(n)|^2}{\sum_{i=n-L_{long}}^{n+L_{long}} |C_{long}(i)|^2}, \tag{11}$$

respectively.



(a) Preamble signal including 10 STSs and 2 LTSs.

(b) Correlation results for fine synchronization.

FIGURE 4. **Sampling points and correlation results in fine synchronization.**

Since there are 10 STSs, the start point of STS and LTS are separated by 160 points. When $\xi_{short}(m)$ and $\xi_{long}(n)$ achieve the largest CCRs among all points and $m - n = 160$, the signal is considered to be fine synchronized. Fig. 4 shows the received preamble signal and its correlation coefficient with the ideal preamble signal. The correlation coefficients are calculated according to (8) and (9), respectively. The circled points achieve the largest CCRs and they are also the start points of STS and LTS, respectively.

Next, we will introduce two location-invariant RFF feature extraction and identification approaches using pilots and LTSs, respectively.

III. RFF IDENTIFICATION USING DPOP

In 802.11n OFDM frames, four sub-carriers are deployed for pilot transmission. The phase of received pilots at location l is denoted as ϕ^l, which is calculated from the I/Q components:

$$\phi^l = tan^{-1}\left(\frac{Q^l}{I^l}\right), \tag{12}$$

where Q^l and I^l denote the in-phase and quadrature components of the received pilots, respectively.

According to [36], for a particular pair of transmitter and receiver, the phase of the received OFDM symbol m_s and the sub-carrier k measured in one frame at location l can be expressed as

$$\begin{aligned} \phi^l(m_s,k) &= \varphi(m_s,k) + \omega(m_s,k) + \theta(k) + \varepsilon(k) + \psi^l(k), \\ & m_s \in \{1,2,\cdots,M_s\}, \quad k \in \mathrm{K}_{pilot}, \\ & l \in \{Location\ 1, Location\ 2, \cdots, Location\ L\}, \end{aligned} \tag{13}$$

where M_s denotes the symbol number, $\varphi(m_s, k)$ denotes the ideal phase of pilots, $\omega(m_s, k)$ denotes the phase caused by the frequency offset, $\theta(k)$ denotes the phase caused by the frame detection delay. Besides, $\varepsilon(k)$ denotes the error caused by the I/Q imbalance. The last element $\psi^l(k)$ denotes the phase caused by the time of flight, which changes with locations. In general, the received phase is affected by sub-carriers, symbols and locations.

In one frame, phases caused by frame detection delay, I/Q imbalance and time of flight remain unchanged for all symbols, thus we omit the variable m_s in these terms. On the contrary, $\varphi(m_s, k)$ changes with m_s since it is the phase of a pseudo-random binary sequence. The phase caused by frequency offset can be further written by

$$\omega(m_s, k) = m_s\left(\omega^r(k) - \omega^t(k)\right)T_s = m_s\Delta\omega(k)\,T_s, \tag{14}$$

where $\omega^r(k)$ and $\omega^t(k)$ denote the carrier frequencies of a pair of receiver and transmitter, respectively. $\Delta\omega(k)$ denotes the frequency offset of sub-carrier k and T_s denotes the time interval between two adjacent pilots. There are 80 sampling points during time T_s.

Since the frequency offset is caused by the typical slight frequency difference between the transmitter and receiver crystal oscillators, it is robust to locations. Thus, we use it for fingerprinting purpose. We compute the phase difference between two adjacent received pilots by

$$\begin{aligned}\Delta\phi(k) &= \phi(m_s+1, k) - \phi(m_s, k)\\ &= \varphi(m_s+1, k) - \varphi(m_s, k) + \omega(m_s+1, k) - \omega(m_s, k)\\ &= \varphi(m_s+1, k) - \varphi(m_s, k) + \Delta\omega(k)\,T_s.\end{aligned} \tag{15}$$

Then, the frequency offset is derived by

$$\Delta\omega(k) = \frac{\Delta\phi(k) - \Delta\varphi(m_s, k)}{T_s}, \tag{16}$$

where $\Delta\varphi(m_s, k) = \varphi(m_s+1, k) - \varphi(m_s, k)$.

Since the frequency difference among sub-carriers is far less than the carrier frequency, the frequency offset remains stable among different sub-carriers

$$\Delta\omega(k) \approx \Delta\omega. \tag{17}$$

To reduce the noise-induced variations of $\Delta\omega$ due to noise, we compute the average frequency offset over sub-carriers, multiple OFDM symbols, and multiple frames by

$$\overline{\Delta\omega} = avg\,\Delta\omega. \tag{18}$$

Algorithm 1 illustrates the detailed feature extraction approach based on the differential phase.

Then, we use Support Vector Machine (SVM) for DPoP identification. The SVM is a popular and powerful binary classifier, which aims to find a hyperplane within the feature space that separates two classes. We divide the collected data into two categories, i.e., training data and testing data. From the training data, the SVM parameter is optimized. Define the training percentage P_{train} as the ratio of the number of training data to the total number of collected data. Fig. 5 shows the identification accuracy of RFF systems using DPoP versus P_{train}. For 10 WDR-5660 NICs, both identification accuracies of training and testing sets achieve 98% when P_{train} is larger than 0.1. Therefore, DPoP could well identify the differences between these WDR-5660 NICs, even in different locations. However, for 55 mixed NICs, their accuracies reduce to only about 70% even when P_{train} is larger than 0.3.

Algorithm 1 Differential Phase Algorithm

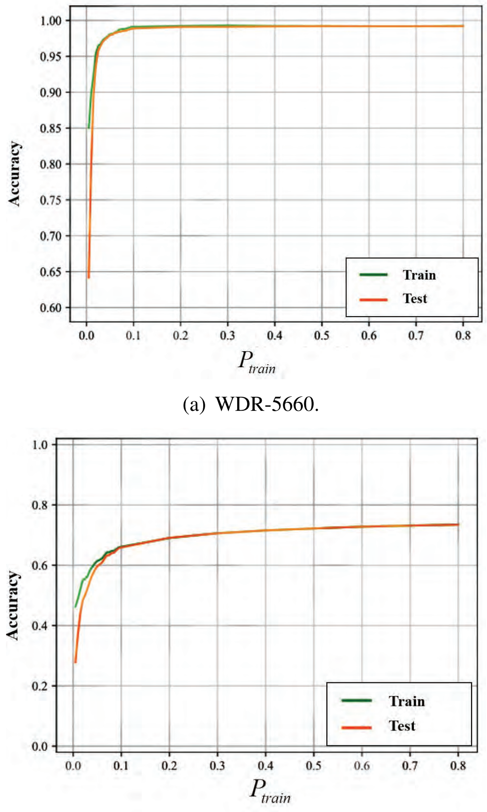
```
Input: The in-phase and quadrature components of
       received pilots, $I^l$ and $Q^l$, respectively.
The number of received OFDM symbols, $M_s$.
The time interval between two adjacent pilots, $T_s$.
The ideal phases of pilots, $\varphi(m_s, k)$, $m_s \in \{1, 2, \cdots, M_s\}$, $k \in K = [-21, -7, 7, 21]$;
Output: The average frequency offset $\overline{\Delta\omega}$
;
Initialize the index of OFDM symbols $m_s = 1$; Set the number of sub-carriers $N_k = 4$;
Initialize the index of sub-carrier, $k_p = 1$;
Compute the phase of the received signal $\phi^l = tan^{-1}\left(\frac{Q^l}{I^l}\right)$;
while $k_p \le N_k$ do
    while $m_s \le M_s$ do
        Set $\hat{k} = K(k_p)$;
        Compute the phase difference of the received signal $\Delta\phi\left(\hat{k}\right) = \phi\left(m_s+1, \hat{k}\right) - \phi\left(m_s, \hat{k}\right)$;
        Compute the ideal phase difference of the pilots $\Delta\varphi\left(m_s, \hat{k}\right) = \varphi\left(m_s+1, \hat{k}\right) - \varphi\left(m_s, \hat{k}\right)$;
        Compute the frequency offset $\Delta\omega\left(\hat{k}\right) = \frac{\Delta\phi\left(\hat{k}\right) - \Delta\varphi\left(m_s, \hat{k}\right)}{T_s}$;
        Compute $m_s = m_s + 1$ and $k_p = k_p + 1$;
    end
end
Return the average frequency offset $\overline{\Delta\omega} = avg\,\Delta\omega$;
```

IV. RFF IDENTIFICATION USING AOQ OF LTS

Although the DPoP feature in Algorithm 1 is both stable and channel-robust, it is a single dimensional feature and thus can be hardly used to distinguish a large number of devices. It is also verified by the experimental results in Fig. 5. Next, we seek for another location-invariant feature which is not constrained by a certain low-dimensional feature space.

A. AOQ OF LTS

According to the process of signal transmission, the transceiver can be modeled as filters cascaded to the wireless channel in the time domain or extra scalars multiplying the channel frequency response in each sub-carrier in the frequency domain [37]. In the f-th frame, the received signal



(a) WDR-5660.

(b) Mixed NICs.

FIGURE 5. Identification accuracy of RFF systems using DPoP. (a) WDR-5660. (b) Mixed NICs.

frequency response of the j-th sub-carrier in the p-th LTS at location l satisfies that

$$\begin{aligned} Y_f^l(p,j) &= G_f^r(p,j)H_f^l(p,j)G_f^t(p,j)S(p,j)+N_f^l(p,j),\\ l &\in \{Location\ \ 1, Location\ \ 2, \cdots, Location\ \ L\},\\ f &\in \{1,2,\cdots,F\}, \quad p \in \{1,2\}, \quad j \in \mathrm{K}_{long}, \end{aligned} \tag{19}$$

where $S(p,j) = S(j)$ is the frequency spectrum of each transmitted LTS at j-th sub-carrier, $G_f^r(p,j)$ and $G_f^t(p,j)$ represent the RFFs of the receiver and target transmitter, respectively.

In general, $G_f^r(p,j)$ and $G_f^t(p,j)$ are assumed to be consistent and invariant to time and locations. Thus, we can omit the subscript f, $G_f^r(p,j) \approx G^r(p,j)$ and $G_f^t(p,j) \approx G^t(p,j)$. $H_f^l(p,j)$ and $N_f^l(p,j)$ are respectively the Channel Frequency Response (CFR) and the additive noise which change over time and locations.

According to (19), $Y_f^l(p,j)$ is variant to location l due to $H_f^l(p,j)$ and $N_f^l(p,j)$, and thus it cannot be used to identify one device in two different locations. The impact of additive noise can be effectively reduced by smoothing through frames. However, it is challenging to eliminate the negative effect of the multipath channel because $H_f^l(p,j)$ is multiplicative and mixed with the frequency responses of devices.

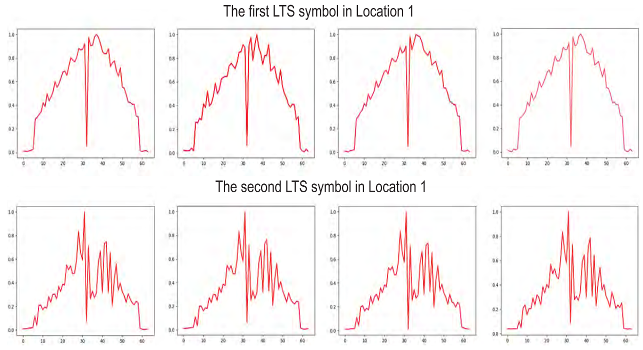


FIGURE 6. Frequency spectrums of the first and second LTS in Location 1.

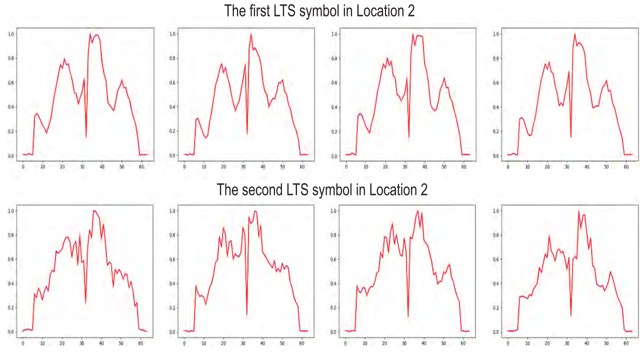


FIGURE 7. Frequency spectrums of the first and second LTS in Location 2.

Fig. 6 and Fig. 7 show the frequency spectrums of two LTSs for four frames from the device WDR-5620 No.4 at Location 1 and Location 2, respectively. The environment remains static for each location. It is observed that the frequency spectrums of the first LTS and the second LTS are not the same. Besides, the frequency spectrums of each LTS change little over time in the same location. However, the frequency spectrums of the same device have significant changes from Location 1 to Location 2.

In order to obtain an RFF that is invariant to locations, we aim to extract a novel robust feature from the quotient of two successive received LTS spectrums. Due to the coherence of wireless channels, their CFRs remain unchanged within a very short time interval of 8 μs as

$$H_f^l(1,j) = H_f^l(2,j) = H_f^l(j). \tag{20}$$

However, the frequency spectrums of two LTSs are different. It is caused by the semi-steady characteristics of their RFFs, since they are located in the header of the IEEE 802.11n OFDM frame. According to [22], it was found that the first few symbols in the preamble are unstable in the sleep mode switching scenarios. The unstable part during the settling time is defined as the semi-steady portion to distinguish from the traditional steady-state definition. In our experiments, we further observe that the semi-steady portion also shows stable characteristics between frames. It might be explained that for every frame, some minor components, e.g., the crystal oscillator experience the same variation in a frame. It is also verified by the work of [38] for ZigBee devices identification.

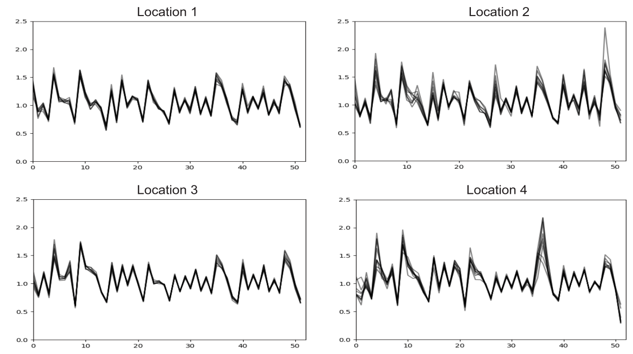


FIGURE 8. AoQs of device WDR-5620 No.4 at four different locations.

Define the AoQ of the received LTS spectrums for the f-th frame at Location l as

$$\tilde{\mathbf{Y}}_f^l = [\tilde{Y}_f^l(-26), \tilde{Y}_f^l(-25), \cdots, \tilde{Y}_f^l(26)]^T, \tag{21}$$

where the matrix superscript $(\cdot)^T$ denotes its transpose. Among it, the AoQ of the j-th sub-carrier is

$$\begin{aligned}\tilde{Y}_f^l(j) &= \left|\frac{Y_f^l(1,j)}{Y_f^l(2,j)}\right| \\ &= \frac{\left|G^r(1,j)H_f^l(j)G^t(1,j)S(j) + N_f^l(1,j)\right|}{\left|G^r(2,j)H_f^l(j)G^t(2,j)S(j) + N_f^l(2,j)\right|},\end{aligned} \tag{22}$$

where $|\cdot|$ represents the absolute value. Neglecting the influence of noise, the approximate result of AoQ is derived as

$$\begin{aligned}\tilde{Y}_f^l(j) &\approx \frac{\left|G^r(1,j)H_f^l(j)G^t(1,j)S(j)\right|}{\left|G^r(2,j)H_f^l(j)G^t(2,j)S(j)\right|} \\ &\approx \left|\tilde{G}^r(j)\tilde{G}^t(j)\right|,\end{aligned} \tag{23}$$

where $\tilde{G}^r(j) = \left|\frac{G^r(1,j)}{G^r(2,j)}\right|$ and $\tilde{G}^t(j) = \left|\frac{G^t(1,j)}{G^t(2,j)}\right|$. It is observed that $\tilde{G}^t(j)$ reflects the inherent frequency response characteristics of the transmitter and does not change with l. In this paper, we assume that all target devices are authenticated by the same receiver, so $\tilde{G}_r(j)$ becomes a constant value for all target devices. According to (23), AoQ is a location-invariant RFF feature. Fig. 8 shows the AoQs of device WDR-5620 No.4 at four different locations. In each location, AoQs of 10 frames are overlapped. It is observed that AoQ keeps almost constant over frames and locations. However, division may lead to the problem of noise amplification, especially when the divisor is small. Thus, there are some sharp points in Fig. 8.

Fig. 9 and Fig. 10 show the AoQs of devices with different models and the same model, respectively. It is observed that AoQs have significant discrimination among different devices, especially devices with different models.

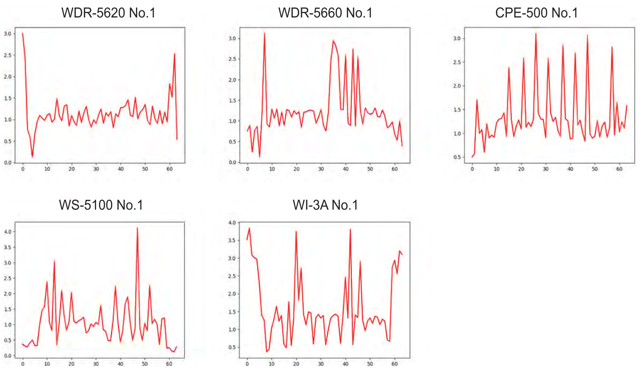


FIGURE 9. AoQ of devices with five different models.

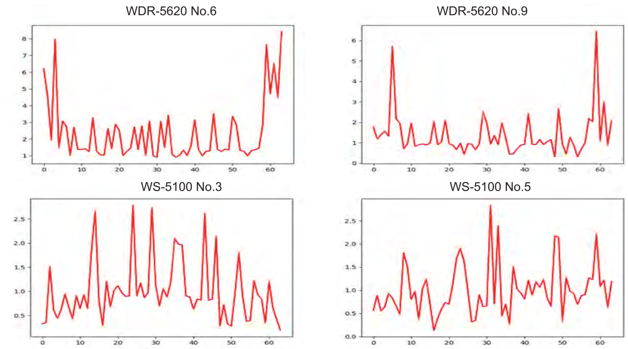


FIGURE 10. AoQ of devices with the same models.

B. AOQ EXTRACTION ALGORITHM

In order to address this problem, we collect AoQs of devices from L locations. In each location, F frames of IEEE 802.11n OFDM signals are measured. Denote the collected AoQs at location l as

$$\tilde{\mathbf{Y}}^l = [\tilde{Y}_1^l, \tilde{Y}_2^l, \cdots, \tilde{Y}_f^l, \cdots, \tilde{Y}_F^l], \tag{24}$$

where $\tilde{Y}_f^l$ represents the AoQ for frame $f \in \{1, 2, \cdots, F\}$ at Location l. We calculate the mean and variance of AoQs for sub-carrier j over F frames as

$$\mu_l(j) = avg\,\tilde{\mathbf{Y}}^l(j) = \frac{1}{F}\sum_{f=1}^{F}\tilde{Y}_f^l(j), \tag{25}$$

$$\sigma_l^2(j) = var\,\tilde{\mathbf{Y}}^l(j) = \frac{1}{F}\sum_{f=1}^{F}\left(\tilde{Y}_f^l(j) - \mu_l(j)\right)^2. \tag{26}$$

For each sub-carrier, we select the optimal location $l^*(j)$ where the AoQ has the smallest variance,

$$l_j^* = \arg\min_l \sigma_l^2(j), \tag{27}$$

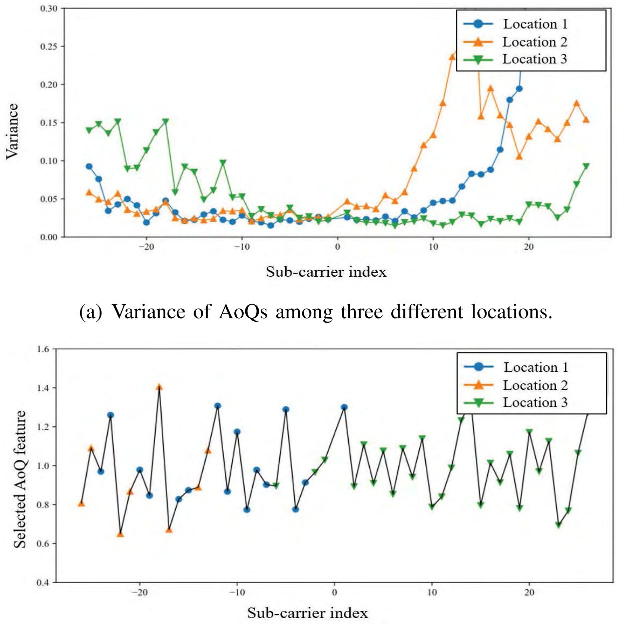
then the final selected AoQ feature is

$$\tilde{\mathbf{Y}} = \left[\mu_{l_{-26}^*}(-26), \mu_{l_{-25}^*}(-25), \cdots, \mu_{l_j^*}(j), \cdots, \mu_{l_{26}^*}(26)\right]. \tag{28}$$

Fig. 11 illustrates the selection process of AoQ feature. According to the variance of AoQs at three different locations

Algorithm 2 AoQ Algorithm

```
Input: Received signal frequency response of the $j$-th
       sub-carrier for the LTS $p$ at location $l$ in the $f$-th
       frame, $Y_f^l(p, j)$.
Location number $L$.
Output: The AoQ feature $\tilde{\mathbf{Y}}$
while $l \leq L$ do
    Compute the AoQ of $Y_f^l(p, j)$ for the $j$-th sub-carrier,
    $\tilde{Y}_f^l(j) = \left| \frac{Y_f^l(1,j)}{Y_f^l(2,j)} \right|$;
    Set the AoQ for the $f$-th frame,
    $\tilde{\mathbf{Y}}_f^l = [\tilde{Y}_f^l(-26), \tilde{Y}_f^l(-25), \cdots, \tilde{Y}_f^l(26)]^T$;
    Set AoQs of $F$ frames at location $l$,
    $\tilde{\mathbf{Y}}^l = [\tilde{Y}_1^l, \tilde{Y}_2^l, \cdots, \tilde{Y}_F^l]$;
    Compute the mean $\mu_l(j)$ and variance $\sigma_l^2(j)$ of
    $\tilde{\mathbf{Y}}^l(j)$;
end
Compute the optimal location $l_j^* = \arg\min_l \sigma_l^2(j)$;
Set AoQ feature $\tilde{\mathbf{Y}} =$
$\left[\mu_{l_{-26}^*}(-26), \mu_{l_{-25}^*}(-25), \cdots, \mu_{l_j^*}(j), \cdots, \mu_{l_{26}^*}(26)\right]$.
```



(a) Variance of AoQs among three different locations.

(b) Selected AoQ feature.

FIGURE 11. Selected AoQs among three different locations. (a) Variance of AoQs among three different locations. (b) Selected AoQ feature.

in Fig. 11(a), l_j^* achieves the minimal variance for each sub-carrier. For example, for sub-carriers −26 and −25, the AoQs at Location 2 have the minimal variances and thus they are selected as the AoQ features for these two sub-carriers. While for sub-carriers −24 and −23, the AoQs at Location 1 have the minimal variances and thus they are selected as the AoQ features for these two sub-carriers.

Algorithm 2 describes the complete process of AoQ feature extraction.

C. DEVICE AUTHENTICATION AND IDENTIFICATION

As mentioned above, an RFF-based device identification system generally includes two phases, i.e., training and identification [12]. In the training stage, the receiver collects LTS signals of target devices from multiple locations. AoQ features are then extracted and saved as templates in the library according to the approach described in Section IV-B. The recorded AoQ of device $d \in \{1, 2, \cdots, N_d\}$ is denoted as $\tilde{\mathbf{Y}}^{lib}$. In the identification stage, the receiver will first capture samples from the target device, then extract its AoQ feature which is denoted by $\tilde{\mathbf{Y}}^{test}$, and at last, compare it with all templates for identification. In this section, we describe the AoQ authentication and identification methods using Euclidean distance and DNN, respectively.

1) AUTHENTICATION USING EUCLIDEAN DISTANCE

Firstly, we quantitatively use the Euclidean distance as the metric to evaluate the similarity between $\tilde{\mathbf{Y}}_d^{lib}$ and $\tilde{\mathbf{Y}}^{test}$ as

$$D\left(\tilde{\mathbf{Y}}_d^{lib}, \tilde{\mathbf{Y}}^{test}\right) = \left\| \tilde{\mathbf{Y}}_d^{lib} - \tilde{\mathbf{Y}}^{test} \right\|, \quad (29)$$

where $\|\cdot\|$ denotes the two-norm. When the Euclidean distance is less than the threshold d_{th}

$$D\left(\tilde{\mathbf{Y}}_{d^*}^{lib}, \tilde{\mathbf{Y}}^{test}\right) < d_{th}, \quad (30)$$

the testing device is identified as the legitimate one in the library. Otherwise, it is identified as a rogue device.

2) IDENTIFICATION USING DNN

To further improve the identification accuracy, we also use DNN for identification. The AoQ feature is a 52-dimensional complex-valued vector. By connecting its in-phase channel and quadrature channel, we can get a 104-dimensional real-valued feature vector for identification. Since the feature dimension is not very high, we select a two-layer DNN for device identification as shown in Fig. 12. The sizes of these two hidden layers are the same as the input layer, namely, 104 neurons in each layer. Besides, Rectified Linear Unit (ReLU) activation functions are used for hidden layers. Then, the DNN outputs the predicted probability distribution of each possible label by using a Softmax layer. At last, the index of the maximum value of the predicted probability distribution is just the predicted device label. To train the DNN, the categorical cross-entropy is used as the loss function, which is a measure of the difference between the predicted probability distribution and the real probability distribution. The loss is calculated in the forward pass and weights are updated using the chain rule, which is known as the backward propagation.

V. EXPERIMENTAL RESULTS

In this section, we present some experimental results on our proposed AoQ approach.

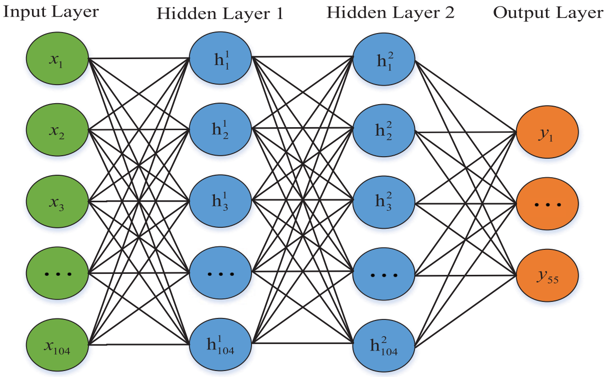


FIGURE 12. Structure of DNN for AoQ identification.

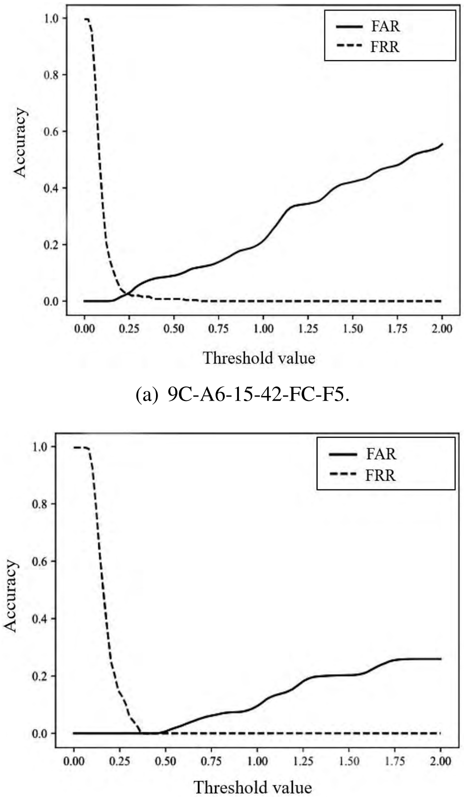
TABLE 2. Authentication EERs of target NICs using single model devices and mixed model devices.

Verified device model (single)	Illegal device	Min(%)	Max(%)	Average(%)
WDR-5620	All other devices of the same model	0	10.6	5.2
WDR-5660		0	21.6	8.9
CPE-500		0	6.3	1.1
WS-5100		0	10.5	1.4
MI-3A		0.3	17.0	8.5
Mixed NICs	All other devices	0	18.0	4.0

A. AUTHENTICATION USING EUCLIDEAN DISTANCE

We choose one NIC as the legitimate device, and the other 54 NICs are regarded as the targets for identification. We measure the signals from four different locations in a 5 m × 8 m room. The distance between the receiver and the target devices was approximately 4 meters. Fig. 13 shows the False Acceptance Rate (FAR) and False Rejection Rate (FRR) versus the threshold when NICs with MAC addresses 9C-A6-15-42-FC-F5 and D0-D7-83-EE-DD-28 act as the legitimate ones, respectively. FAR represents the error ratio when a rogue device is identified as a legitimate one, while FRR represents the error ratio when a legitimate device is identified as a rogue one. The FAR rises with the increase of the threshold d_{th} while the opposite is true for FFR. We aim to find an appropriate threshold d_{th} by trading off FAR and FRR. According to Fig. 13, it can be seen that the optimal threshold value that FAR equals to FRR is 0.25 and 0.4 for 9C-A6-15-42-FC-F5 and D0-D7-83-EE-DD-28, respectively. When the rates of FAR and FRR are equal, the common Y-axis value is referred to as the EER. The value indicates that the proportion of false acceptances is equal to the proportion of false rejections. The lower the EER, the better the performance of the authentication system.

Table II shows the maximal, minimal and average identification EERs of target NICs. We first carry out experiments for the NICs of each model. One NIC is randomly selected as the legitimate device and all other NICs of the same model are the illegal ones for identification. The results are shown in the first five rows. It can be seen that CPE-500 achieves the best performance among individual models, with only 1.1% EER on average. WDR-5660 has the worst identification accuracy, but its average EER is still less than 10%. We also evaluate the EER performance for mixed devices, and the EER is 18.1% for the worst case and 4.0% on average. From the experimental results, our proposed approach achieves complete resilience to the wireless channel allowing a device to be correctly classified with near-perfect accuracy in unknown environments.



(a) 9C-A6-15-42-FC-F5.

(b) D0-D7-83-EE-DD-28.

FIGURE 13. FAR and FRR versus the threshold for two different NICs. (a) 9C-A6-15-42-FC-F5. (b) D0-D7-83-EE-DD-28.

B. IDENTIFICATION USING DNN

Next, we perform a cross-validation to illustrate the effectiveness of AoQ. DNN is chosen as the identification method. Our training is carried out through optimizing the cross-entropy loss function using an Adam solver with batch size setting to 256 on the collected dataset. All our network models were trained and tested running on Keras 2.1.6 using TensorFlow 1.12.0 as backend with an NVIDIA GeForce GTX 1070Ti GPU. Moreover, the L2 regularization of on both hidden layers was used to 0.001 prevent overfitting. The initial learning rate was set to 0.001 and the Xavier initialization was used to initialize the hidden layer weights.

We divide the data set into four categories, i.e., Location A, B, C, and D, according to the measured locations. By comparison, we first cross-check the identification accuracy using the received frequency responses of two LTSs over different data sets. In the testing process, when a device is

TABLE 3. Identification accuracy ξ using received frequency response of two LTSs. The signals were measured from four different locations in a 5 m × 8 m room. The distance between the receiver and the target devices was approximately 4 meters.

ξ (%) Test / Train	Location A	Location B	Location C	Location D
Location A	100.0	0.9	1.4	9.0
Location B	0.6	100.0	17.6	14.1
Location C	7.9	24.3	100.0	0.1
Location D	9.1	9.7	0.4	100.0

TABLE 4. Identification accuracy using AoQ. The signals were measured from four different locations in a 5 m × 8 m room. The distance between the receiver and the target devices was approximately 4 meters.

Devices	Device number	Accuracy 1(%)	Accuracy 2(%)
WDR-5620	15	100.0	100.0
WDR-5660	10	100.0	100.0
CPE-500	10	100.0	100.0
WS-5100	10	100.0	100.0
MI-3A	10	99.0	99.2
Mixed NICs	55	99.3	99.4

correctly identified as the real one, we call it a successful identification. Otherwise, we call it a failure identification. The identification accuracy ξ is defined as the ratio of the number of successful identifications to that of failure identifications during the testing process in the experiments. The identification results are shown in Table III. It is observed that the identification accuracy approximates 100.0% when the training and testing data are in the same location. However, the identification accuracy falls sharply when the training and testing data are in different locations, with a maximal value of 24.3% on the training of Location C and the testing of Location B. The results of Table III indicates that the received frequency responses of two LTSs are seriously influenced by the locations, which is consistent with the assumption in Section IV-A.

We also perform a cross-validation using the RFF feature of AoQ. Table IV shows the identification accuracy using AoQ for NICs with 5 types of models and all mixed NICs. Accuracy 1 and Accuracy 2 are the identification accuracies where training and testing data sets are measured at the same and different locations, respectively. It is observed that the accuracies is 100% for the NICs with WDR-5620, WDR-5660, CPE-500 and WS-5100 models and about 99% for MI-3A and the mixed NICs. There is no significant difference between Accuracy 1 and Accuracy 2, which indicates that AoQ is still effective in new locations.

Then, we explore the impact of noise to identification accuracy of AoQ by adding AWGN to the received time-domain LTSs signals. After signal acquiring, additive noise was imposed on the I/Q signal via MATLAB's awgn() function. Fig. 14 shows the identification accuracy using AoQ versus SNR for NICs with 5 types of models and all mixed NICs. The SNR is defined as the power of the received signal to that of the added artificial AWGN. It is observed that all the identification accuracies are higher than 95% when SNR is larger than 40 dB, while the accuracy of the mixed NICs declines to 90% when SNR decreases to 30 dB. However, the performance reduces seriously for SNR is below 30 dB which indicates that AoQ is still heavily influenced by noise. It is caused by the division. Although we attempt to alleviate this problem by selecting the optimal location where the AoQ has the smallest variance, the performance of AoQ in low SNR regions is still far from satisfactory, which needs to be addressed further.

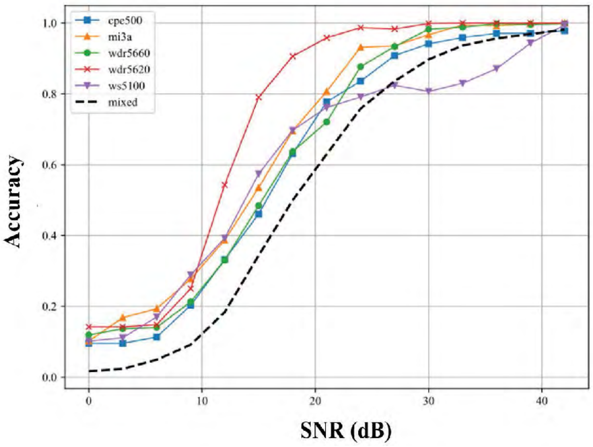


FIGURE 14. Identification accuracy using AoQ versus SNR(dB).

VI. CONCLUSION

This paper investigated the RFF feature extraction and identification issue for 802.11n devices in practical scenarios, in which the training and testing locations are different. We presented a differential phase approach using received pilots. We found that it is efficient for a small number of devices even at different training and testing locations. However, it is not applicable to the identification for a large number of devices due to the low-dimensional feature space. Therefore, we explored another location-invariant RFF feature suitable for large-scale devices. We found that the RFFs of two LTSs exhibit semi-steady characteristics since their frequency spectrums are different. Inspired by this fact, we proposed a novel RFF feature AoQ leveraging the channel coherence between two LTSs in an 802.11n beacon frame preamble. We demonstrated that AoQ is invariant to wireless channels. We further addressed the problem of noise amplification by collecting AoQs from multiple locations to constitute a robust AoQ feature. Simulation and experiment results indicated that our proposed AoQ approach can provide a good identification accuracy higher than 95% when SNR is higher than 40 dB and an EER around 4% for 55 WiFi NICs. In the future work, we will study how to improve the performance of AoQ in low SNR regions. Furthermore, more deep learning methods can be further investigated [39]–[41].

REFERENCES

[1] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, 1st Quart., 2016.

[2] L. Wang, J. Liu, M. Chen, G. Gui, and H. Sari, "Optimization-based access assignment scheme for physical-layer security in D2D communications underlaying a cellular network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5766–5777, Jul. 2018.

[3] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities," *Entropy*, vol. 21, no. 5, p. 497, 2019.

[4] H. Huang, S. Guo, G. Gui, Z. Yang, J. Zhang, H. Sari, and F. Adachi, "Deep learning for physical-layer 5G wireless techniques: Opportunities, challenges and solutions," 2019, *arXiv:1904.09673*. [Online]. Available: https://arxiv.org/abs/1904.09673

[5] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Commun.*, to be published.

[6] Y. Pan, S. Yang, H. Peng, T. Li, and W. Wang, "Specific emitter identification based on deep residual networks," *IEEE Access*, vol. 7, pp. 54425–54434, 2019.

[7] F. Shi, Z. Chen, and X. Cheng, "Behavior modeling and individual recognition of sonar transmitter for secure communication in UASNs," *IEEE Access*, to be published.

[8] Z. Zhang, X. Guo, and Y. Lin, "Trust management method of D2D communication based on RF fingerprint identification," *IEEE Access*, vol. 6, pp. 66082–66087, 2018.

[9] J. Li, D. Bi, Y. Ying, K. Wei, and B. Zhang, "An improved algorithm for extracting subtle features of radiation source individual signals," *Electronics*, vol. 8, no. 2, p. 246, 2019.

[10] Q. Tian, Y. Lin, X. Guo, J. Wen, Y. Fang, J. Rodriguez, and S. Mumtaz, "New security mechanisms of high-reliability IoT communication based on radio frequency fingerprint," *IEEE Internet Things J.*, to be published.

[11] L. J. Wong, W. C. Headley, and A. J. Michaels, "Specific emitter identification using convolutional neural network-based IQ imbalance estimators," *IEEE Access*, vol. 7, pp. 33544–33555, 2019.

[12] Y. Xing, A. Hu, J. Zhang, L. Peng, and G. Li, "On radio frequency fingerprint identification for DSSS systems in low SNR scenarios," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2326–2329, Nov. 2018.

[13] G. Verma, P. Yu, and B. M. Sadler, "Physical layer authentication via fingerprint embedding using software-defined radios," *IEEE Access*, vol. 3, pp. 81–88, 2015.

[14] Y. Tu, Z. Zhang, Y. Li, C. Wang, and Y. Xiao, "Research on the Internet of Things device recognition based on RF-fingerprinting," *IEEE Access*, vol. 7, pp. 37426–37431, 2019.

[15] W. Wang, Z. Sun, K. Ren, and B. Zhu, "User capacity of wireless physical-layer identification," *IEEE Access*, vol. 5, pp. 3353–3368, 2017.

[16] Y. Lin, X. Zhu, Z. Zheng, Z. Dou, and R. Zhou, "The individual identification method of wireless device based on dimensionality reduction and machine learning," *J. Supercomput.*, vol. 75, no. 6, pp. 3010–3027, Jun. 2019.

[17] M. Kheir, H. Kreft, and R. Knöchel, "UWB on-chip fingerprinting and identification using carbon nanotubes," in *Proc. IEEE Int. Conf. Ultra-WideBand (ICUWB)*, Paris, France, Sep. 2014, pp. 462–466.

[18] G. Baldini, C. Gentile, R. Giuliani, and G. Steri, "Comparison of techniques for radiometric identification based on deep convolutional neural networks," *Electron. Lett.*, vol. 55, no. 2, pp. 90–92, Jan. 2019.

[19] D. R. Reising, M. A. Temple, and M. E. Oxley, "Gabor-based RF-DNA fingerprinting for classifying 802.16e WiMAX mobile subscribers," in *Proc. IEEE Int. Conf. Comput. Netw. Commun. (ICNC)*, Maui, HI, USA, Jan./Feb. 2012, pp. 7–13.

[20] F. Demers and M. St-Hilaire, "Radiometric identification of LTE transmitters," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Atlanta, GA, USA, Dec. 2013, pp. 4116–4121.

[21] T. Zheng, Z. Sun, and K. Ren, "FID: Function modeling-based data-independent and channel-robust physical-layer identification," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Paris, France, Apr./May 2019, pp. 199–207.

[22] J. Yu, A. Hu, G. Li, and L. Peng, "A robust RF fingerprinting approach using multisampling convolutional neural network," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6786–6799, Aug. 2019.

[23] X. Zhou, A. Hu, G. Li, L. Peng, Y. Xing, and J. Yu, "Design of a robust RF fingerprint generation and classification scheme for practical device identification," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Washington, DC, USA, Jun. 2019, pp. 1–9.

[24] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelée, and B. Preneel, "Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning," in *Proc. 10th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, Boston, MA, USA, Jul. 2017, pp. 58–63.

[25] J. Hall, M. Barbeau, and E. Kranakis, "Detection of rogue devices in Bluetooth networks using radio frequency fingerprinting," in *Proc. IASTED Int. Conf. Commun. Comput. Netw. (CCN)*, Lima, Peru, Oct. 2006, pp. 108–113.

[26] A. M. Ali, E. Uzundurukan, and A. Kara, "Assessment of features and classifiers for Bluetooth RF fingerprinting," *IEEE Access*, vol. 7, pp. 50524–50535, 2019.

[27] J. Han, C. Qian, P. Yang, D. Ma, Z. Jiang, W. Xi, and J. Zhao, "GenePrint: Generic and accurate physical-layer identification for UHF RFID tags," *IEEE/ACM Trans. Netw.*, vol. 24, no. 2, pp. 846–858, Apr. 2016.

[28] D. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, and X.-Y. Li, "S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88–100, Feb. 2017.

[29] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "ORACLE: Optimized radio classification through convolutional neural networks," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Paris, France, Apr./May 2019, pp. 370–378.

[30] 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 Things J.*, vol. 6, no. 1, pp. 349–360, Feb. 2019.

[31] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom)*, San Francisco, CA, USA, Mar. 2008, pp. 116–127.

[32] M.-W. Liu and J. F. Doherty, "Nonlinearity estimation for specific emitter identification in multipath channels," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1076–1085, Sep. 2011.

[33] A. C. Polak, C. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1469–1479, Aug. 2011.

[34] S. Andrews, R. M. Gerdes, and M. Li, "Towards physical layer identification of cognitive radio devices," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Las Vegas, NV, USA, Oct. 2017, pp. 1–9.

[35] G. Baldini, R. Giuliani, C. Gentile, and G. Steri, "Measures to address the lack of portability of the RF fingerprints for radiometric identification," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Paris, France, Feb. 2018, pp. 1–5.

[36] 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 *Proc. IEEE INFOCOM*, Pairs, France, May 2019, pp. 190–198.

[37] G. Li, A. Hu, Y. Zou, L. Peng, and M. Valkama, "A novel transform for secret key generation in time-varying tdd channel under hardware fingerprint deviation," in *Proc. IEEE 82nd Veh. Technol. Conf. (VTC Fall)*, Sep. 2015, pp. 1–5.

[38] J. Yu, A. Hu, F. Zhou, Y. Xing, Y. Yu, G. Li, and L. Peng, "Radio frequency fingerprint identification based on denoising autoencoders," 2019, *arXiv:1907.08809*. [Online]. Available: https://arxiv.org/abs/1907.08809

[39] Y. Wang, M. Liu, J. Yang, and G. Gui, "Data-driven deep learning for automatic modulation recognition in cognitive radios," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 4074–4077, Apr. 2019.

[40] J. Wang, Y. Ding, S. Bian, Y. Peng, M. Liu, and G. Gui, "UL-CSI data driven deep learning for predicting DL-CSI in cellular FDD systems," *IEEE Access*, vol. 7, pp. 96105–96112, 2019.

[41] Y. Tu, Y. Lin, J. Wang, and J.-U. Kim, "Semi-supervised learning with generative adversarial networks on digital signal modulation classification," *Comput. Mater. Continua*, vol. 55, no. 2, pp. 243–254, 2018.

GUYUE LI received the B.S. degree in information science and technology and the Ph.D. degree in information security from Southeast University, Nanjing, China, in 2011 and 2017, respectively.

She is currently a Lecturer with Southeast University. Her research interests include physical layer security, secret key generation, radio frequency fingerprint, and link signature.

JIABAO YU received the B.S. degree from the Chien-Shiung Wu College, Southeast University, Nanjing, China, in 2014, where he is currently pursuing the Ph.D. degree. His current research interests include the Internet of Things, physical layer security in wireless communications, and optical networks.

YUEXIU XING received the B.E. degree in information engineering and the M.Eng. degree in electronic and communication engineering from Southeast University, Nanjing, China, in 2014 and 2016, respectively, where she is currently pursuing the Ph.D. degree. Her current research interests include the Internet of Things, physical layer security in wireless communications, and optical networks.

AIQUN HU received the B.Sc. (Eng.), M.Eng.Sc., and Ph.D. degrees from Southeast University, in 1987, 1990, and 1993, respectively.

He was invited as a Postdoctoral Research Fellow at The University of Hong Kong, from 1997 to 1998, and a TCT Fellow with Nanyang Technological University, in 2006. His research interests include data transmission and secure communication technology. He has published two books and over 100 technical papers in wireless communications fields.