



Reliable Digital Forensics in the Air: Exploring an RF-based Drone Identification System

ZHENGXIONG LI* *, University of Colorado Denver, United States

BAICHENG CHEN* , University at Buffalo, SUNY, United States

XINGYU CHEN , University of Colorado Denver, United States

CHENHAN XU , University at Buffalo, SUNY, United States

YUYANG CHEN , University at Buffalo, SUNY, United States

FENG LIN , Zhejiang University, China

CHANGZHI LI , Texas Tech University, United States

KARTHIK DANTU , University at Buffalo, SUNY, United States

KUI REN , Zhejiang University, China

WENYAO XU , University at Buffalo, SUNY, United States

63

As the drone becomes widespread in numerous crucial applications with many powerful functionalities (e.g., reconnaissance and mechanical trigger), there are increasing cases related to misused drones for unethical even criminal activities. Therefore, it is of paramount importance to identify these malicious drones and track their origins using digital forensics. Traditional drone identification techniques for forensics (e.g., RF communication, ID landmarks using a camera, etc.) require high compliance of drones. However, malicious drones will not cooperate or even spoof these identification techniques. Therefore, we present an exploration for a reliable and passive identification approach based on unique hardware traits in drones directly (e.g., analogous to the fingerprint and iris in humans) for forensics purposes. Specifically, we investigate and model the behavior of the parasitic electronic elements under RF interrogation, a particular passive parasitic response modulated by an electronic system on drones, which is distinctive and unlikely to counterfeit. Based on this theory, we design and implement DroneTrace, an end-to-end reliable and passive identification system toward digital drone forensics. DroneTrace comprises a cost-effective millimeter-wave (mmWave) probe, a software framework to extract and process parasitic responses, and a customized deep neural network (DNN)-based algorithm to analyze and identify drones. We evaluate the performance of DroneTrace with 36 commodity drones. Results show that DroneTrace can identify drones with the accuracy of over 99% and an equal error rate (EER) of 0.009, under a 0.1-second sensing time budget. Moreover, we test the reliability, robustness, and performance variation under a set of real-world circumstances, where DroneTrace maintains accuracy of over 98%. DroneTrace is resilient to various attacks and maintains functionality. At its best, DroneTrace has the capacity to identify individual drones at the scale of 10^4 with less than 5% error.

*Zhengxiong Li and Baicheng Chen are co-primary authors.

Authors' addresses: Zhengxiong Li* , University of Colorado Denver, Denver, CO, United States; Baicheng Chen* , University at Buffalo, SUNY, Buffalo, NY, United States; Xingyu Chen , University of Colorado Denver, Denver, CO, United States; Chenhan Xu , University at Buffalo, SUNY, Buffalo, NY, United States; Yuyang Chen , University at Buffalo, SUNY, Buffalo, NY, United States; Feng Lin , Zhejiang University, Hangzhou, Zhejiang, China; Changzhi Li , Texas Tech University, Lubbock, TX, United States; Karthik Dantu , University at Buffalo, SUNY, Buffalo, NY, United States; Kui Ren , Zhejiang University, Hangzhou, Zhejiang, China; Wenyao Xu , University at Buffalo, SUNY, Buffalo, NY, United States.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2022 Association for Computing Machinery.

2474-9567/2022/6-ART63 \$15.00

<https://doi.org/10.1145/3534598>

CCS Concepts: • Security and privacy → Biometrics; • Applied computing → System forensics.

Additional Key Words and Phrases: Digital Forensics, Drone, Identification System

ACM Reference Format:

Zhengxiong Li* , Baicheng Chen* , Xingyu Chen , Chenhan Xu , Yuyang Chen , Feng Lin , Changzhi Li , Karthik Dantu , Kui Ren , and Wenyao Xu . 2022. Reliable Digital Forensics in the Air: Exploring an RF-based Drone Identification System. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 6, 2, Article 63 (June 2022), 25 pages. <https://doi.org/10.1145/3534598>

1 INTRODUCTION

In past decades, drones have been developed in many critical areas, from law enforcement, and commerce, to education and recreation. By 2026, the market for drones is estimated to exceed \$63.6 billion [1]. Over time, drones have developed advanced recording, mechanical triggering, and carriage load functionalities at a low cost. Unfortunately, such technology also led to new forms of cyber-crime (e.g., weaponized drone robbery, voyeurism, trespassing, etc.). Even worse, drone forensic technologies are largely insufficient to match criminal drones even when captured [38].

Meanwhile, the traditional physical investigation may be impractical for inventory drone forensics and cause a set of law issues [19]. The U.S. Federal Aviation Administration (FAA) does not have criminal enforcement authority and cannot force drone registration. In addition, local and state authorities are limited by federal law from intercepting drones in flight, potentially even when a crime is in progress. Moreover, the current digital forensics based on the broadcast is infeasible for the inventory drone [4] (see Section 10 for details), and the flight log-based methods are not reliable that can be fake or altered [81]. Furthermore, existing advanced digital forensics such as camera- and lidar-based techniques are also not reliable, limited by significant ambiguities caused by ambient noise, illumination, and the similar exterior appearance [80].

To this end, we propose our digital drone forensics system (hereafter, DroneTrace), featuring the following characteristic: (1) **Reliable**: the fingerprint of each drone is clung to its intrinsic hardware characteristics that is *unique* and *unclonable*. (2) **Secure**: each drone can be accurately recognized without any drone's voluntary operation or compliance under the following premises (e.g., *passively - without drone compliance/cooperation, remotely - without contact, and in-situ - without interfering with drone's operation*). (3) **Robust**: it is strenuous to design a robust forensic tool resilient to the ambient noise, working location, and environmental conditions; (4) **Universality**: the digital fingerprinting technique should be cost-effective and pervasive and work on all drones without additional software/hardware adjustment. We first validate the existence of such fingerprints and discover a new fingerprint for forensics that is based on the parasitic elements of the drone due to the inevitable variations during the manufacturing process in electronic circuitry (see Section 3.2). Subsequently, we set out to investigate a non-contact electronics fingerprinting system as shown in Figure 6, for digital drone forensics. Specifically, we address the following two technical challenges in DroneTrace. (a) *How to sense and analyze parasitic element parameters from each drone in a non-contact and passive manner?* We discover and utilize the ‘interference’ of parasitic elements to the radio frequency (RF) stimuli. Parasitic elements on each drone modulate the RF stimuli signals and generate unique non-linear distortions to the RF wave reflection (hereafter *parasitic response*). In DroneTrace, we propose to utilize a cost-efficient millimeter-wave (mmWave) probe to passively illuminate the drone and capture the corresponding *parasitic response* from a distance as the fingerprint for identification. (b) *How to develop a robust forensic protocol and software framework for drone identification?* First, we design and implement an infinite impulse response (IIR) filter to remove diverse artifacts in RF reflection signals and extract the critical *parasitic response*. Next, we perform the joint tempo-spectral analysis (e.g., piece-wise spectrograms) and augment the subtle traits in the *parasitic response*. Finally, we develop a fine-tuned DroneTraceNet for drone identification, including a customized DNN model through training-aware neural architecture search (NAS) and compound scaling method.

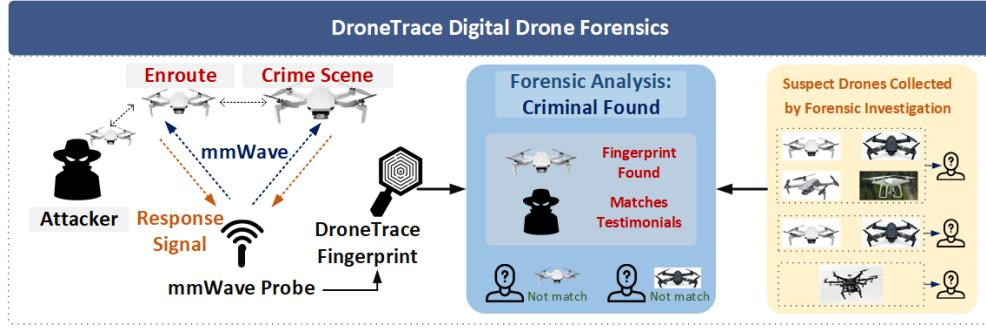


Fig. 1. The DroneTrace system can narrow down the scope of the investigation and provide important digital evidence to identify the adversary drone when its enroute or on crime scenes of dangerous/criminal activities [21, 43, 46, 60]. After the forensics team collected exhibits (e.g., drones) and testimonials from witnesses and suspects, the final decision is drawn from a combination of DroneTrace drone fingerprinting as well as exhibits/testimonials from traditional forensic methods.

To the best of our knowledge, DroneTrace is one of the first few works to investigate the possibility of non-contact electronics fingerprinting based on parasitic parameters, with applications to achieve secure and passive drone identification for forensics. Moreover, DroneTrace can be conveniently integrated with existing drone infrastructures (e.g., radar-based drone detection [12, 64] and tracking [24, 57] and defense [84]) and promising in real-world applications.

Our contributions can be summarized three-fold:

- We investigated a novel digital forensic approach based on RF-electronic parasitic effect in drones due to inevitable manufacturing variations in electronics.
- We design and implement the digital forensic system, DroneTrace, that can remotely and passively identify drones using a cost-effective mmWave probe, without any hardware addition or modification to drones, nor requiring drone compliance. In theory, the system will succeed identification of over 10^4 drones with less than 5% error.
- We carry out comprehensive evaluations to examine the performance of DroneTrace under different distances, interference, disguise, and occlusion conditions. The overall identification accuracy achieves up to 99.02% with 0.1s sensing time. Moreover, we conduct an in-depth study of capacity analysis and vulnerability analysis with real-world scenarios.

2 THREAT MODEL AND DIGITAL FORENSICS

2.1 Threat Model

We consider a team of drone forensic experts (i.e., Alice) are trying to solve a crime scene where an adversary, hereafter Bob, used a drone for criminal activities (e.g., voyeurism). Unwilling to leave any trace, the adversary (denoted as Bob) decides to use a malicious drone without compliance with any drone remote identification system (e.g., wireless broadcasting/visible label [3]). Meanwhile, the victim senses the drone approach during the attack at the crime scene. Rather than working in a physical way, such as intercepting the drone flight or hitting it down by the ultrasound gun (due to the law constricts or drone mobility), Alice can use a portable/handheld/station-deployed device to capture the distinct characteristics (i.e., the fingerprint) of the malicious drone swiftly. After the crime is conducted, Bob may leave the crime scene without leaving any personal marks such as body hair or fingerprint. But a list of prominent suspected drones related to this criminal activity is prepared from other pieces of evidence (e.g., reports from witnesses, suspicion from nearby people's presence/actions/testimonial) acquired

by the forensic team. However, the forensic team encounters difficulties narrowing down the investigation scope on a collection of suspected drones, assuming Bob's malicious drone is among these. Unlike software-based approaches, DroneTrace utilizes the drone's intrinsic hardware characteristics and extracts the associated drone's fingerprint contained inside, which acts as a traceable identifier for the drone. With the fingerprint of the malicious drone collected at the crime scene, the forensic team can match it with these suspected drones' fingerprints to reveal the malicious drone utilized by Bob as the criminal tool. In that way, DroneTrace can also provide an important digital evidence to identify the malicious drone to aid the forensic team and identify the drone and the adversary.

2.2 Digital Drone Forensics

Digital forensics primarily consists of three phases, the preparation (i.e., pre-investigation) phase that plans on what to identify or collect, the investigation phase that executes the plan (e.g., obtains evidence for trace matching), and the analysis (i.e., post-investigation) phase that reports the case with comprehensive results and evidence [102]. In the preparation phase, DroneTrace enables the feasibility of passively and conveniently record malicious drone fingerprints for later matching process. Once a collection of all suspect drones are confiscated by the forensic team, the analysis phase will indicate the suspect drone that committed crimes. DroneTrace aims at providing a reliable and deterministic solution to identifying a malicious drone among a collection of suspected drones based on suspect drones' intrinsic physical properties that are unique and unclonable.

3 DRONETRACE FUNDAMENTALS

3.1 Electronic Systems in Drones

For a drone to perform basic three-dimensional controlled motion actuation, it must carry at least a communication device, a control board, one or more actuators, and a power supply. These electronic components are interconnected to make up the drone's electronic system and define the drone's electronic system [5]. Although commercial drones are often mass-produced, each drone's electronic component will vary during manufacturing's imperfect fabrication process. As shown in Figure 2, the parasitic elements (i.e., resistance R_p , inductance L_p or capacitance C_p) on the control board are the circuit elements undesirably produced during the manufacture, which can cause different system responses compared to the original circuitry design [83]. In detail, the chassis for most drones are usually made of plastic or carbon fiber, therefore, mmWave signal can sense through-the-case and make the electronic system exhibit responses to mmWave excitations [18]. Such wireless sensing relations are expressed as in Equation 1 and 2 [36].

$$D(\omega) = \varepsilon_0 (\varepsilon_\infty + \underbrace{\int_0^\infty z_{ee}(t) e^{j\omega t} dt}_{\text{Parasitic Response}}) \cdot E(\omega), \quad (1)$$

$$B(\omega) = \mu_0 (\mu_\infty + \underbrace{\int_0^\infty z_{mm}(t) e^{j\omega t} dt}_{\text{Parasitic Response}}) \cdot H(\omega), \quad (2)$$

where ω is the angular frequency variable, E is the macroscopic electric field, and H is the macroscopic magnetic field in space and time with mmWave sources. D is the electric flux density, and B the magnetic flux density. ε_0 and μ_0 are the electrical permittivity and permeability of vacuum, respectively. ε_∞ and μ_∞ are the dimensionless dyadics corresponding to the reflection signal of an object to an input field. j is the imaginary unit, z_{ee} and z_{mm} are dimensionless dyadics called susceptibility functions that constitute the convolution kernels specifying the

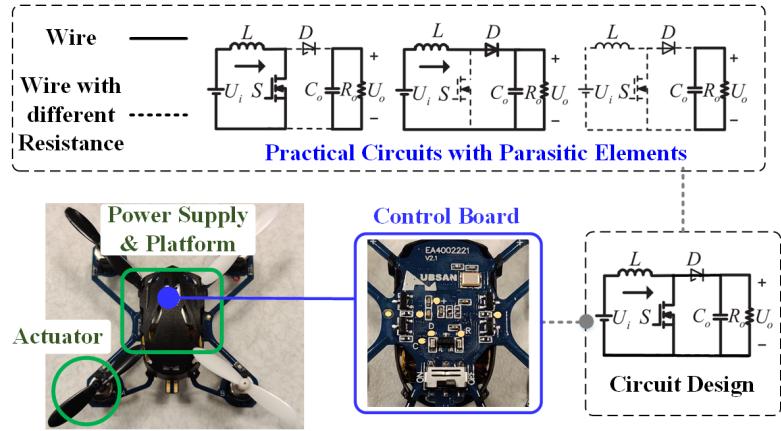


Fig. 2. The practical circuitry on the drone includes designated components and inevitable parasitic elements formed during the manufacture.

drone electronics' response to an input field, which are related to drone electronics' physical properties (e.g., parasitic elements) (see Section 3.3).

3.2 Hardware Variation-Based Fingerprint

3.2.1 Variation of Parasitic Elements. Variation caused by parasitic elements in electronic devices is inevitable, given electric components produced in mass-assembly with high-density circuits wiring introduce a significant impact on circuit behavior. Parasitic resistance, parasitic inductance, and parasitic capacitance are the three representative parasitic parameters, ranging from hundreds to thousands of electrons or sub-circuits in a control board with moderate complexity. Besides, all parasitic elements are subject to random intrinsic manufacturing process variations, such as an unanticipated shift in the size of metal trace beyond the accuracy of the controller or simple variance in the physio-chemical process of electronic components such as capacitors, diodes, and transistors. These variations reflect the unique characteristic frequency responses when circuits are probed by broadband radio frequency (RF) signals [51]. In other words, no two circuitry implementations have exactly the same parasitic equivalent circuits and parameters.

3.2.2 Parasitic Response. When the fundamental tone of a wireless signal is passed through the drone, the parasitic elements on the drone modulate the response signal and generate additional frequency tones besides the fundamental one [44]. The *parasitic response* is generated when these sub-carrier frequencies are generated due to the parasitic properties of the drone (e.g., material reflection efficiency, equivalent microstrip transmission lines, and inter-modulation) [69].

Hypothesis: *The parasitic response contains the unique characteristics of the drone (i.e., parasitic elements), that can be treated as the intrinsic and highly secure non-contact electronics fingerprinting for digital drone forensics.*

3.3 Forensics Feasibility Study

Electronic Circuit Characterization: The first uncertainty is if *parasitic effects* are sensitive enough to the parasitic elements of the electronics such that even circuits with the same design will produce different *parasitic responses*. To settle this skepticism, we employ the two most basic circuits with the same circuitry design, as shown in Figure 3. It is not hard to find that two circuits with the same element design have completely different parasitic elements. Due to the *parasitic effects*, the simulation system responses (i.e., transfer function model [31])

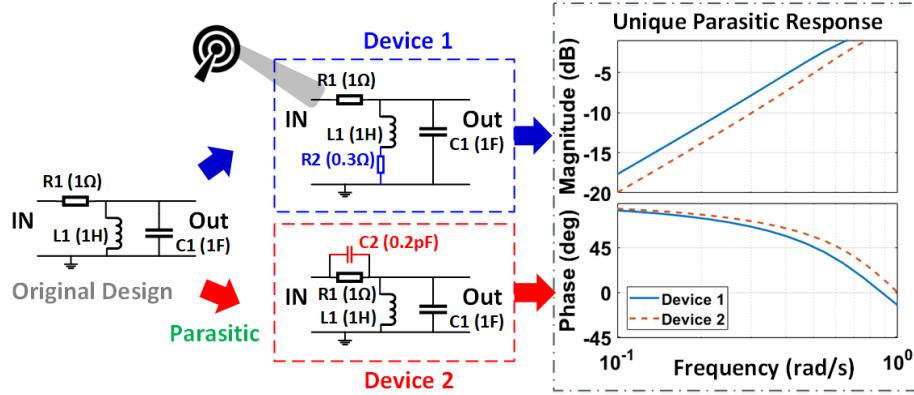


Fig. 3. An example of *parasitic effects* caused by parasitic elements of the most basic electronics. Devices 1 and 2 are with the same design, but generate different *parasitic responses* (under Bode plot [39]).

of the two circuits are different. In this example, the response of Device 1 is $sys_1 = \frac{1.3s}{1.3s^2+1.3s+1}$, while the response of Device 2 is $sys_2 = \frac{2e^{-13}s^2+s}{s^2+s+1}$, where s is a complex variable. From the simulation analysis results in the parasitic response, we observe their *parasitic responses* are significantly distinct owing to their uncontrollable parasitic elements during the circuit manufacture, which can be utilized to differentiate them. Moreover, there are dozens of such circuits on a single control board (see Figure 2), and these response differences will accumulate together to amplify the response differences further. As a result, our proposed *parasitic response* successfully distinguishes two circuits with identical designs from parasitic elements in electronics.

A Closer Look at Parasitic Response: In this part, we further explore the *parasitic response* on real electronics. First, one of the significant concerns is whether the *parasitic response* comes from electronics rather than artifacts (e.g., geometric shape). To address this doubt, we employ two off-the-shelf control boards and a counterfeit by 3D printing. As shown in Figure 4, these three objects share a similar geometric shape and the layout, all around $5.0 \times 3.6 \times 0.4$ cm (i.e., $1.97 \times 1.42 \times 0.16$ inches). These three objects are set at one meter (i.e., 39.37 inches) away, right over the mmWave probe. In Figure 4, the x-axis is the frequency of the received signal after the modulation, and the y-axis is the amplitude of the received signal after the demodulation. The *parasitic responses* (varied sub-carrier frequencies and amplitude) of the two control boards can be observed. Compared with the two control

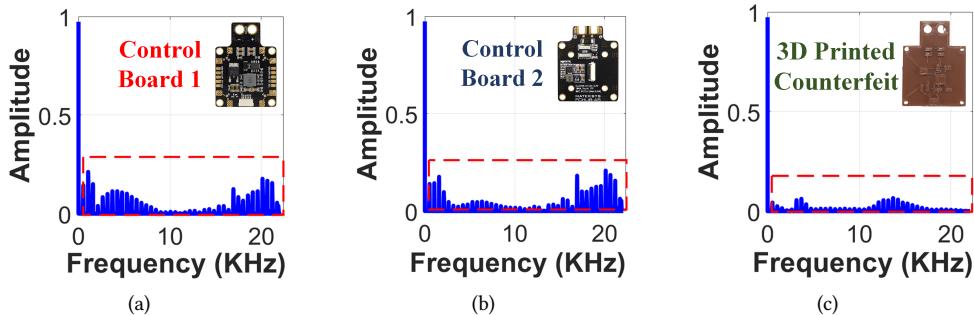


Fig. 4. The spectrums of the *parasitic response* from three different boards are distinct. (a) and (b) are two off-the-shelf circuitry control boards, and (c) is the 3D printed counterfeit of (a), which indicates parasitic responses come from the electronics.

board response spectrums, we notice the *parasitic responses* of the counterfeit are relatively negligible, which indicates the *parasitic response* comes from the electronics.

Proof-of-concept: Four different drones with different make and models are stimulated with the mmWave probe at one-meter distance. As shown in the periodogram (see Figure 5), the x-axis is the frequency of the received signal, and the y-axis is the power spectral density (PSD) of the received signal after the demodulation. The image of each corresponding drone is shown in the upper right corner. Their electronic systems vary in terms of size, components, and layout. The various sub-carrier frequencies can be observed such that separated from the signals of the artifacts, their *parasitic responses* varied from electronics are distinct at the frequency and PSD. Moreover, the results are promising, implying that given the massive amount of electronics on the drone, *parasitic responses* have sufficient space to be served as a powerful identity for drone forensics (See Section 7.2 for details).

4 DRONETRACE OVERVIEW

As shown in Figure 6, we propose DroneTrace, a system for secure and passive drone identification.

Parasitic Response Stimulation and Modeling: We introduce the RF hardware in *DroneTrace* to stimulate and acquire the *parasitic response* from electronics. Compared to other traditional radar technologies (e.g., Pulse-Doppler radar), the frequency modulated continuous wave (FMCW) radar continuously emits periodic chirp signals and has a superior performance to catch the distinguishable *parasitic responses* after the stimuli signals hit the target drone. Therefore, *DroneTrace* selects an FMCW radar with a narrow passband filter [68]. When

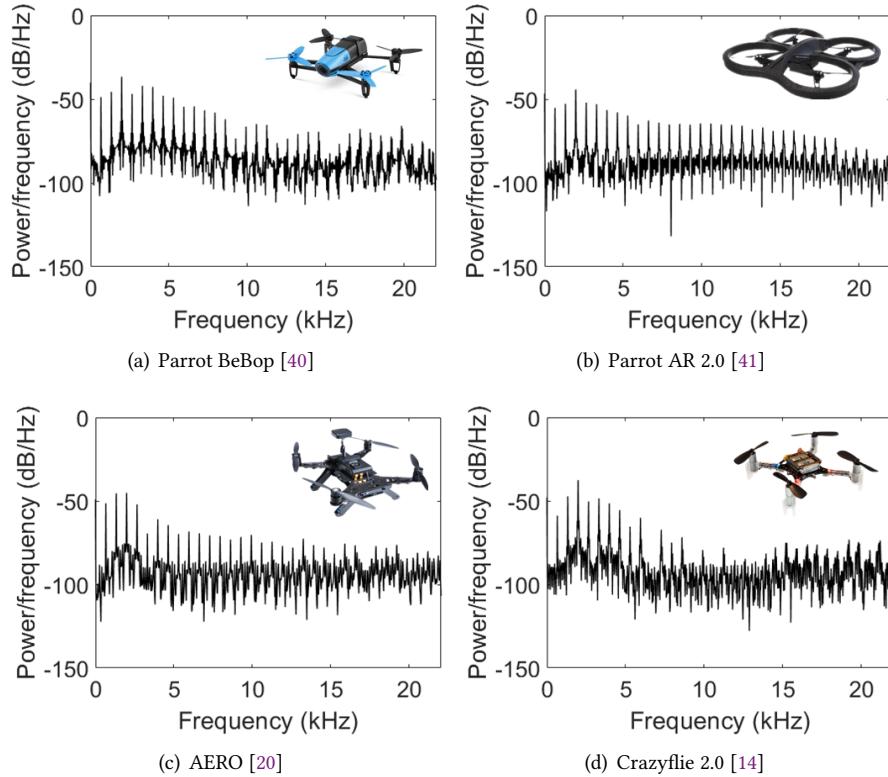


Fig. 5. Periodogram [94] analysis depicts distinct demodulated *parasitic responses* from four drones.

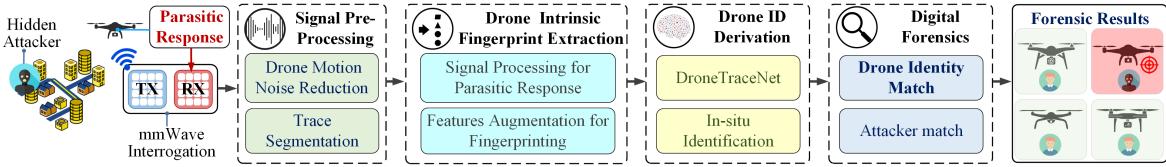


Fig. 6. DroneTrace is a reliable digital drone forensic identification system based on the non-contact electronics fingerprint. By capturing the *parasitic response* returned from the drone after RF stimulation, a drone's unique fingerprint can be extracted. Owing to the effective ID matching with a passively collected fingerprint from the crime scenes and fingerprints from confiscated suspected drones, the malicious drone, and attacker that appeared around forensic scenes can be precisely identified.

an incident signal passes through the drone, electronics on the drones with their parasitic elements act as a passive convolutional processor (see Figure 1), and generate non-linear distortions to the original signal. After the manipulated signal radiates from the drone, the *parasitic response* will be captured by the RF probe receiver antenna (Rx). The process can be formulated as $E(t) = m(z(t), \tau(t)) \otimes h_f(t)$, where $E(t)$ is the reflected signal, $m(\cdot)$ is the non-linear modulation function of the parasitic elements, $z(t)$ is the parasitic response signal, $\tau(t)$ is the admittance and impedance matrix descriptions for the non-linear system, \otimes stands for convolution computing and $h_f(t)$ is the ideal bandpass filter function for the carrier bandwidth [30].

DroneTrace Forensic Processing: Once *parasitic response* signals are received, DroneTrace will first remove the ambient noise and extract the effective non-contact electronics fingerprints from the *parasitic response*. After that, a deep learning-based identification model is developed to verify the drone's identity.

5 RELIABLE DRONE FINGERPRINTING

5.1 Signal Pre-processing

5.1.1 Ambient Noise Reduction. Motion noise reduction is to reduce the noise level in the received signal and simultaneously prevent the waveform from distortion. Thereby, before we extract the fingerprint from the *parasitic response*, we employ a filter to remove these components as depicted in Figure 6. However, filtering the *parasitic response* is complicated, which requires smoothing the noise and preserving the frequency response at the same time. Consequently, we apply an IIR filter, xyra 12-order low pass Butterworth filter [72]. Compared with the Finite Impulse Response (FIR) filter, the IIR filter is composed of a few optical sources and a recursive delay line, so it can be implemented with a simple structure. Moreover, IIR filters with a large number of optical taps can provide high-Q band-pass filtering [45]. Also, compared to other IIR filters, the Butterworth filter has a better linear phase and flatter response within the bandwidth, thereby making this approximation suitable for motion noise cancellation. The Butterworth filter is a type of signal processing filter as $|H(j\omega)| = \frac{1}{\sqrt{1+\epsilon^2(\frac{\omega}{\omega_p})^{2n}}}$, where n represents the filter order, ω is the natural frequency ($2\pi f$), and ϵ is the maximum passband gain.

5.1.2 Trace Segmentation. After the noise cancellation process, we treat each probe sensing measurement as the *sample*, which is a one-dimension time sequence signal. In DroneTrace, it usually lasts 10s. To extract the fingerprint more effectively and decrease the computation overhead, we introduce a concept, *trace* noted as γ , which is defined as a sub-segment of a *sample*. We empirically select 0.1s as its length (evaluated in Section 8.3). Finally, we obtain the effective *parasitic response* signal, a *trace*, for the fingerprint extraction.

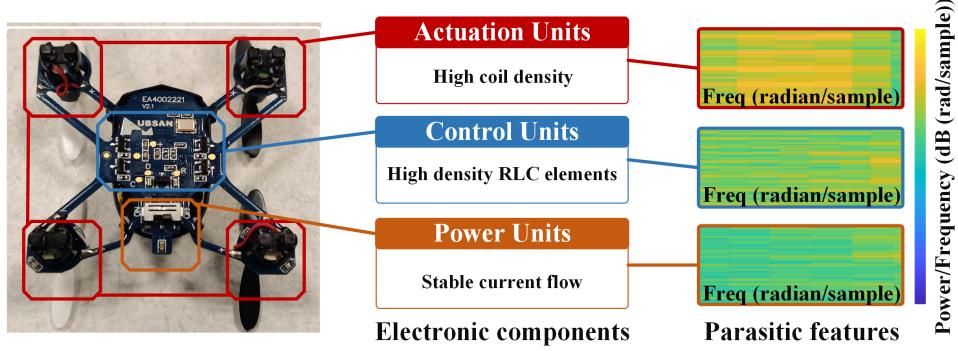


Fig. 7. DroneTrace feature representation in spectrogram form. Different electronic components complement different parasitic features in the response signals, which uniquely characterizes each drone. The x-axis is frequency, the y-axis is sample count, and the color represents power density.

5.2 Drone Intrinsic Feature Extraction

5.2.1 Parasitic Response Analysis. The response analysis is the function that demodulates the response, reflects the drone's parasitic characteristics, obtains the integration of content features, and outputs a feature vector. We use Variational Mode Decomposition (VMD) as $P()$ to represent the *parasitic response* analysis function, which is an effective multi-resolution analysis tool for signal decomposition [26]. This approach $P()$ decomposes the input signal into different amplitude and frequency modulated waves, which has superior performance in keeping all inner characteristics of the signal and efficiently eliminating the noises [59].

By using VMD, a multi-component signal can be non-recursively decomposed into a series of quasi-orthogonal intrinsic element signals. Subsequently, the resulting constrained variational problem analysis is achieved as Eq. (3):

$$\left\{ \begin{array}{l} \min_{\{u_k\}, \{w_k\}} \left\{ \sum_k \left\| \partial_t [(\delta(t) + \frac{j}{\pi t}) * u_k(t)] e^{-j\omega_k t} \right\|_2^2 \right\}, \\ \text{s.t. } \sum_k u_k = f, \end{array} \right. \quad (3)$$

where $\{u_k\} := \{u_1, \dots, u_k\}$ and $\{\omega_k\} := \{\omega_1, \dots, \omega_k\}$ are shorthand notations for the set of all modes and their center frequencies, respectively. f is the input signal, $j^2 = -1$, and $\sum_k := \sum_{k=1}^K$ for summation operation. Thus, we can get $s(t) = \Gamma(P_0, P_1, P_2, P_3)$, where $s(t)$ is the effective *parasitic response*, η is the part number, P_0 is the approximation, P_1 is the Level 1 detail part, P_2 is the Level 2 detail part, P_3 is the Level 3 detail part, $F_W(a_0, b)$, $F_W(a_1, b)$, $F_W(a_2, b)$ and $F_W(a_3, b)$ are the coefficients [91]. $\Gamma(\cdot)$ is a function to construct an initial feature vector by combining the approximation, Level 1, Level 2, Level 3 parts in order (See Section 7.1). As a result, we exploit the inherent traits in the *parasitic response* by exploring the frequency band.

5.2.2 Features Augmentation for Fingerprinting. Previous studies have found that the discrete cosine transform (DCT) can provide more fine-grained information in learning signal models [76], and less information is being lost at the beginning phase [25]. Therefore, to better augment and visualize the features, we utilize the joint tempo-spectral analysis to represent the *parasitic response* into a set of spectral sub-bands, where literally a high-dimensional image-alike representation is formed.

Let $W(k)$ be the function to generate the spectral image from the input signal x of length N , which is defined in as follows:

$$\begin{aligned} W(k) = & \sqrt{\frac{2}{N-1}} \sum_{n=1}^N x(n) * \frac{1}{\sqrt{1+\delta_{n1}+\delta_{nN}}} \\ & * \frac{1}{\sqrt{1+\delta_{k1}+\delta_{kN}}} \\ & * \cos\left(\frac{\pi}{N-1}(n-1)(k-1)\right), \end{aligned} \quad (4)$$

where the X-axis presents the time dimension, and the y-axis represents the frequency dimension. The third dimension shows the amplitude of a particular frequency at a specific time represented by the color. Finally, the converted DCT inputs to drone identification model. As shown in Figure 7, the resulting parasitic features in spectrogram image shows unique patterns in spectral temporal domain. The high amplitude response from actuation units with high coil density as well as high current flow. The sparse response from control unit resulted from high density of electric components each contributing their parasitic response. The nearly plain response from power unit's simple circuitry design and stable current flow. All these signifies parasitic response from the drone's electronic system uniquely labeling the drone under mmWave interrogation.

5.3 Drone Identification

5.3.1 Passive Identification Method. The drone identification problem can be formulated as a multi-class classification problem, as shown in Algorithm 1. A traditional approach to address this problem is first to extract a set of invariant statistical features from the fingerprint forming a feature vector, and then feed this feature vector into a classifier (e.g., SVM, KNN). However, suffering from a considerable variation in amplitudes as well as frequencies among different working conditions, it is an intractable task. Thus, rather than manually design filters or rules to decode features from the *parasitic response* signals, we employ a customized Deep Neural Network (DNN), namely DroneTraceNet (see Section 5.3.2), inspired by other work investigating identification systems [82]. With the feature descriptors accurately capturing the parasitic response from the previous step, DroneTraceNet's goal is to link these features to their corresponding ID as accurately as possible. Moreover, this identification framework can be applied to new scenarios without retraining every domain knowledge. Given the received *parasitic responses*, we analyze MDCT (Modified Discrete Cosine Transform) [16] to identify the drone fingerprint in the form of the time-frequency graph. The response augmentation visualization will be further employed as the input of the model.

To detect alien drones which are not registered in the database, we define the maximum probability as the classification score. If the classification score is less than the threshold, the trace will be declared as an alien device with a second manual check; if not, the predicted type with the maximum probability will be regarded as the identification result. To effectively eliminate false positives, we empirically select the threshold value of 0.85. In practice, this guarantees DroneTrace's model to return matched drone fingerprints at least 85 % alike, similar to human fingerprinting's 70 % confidence level in legal uses [74]. Finally, the majority vote algorithm is employed to make the final identification decision from these DroneTraceNet results.

5.3.2 DroneTraceNet: A DNN-based Model for Drone Identification. The DroneTraceNet is based on EfficientNet-B3 [88]. It combines a training-aware neural architecture search (NAS) and compound scaling method. Compared to other representative DNN models (e.g., ResNet and DenseNet), it can achieve higher accuracy and higher parameter efficiency, making it compact for portable devices. DroneTraceNet mainly consists of a stack of convolutional operations (MBConv, Fused-MBConv), adaptive average poolings, and identity activation function for passive drone identification. The number of layers, kernel size, and expansion ratio is decided by Neural

Algorithm 1 DroneTrace Identification

Input: θ : parasitic response traces from a drone
Output: R : The identification result

```

1:  $R, E_\theta \leftarrow 0$ ;                                ▷ Initialize parameters
2: Initialize  $T$  ;                                     ▷ Classification score threshold
3: for  $\theta_i = \theta_1, \theta_2, \dots, \theta_L$  do
4:    $\varrho = Feature(\theta_i)$ ;                         ▷ Feature extraction
5:    $E = Cls(\varrho)$ ;                               ▷ Drone identity profiling
6:   if  $Score(E) < T$  then                         ▷ Generate identity match score
7:      $E \leftarrow Reject!$ 
8:   end if
9:    $E_\theta.append(E)$ ;
10:  end for
11:  $R = Res(E_\theta)$                                 ▷ Decide the identity result
12: return  $R$ 
```

Architecture Search (NAS) with the optimization goal of $ACC(m) \times [FLOPS(m)/T]^w$ and the constrain of $\alpha \cdot \beta^2 \cdot \gamma^2 \approx 2$ [88, 89], where $ACC(m)$ denotes the accuracy, $FLOPS(m)$ means the floating-point operations per second, and $FLOPS$ represents the number of operations required to run a single instance of the model. T is the target FLOP, w is the trade-off between accuracy and FLOPS. α, β, γ denotes the network width, depth, and resolution. In our implementation, we train the DroneTraceNet with the cross-entropy loss, and we choose a lightweight stochastic gradient descent optimizer to fine-tune the parameters.

5.4 Drone Forensics

In terms of drone forensics in real life, DroneTrace will serve three purposes, 1) identifying the criminal drone, 2) leading clue to the criminal, 3) deterrent for potential criminals. First, the DroneTrace system can accurately identify the malicious drone from collected suspect drones through the signature captured from the crime scene in a digital way. Second, DroneTrace system provides the additional clues to information collected from other forensic methods (e.g., location, drone appearance, drone behavior, fly path, timing, etc.) to confirm the malicious drone presence and aid to trace the attacker. Lastly, the ability for DroneTrace system to securely and accurately recognize the criminal drone, which leads to the finding of criminals, can also deter potential criminals that plan to use drones as a malicious tools.

6 SYSTEM PROTOTYPE & EVALUATION

Experimental Setup: We conducted experiments in several environments simulating potential drone crime scenes, e.g., a parking lot around a detached house, a large meadow within the university campus (voyeurism on dorm rooms), and an open square in the downtown area, as depicted in Figure 8(a). The drones are programmed to take off, hover, or maneuver the probe to mimic different stages of the crime (e.g., approach victim, extorting victim, and retreat) as demonstrated in Figure 9. At each stage of experiments, the drone's signature data is collected with different robustness parameters from our receiver. After data collection is complete, DroneTrace's model training is completed on a workstation equipped with an Intel Xeon CPU and one Nvidia Titan Xp 12 GB GPU. Finally, the forensic identification system is implemented on a laptop with Intel i7-6700HQ mobile processor for real-time testing.

Data Collection: The experiments were conducted on 36 drones and labeled into 36 different classes, unless specified otherwise. Notably, among these collected drones, there were 13 identical Crazyflie 2.0, two Cheerwing

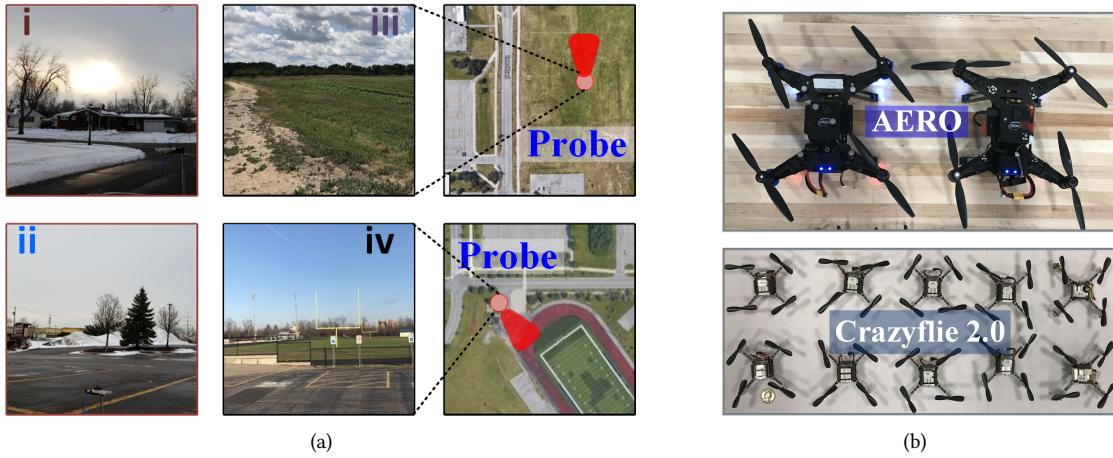


Fig. 8. DroneTrace experimentation areas: (a) Different sites: (i) around a house, (ii) an open square near downtown area, (iii) a large meadow, and (iv) outdoor sport area. (b) Examples of drones in experiments.

Syma X5SW, two Holy Stone HS110D, and two AERO (some examples are shown in Figure 8(b)). These drones are made of typical anisotropic materials and are commercially available. The drone sizes range from $10.16 \times 7.62 \times 2.54$ cm ($4 \times 3 \times 1$ inches) to $63.50 \times 63.50 \times 15.24$ cm ($25 \times 25 \times 6$ inches). In every evaluation experiment trial, the drone signature is acquired while hovering/charging through the mmWave probe at a fixed distance (two meters away for default). In this work, the maximum drone speed for signature acquisition determined to be $6.3m/s$, which is larger than most drone moving speeds in actual tasks [57]. The speed of the drone is controlled by the program or calibrated by the velocity speed gun [86]. Unless specified, we collect 1,000 traces for each drone in each of the 5 experimentation areas (1 indoor lab environment, 4 outdoor field environments), partitioning 700 traces for training and 300 traces for testing. As a result, there are entirely 126,000 traces for training and 54,000 for testing in total. A 10-fold cross-validation method is employed to ensure model robustness.

mmWave Probe: DroneTrace employs a FMCW mmWave probe, whose carrier frequency is set up as 24GHz with 450 MHz bandwidth [51, 67]. A pair of four-by-four patch antenna arrays is designed, offering an antenna directionality of 19.8 dBi. The weight of the probe is 45.5 g, and the cost for the probe is less than \$100. The

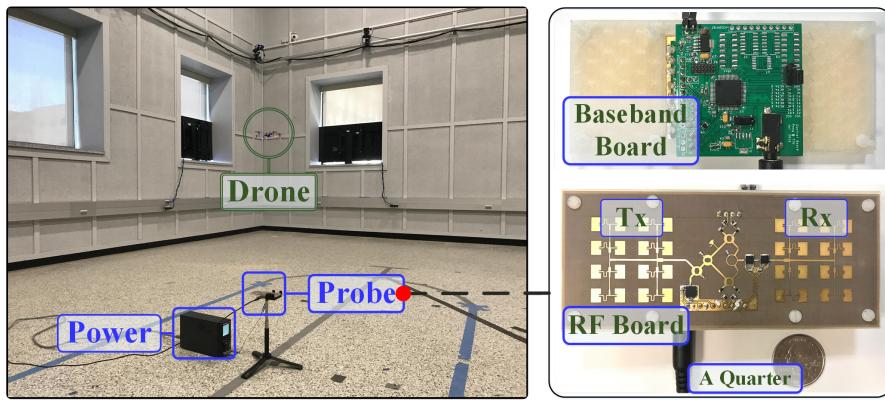


Fig. 9. The experimental implementation for drone authentication in an indoor environment.

transmitting power of this probe is typically 8 dBm with a 5.5 V supply voltage under 1.2 W DC power consumption. Using rough approximation of a drone with radar cross section (RCS) of 0.5 m^2 for drone response, single pulse duration of 6.45 ms , acceptable signal to noise ratio (SNR) of -21 dB , total gain of 24 dB , the maximum sensing distance calculated is 8.2 m [78].

Performance Metrics: To evaluate the system performance, we adopted Equal Error Rate (EER) and Receiver Operating Characteristic (ROC), in addition to typical techniques such as accuracy, precision, and recall [15].

7 PERFORMANCE EVALUATION

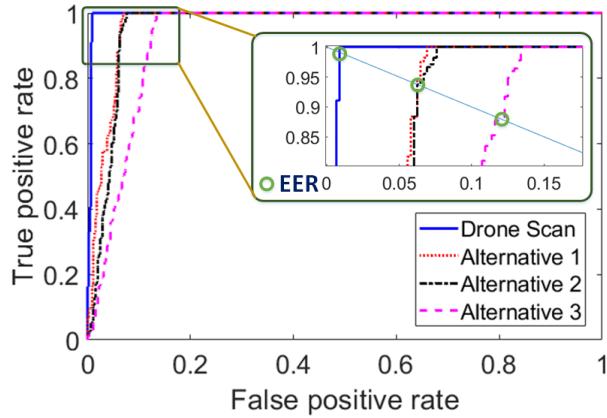


Fig. 10. The overall performance of DroneTrace with different schemes.

7.1 Drone Identification Accuracy

We evaluate the ability of DroneTrace to identify different drones' identities in a lab environment. Performance analysis is based on the dataset gathered from *Data Collection* process. First, we exploit the overall identification performance of *DroneTrace* with different schemes (see Section 5). Then, we apply the sensing data without the noise cancellation module (denoted as Alternative 1). Further, to study whether the signal processing is effective, we reconstruct the *parasitic response* with the combination of (P_0, P_1, P_2) and (P_0, P_1) , respectively (denoted as Alternative 2 and Alternative 3). The identification performance (ROC curve) is shown in Figure 10 in which the drone fingerprints are corresponding to the fingerprint explored in Section 5. The performance results achieve the EER of 0.009 , 0.062 , 0.062 , and 0.121 , respectively in four schemes. The comparatively low EER in this approach indicates that our solution does not have the over-fitting issue and can adapt to various usage scenarios. Additionally, the accuracy of the overall system (i.e., DroneTrace) is 99.02% . This result proves the effectiveness of DroneTrace's fingerprint well-representing the uniqueness of various drones in different environments.

7.2 DroneTrace Capacity Analysis

Similar to other biometric fingerprints (e.g., fingerprint and Face ID), DroneTrace will first interrogate Drone α and obtain its *parasitic response* samples β for k times. And then DroneTrace utilizes the fingerprint extraction algorithm p_k to process these k samples and build the identity profile I_α . To comprehensively and systematically analyze the drone fingerprint, we evaluate it in the following three dimensions: uniformity, reliability, and uniqueness with the data in the *Data Collection* [58].

7.2.1 Uniformity. This dimension is concerned with value variations with respect to the locations of the values *in a trace*, which shows how uniform values are in a fingerprint. The ideal value for this metric is less than 10% [65]. Uniformity of the fingerprints from total $\gamma = L$ traces among β -th sample on the α -th drone is calculated as follows:

$$U(\alpha, \beta) = \frac{1}{\mu} \sqrt{\frac{1}{m * n * L} \sum_{\gamma=1}^L \sum_{\theta=1}^m \sum_{\vartheta=1}^n (I_{\alpha\beta\gamma}(\theta, \vartheta) - \mu)^2}, \quad (5)$$

where μ is the average of $I_{\alpha\beta\gamma}$, m and n are the length and width of $I_{\alpha\beta\gamma}$ respectively. We achieve the average uniformity of all fingerprints from collected drones as 9.01%, proving the values in the fingerprint is even.

7.2.2 Reliability. Aiming to illustrate how consistent fingerprints are reproduced by the same drone, this dimension evaluates the overall *intra-drone* fingerprint persistence of within multiple traces. The ideal value for this metric is around 1 [95]. Reliability of the fingerprints from a total $\beta = T$ samples on the α -th drone is calculated as follows:

$$\left\{ \begin{array}{l} R(\alpha) = \frac{2}{T(T-1)} \sum_{\beta_1}^{T-1} \sum_{\beta_2=\beta_1-1}^T \Phi(I_{\alpha\beta_1}, I_{\alpha\beta_2}) \\ \Phi(I_{\alpha\beta_1}, I_{\alpha\beta_2}) = \frac{(2\mu_{\alpha\beta_1}\mu_{\alpha\beta_2} + c_1)(2\sigma_{\alpha\beta_1\alpha\beta_2} + c_2)}{(\mu_{\alpha\beta_1}^2 + \mu_{\alpha\beta_2}^2 + c_1)(\sigma_{\alpha\beta_1}^2 + \sigma_{\alpha\beta_2}^2 + c_2)}, \end{array} \right. \quad (6)$$

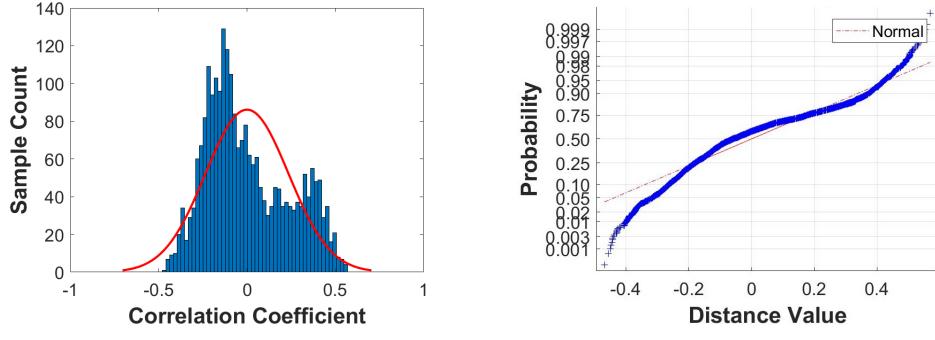
where $\Phi(\cdot)$ is the function for the structural similarity index, $I_{\alpha\beta_1}$, $I_{\alpha\beta_2}$ are the feature element of two fingerprints that belong to different samples on the α -th drone. $\mu_{\alpha\beta_1}$ and $\mu_{\alpha\beta_2}$ are the mean of the fingerprints from that two samples respectively. $\sigma_{\alpha\beta_1}$ and $\sigma_{\alpha\beta_2}$ are the standard deviation of those two respectively. $\sigma_{\alpha\beta_1\alpha\beta_2}$ is the covariance of $I_{\alpha\beta_1}$ and $I_{\alpha\beta_2}$. c_1 and c_2 are two variables to stabilize the division with weak denominator. Specially, $T = 36$ in this evaluation. The average reliability of all drones is 0.8094, which implies the fingerprint is steady among different traces.

7.2.3 Uniqueness. The purpose of this dimension is to evaluate DroneTrace's *inter-drone* fingerprint uniqueness, represented with the ability to distinguish a potential innocent drone from a group of suspect drones. We employ the data from in the *Data Collection* and specifically use the Pearson's correlation coefficient, \mathfrak{U} , which is defined by the following Equation (7) [55]. We first suppress the feature trend by normalizing each fingerprint with the mean of all fingerprints.

$$\mathfrak{U} = \frac{2}{T(T-1)} \sum_{\alpha_1}^{T-1} \sum_{\alpha_2=\alpha_1-1}^T \frac{(I_{\alpha_1} - \mu_{\alpha_1})(I_{\alpha_2} - \mu_{\alpha_2})}{\sigma_{\alpha_1} \sigma_{\alpha_2}}, \quad (7)$$

where I_{α_1} , I_{α_2} are the feature elements of two fingerprints that belong to different drones. μ_{α_1} and μ_{α_2} are the mean of the fingerprints from the two drones, respectively. σ_{α_1} and σ_{α_2} are the standard deviation of those two respectively.

As shown in Figure 11(a), the Gaussian curve of the results centers at zero, which indicates that drone fingerprints are highly independent. Its mean, $\mu = 5.8E - 16$, is in its 95% significance level [-0.0122, 0.0122] with a high accuracy. In addition to the frequency distribution histogram, Figure 11(b) shows the normal probability plot to identify any substantive departure from normality. The dotted line in red provides the reference for perfect normality. The upper end of the plot bends below the diagonal line while the lower end bends above that line, forming an S shaped-curve, which indicates the distribution is similar to the normal. Lastly, we conduct a *t*-test. The test decision h is 1.0, and p value is 0.01, significantly lower than $\alpha = 0.05$, which indicates that the result distribution is intensely akin to the normal distribution. Thereby, we prove the independence between two fingerprints and ensure that the forensic team can accurately determine the malicious drone.



(a) Histogram with a Gaussian distribution fit of correlation coefficient, which concentrates towards 0, indicates the fingerprints are independent.

(b) Normal probability plot. The probability from 0.05 to 0.95 has the correlation ranging from -0.3 to 0.3, which is considered as a weak strength of association.

Fig. 11. The correlation test between fingerprints among different drones.

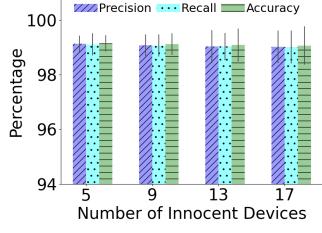


Fig. 12. DroneTrace identification performance toward different number of innocent devices.

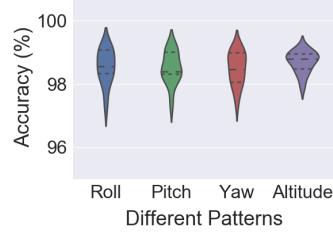


Fig. 13. DroneTrace identification performance under different flying patterns.

7.3 Fingerprint Capacity

For drone forensics, the fingerprinting capacity is a significant concern for practical system designers and can also be a key metric to evaluate identification performance. Thus, an information-theoretic approach, based on Fano's Inequality and the mutual information between drone fingerprint and identity, is established to comprehend the drone capacity of DroneTrace [93]:

$$N_C = \max(N_Y | \frac{\log(N_Y) - I(X; Y) - H(\lambda)}{\log(N_Y - 1)} \leq \lambda), \quad (8)$$

where N_C is the identity capacity, N_Y is the set of all possible drone numbers, Y is the user identity, $I(X; Y)$ is the mutual information between drone fingerprint and identification, λ is the performance threshold for classification error rate, and $H(\lambda)$ is the entropy of the performance threshold. By far, the theoretical tool to derive the user capacity of the drone fingerprint is given in Equation (8). Given the 5% identification performance error, the fingerprinting capacity in DroneTrace is 14 bits, which allows more than ten thousand drones to be reliably identifiable at a given time. Thus, DroneTrace contains a sufficient fingerprint capacity for most drone forensic applications.

7.4 Impact of Innocent Drones

As discussed in Section 5.3.1, in the real-world application, DroneTrace may face innocent drones, and it would be ideal if DroneTrace could reject the innocent drones, for which they are not trained in advance. We design an

experiment to explore the performance of the innocent drones. Out of 36 drones, only 19 drones are randomly selected for training and the remaining untrained 17 drones are used for testing. We gradually increase the number of innocent devices from 5 to 17 (increment of 4) and verify whether our specifically designed Algorithm 1 can successfully reject them. As shown in Figure 12, the results remain stable in detection accuracy (99.0%-99.5%), showing no tendency to decrease in performance. In this way, we prove the effectiveness of innocent device rejection and the excellent scalability of DroneTrace when used in real practice. Under these circumstances, after discovering the innocent device, the inspector can use the second check (e.g., manual inspection) for further security verification.

8 PRACTICABILITY STUDY

In this section, we evaluate the reliability and robustness of DroneTrace identification performance under various real-world forensic circumstances. We select the 20 most representative drones including both intra- and inter-drone evaluation settings. For each time setting, we follow the same preparation described in Section 6. The training data will consist a group of suspect drones collected from forensics, and the testing data will be collected from crime scene.

8.1 Impact of Flying Patterns

It is highly likely that the drones in a motion when being identified, thus, we examine DroneTrace's resilience against drone motion. To stabilize and maneuver drones, typical drone movements can be categorized into four categories, i.e., roll, pitch, yaw, and altitude [79]. Thus, we study the authentication accuracy under each flying pattern. The violin plot [37] illustrates the probability density of the results at different conditions. As shown in Figure 13, the accuracy of identification maintains the stable accuracy ranging from 98.3% to 99.0% with a high probability in different flying patterns, which implies DroneTrace can work robustly when drones cannot fly smoothly.

8.2 Impact of Sensing Distance

To validate the usability and effectiveness of DroneTrace in the non-contact forensic scenario as mentioned in Section 6, we set up the device to stimulate the operation distance from 0.3m to 8m considering the mmWave coverage of the majority of commercial drones in relation to their non-linear response magnitude. Figure 14 shows that their performances can achieve up to 99.04% precision, 99.02% recall and 99.05% accuracy, with 0.008 EER. Besides, the identification performance precision, recall, accuracy, and EER still keep at 92.11%, 92.15%, 92.12%, and 0.078, respectively, when the sensing distance increases to eight meters. The results indicate DroneTrace can fully prevent a user from attacks from 8 m range, and surpassed the ($>7.01\text{m}$ [90]) distance requirement in practice. Therefore, DroneTrace can facilitate passive and convenient forensic identification in real practice.

8.3 Impact of Sensing Time

In drone forensics, evidence acquisition is often difficult due to criminal drone's agility (e.g., short presence timespan, high moving speed, physically threatening to victims). Thus, we are interested in analyzing the performance of *DroneTrace* with regard to different time budgets. Specifically, we manually select four different time settings between 0.02s to 0.2s. Figure 15 shows the performance results. For the lowest time budget of 0.02s, DroneTrace only obtains 87.68% accuracy with 0.118 EER. This is due to the contained information in traces with 0.02s cannot comprehensively represent the characteristics of DroneTrace. After increasing the time budget, the performance gradually increases. Finally, we find a sweet-spot at 0.1s, where the performance saturates afterward (reaching 99.16% accuracy and 0.008 EER). This observation can guide us to the proper identification time setting to guarantee authentication accuracy without sacrificing identification efficiency.

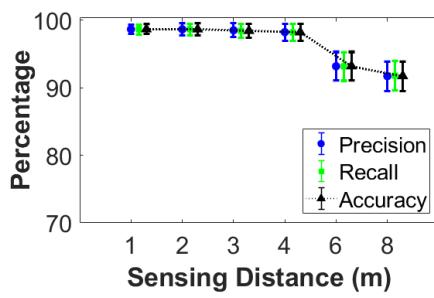


Fig. 14. DroneTrace identification performance under different sensing distances. The performance accuracy maintains well even at the peak sensing range of the mmWave radar.

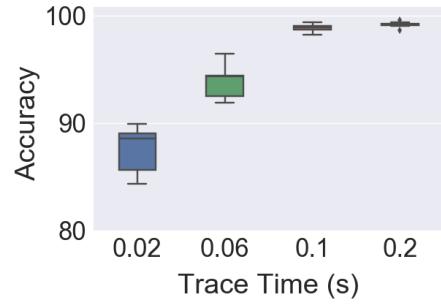


Fig. 15. DroneTrace identification performance under 4 levels of time budgeting. It can achieve 99% accuracy with a fingerprint trace of only 0.1 s.

8.4 Impact of Drone Carriage Load

Some malicious drones can be deployed for cargo transportation, it is important to investigate if the loaded materials will occlude the drone. Thus, we also investigate if loaded objects on the drone surface will influence the performance of DroneTrace. In experiments, we select four types of material (paper, plastic, wood, and leather) and evaluate the identification accuracy with each of them occluding the drone. Each occlusion object is designed to completely cover the drone from radar line of sight, and the thickness is 1 inch, using everyday objects. The performance is shown in Figure 16, where we can see that the overall precision, recall, accuracy, and EER for each are above 98.2%, 98.4%, 98.2% and 0.015, respectively. Specific loads slightly affect the performance to some extent. This is because DroneTrace utilizes the *parasitic response* and, therefore, has a small wavelength and limited penetration ability. In addition, metal blockage didn't fully block signature acquisition, DroneTrace can also withstand aluminum foil covering one side of the drone circuitry as shown in Shield Attack, Sec. 9. As a result, it is prone to scattering reflection upon some specific load. But in general, DroneTrace still provides reliable performance in drone identification.

8.5 Robustness with Ambient Obstacles

When identifying drones in real world environment, there are usually a lot of static obstacles (e.g., buildings, trees, and flashlights) or moving obstacles (e.g., birds and cars) around the probe. It is critical to examine robustness with ambient obstacles. In this evaluation, we consider these obstacles within different complex scenarios involving

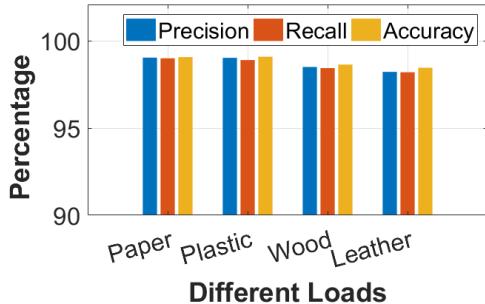


Fig. 16. Performance with the drone carrying different material loads.

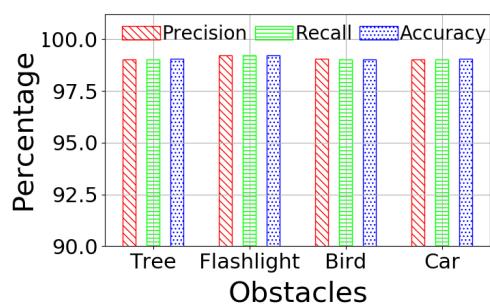


Fig. 17. Performance to identify drones while facing various interference.

various obstacles to examine the performance. Four representative interferences are employed here. We first test drones when flying near the tree and flashlight (both around one meter away) smoothly over the probe. Then we continue to check if our system is robust when remote birds and cars are moving around (both around two meters away). As shown in Figure 17, the accuracy performances keep over 99.01% and can achieve up to 99.02% precision, 99.01% recall, 99.05% accuracy, and 0.008 EER. Due to the high directional beam-forming of mmWave, these surrounding obstacles have little impact on system performance. Generally, DroneTrace still provides reliable performance in drone identification.

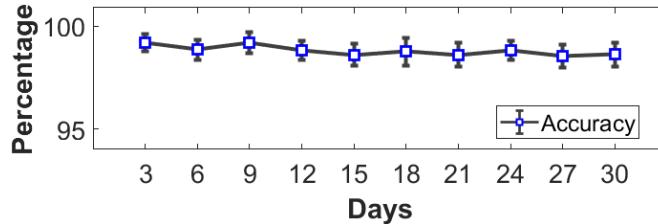


Fig. 18. Performance is stably maintained over a 30-day longitudinal study.

8.6 Longitudinal Study

It is possible that a criminal case is open for weeks before settlement, thus, proving the permanence of DroneTrace for that period is crucial. Our generated dataset includes multiple sessions as part of a longitudinal approach to establishing a baseline comparison of long-term persistence. Ten drones participated in the longitudinal study lasting 30 days, as shown in Figure 18. At the beginning of the study, 36 drones' fingerprints are extracted and stored for later inference. Over the period of 30 days, 100 samples from each of the 36 drone's fingerprint is extracted every three days, and the identification accuracy is calculated based on the average inference accuracy. The accuracy measurement is depicted in Figure 18. Over the 30-day duration, mean values of accuracy measurement are between 98% and 99%, and standard deviations are between 0.72 and 1.71. Thus, we concluded the accuracy has no significant performance decreasing or ascending tendency, which demonstrates DroneTrace is robust against time change (or aging effect).

9 VULNERABILITY ANALYSIS

We examine the DroneTrace's security in following scenarios.

Zero-Informed Attack: In this attack scenario, we assume the attacker has little knowledge or consciousness about the anti-forensic technology. The most straightforward way for the naive attacker is to purchase multiply drones with the same model aiming to bewilder or disturb the investigation. As proven in Section 7.1, we test 13 identical drones, and DroneTrace can precisely identify each drone, which shows such an attack will not succeed.

Disguise and Shield Attack: Assuming the attacker is trying to hide from traditional forensic matching based on testimonies, the attacker will likely change the appearance (e.g., color, cover, propeller length, etc.) of the drone for disguise. However, DroneTrace's signature extraction is based on the intrinsic hardware fingerprinting of the drone, rather than the external geometric shape of the shell, such disguise will serve a null effect with common material, as illustrated in Section 8.4. Furthermore, if the attacker applies a layer of metallic paint or aluminum foil (shown in Figure 19(a)) on the surface of the malicious drone for electromagnetic shielding, the electronic board can be withdrawn from the drone to be separately inspected for true signature, making forensic identification highly accurate regardless of disguise.

Jamming Attack: Considering that attacker is aware about the working range of DroneTrace, it is intuitive to prevent signature extraction (e.g., drone carrying a mmWave jammer shown in Figure 19(b)). However, jamming

device with high amplitude broadband signals are easily recognizable and can be located using RF localization methods [66], which can lead law enforcement agencies for defensive measures [84].

Forgery/Replay Attack: It is also possible that the attacker attempts to forge an innocent drone's signature in order to evade forensic investigation. The most intuitive forgery method is to steal other drones and return drones after the attack. However, such method leaves the attackers' print in the process of burglary and will likely expose attacker's location if the drone uploads its fly path record to the cloud [62]. The next option is to forge a drone's parasitic response captured from innocent drone's signature. One major threat is for the attacker to generate a circuit with equal parasitic values as the innocent drone's circuitry through either hardware or software forgery. It is possible to spoof DroneTrace through forgery by utilizing an advanced reverse engineering manufacturing machine [34], however, millions of dollars of cost make such method infeasible. The attacker may replay imitation signal synthesizing from an innocent drone's parasitic response. To minimize the attack success rate, DroneTrace can implement a randomized binary chirp modulation algorithm, which randomly switches the transmission chirp on or off to serve as the spatial-temporal signature of the probe. Therefore, it is impossible for the attacker to crack the system without knowing the mute chirp information in advance, which implies DroneTrace will not be compromised by such replay attack.

10 DISCUSSION AND LIMITATION

Voluntary Registration Vulnerabilities: The remote ID regulation proposed by FAA has been effective since April 2021 [3], but it is still considered problematic to resist drone threats. (i) Though the remote ID requires drones to be registered, it depends on voluntary action. A criminal will not obey and register drones. (ii) The remote ID does not restrict drones that weigh .55 pounds or less (less than 250 grams) or for recreational flyers [2]. However, various commercial and homemade drones that can be potentially employed weigh .55 pounds or less or can be disguised for recreation [70]. Moreover, similar vulnerabilities can be discovered among the drone regulation of other countries (e.g., Singapore and the UK). Therefore, it is hard for the remote ID to resist these drone threats and aid the forensic investigation as expected.

Malicious Drone Hardware Operations: Drones are often susceptible to physical damages due to operational error that lead to replacement of hardware (e.g., propeller blades, battery, motherboard). Thus, criminals can purposefully alter the hardwares (e.g., damage, replace, reconstruct, hide) after conducting a crime, which may evade DroneTrace's fingerprint matching after forensic team's confiscation. Similar to criminals hiding weapons, drugs, and other illegal physical objects, the forensics team can legally, and reasonably acquire a search warrant

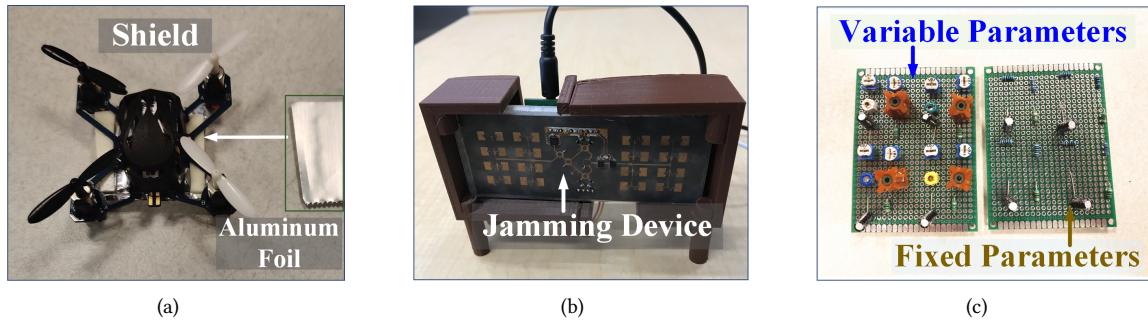


Fig. 19. The experimental setup for (a) a shield attack with aluminum foil, (b) a denial-of-service attack with a jamming device, and (c) a forgery attack to physical circuitry functions.

for the missing parts as long as there is a probable cause [32]. In such cases, the forensics team can also utilize the suspects' actions, words, and behavior for further investigation leveraging traditional forensic methods.

Drone Swarm: Nowadays, drone swarms are often deployed to conduct highly complex tasks, which may challenge drone identification system. Such multiple-drone identification can be solved by employing the existing angle of arrival parsing, source separation, and independent component analysis approaches with the tunable non-linear radar [47, 48].

Probe Cost and Design Analysis: The price of the mmWave radar chip and sensor module is less than \$3 and \$10 respectively on a large scale [6], and will be increasingly scalable. Existing mmWave probes can be effortlessly mounted on hand-held devices, patrol vehicles, and security drones in real-world applications [97], and can be adopted into 5G wireless base stations/hotspots for massive coverage [9]. As a feasibility proof, Soli [52], which is a mini mmWave radar, have been integrated to smartphone devices in commercial devices. In future developments, DroneTrace can be expected to be scaled into smart devices (e.g., smart door bell, smart phone, police car, etc.) for massive coverage. With sensing time being only 0.2 s, malicious drones can be fingerprinted very quickly, faster than having to focus with a camera device. A reasonable sensing distance is 100-200 meters based on mmWave's attenuation pattern over air using commercial devices [100].

Model Confidence Level: The model confidence level mentioned in Section 5.3.1 is a flexible threshold parameter in DroneTrace that allows law enforcement teams to quickly filter out the suspects. When the threshold is set to higher, the model is more confident that the current suspect drone has the same RF fingerprint compared to the drone on crime scene. However, not every fingerprint sample contain every bit of information regarding a drone similar to human fingerprint samples being blurry or incomplete. Thus, we empirically set the threshold to 85% match as a baseline which can be further adjusted to better aid forensics team's decision making process.

DroneTrace for Future Applications: We foresee that digital drone forensics will also supplement solutions toward security and privacy problems brought by autonomous smart mobile devices (e.g., drone, delivery robots, autonomous vehicles). Using a non-contact method for digital forensic will become a necessity in the near future.

Table 1. A Comparison of DroneTrace with existing drone forensic systems. Distance and accuracy is abbreviated.

| System | Sensor | Fingerprint | Compliance | Drone Hardware | Dist. | Accu. | Drone# |
|---------------------|---------------------|-----------------|----------------|---|-------------------|------------|-----------|
| IDrone [80] | Camera | Software | Active | Drone frame (Limited by weather + lighting/clonable) | LOS | 92% | 3 |
| GyrosFinger [85] | On-board memory | Software | Active | Gyroscope log (Limited by memory erasing/formatting) | Contact | 78% | 0 |
| SoundUAV [75] | Microphone | Hardware | Passive | Motor(s) (Limited in loud/noisy environments) | < 1m | 99% | 11 |
| RF Fingerprint [10] | RF receiver | Hardware | Passive | RF Controller (Not unique for each drone) | RF LOS | 99% | 9 |
| DroneTrace | mmWave radar | Hardware | Passive | Electronic Circuit System (Unique and unclonable) | RF LOS | 99% | 36 |

11 RELATED WORK

Digital Drone Forensics: There are two types of identification for digital drone forensics in today's practice, voluntary and passive (i.e. involuntary). Voluntary identification methods include broadcasting an encrypted ID [13, 27, 77, 85], or using camera to examine specific motion sequences [80]. These methods will be avoided by a malicious drone pilot to evade identification, which makes them infeasible for forensic use. On the other hand, passive identifications using cameras and computer vision techniques [28, 87] are limited by weather,

lighting condition, as well as distance with the target drone. In addition, they fail to distinguish drones with physical appearance (e.g., drones with same make/model). Afterwards, the flight log-based methods are believed not reliable that can be fake or altered [8, 81]. Lastly, some work also adopt passive and through side-channel measures, such as electromagnetic interference and acoustic emission [10, 11, 49, 63, 75, 98]). However, these existing measuring solutions either require a contact measure or fail in complex scenarios (e.g., noisy or dark areas) due to the nature of side channels. Therefore, DroneTrace is one of the first few to explore reliable drone identification toward digital drone forensics with our unique and unclonable fingerprinting advantages shown in Table 1.

Hardware Electronics Fingerprinting for Devices: Investigating a hardware trait (e.g., process variation) as a fingerprint has been a historical topic in the security. Many works explored physical properties in integrated chips and electro-mechanical devices for identification applications [7, 29, 50, 92]. However, most require contact access, which is not applicable in drone identification scenarios. Besides, radio frequency (RF) fingerprinting is also explored for physical-layer identification [17, 22, 23, 33]. However, these solutions rely on the broadcasting network and are dependent on specific commercial communication media (e.g., antenna), which still require active cooperation.

mmWave Object Sensing: mmWave has been utilized for various sensing purposes. There are two main mmWave sensing schemes. First, mmWave radars have been studied in a variety of domains (e.g., cardio-respiratory measurements and gesture sensing [42, 53, 54, 61]) based on the detection of a target's motion. These mmWave sensing works mainly rely on analyzing the Doppler effect of moving objects. Second, there are some object detection and imaging applications to explore object inner properties, even "through-wall" [35, 56, 71, 73, 96, 99, 101]. These techniques focus on target's external mmWave modulation properties (e.g., geometric reflection or scattering coefficient). [51] explored the possibility of identifying the presence of electronics through-wall, yet incapable of distinguishing identical electronics circuitry. However, both schemes cannot sense the intrinsic passive fingerprint of the toward forensic use. Therefore, DroneTrace is the first to propose mmWave sensing technology to explore the *parasitic response* for digital drone forensics.

12 CONCLUSION

With the increasing availability and usability of commodity drones, there is an exponential rise in drone threats. In this paper, we proposed a reliable digital forensics system DroneTrace for passive drone identification. We first investigated drones' parasitic response from parasitic elements in drones' electronic systems using RF stimulation. Then, we employed a portable mmWave probe to acquire the *parasitic response* and proposed a robust protocol and framework for drone identification. Furthermore, extensive experiments imply that DroneTrace can achieve 99.02% accuracy in 0.1s sensing time. These research findings are essential for understanding this new digital forensic approach and raising attention to security and privacy issues caused by drones.

ACKNOWLEDGMENTS

We thank all anonymous reviewers for their insightful comments on this paper. This work was partially based upon work supported by the National Science Foundation under Grants #2028872 and #2050910.

REFERENCES

- [1] 2021. *Global Drone Service Market Report 2019*. <https://markets.businessinsider.com/news/stocks/global-drone-service-market-report-2019-market-is-expected-to-grow-from-usd-4-4-billion-in-2018-to-usd-63-6-billion-by-2025-at-a-cagr-of-55-9-1028147695>. Accessed: 2021-04-20.
- [2] Federal Aviation Administration. 2021. Register Your Drone. (20 April 2021). https://www.faa.gov/uas/getting_started/register_drone/
- [3] Federal Aviation Administration. 2021. UAS Remote Identification Overview. (20 April 2021). https://www.faa.gov/uas/getting_starte/d/remote_id/

- [4] Advisory and Rulemaking Committees. 2017. UAS Identification and Tracking ARC Recommendation Final Report. (30 Sept 2017). https://www.faa.gov/regulations_policies/rulemaking/committees/documents/index.cfm/document/information/documentID/3302
- [5] Arafat Al-Dhaqm, Richard A Ikuesan, Victor R Kebande, Shukor Razak, and Fahad M Ghabban. 2021. Research Challenges and Opportunities in Drone Forensics Models. *Electronics* 10, 13 (2021), 1519.
- [6] Amazon.com. 2018. Akozon CDM324 24GHz 15m Radar Induction Single Channel Microwave Sensor Module. https://www.amazon.com/Akozon-CDM324-Induction-Channel-Microwave/dp/B07FMQ37L7/ref=sxbs_sxwds_stvp?. Accessed: 2021-02-18.
- [7] Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, Francois-Xavier Standaert, and Christian Wachsmann. 2011. A formalization of the security features of physical functions. In *2011 IEEE Symposium on Security and Privacy*. IEEE, 397–412.
- [8] S Atkinson, G Carr, C Shaw, and Shahrad Zargari. 2021. Drone Forensics: The Impact and Challenges. In *Digital Forensic Investigation of Internet of Things (IoT) Devices*. Springer, 65–124.
- [9] Carlos Baquero Barneto, Sahan Damith Liyanaarachchi, Taneli Riihonen, Lauri Anttila, and Mikko Valkama. 2020. Multibeam design for joint communication and sensing in 5G New Radio networks. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.
- [10] Sanjoy Basak, Sreeraj Rajendran, Sofie Pollin, and Bart Scheers. 2021. Drone classification from RF fingerprints using deep residual nets. In *2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)*. IEEE, 548–555.
- [11] Andrea Bernardini, Federica Mangiatordi, Emiliano Pallotti, and Licia Capodiferro. 2017. Drone detection by acoustic signature identification. *Electronic Imaging* 2017 (01 2017), 60–64. <https://doi.org/10.2352/ISSN.2470-1173.2017.10.IMAWM-168>
- [12] Simon Birnbach, Richard Baker, and Ivan Martinovic. 2017. Wi-fly?: Detecting privacy invasion attacks by consumer drones. (2017).
- [13] Igor Bisio, Chiara Garibotto, Fabio Lavagetto, Andrea Sciarrone, and Sandro Zappatore. 2018. Unauthorized amateur UAV detection based on WiFi statistical fingerprint analysis. *IEEE Communications Magazine* 56, 4 (2018), 106–111.
- [14] Bitcraze. Accessed: 2021-2-2. *Crazyflie 2.0*. <https://www.bitcraze.io/crazyflie-2/>.
- [15] Ruud M Bolle, Jonathan H Connell, Sharath Pankanti, Nalini K Ratha, and Andrew W Senior. 2013. *Guide to biometrics*. Springer Science & Business Media.
- [16] Vladimir Britanak. 2011. A survey of efficient MDCT implementations in MP3 audio coding standard: Retrospective and state-of-the-art. *Signal Processing* 91, 4 (2011), 624–672.
- [17] William E Cobb, Eric W Garcia, Michael A Temple, Rusty O Baldwin, and Yong C Kim. 2010. Physical layer identification of embedded devices using RF-DNA fingerprinting. In *2010-MILCOM 2010 Military Communications Conference*. IEEE, 2168–2173.
- [18] Anthony P Colombo, Yan Zhou, Kirill Prozument, Stephen L Coy, and Robert W Field. 2013. Chirped-pulse millimeter-wave spectroscopy: Spectrum, dynamics, and manipulation of Rydberg–Rydberg transitions. *The Journal of chemical physics* 138, 1 (2013), 014301.
- [19] Federal Communications Commission. Accessed: 2021-04-01. *Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems*. <https://docs.fcc.gov/public/attachments/DOC-366222A1.pdf>.
- [20] Intel Corp. Accessed: 2021-1-27. INTEL AERO READY TO FLY DRONE. <https://www.intel.com/content/www/us/en/products/drones/aero-ready-to-fly.html>.
- [21] Julia Crawford. 2021. 10 Crimes Committed Using A Drone. (23 April 2021). <https://listverse.com/2018/07/26/10-crimes-committed-using-a-drone/>
- [22] Boris Danev, Heinrich Luecken, Srdjan Capkun, and Karim El Defrawy. 2010. Attacks on physical-layer identification. In *Proceedings of the third ACM conference on Wireless network security*. ACM, 89–98.
- [23] Boris Danev, Davide Zanetti, and Srdjan Capkun. 2012. On physical-layer identification of wireless devices. *ACM Computing Surveys (CSUR)* 45, 1 (2012), 6.
- [24] Dedrone. Accessed: 2020-12-9. *Detect Localize Drone Swarms*. <https://www.dedrone.com/>.
- [25] Bertrand Denis, Jean Côté, and René Laprise. 2002. Spectral decomposition of two-dimensional atmospheric fields on limited-area domains using the discrete cosine transform (DCT). *Monthly Weather Review* 130, 7 (2002), 1812–1829.
- [26] Konstantin Dragomiretskiy and Dominique Zosso. 2013. Variational mode decomposition. *IEEE transactions on signal processing* 62, 3 (2013), 531–544.
- [27] Martins Ezuma, Fatih Erden, Chethan Kumar Anjinappa, Ozgur Ozdemir, and Ismail Guvenc. 2019. Micro-UAV detection and classification from RF fingerprints using machine learning techniques. In *2019 IEEE Aerospace Conference*. IEEE, 1–13.
- [28] Foite.ch. 2015. LightCense – A low-altitude identification system for UASs. (2015).
- [29] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. 2002. Silicon physical random functions. In *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 148–160.
- [30] Khaled M Gharaibeh. 2011. *Nonlinear distortion in wireless systems: Modeling and simulation with MATLAB*. John Wiley & Sons.
- [31] Bernd Girod, Rudolf Rabenstein, and Alexander Stenger. 2001. *Signals and systems*. John Wiley & Sons Incorporated.
- [32] Abraham S Goldstein. 1987. The Search Warrant, the Magistrate, and Judicial Review. *NYUL Rev* 62 (1987), 1173.
- [33] Kenny C Gross, Ramakrishna C Dhanekula, and Andrew J Lewis. 2011. Detecting counterfeit electronic components using EMI telemetric fingerprints. US Patent 8,069,490.

- [34] JY Group. Accessed: 2021-2-9. *PCB Clone-Make The Same PCB without Files*. <http://www.jycircuitboard.com/news/pcb-clone-make-the-same-pcb-without-files-52.html>.
- [35] Junfeng Guan, Sohrab Madani, Suraj Jog, Saurabh Gupta, and Haitham Hassanieh. 2020. Through Fog High-Resolution Imaging Using Millimeter Wave Radar. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*.
- [36] Andreas Hartman. 2019. *Electromagnetic Modeling with Complex Dielectrics A Partial Element Equivalent Circuit Approach*. Ph. D. Dissertation. Lulea University of Technology.
- [37] Jerry L Hintze and Ray D Nelson. 1998. Violin plots: a box plot-density trace synergism. *The American Statistician* 52, 2 (1998), 181–184.
- [38] Graeme Horsman. 2016. Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digital Investigation* 16 (2016), 1–11.
- [39] Jun Huang, Zhe Li, Bor Yann Liaw, and Jianbo Zhang. 2016. Graphical analysis of electrochemical impedance spectroscopy data in Bode and Nyquist representations. *Journal of Power Sources* 309 (2016), 82–98.
- [40] Amazon Inc. Accessed: 2021-1-21. *Parrot Bebop Quadcopter Drone - Blue*. https://www.amazon.com/Parrot-Bebop-Quadcopter-Drone-Blue/dp/B01N6XJJL6/ref=sr_1_17?ie=UTF8&qid=1550165428&sr=8-17.
- [41] Amazon Inc. Accessed: 2021-1-24. *Parrot AR.Drone 2.0 Elite Edition Quadcopter*. <https://www.amazon.com/Parrot-AR-Drone-2-0-Elite-Quadcopter/dp/B00FS7SU7K?th=1>.
- [42] Chengkun Jiang, Junchen Guo, Yuan He, Meng Jin, Shuai Li, and Yunhao Liu. 2020. mmVib: micrometer-level vibration measurement with mmwave radar. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. 1–13.
- [43] Kyle J. Johnston. 2021. Mugged By A Drone | SHORT. <https://www.youtube.com/watch?v=nuDUB93mSqs>. Accessed: 2021-04-23.
- [44] Yasir Karisan, Cosan Caglayan, Georgios C Trichopoulos, and Kubilay Sertel. 2016. Lumped-element equivalent-circuit modeling of millimeter-wave HEMT parasitics through full-wave electromagnetic analysis. *IEEE Trans. Microw. Theory Techn* 64, 5 (2016), 1419–1430.
- [45] Won-Bae Kwon, Chung Ghiu Lee, Dongjun Seo, and Chang-Soo Park. 2018. Tunable Photonic Microwave Band-pass Filter with High-resolution Using XGM Effect of an RSOA. *Current Optics and Photonics* 2, 6 (2018), 563–567.
- [46] Sam LaGrone. 2021. U.S. Navy Says Explosive Drone Attack Killed Two on Merchant Tanker. <https://news.usni.org/2021/07/31/u-s-navy-says-explosive-drone-attack-killed-two-on-merchant-tanker>
- [47] Changzhi Li, Zhengyu Peng, Tien-Yu Huang, Tenglong Fan, Fu-Kang Wang, Tzyy-Sheng Horng, José-María Muñoz-Ferreras, Roberto Gómez-García, Lixin Ran, and Jianshan Lin. 2017. A review on recent progress of portable short-range noncontact microwave radar systems. *IEEE Transactions on Microwave Theory and Techniques* 65, 5 (2017), 1692–1706.
- [48] Changzhi Li, Xiaogang Yu, Chien-Ming Lee, Dong Li, Lixin Ran, and Jianshan Lin. 2010. High-Sensitivity Software-Configurable 5.8-GHz Radar Sensor Receiver Chip in 0.13- μ m CMOS for Noncontact Vital Sign Detection. *IEEE Transactions on Microwave Theory and Techniques* 58, 5 (2010), 1410–1419.
- [49] Hualiang Li, Garrett Johnson, Maverick Jennings, and Yingfei Dong. 2017. Drone profiling through wireless fingerprinting. In *2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*. IEEE, 858–863.
- [50] Zhengxiong Li, Aditya Singh Rathore, Chen Song, Sheng Wei, Yanzhi Wang, and Wenyao Xu. 2018. PrinTracker: Fingerprinting 3D Printers using Commodity Scanners. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1306–1323.
- [51] Zhengxiong Li, Zhuolin Yang, Chen Song, Changzhi Li, Zhengyu Peng, and Wenyao Xu. 2018. E-Eye: Hidden Electronics Recognition through mmWave Nonlinear Effects. In *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*. ACM, 68–81.
- [52] Jaime Lien, Nicholas Gillian, M Emre Karagozler, Patrick Amihood, Carsten Schwesig, Erik Olson, Hakim Raja, and Ivan Poupyrev. 2016. Soli: Ubiquitous gesture sensing with millimeter wave radar. *ACM Transactions on Graphics (TOG)* 35, 4 (2016), 142.
- [53] Jaime Lien, Nicholas Gillian, M. Emre Karagozler, Patrick Amihood, Carsten Schwesig, Erik Olson, Hakim Raja, and Ivan Poupyrev. 2016. Soli: Ubiquitous Gesture Sensing with Millimeter Wave Radar. *ACM Trans. Graph.* 35, 4, Article 142 (July 2016), 19 pages. <https://doi.org/10.1145/2897824.2925953>
- [54] Feng Lin, Chen Song, Yan Zhuang, Wenyao Xu, Changzhi Li, and Kui Ren. 2017. Cardiac Scan: A Non-contact and Continuous Heart-based User Authentication System. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (Snowbird, Utah, USA) (MobiCom '17)*. ACM, New York, NY, USA, 315–328.
- [55] Joseph K Liu and Ron Steinfeld. 2016. *Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings*. Vol. 9723. Springer.
- [56] Chris Xiaoxuan Lu, Muhamad Risqi U Saputra, Peijun Zhao, Yasin Almalioogl, Pedro PB de Gusmao, Changhao Chen, Ke Sun, Niki Trigoni, and Andrew Markham. 2020. milliEgo: single-chip mmWave radar aided egomotion estimation via deep sensor fusion. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems (SenSys)*.
- [57] Yunfei Ma, Nicholas Selby, and Fadel Adib. 2017. Drone relays for battery-free networks. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*. ACM, 335–347.
- [58] Roel Maes. 2013. Physically Unclonable Functions: Properties. In *Physically Unclonable Functions*. Springer, 49–80.
- [59] Uday Maji and Saurabh Pal. 2016. Empirical mode decomposition vs. variational mode decomposition on ECG signal processing: a comparative study. In *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE,

- 1129–1134.
- [60] John Newsome Michael Martinez and Rene Marsh. 2015. Handgun-firing drone appears legal in video, but FAA, police probe further. <https://edition.cnn.com/2015/07/21/us/gun-drone-connecticut/index.html/>
 - [61] I. V. Mikhelson, S. Bakhtiari, T. W. Elmer II, and A. V. Sahakian. 2011. Remote Sensing of Heart Rate and Patterns of Respiration on a Stationary Subject Using 94-GHz Millimeter-Wave Interferometry. *IEEE Transactions on Biomedical Engineering* 58, 6 (June 2011), 1671–1677. <https://doi.org/10.1109/TBME.2011.2111371>
 - [62] Dinh-Dung Nguyen. 2021. Cloud-Based Drone Management System in Smart Cities. *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead* (2021), 211–230.
 - [63] Phuc Nguyen, Vimal Kakaraparthi, Nam Bui, Nikshep Umamahesh, Nhat Pham, Hoang Truong, Yeswanth Gudde, Dinesh Bharadia, Richard Han, Eric Frew, et al. 2020. DroneScale: drone load estimation via remote passive RF sensing. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. 326–339.
 - [64] Phuc Nguyen, Hoang Truong, Mahesh Ravindranathan, Anh Nguyen, Richard Han, and Tam Vu. 2017. Matthan: Drone Presence Detection by Identifying Physical Signatures in the Drone’s RF Communication. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 211–224.
 - [65] Martin Oberholzer, Marc Östreich, Heinz Christen, and Marcel Brühlmann. 1996. Methods in quantitative image analysis. *Histochemistry and cell biology* 105, 5 (1996), 333–355.
 - [66] Konstantinos Pelechrinis, Iordanis Koutsopoulos, Ioannis Broustis, and Srikanth V Krishnamurthy. 2009. Lightweight jammer localization in wireless networks: System design and implementation. In *GLOBECOM 2009-2009 IEEE Global Telecommunications Conference*. IEEE, 1–6.
 - [67] Zhengyu Peng, José-Maria Muñoz-Ferreras, Roberto Gómez-García, Lixin Ran, and Changzhi Li. 2016. 24-GHz biomedical radar on flexible substrate for ISAR imaging. In *Wireless Symposium (IWS), 2016 IEEE MTT-S International*. IEEE, 1–4.
 - [68] Zhengyu Peng, Lixin Ran, and Changzhi Li. 2015. A 24-GHz low-cost continuous beam steering phased array for indoor smart radar. In *2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 1–4.
 - [69] Adam C Polak and Dennis L Goeckel. 2011. RF fingerprinting of users who actively mask their identities with artificial distortion. In *Signals, Systems and Computers (ASILOMAR), 2011 Conference Record of the Forty Fifth Asilomar Conference on*. IEEE, 270–274.
 - [70] Mario Poljak. 2021. *15 Best Drones Under 250 Grams (0.55 Pounds) in 2021*. <https://www.dronetechplanet.com/15-best-drones-under-250-grams-0-55-pounds-in-2020/> Accessed: 2021-04-23.
 - [71] Akarsh Prabhakara, Vaibhav Singh, Swarun Kumar, and Anthony Rowe. 2020. Osprey: a mmWave approach to tire wear sensing. In *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*. 28–41.
 - [72] John G Proakis. 2001. *Digital signal processing: principles algorithms and applications*. Pearson Education India.
 - [73] Kun Qian, Zhaoyuan He, and Xinyu Zhang. 2020. 3D point cloud generation with millimeter-wave radar. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 4 (2020), 1–23.
 - [74] Khurram Yasin Qureshi and Shoab A Khan. 2009. Effectiveness of assigning confidence levels to classifiers and a novel feature in fingerprint matching. In *2009 IEEE International Conference on Systems, Man and Cybernetics*. IEEE, 2181–2186.
 - [75] Soundarya Ramesh, Thomas Pathier, and Jun Han. 2019. SoundUAV: Towards Delivery Drone Authentication via Acoustic Noise Fingerprinting. In *Proceedings of the 5th Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*. ACM, 27–32.
 - [76] K Ramamohan Rao and Ping Yip. 2014. *Discrete cosine transform: algorithms, advantages, applications*. Academic press.
 - [77] ARC Recommendations Final Report. 2017. UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC). (2017).
 - [78] Mark A Richards. 2014. *Fundamentals of radar signal processing*. McGraw-Hill Education.
 - [79] Matthew Ritchie, Francesco Fioranelli, Hugh Griffiths, and Borge Torvik. 2015. Micro-drone RCS analysis. In *Radar Conference, 2015 IEEE*. IEEE, 452–456.
 - [80] Carlos Ruiz, Shijia Pan, Adeola Bannis, Xinlei Chen, Carlee Joe-Wong, Hae Young Noh, and Pei Zhang. 2018. IDrone: Robust Drone Identification through Motion Actuation Feedback. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (2018), 80.
 - [81] Fahad E Salamh, Mohammad Meraj Mirza, and Umit Karabiyik. 2021. UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies. *Electronics* 10, 6 (2021), 733.
 - [82] Sajid Saleem, Fazli Subhan, Noman Naseer, Abdul Bais, and Ammara Imtiaz. 2020. Forensic speaker recognition: A new method based on extracting accent and language information from short utterances. *Forensic Science International: Digital Investigation* 34 (2020), 300982.
 - [83] John Semmlow. 2017. *Circuits, Signals and Systems for Bioengineers: A MATLAB-based Introduction*. Academic Press.
 - [84] Xiufang Shi, Chaoqun Yang, Weige Xie, Chao Liang, Zhiguo Shi, and Jiming Chen. 2018. Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges. *IEEE Communications Magazine* 56, 4 (2018), 68–74.
 - [85] Yunmok Son, Juhwan Noh, Jaeyeong Choi, and Yongdae Kim. 2018. GyroFinger: Fingerprinting Drones for Location Tracking Based on the Outputs of MEMS Gyroscopes. *ACM Transactions on Privacy and Security (TOPS)* 21, 2 (2018), 10.
 - [86] Google Play Store. Accessed: 2021-2-1. *Speed Gun Mph*. <https://play.google.com/store/apps/details?id=zyra.kayle>.

- [87] Yue Sun. 2012. Modeling, identification and control of a quad-rotor drone using low-resolution sensing. (2012).
- [88] Mingxing Tan and Quoc Le. 2019. Efficientnet: Rethinking model scaling for convolutional neural networks. In *International Conference on Machine Learning*. PMLR, 6105–6114.
- [89] Mingxing Tan and Quoc V Le. 2021. EfficientNetV2: Smaller Models and Faster Training. *arXiv preprint arXiv:2104.00298* (2021).
- [90] Peter Lane Taylor. Accessed: 2020-6-1. Could ‘Pandemic Drones’ Help Slow Coronavirus? Probably Not—But COVID-19 Is A Boom For Business. <https://www.forbes.com/sites/petertaylor/2020/04/25/could-pandemic-drones-help-slow-coronavirus-probably-not-but-covid-19-is-a-boom-for-business/#3f57068762a4>.
- [91] Christopher Torrence and Gilbert P Compo. 1998. A practical guide to wavelet analysis. *Bulletin of the American Meteorological society* 79, 1 (1998), 61–78.
- [92] Ingrid Verbauwhede and Roel Maes. 2011. Physically unclonable functions: manufacturing variability as an unclonable device identifier. In *Proceedings of the 21st edition of the great lakes symposium on Great lakes symposium on VLSI*. ACM, 455–460.
- [93] Wenhao Wang, Zhi Sun, Kui Ren, and Bocheng Zhu. 2016. User capacity of wireless physical-layer identification: An information-theoretic perspective. In *Communications (ICC), 2016 IEEE International Conference on*. IEEE, 1–6.
- [94] Xiaolei Wang, Qin Zhang, and Shuangcheng Zhang. 2018. Water levels measured with SNR using wavelet decomposition and Lomb-Scargle periodogram. *GPS Solutions* 22, 1 (2018), 22.
- [95] Zhou Wang, Alan C Bovik, Hamid R Sheikh, Eero P Simoncelli, et al. 2004. Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing* 13, 4 (2004), 600–612.
- [96] Teng Wei and Xinyu Zhang. 2015. mtrack: High-precision passive tracking using millimeter wave radios. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 117–129.
- [97] Qingqing Wu, Jie Xu, Yong Zeng, Derrick Wing Kwan Ng, Naofal Al-Dhahir, Robert Schober, and A Lee Swindlehurst. 2020. 5G-and-Beyond Networks with UAVs: From Communications to Sensing and Intelligence. *arXiv preprint arXiv:2010.09317* (2020).
- [98] Chengtao Xu, Bowen Chen, Yongxin Liu, Fengyu He, and Houbing Song. 2020. Rf fingerprint measurement for detecting multiple amateur drones based on stft and feature reduction. In *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*. IEEE, 4G1–1.
- [99] Hongfei Xue, Yan Ju, Chenglin Miao, Yijiang Wang, Shiyang Wang, Aidong Zhang, and Lu Su. 2021. mmMesh: towards 3D real-time dynamic human mesh construction using millimeter-wave. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. 269–282.
- [100] Zhenliang Zhang, Jung Ryu, Sundar Subramanian, and Ashwin Sampath. 2015. Coverage and channel characteristics of millimeter wave band using ray tracing. In *2015 IEEE International Conference on Communications (ICC)*. IEEE, 1380–1385.
- [101] Yanzi Zhu, Yibo Zhu, Ben Y Zhao, and Haitao Zheng. 2015. Reusing 60ghz radios for mobile radar imaging. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 103–116.
- [102] Nurul Huda Nik Zulkipli, Ahmed Alenezi, and Gary B Wills. 2017. IoT forensic: bridging the challenges in digital forensic and the internet of things. In *International Conference on Internet of Things, Big Data and Security*, Vol. 2. SCITEPRESS, 315–324.