E-Eye: Hidden Electronics Recognition through mmWave Nonlinear Effects

Zhengxiong Li[1], Zhuolin Yang[1], Chen Song[1], Changzhi Li[2], Zhengyu Peng[3], Wenyao Xu[1]
[1] CSE Department, SUNY University at Buffalo, Buffalo, NY, USA
[2] ECE Department, Texas Tech University, Lubbock, TX, USA
[3] Aptiv Corporation, Kokomo, IN, USA
Email: [1]{zhengxio, zhuoliny, csong5, wenyaoxu}@buffalo.edu
[2]{changzhi.li}@ttu.edu, [3]{zpeng.me}@gmail.com

ABSTRACT

While malicious attacks on electronic devices (e-devices) have become commonplace, the use of e-devices themselves for malicious attacks has increased (*e.g.*, explosives and eavesdropping). Modern e-devices (*e.g.*, spy cameras, bugs or concealed weapons) can be sealed in parcels/boxes, hidden under clothing or disguised with cardboard to conceal their identities (named as hidden e-devices hereafter), which brings challenges in security screening. Inspection equipment (*e.g.*, X-ray machines) is bulky and expensive. Moreover, screening reliability still rests on human performance, and the throughput in security screening of passengers and luggages is very limited. To this end, we propose to develop a low-cost and practical hidden e-device recognition technique to enable efficient screenings for threats of hidden electronic devices in daily life. First, we investigate and model the characteristics of *nonlinear* effects, a special passive response of electronic devices under millimeter-wave (mmWave) sensing. Based on this theory and our preliminary experiments, we design and implement, *E-Eye*, an end-to-end portable hidden electronics recognition system. *E-Eye* comprises a low-cost (*i.e.*, under $100), portable (*i.e.*, 11.8cm by 4.5cm by 1.8cm) and lightweight (*i.e.*, 45.5g) 24GHz mmWave probe and a smartphone-based e-device recognizer. To validate the *E-Eye* performance, we conduct experiments with 46 commodity electronic devices under 39 distinct categories. Results show that *E-Eye* can recognize hidden electronic devices in parcels/boxes with an accuracy of more than 99% and has an equal error rate (EER) approaching 0.44% under a controlled lab setup. Moreover, we evaluate the reliability, robustness and performance variation of *E-Eye* under various real-world circumstances, and *E-Eye* can still achieve accuracy over 97%. Intensive evaluation indicates that *E-Eye* is a promising solution for hidden electronics recognition in daily life.

CCS CONCEPTS

• **Security and privacy → Security in hardware**;

KEYWORDS

Wireless Sensing; Pattern Recognition; Hardware Security.

ACM Reference Format:
Zhengxiong Li[1], Zhuolin Yang[1], Chen Song[1], Changzhi Li[2], Zhengyu Peng[3], Wenyao Xu[1] [1] CSE Department, SUNY University at Buffalo, Buffalo, NY, USA [2] ECE Department, Texas Tech University, Lubbock, TX, USA [3] Aptiv Corporation, Kokomo, IN, USA Email: [1]{zhengxio, zhuoliny, csong5, wenyaoxu}@buffalo.edu [2]{changzhi.li}@ttu.edu, [3]{zpeng.me}@gmail.com . 2018. *E-Eye*: Hidden Electronics Recognition through mmWave Nonlinear Effects. In *The 16th ACM Conference on Embedded Networked Sensor Systems (SenSys '18), November 4–7, 2018, Shenzhen, China.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3274783.3274833

SenSys '18, November 4–7, 2018, Shenzhen, China

ACM ISBN 978-1-4503-5952-8/18/11…$15.00
https://doi.org/10.1145/3274783.3274833

1 INTRODUCTION

Hidden electronic devices (hereafter, e-devices) bring both security and privacy threats in our daily life. For instance, explosion tragedies continuously occur due to the ineffective detection of remote-controlled disguised bombs [1, 3, 7, 14], which can be triggered by electronic initiators. Apart from these life-threatening hazards, e-devices (*e.g.*, smartphones and spy camera) can also be used for eavesdropping, cheating in private zones [13] or accessing other areas that restrict electronics [4, 15, 16]. The fact that these e-devices (hereafter, hidden e-devices) can be sealed in parcels or boxes, hidden insides in clothing and disguised in appearance increases the risk that they can easily pass undetected through security check points.

Entry security check is the current method for defending against malicious, hidden e-devices requiring an X-ray machine [58] at safety-critical sites (*e.g.*, airports and embassy offices). Unfortunately, their expensive cost and poor portability make it an infeasible solution against the proliferation and the deployment of portable e-devices [45]. Moreover, the radiation emitted from X-rays is harmful to workers and persons passing through the checkpoints. Other scanning methods based on metal scanners can only detect the existence of the e-device rather than recognize the specific type directly (see Sec. 9.1). Conventional computer vision methods cannot be applied because the camera can not see through containers or bodies. Thermal imaging also fails because it only can detect the temperature of the hidden e-device [39], which can be easily interfered with by other heat sources. As a result, how to recognize hidden e-devices in a cost-efficient, user-friendly and non-invasive manner remains an unsolved challenge for public security and privacy.

Recently, there is a rising trend of applying radio-frequency signals, such as millimeter wave (mmWave [10]), in sensing and

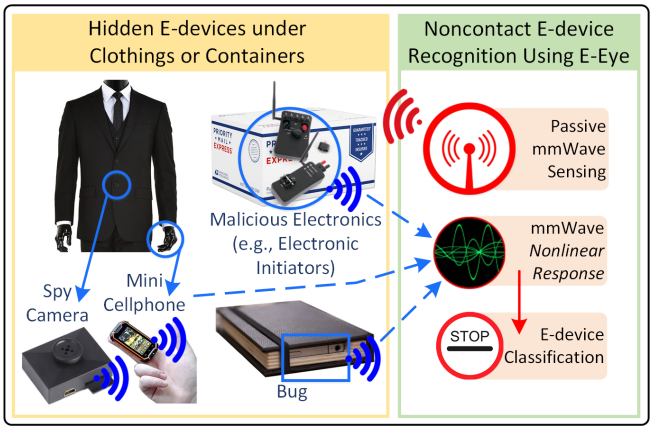


Figure 1: Examples of hidden electronics in different malicious applications. The proposed *E-Eye* system can detect and recognize hidden electronic devices under different circumstances in real world.

tracking applications, because mmWave can penetrate obstacles and "image" hidden objects due to its highly-directional beamforming and strong reflection properties on objects [64]. For example, Adib *et al.* studied the possibility of sensing human occurrence and vitals through WiFi signals [17]. Zhu *et al.* developed a 60GHz mmWave imager for object detection and classification [66]. Wei *et al.* designed mTrack, a mmWave instrument for precision object tracking [64]. However, existing works mainly target either human or non-electronic object detection and tracking. The capability of accurately recognizing hidden electronic devices through mmWave sensing is unknown.

To this end, we propose our system, *E-Eye*, to facilitate hidden e-device recognition in public security inspections. Its features are (1) **cost-efficient**: the cost of the solution is affordable in daily life for large scale deployment; (2) **portable**: it is easy to use in the inspection of different containers (*e.g.*, delivery boxes, check-in luggages or even human body) and various environments (*e.g.*, postal offices, airports or factories); (3) **non-invasive**: it can avoid the obtrusive (even illegal) opening of the container in real practice which sacrifices efficiency and may cause privacy issues.

The foundation of *E-Eye* rests on the *nonlinear response* effect from electronic circuits when probed by the mmWave. The intrinsic difference in circuits' hardware characteristics (*e.g.*, a circuits' components and circuit layout) generates a distinct nonlinear response, which can serve as the identity of a certain e-device brand. This way, we enable a novel sensing modality for non-invasive and cost-effective hidden e-devices recognition based on the mmWave field. Specifically, we design and prototype a portable ($11.8cm \times 4.5cm \times 1.8cm$) and light-weight ($45.4g$) 24GHz mmWave probe device which is enabled to probe the mmWave and capture the returned *nonlinear responses*. We address the challenges in noise-isolation and coherence to achieve high-quality signal with low complexity and cost (less than US $100). Afterwards, the signal is transferred to the smartphone and we propose the wavelet-based analysis module taking into consideration the unavoidable variance in the signal's scaling and magnitude in practical usage. Eventually, we develop a fine-tuned support vector machine (SVM) classifier for robust recognition under various conditions. In the experiment, we employ 46 e-devices and the comprehensive results show that *E-Eye* can accurately recognize each e-device brand under different scenarios.

Our contributions are summarized as follows:

- We propose a novel form of recognizing hidden e-devices by exploring the *nonlinear response* effect of mmWave of e-devices. We find that the circuit inside an e-device acts as a passive signal modulator which reflects back radio frequency (RF) signals with intrinsic identity information.
- We develop *E-Eye*, an end-to-end system to facilitate the low-cost, non-invasive and robust hidden electronics recognition. We prototype the sensing hardware and implement the recognition algorithm for efficient and effective classification.
- We evaluate *E-Eye* under different sensing time efficiencies, sensing distances, and device orientations; *E-Eye* achieves more than 99% recognition rate. Moreover, a field study and a threat model study are deployed for evaluating the robustness of *E-Eye* under the impact of ambient environment, alien device, combined e-devices, and various cover materials. In both studies, the system obtains over 97% accuracy.

2 MMWAVE NONLINEAR EFFECT: NEW CONCEPT AND PRELIMINARIES

2.1 Concept: Radio-Frequency Response of E-devices

There are usually two following forms of radio frequency (RF) response when probing a continuous wave (CW) with the transmit frequency f_0 towards a target.

Linear Effects: The main carrier frequency of the received signal is the same as that of the transmitted signal. The phase change in the linearly demodulated signals is related to the geometrical information, such as object distance, shape and size [42]. However, these linear effects do not reflect the material properties and we need to seek other information in the application of e-device detection and recognition.

Nonlinear Effects: Besides the main carrier frequency, the received signal wave is also modulated with a set of the sub-carrier frequencies with more side lobes in the spectrum. These sub-carrier frequencies are generated due to the nonlinear properties of the target (*e.g.*, material reflection efficiency) [48, 49]. In the remaining part of this section, we provide an in-depth analysis of non-linear effects in recognizing electronics.

Nonlinear Effects from E-device: As shown in Figure 2, when the e-device enters the RF beam field, chips, connectors and metal traces of printed circuit board (PCB) on an e-device are viewed as an array of antennas in the resolution of mmWave, and these antenna with inductance (L), capacitance (C) and resistance (R) act as a passive processor and manipulates the transmit mmwave signals. More specifically, antennas can conduct and transform the mmWave signal to a high-frequency current along the conductors between the electronic components within the device [38]. The components (*e.g.*, a diode) or parasitic parameters (*e.g.*, a parasitic

circuit) on the PCB modulate the response signal and generate the nonlinear distortion [33], formulated as Equation (1):

$$r(t) = m(z(t), \hat{a}(t)) \otimes h_f(t), \quad (1)$$

where $z(t)$ is the response signal, $m(\cdot, \hat{a}(t))$ is the nonlinear modulation function of the PCB, $\hat{a}(t)$ is the complex power-series for the nonlinear system, $\otimes$ stands for convolution computing and $h_f(t)$ is the ideal bandpass filter function for the carrier bandwidth [26, 27]. After the modulated signal radiate from the e-device, they would be captured by the probe receive (Rx) antenna. Thus, this *nonlinear response* of the e-device contains rich information of its physical characteristic and holds the potential to serve as the device's identity.

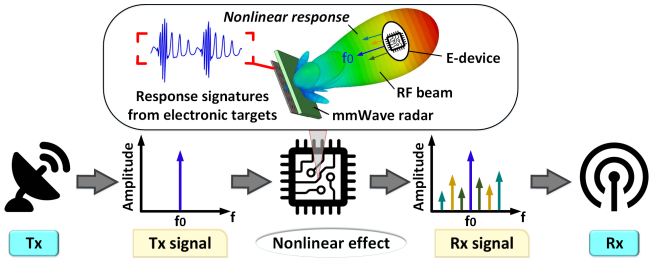


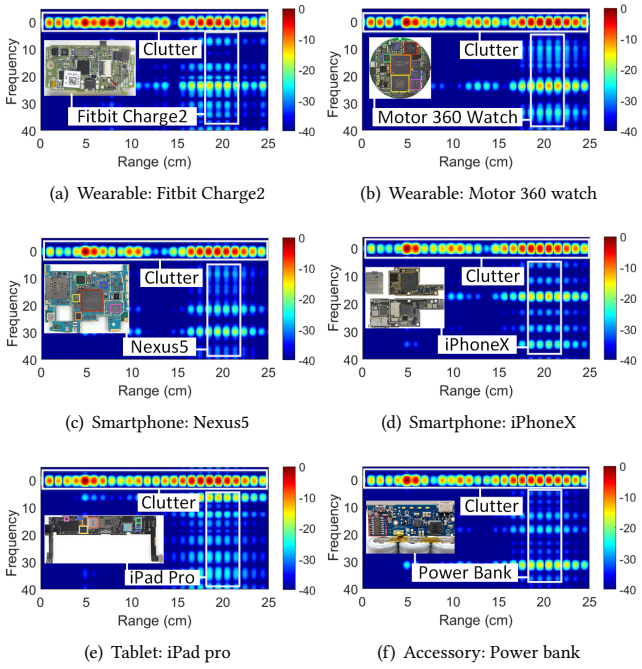
Figure 2: The e-device generates a *nonlinear response* signature under the RF beam. The response is determined by its intrinsic physical characteristics.

2.2 A Preliminary Study: mmWave Nonlinear Effects from Electronic Circuits

Carrier Frequency Selection: Selecting a transmit frequency (and consequently a receive frequency) requires all of the typical trade-offs associated with longer versus shorter wavelengths for radar, which include availability of components (*e.g.*, amplifiers and filters), realization of an acceptable gain for the antennas to achieve a sufficient signal-to-noise ratio (SNR) and exploitation of the radar cross-section (RCS) associated with a particular set of targets [28, 46].

If it is assumed, as a very rough approximation [41], that the length of a typical trace along a PCB is $l = 3mm$ on the High-frequency high-speed circuits (illustrated in Figure 3), and the effective dielectric constant of the board is close to $\varepsilon = 4$, the traces along the board become half-wave resonant dipoles ($l = \frac{\lambda}{2}$) at a frequency of $f_0 = \frac{c}{\sqrt{\varepsilon}\lambda} = \frac{3{\cdot}10^8 m/s}{\sqrt{4}{\cdot}2{\cdot}0.003m} \approx$24GHz, where c is the propagation speed of a radar wave in air. Thus, it is reasonable to expect that, for nonlinear effect, the radar will transmit frequencies in or near Super high frequency band, range from 3GHz to 30GHz [8, 52]. Considering the technology for 24GHz radar is significantly mature and 24GHz is unrestricted in the industrial scientific medical (ISM) band [2], we apply the 24GHz as the transmit frequency, which is loosely known as mmWave.

Owing to different product design goals and the circuit IP protection, the circuits in different e-device brands are different. Thus, the amplitude, frequency and phase of the *nonlinear responses* are different among different e-devices. Therefore, it is possible to design a mmWave probe to force e-devices to radiate the *nonlinear response* signature that reflects their unique properties and can be used for recognition.



(a) Wearable: Fitbit Charge2 (b) Wearable: Motor 360 watch

(c) Smartphone: Nexus5 (d) Smartphone: iPhoneX

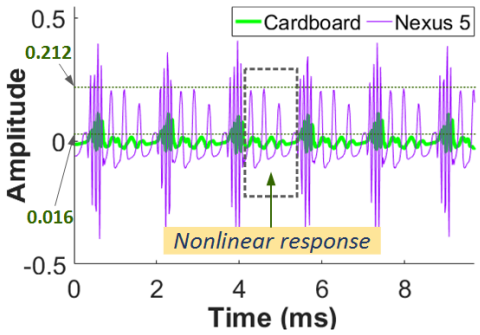
(e) Tablet: iPad pro (f) Accessory: Power bank

Figure 3: Six different e-devices present different *nonlinear responses* (the spectrums in the white box are distinct in frequency and amplitude) when forced by the same mmWave probe. The main circuit board of each e-device is displayed on the left.

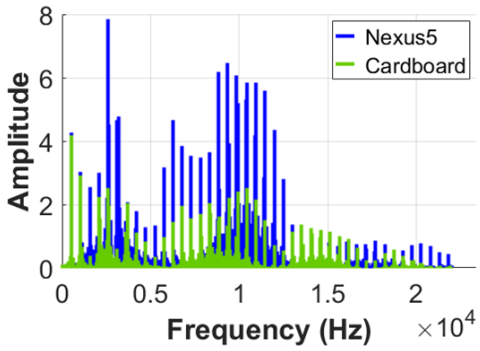
Proof-of-concept: Six different e-device types from four different representative device categories are stimulated with the mmWave probe fixed 20cm in distance from the devices. The main circuit board of each e-device is attached on the left. These circuits are different from aspects of the size, the components and layout. As shown in Figure 3, the x-axis is the sensing range, the y-axis is the frequency of the received signal and the color bar represents the amplitude of the signal. The varied sub-carrier frequencies can be clearly observed that their *nonlinear responses* are significantly distinct at the frequency, amplitude and phase, which matches Section 2.1. Given the huge amount of electric units integrated on the control board, parasitic variations have sufficient space to be served as powerful resources for device recognition.

A Study on Package Effects: In real-world applications, electronics can be placed inside the container or covered by different materials. As a result, we need to investigate whether the hidden materials will generate *nonlinear responses* or have a nonlinear effect [54]. It is proved in Figure 4(a) that within the area of the *nonlinear response*, there is little demodulated signal amplitude for cardboard (less than 0.016V, ambient noise and thermal noise actually), while for Nexus 5, the demodulated *nonlinear response* signal is quite visible (more than 0.212V, 13.5× larger than cardboard's) (more detailed analysis about the *nonlinear response* in Section 5). In Figure 4(b), we

can observe their signal spectrum are significantly different, which proves the feasibility of unobtrusive hidden e-device recognition.



(a) The detected *nonlinear response* from the cardboard and Nexus 5.



(b) The significant difference of two responses in spectrum.

Figure 4: The cardboard's *nonlinear responses* are negligible when compared to Nexus 5's, indicating the feasibility of hidden e-device recognition.

2.3 Practical Challenges

There are two technical challenges in our system design:

Low-cost and portable sensing modality: There are significant challenges in fulfilling such mmWave probe, especially in RF front-end, antenna, signal processing and manufacture craft parts. Moreover, to make the mmWave probe low-cost and compact with the portable size and excellent flexibility is arduous.

Effective and robust recognition: Taking into account the ambient noise, unavoidable variance in signal's scaling as well as diverse intervention sources, it is not easy to accurately and efficiently discriminate the *nonlinear responses* from different e-devices in a limited time.

3 *E-EYE*: HIDDEN E-DEVICE RECOGNITION SYSTEM

We propose *E-Eye*, a portable, non-invasive and robust system to facilitate recognition of the hidden e-devices. Typically, we consider the real world practice where the inspector conducts the on-site inspection of the object for forbidden e-devices that may be contained in it. The end-to-end system overview is shown in Figure 5.

***E-Eye* Hardware:** A new mmWave probe with the smartphone is designed to remotely and robustly acquire the e-device's *nonlinear response* for recognition. Specifically, the probe transmits the continuous wave and process/demodulate the reflected signal. After that, the kilobyte (KB) size data is sent to smartphone for recognition via the line-in audio card converter [6].

***E-Eye* Software:** Once receiving the data, the e-device recognition module first performs the preprocessing and demodulation to filter the interference and noise. Then, it extracts the effective features from the *nonlinear responses* via wavelet-based analysis. After that, a fine-tuned classification algorithm is developed to recognize the e-device type. The result will eventually be displayed on the smartphone to the inspector.

4 A PORTABLE AND COST-EFFECTIVE MMWAVE PROBE DESIGN

In this section, we introduce the hardware design of *E-Eye*, which is capable of transmitting the 24GHz carrier signal and capturing the returned *nonlinear responses*.

4.1 Hardware Architecture

The schematic of the proposed mmWave probe is shown in Figure 6. It consists of a radio frequency board and a baseband board. The RF board includes a pair of array antennas (i.e., Tx and Rx), a voltage controlled oscillator (VCO), a pair of low noise amplifiers (LNA) and a six-port structure. The baseband board contains baseband amplifiers (BA) and an on-board sawtooth voltage generator (SVG).

4.1.1 Six-port Structure. A six-port circuit is a simple structure, as a quadrature mixer, to down-convert RF signal into baseband, avoiding the use of expensive integrated mixer chips [60]. The six-port structure consists of three quadrature couplers and one rat-race coupler. Ports 1 and 2 of the six-port structure are the inputs for the local oscillator (LO) drive and the RF signal respectively. Four Schottky diodes are connected at ports 3, 4, 5 and 6. Ports 3 are 4 are for the I-channel differential baseband signal, and ports 5 and 6 are for the Q-channel differential baseband signal.

4.1.2 Coherence. Coherence is one of the most important requirements for the mmWave probe to obtain the effective information of the e-device [41, 63]. Opposite to sharing the synchronous clocks at the signal generation and acquisition stages, which increases the complexity and cost of the system [47], in *E-Eye*, the coherence property of the mmWave probe is obtained by simultaneously sampling the reference signal and the baseband signal (see Section 5.1.2). In order to control the VCO, the reference signal is phase locked to the sawtooth voltage signal. In the synchronization procedure, the phase of each beat-signal period is aligned in the digital domain after sampling the reference signal and the baseband signal. Thus, in this method, the synchronous clocks are not demanded to share between the generation and acquisition stages, which simplifies the hardware.

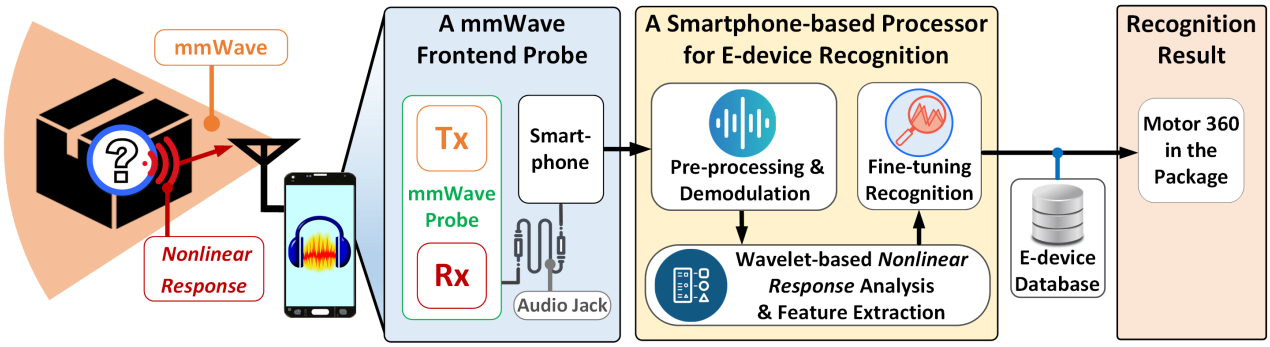


Figure 5: The system overview for *E-Eye* to non-invasively recognize the e-device hidden in the container. It comprises of a mmWave sensing module in the front-end and an e-device recognition module in the back-end.

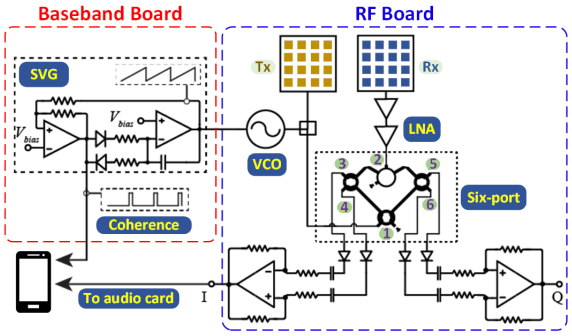


Figure 6: The hardware schematic for the cost-effective and portable 24GHz mmWave probe.

4.2 System Integration Design

4.2.1 System Parameters Consideration. Parameters in the mmWave probe design are significant and should be carefully selected. There are three key factors that determine the performance of the mmWave probe, detection range, range resolution and the maximum non-ambiguous wireless signal velocity as follows: $R_d = \frac{cf_sT}{4B}$, $\Delta_R = \frac{c}{2B}$ and $v_{max} = \frac{c}{4f_cT}$, where c is the speed of the light, f_s is the sampling frequency on the baseband board and f_c is the center frequency, which is 24GHz. A larger detection range R_d requires a longer frequency ramp repetition period T and smaller transmitted bandwidth B. However, the higher range resolution Δ_R requires the wider bandwidth B. At the same time, the faster non-ambiguous wireless signal velocity v_{max} requires the shorter T. Thus there exists a trade-off between the bandwidth and the frequency ramp repetition period in the *E-Eye* system design.

4.2.2 System Integration. The Federal Communications Commission (FCC) in the United States proposed that new flexible service among the 24GHz band is roughly in the 24-24.45GHz band [22]. Also, the wider bandwidth of the probe means more cost for the probe hardware. Thus, in *E-Eye*, the bandwidth of the transmitted signal (B) is $450MHz$ with a center frequency (f_c) of 24GHz, and the transmitted average power is around $8dBm$. The frequency ramp repetition period (T) is $6.45ms$. The sampling frequency on the baseband board (f_s) is $192KHz$. In addition, an operational-amplifier-based SVG is employed to generate the sawtooth voltage to tune the free running VCO. The frequency of the sawtooth signal and the reference signal is $155Hz$.

5 E-DEVICE RECOGNITION

E-Eye listens to the *nonlinear response* reflected from the e-device and extracts unique identity from it. We first propose preprocessing and demodulation to extract the effective *nonlinear response* $y(t)$. Then, considering that $y(t)$ is irregular and asymmetric, we employ the wavelet decomposition to obtain the statistical features representing the device inner characteristics. In the end, a fine-tuning classifier is designed.

5.1 *Nonlinear Response* Preprocessing and Demodulation

5.1.1 Signal Preprocessing. As depicted in Figure 7, the data sensed by the mmWave probe is forwarded through the audio channel as two-channel signals. After parsing the audio signal, we get the baseband signal and the reference signal respectively. The reference signal is usually mixed with high frequencies from ambient noise and thermal noise. Thereby, we employ a filter to remove these components. However, filtering the reference signal of synchronous clock shape is difficult, which requires smoothing the shape and preserving the sharp edge at the same time. Specifically, we apply a Savizky-Golay and median combined filter [20]. Savitzky-Golay filter mainly fits successive sub-sets of adjacent data points with a low-degree polynomial by the method of linear least squares. Although it is more effective at preserving the sharp edge for the pertinent high frequency components in the signal, it is less effective in noise filtering. Thus, the median filter is combined as it runs through the signal entry by entry, replacing each entry with the median of neighboring entries to remove the high frequency noise.

5.1.2 Signal Demodulation. As shown in Figure 8(a), we observe the reference signal has an edge effect on the baseband signal, making some parts distorted. Therefore, we utilize the reference signal to extract the effective parts in the baseband signal. First, we define that a *cycle* is the interval wave between the falling and rising

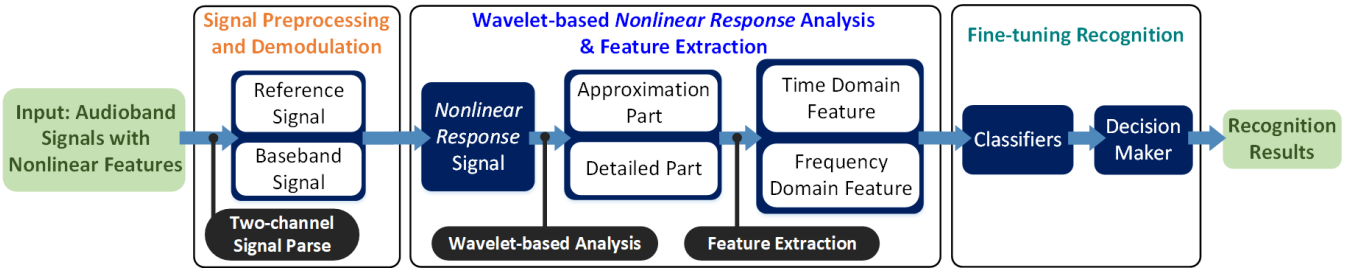


Figure 7: The flowchart of e-device recognition module, including three parts signal preprocessing and demodulation, wavelet-based *nonlinear response* analysis & feature extraction and fine-tuning recognition.

edges of two adjacent pulses in the reference signal (see Figure 8(b)). Specifically, we use the falling and rising edges detection method to locate each *cycle* [50]. With the *cycle* information, we demodulate and extract the effective parts in the baseband signal based on the synchronized time. As a result, we obtain the effective *nonlinear response* signal consisting of N consecutive *cycles* in Figure 8(c). Intuitively, the signal with more *cycles* will contain more unique physical characteristics of the e-device and thereby achieve better recognition accuracy. However, it also increases the computation overhead. To balance this trade-off, we empirically choose $N = 5$ and the corresponding original baseband signal has the length within $0.013s$ (we will investigate the performance of E-Eye with different N setups in Section 7.1.2).

5.2 Wavelet-based *Nonlinear Response* Analysis and Feature Extraction

Given the *nonlinear response* signal, we find it is hard to classify them directly using the similarity distance because *nonlinear responses* have a large variation in magnitudes as well as frequencies, which leads to irregularity and asymmetry. Therefore, we present the wavelet-based analysis which is resilient to the scale and magnitude variation.

5.2.1 Wavelet-based Nonlinear Response Analysis. Wavelet transform (WT) is an effective multi-resolution analysis tool for signal decomposition [29, 40]. The WT approach can overcome the shortcoming of Fourier analysis, which only works in the frequency domain, not in the time domain [34]. The signal can be decomposed into many groups of coefficients in different scales with WT through different scaled versions. After removing the DC component, $y(t)$ becomes a signal with zero-mean and some variance and satisfies the following condition: $\int_{-\infty}^{\infty} f(t)dt = 0$, which indicates $y(t)$ is a waveform. WT uses $\psi_{a,b}$ and $\phi_{a,b}$, where $\phi_{a,b} = \frac{1}{\sqrt{a}}\phi(\frac{t-b}{a})$ and $\psi_{a,b} = \frac{1}{\sqrt{a}}\psi(\frac{t-b}{a})$, as the mother wavelet function that satisfies the condition of dynamic scaling and shifting, where a and b are the scale and translation parameters accordingly [55]. In order to get high and low-frequency signal properties separately, the wavelet-based analysis is achieved as Equation (2):

$$\underbrace{y(t)}_{\text{Nonlinear response}} = \underbrace{\frac{1}{C_\phi}\int_{-\infty}^{\infty} F_W(a_0,b)\phi_{a_0,b}\frac{db}{\sqrt{a_0}}}_{\text{The approximation part}} + \underbrace{\frac{1}{C_\psi}\int_{a_1}^{\infty}\int_{-\infty}^{\infty} F_W(a,b)\psi_{a,b}\frac{da}{a^2}\frac{db}{\sqrt{a}}}_{\text{The detail part}}, \tag{2}$$

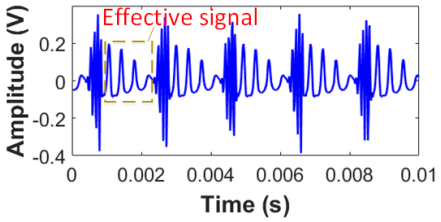
where $F_W(a_0,b)$ and $F_W(a,b)$ are the coefficients.

For the inverse transform to exist, we require that the analyzing wavelet satisfies the admissibility condition, given in the following: $C_\phi = 2\pi\int_{-\infty}^{\infty}\frac{|\hat{\phi}(\omega)|^2}{\omega}d\omega < \infty$ and $C_\psi = 2\pi\int_{-\infty}^{\infty}\frac{|\hat{\psi}(\omega)|^2}{\omega}d\omega < \infty$, where $\hat{\phi}(\omega)$ and $\hat{\psi}(\omega)$ are the Fourier transform of $\phi(t)$ and $\psi(t)$ respectively. Also, C_ϕ and C_ψ are constants for corresponding wavelets. Subsequently, we get the approximation signal as shown in Figure 9(a) and the detail signal in Figure 9(b). Finally, for comprehensive characterization of the *nonlinear response*, we also get the spectral approximation and detail signals by Fast Fourier Transform (FFT) for further feature extraction.

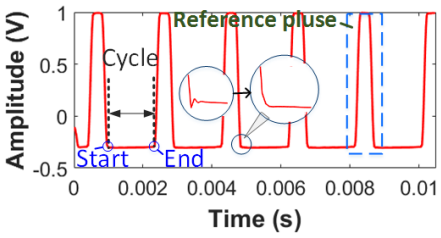
5.2.2 Spatial-temporal Domain Feature Extraction. As the above mentioned, the *nonlinear response* contains the unique identity of the device. As a result, we exploit the internal traits in the *nonlinear response* signal by extracting extract 13 scalar features in spatial-temporal domains. The feature names and descriptions are listed in Table 1 and 2. These features represent the *nonlinear response* signal shape from different aspects [19]. For example, *skewness* is a scale of symmetry to judge if a distribution looks the same to the left and right of the center point, *kurtosis* is to estimate whether the data are heavy-tailed or light-tailed relative to a normal distribution and *flatness* describes the degree to which they approximate the Euclidean space of the same dimensionality (marked with * in Table 1 and 2). Thus, in total, a feature vector containing these 26 features from the approximation and detail parts is formed.

5.3 Fine-tuning Recognition

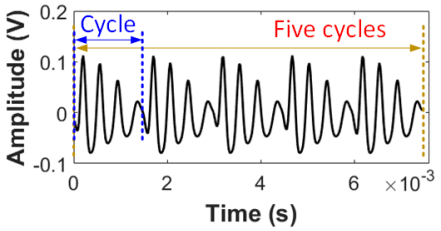
Electronics recognition can be treated as a classification problem. *E-Eye* uses supervised learning to classify e-device types, beginning with a training phase followed by testing, as illustrated in **Algorithm 1**. However, it is possible that some e-devices (known as alien devices) are not included in the database before, which may spoof the check or cause false alarms. Therefore, to overcome



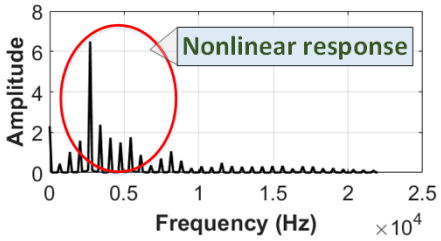
(a) The baseband signal parsed from the audio signal.



(b) The preprocessed reference signal.



(c) The *nonlinear response* signal after the signal demodulation.

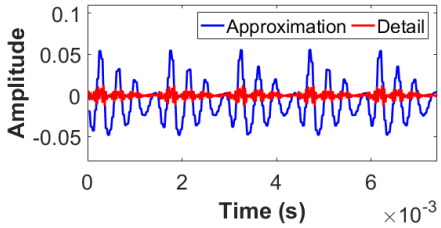


(d) The spectrum for the *nonlinear response* signal.

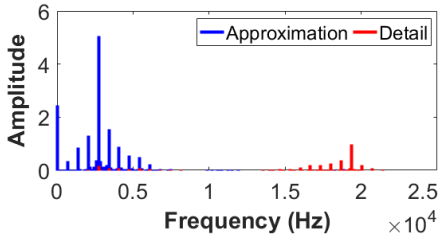
Figure 8: A Nexus 5 smartphone is sensed within a USPS box at 20cm distance using the portable 24GHz mmWave probe. We preprocess and demodulate the raw sensing signal to extract the *nonlinear response*.

this problem, we design the **Classifier** and the **Decision maker** to output the final recognition result.

During the training of the **Classifier**, n traces of *nonlinear response* signals from each e-device type are collected. For m e-device types in the database (namely, m pre-registered classes), $n \times m$ feature vectors are used to train the classifier altogether. In *E-Eye*, we employ SVM. The Gaussian radial basis function is selected as the kernel function to map the original data to a higher dimensional space [56]. During the testing phase, *E-Eye* collects a trace, extracts a feature vector, and inputs to the SVM model. The SVM model



(a) The approximation and detail parts of the Nexus 5 *nonlinear response* signal.



(b) The spectrum for the approximation and detail parts of the Nexus 5 *nonlinear response* signal.

Figure 9: The first level wavelet decomposition result of Nexus 5 *nonlinear response*. (a) and (b) represent its low and high frequency information respectively.

Table 1: List of Time Domain Features.

Name	Description
Mean Value	$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x(i)$
Standard Deviation	$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x(i)-\bar{x})^2}$
* Skewness	$\gamma = \frac{1}{N}\sum_{i=1}^{N}(\frac{x(i)-\bar{x}}{\sigma})^3$
* Kurtosis	$\beta = \frac{1}{N}\sum_{i=1}^{N}(\frac{x(i)-\bar{x}}{\sigma})^4 - 3$
RMS Amplitude	$\lambda = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x(i))^2}$
Lowest Value	$l = \min_{i=1}^{N} x(i)$
Highest Value	$h = \max_{i=1}^{N} x(i)$

Table 2: List of Frequency Domain Features.

Name	Description
Mean Value	$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y(i)$
Standard Deviation	$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(y(i)-\bar{y})^2}$
* Skewness	$\gamma = \frac{1}{N}\sum_{i=1}^{N}\frac{y(i)-\bar{y}}{\sigma}^3$
* Kurtosis	$\beta = \frac{1}{N}\sum_{i=1}^{N}\frac{y(i)-\bar{y}}{\sigma}^4 - 3$
Crest Factor	$\varepsilon = 20\log(\frac{\max_{i=1}^{N}\lvert y(i)\rvert}{\sigma})$
* Flatness	$F_s = (\prod_{i=1}^{N} y_{m(i)})^{\frac{1}{N}} / ((\sum_{i=1}^{N} y_{m(i)})/N)$

generates the probability set of classifying this test trace into each pre-trained class.

In the **Decision maker**, we define the maximum probability as the classification score. To distinguish an alien device, a threshold

Algorithm 1: Fine-tuning Recognition

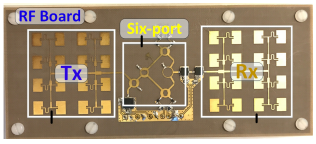
Input: $Q(n)$: n test nonlinear response traces from an e-device
Output: R: the predicted result

$E_i, S, R \leftarrow 0$;
Initialize T;
%Classifier:
for $i \in \{1, \ldots, n\}$ **do**
    $E(i) = Cls(Q(i))$;
    ▷ `Classify` m `traces`
%Decision maker:
$S = Tun(E)$;
▷ `Make the classification score`
if $S < T$ **then**
    return 'Alien!';
else
    $R = Rec(E)$;
    ▷ `Decide the final predicted result` **return** R;

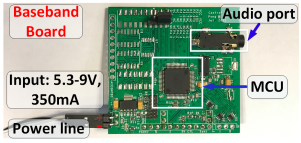
is applied: If the classification score is less than the threshold, the trace will be declared as an alien device with a second manual check; if not, the predicted type with the maximum probability will be regarded as the recognition result. In *E-Eye*, we select the threshold as 0.9 empirically.

6 SYSTEM PROTOTYPE AND EVALUATION

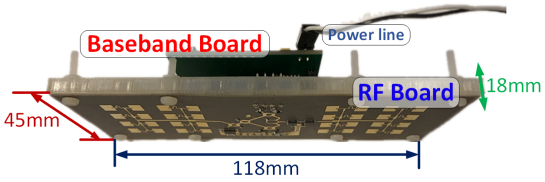
6.1 *E-Eye* System Implementation and Integration



(a) RF board.



(b) Baseband board.



(c) The integrated mmWave probe with two boards.

Figure 10: The design of 24GHz mmWave front-end probe comprises two parts, i.e., (a) a radio-frequency Tx/Rx board and (b) a down-frequency baseband board. E-Eye probe integration is shown in (c).

The prototype of the proposed mmWave probe is shown in Figure 10. The flexible RF board is based on a 0.245mm (0.0096in) thick substrate Rogers RT/duroid 5880 (Figure 10(a)). The rigid baseband board is fabricated on an FR4 substrate, which includes the SVG

Figure 11: Commodity electronic devices in our study.

and the baseband amplifiers (Figure 10(b)). The Microprocessor Control Unit (MCU) is MSP430F2610, a widely used ultra low-power controller unit [5]. The baseband signals are fed to a 3.5mm audio jack directly supported by embedded MCU inner driver, which naturally has two channels for the reference signal and baseband signal without the extra need of the analog-to-digital converter or expensive communication chips. It can be easily connected to the audio interface of a smartphone or a tablet for signal processing.

The mmWave probe is 11.8cm (4.65in) × 4.5cm (4.65in) × 1.5cm (0.59in) and weights only 45.4g, which is lightweight for ease of adoption in security inspections. Moreover, it costs within 100 U.S. dollars. Figure 10(c) illustrates the integrated proposed mmWave probe. It typically has a 8dBm transmit power with a 3.7-5V supply voltage and a 350mA maximum operating current under the 1.2W DC power consumption. The carrier frequency used in this work is 24GHz. To enhance the directivity, a pair of 4×4 antenna arrays are designed, offering an antenna directivity of 19.8dBi. The received RF gain and baseband gain are 34dB and 26dB, respectively.

6.2 Evaluation

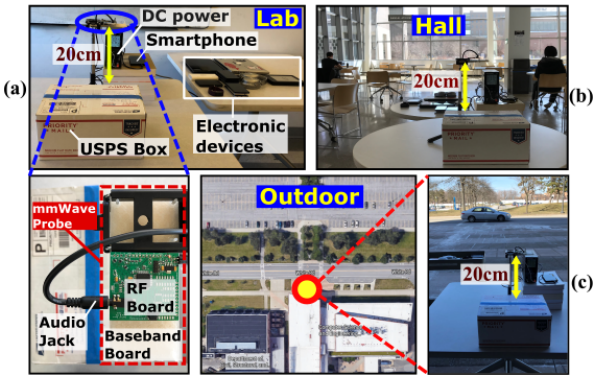


Figure 12: The setup for the evaluation: (a) in a controlled lab environment, (b) in an open hall at the first floor of the building, and (c) at the entrance of an outdoor public parking lot.

Experiment Preparation: As shown in Table 3, we select 46 common e-devices and label them into 39 classes as we collect four duplicate Nexus 5 and three duplicate Uno R3. We also group them into seven categories based on their functions for ease of description. The corresponding circuit sizes range from 0.42in (diagonal)

Table 3: E-devices employed during experiments.

#	Device Category	Specific Device Brand
1	Laptop	Lenovo Xiaoxin310, Macbook Air, Asus LN4200, Macbook Pro, Mac mini
2	Tablet	iPad Pro, Asus ZenPad 3S, Nexus 10
3	Smart-phone	Nexus 5*4, iPhone 6s, iPhone 6, iPhone X*2, iPhone 7plus, LG Leon, Nexus4, Smartisan T1*2, Jianguo Pro2, iPhone 4s, HTC One M8, Samsung S7
4	Wearable	Motor 360, Apple watch3, Fitbit Charge2, Mi band2
5	Mouse	Logitech M510, Rapoo 7200P, Dell MS111
6	Head-phone	Bose QuietComfort 35, Status Audio CB-1, Air Pods
7	Others	Auduino Uno R3*3, iPhone Charger, Empty Box1, Empty Box2, Philips Sonicare 2 Series, Philips Norelco PQ208, Toshiba Canvio Basics, Kindle Paperwhite, Pisen power bank

to 13.3in (diagonal). Without loss of generality, we employ two common containers to conceal the e-devices: a USPS package box (marked as Box1) and an Amazon package box (named as Box2).

Data Collection: During the experiment, the mmWave probe is placed 20cm from the container (see Figure 12). We record its initial position as 0° orientation in the horizontal plane. In every test trail, we conceal an e-device in one particular box and switch it on (if possible). We collect 10s sensing data with 44.1K sampling rate. In Section 5.1.2, we define one trace as the subsegment in the sensing data with the length of 0.013s (13ms), which contains $N = 5$ consecutive *cycles*. Eventually, we will randomly extract 100 traces for each device with regard to one container.

Data Partition: Unless specified, each time we randomly choose 70 out of 100 traces from each device as our training set and use the rest for testing. Thus, 3220 traces are used for training and 1380 traces are used for testing. Specifically, a 10-fold cross validation method is employed in classification. It is worth mentioning that we conduct other types of cross validation experiments in Section 7.2 and 7.3 to examine the system performance under real-world environments.

Evaluation Metrics: We use accuracy, precision and recall as the performance metrics for evaluation [44]. Besides, we also adopt the Equal Error Rate (EER) and the Receiver Operating Characteristic (ROC). The lower the EER, the better the system performance [18].

7 PERFORMANCE EVALUATION

We evaluate the performance of *E-Eye* from three aspects:

- The control study validates the system under the ideal environmental condition, which proves the legitimacy of our system design.
- The field study considers the variation of system parameters in the practical usage and gives insights to how to achieve the best performance.
- The threat study exploits the vulnerability of the system from the attacker's perspective by examining more extreme conditions.

These three strategies serve different roles, which are complementary to each other.

7.1 *E-Eye* Control Study

7.1.1 Recognition Performance. We evaluate the ability of *E-Eye* to recognize the different e-devices in the optimal lab environment. First, we exploit the overall performance based on the training and testing data sensed from Box1 and Box2 respectively (denoted as Scheme1 and Scheme2). Then, we further apply the testing data from Box2 upon the training data from Box1 to study the system's universality (denoted as Scheme3). For each scheme, we make a comparison between two commonly used classifiers, SVM and KNN [61], to determine which classifier is more suitable.

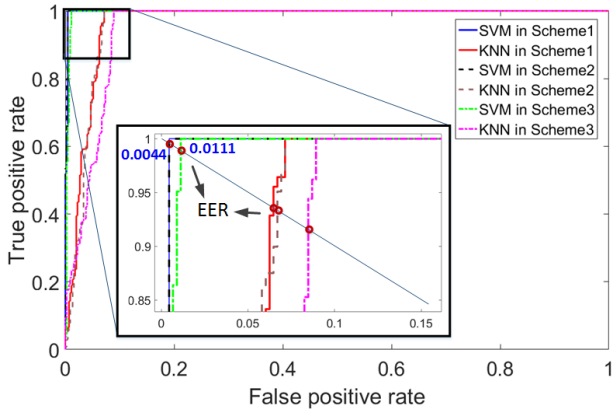


Figure 13: The overall performance of *E-Eye* with two different classification configurations.

The ROC results are shown in Figure 13. SVM achieves the EER of 0.0044, 0.0045 and 0.0111 respectively in three schemes. Correspondingly, KNN achieves the EER of 0.0647, 0.0669 and 0.0848 respectively. Both classifiers have excellent performance, which implies that the feature vector effectively reflects the unique *nonlinear response* characteristics in each e-device. The comparatively low EER in scheme3 indicates that our trained classifier does not have the over-fitting issue and can adapt to various usage scenarios.

Moreover, we conduct the McNemar test to determine if there is a significant difference in two classifiers [24]. McNemar test is a frequently used test for matched-pair data, with a significance level of $\alpha = 0.05$. Under the null hypothesis, the two classifiers have no significant difference. If the null hypothesis is rejected, the p value is below 0.05. In our test, the p value maintains around 0.01, which is less than 0.05 and thereby rejects the null hypothesis. Based on the above analysis, we prove that SVM has the better classifier and will employ SVM in the following evaluation unless otherwise specified. In conclusion, our results demonstrate that a hidden e-device can be precisely recognized by *E-Eye*.

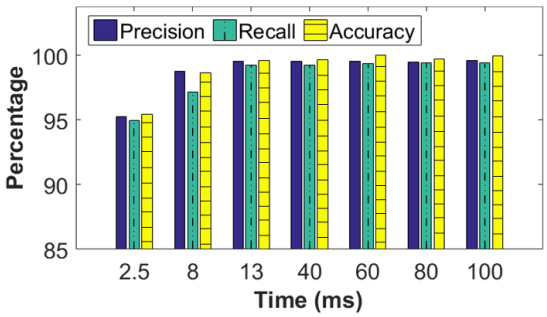


Figure 14: Recognition performance with seven different screening times.

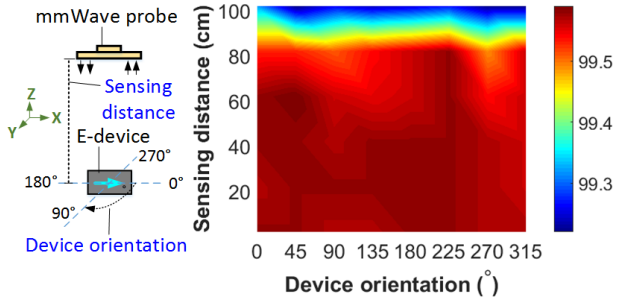


Figure 15: Measurement accuracy under different sensing distances.

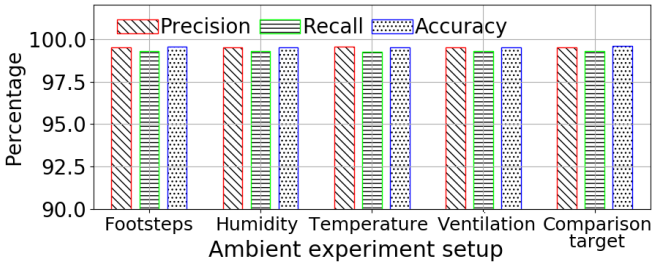


Figure 16: *E-Eye* recognition performance in different experiment setups.

7.1.2 Screening Time Efficiency. In public security, e-device screening tasks are challenging due to the limited time budgeted for efficiency. As a result, we are interested in analyzing the performance of *E-Eye* with regard to different time budgets. Specifically, considering that 2.5*ms* audio segment usually represents one *cycle*, we manually select seven different time settings between 2.5*ms* to 100*ms*. For each time setting, we follow the same methodology described in Section 6.2 and re-prepare the training and testing set. Figure 14 shows the performance results. For the lowest budget of 2.5*ms*, *E-Eye* only obtains 95.25% precision, 94.95% recall and 95.47% accuracy. These results are because the contained one *cycle* cannot comprehensively represent the characteristics of the e-device. After increasing the time, the performance gradually increases. Generally, we find a turning point at 13*ms* where the performance saturates afterwards (reaching 99.61% precision, 99.41% recall and 99.68% accuracy at 100*ms*). This observation can guide us to the proper screening time setting to guarantee recognition accuracy without sacrificing screening efficiency.

7.1.3 Impact of Sensing Distance and Device Orientation. In practical scenarios, the inspector should be able to walk around with *E-Eye* according to different container shapes and inspection environments to accelerate inspection progress. Such a convenient practice, however, will lead to the changing distance and orientation between the hidden e-device and the mmWave probe. Therefore, it is important to investigate whether these aspects will affect system performance. Specifically, we measure the different device orientations (from 0° to 315°) at different distances (from 2*cm* to 100*cm*). The results are shown in Figure 15. The average recognition accuracy over 46 devices remains high when the sensing distance varies within 80*cm* (above 99.5%). As for the orientation, although the reflected signal slightly changes due to the different probe angles for each e-device, the inter-device distinguishability among 46 devices is significant such that each device can be correctly recognized. Thereby, *E-Eye* can facilitate portable and convenient public screening in real practice.

7.2 Field Study

7.2.1 Robustness to Ambient Environment. The ambient environment can introduce random noises or even interfere with the probe hardware operation. We consider common noises in daily life in terms of human factors and ambient factors. Typically, we select four conditions where (1) five people are walking around the mmWave probe within 2 meters range; (2) the humidity of the testing location is controlled at 70%; (3) the environment temperature is 0°C (32°F); (4) There is a working ventilation around. Moreover, we use the result of the optimal lab environment as the comparison target (humidity is 30% and the temperature is 20°C (68°F)). Again, we evaluate the above four conditions using 46 e-devices with scheme1. Figure 16 shows that their performances can achieve up to 99.6% precision, 99.3% recall and 99.6% accuracy. In conclusion, *E-Eye* presents a strong tolerance to different ambient environments.

7.2.2 Impact of Alien Devices. As discussed in Section 5.3, it is highly likely that *E-Eye* needs to classify the traces of the alien devices. In this section, we design an experiment to explore the ability of *E-Eye* to detect alien devices. In detail, we randomly include 9 out of 39 classes in the database as the training set as aforementioned (note that these data are never used for testing). Consequently, the remaining 30 classes are all regarded as the alien ones. Afterwards, we gradually increase the amount of alien devices from 5 to 30 and verify whether our specifically designed **Algorithm 1** can successfully identity them. For each amount, we report the average performance. As shown in Figure 17, the results remain stable in detection accuracy (*99.1%-100%*) showing no tendency to decrease in performance. In this way, we prove the effectiveness of fine-tuning the algorithm and the good scalability of *E-Eye* when used in real practice. Under these circumstances, the inspector can use the second check (*e.g., manual inspection*) for further security verification.

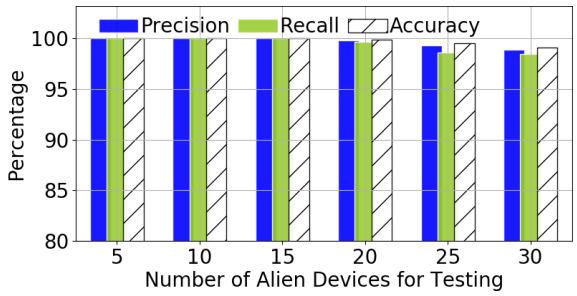


Figure 17: The alien device detection under six different alien device numbers.

7.3 Threat Model Study

7.3.1 Human Body Intervention. Due to the advanced IC technology, e-devices are getting smaller in size such that they can be easily hidden upon the human body to bypass the security check. Therefore, we assume the attacker hides the device in different body positions, as listed in Figure 18. We specifically consider the devices in groups 3 and 4 as they are pervasive and can be used in multiple malicious activities (see Table 3). We recruit five participants carrying the device and we use *E-Eye* to scan them at target areas keeping an approximate distance of 50*cm*. The reported average accuracy keeps higher than 97.7%, which implies that our system is resistant to human intervention.

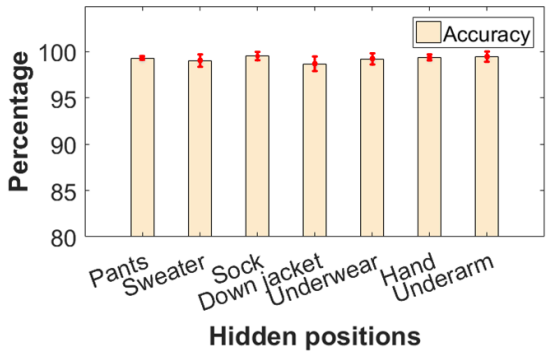


Figure 18: Detection accuracy under six different human interventions.

7.3.2 Impact of Cover Materials. We consider the scenario where the attacker intentionally hides the e-device in other materials to pass through screening. Particularly, we collect seven different daily-achievable materials as shown in Figure 19. We place the e-device inside each of them and evaluate the recognition accuracy for all 46 e-devices. The performance is reported in the figure, where we can see that the overall accuracy for each is above 98%. Certain materials slightly affect the performance to some extent. This is because *E-Eye* utilizes high frequency signal and therefore, has small wavelength and limited penetration ability. As a result, it is prone to the scattering reflection upon some specific materials. But in general, *E-Eye* still provides reliable performance in device recognition.

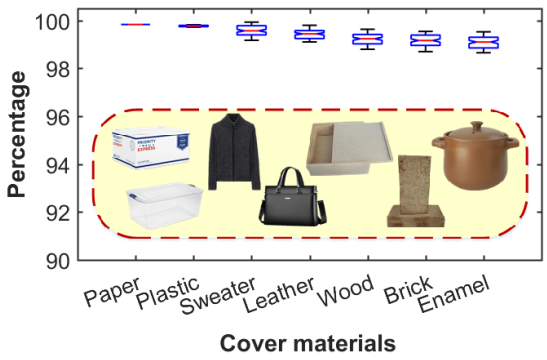


Figure 19: Detection accuracy with six different cover materials.

7.3.3 Impact of Combined E-devices. In another scenario, the attack may know the benign devices registered in the database and try to physically stack the malicious device with the benign one to confuse the system. To explore whether *E-Eye* can still regard it as the alien device, we continue with the setup in Section 7.2.2. We randomly select 2 (labeled as No.1, No.2) devices from the 9 benign classes and 3 (labeled as No.3, No.4, No.5) from the remaining 30 alien classes. As shown in Figure 20, we enumerate all six combinations of the benign and alien devices and physically tap them together. For the sake of generality, we report the average and standard deviation of accuracy. From the results, we can observe that the average recognition accuracy are higher than 98%. This is owing to the fact that the equivalent circuit changes if we combine two devices together along with the *nonlinear response*.

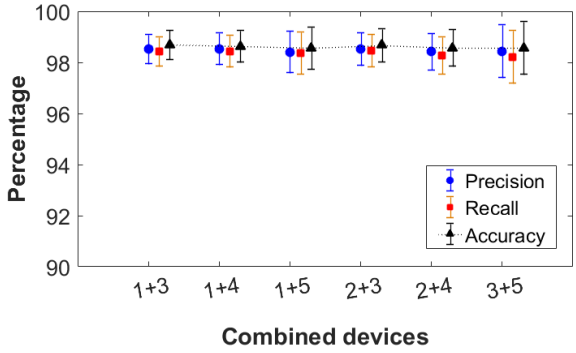


Figure 20: Detection of combined e-devices.

7.3.4 Impact of E-device Status. Considering the fact that many detection methods rely on the operation status of the hidden device (see Section 9.1), we simulate a scenario where the attacker wants to spoof the inspector by switching off the device or removing the battery. Thus, we repeat the experiment by shutting down all e-devices when collecting the data (as described in Section 6.2). Importantly, we still use the previously trained model where the devices were switched on. We apply the new 30 traces for each device for this test. Table 4 illustrates the precision, recall and accuracy for schemes 1 and 2, which are 99%. For scheme3, the

accuracy is 98.75% which is in coherence with the results in Section 7.1.1. The high accuracy proves that *E-Eye* is not sensitive to the hidden device's operation status.

Table 4: System performance with the e-device status OFF at 50cm sensing distance.

Setup	Precision(%)	Recall(%)	Accuracy(%)
Scheme1	99.54	99.24	99.57
Scheme2	99.51	99.20	99.55
Scheme3	98.70	98.52	98.75

8 DISCUSSION

Health Hazards: Compared to other security screening techniques (*e.g.*, Terahertz and X-ray imaging systems), *E-Eye* has a much smaller radiation factor, i.e., a 1.2W power consumption and an 8dBm radio transmission power. Considering that typical public WiFi spots have about 20 to 30 dBm of output power, *E-Eye* is a considerably safe screening tool, even for cardiac device patients.

Metal Intervention: Metal has a stronger reflection on EM wave compared to other materials. We realize that a metal case shields a large portion of RF signals. By deploying an additional metal hidden material (*e.g.*, an e-device inside a metal box), it is difficult for *E-Eye* to recognize the covered e-device. This limitation can be solved by detecting the existence of metal [59].

Manual Check: We notice that mechanical motion in the electronic device and other intruders can affect the sensing performance. However, it is safe to assume that the security checker controls the environment thoroughly. If an unusual behavior happens, they initiate a manual check.

Database Storage: In this pioneering work, we have established 39 classes of an e-device database. Particularly, each feature vector has 26 dimensions data of size 0.2KB around. Thus, the template for each device seizes 14KB size data in the experiment setup. Therefore, it is practical to maintain a vast amount of templates on the mobile platform or the server (*e.g.*, 1,000 e-device types only require $13.67MB$ physical storage).

Multiple E-devices: Nowadays, it is normal for more than one e-device to be concealed in a container [11]. Therefore, it can bring huge convenience if *E-Eye* can automatically recognize each type when multiple devices are present. This problem can be further solved by employing the existing blind source separation and independent component analysis approaches in the speech processing domain [21, 65].

9 RELATED WORK

9.1 Hidden E-device Detection

Currently, there are three main methods to detect hidden e-devices:

- **X-ray Imaging:** The X-ray baggage scanner operates based on the different X-radiation absorption rates of the penetrated objects and can accordingly produce the shape image of the objects [23]. The typical cost of such a scanner can reach US $50,000. Besides the undesired privacy concerns raised by the image of personal belongings [30], x-radiation also has harmful effects on human [30, 53].
- **Terahertz Imaging:** Terahertz (THz) imaging is also exploited in package screening by analyzing object transmissions or reflections of the THz electromagnetic wave. However, its optical image causes privacy issues and its resolution is too low for hidden e-devices recognition [38]. The current THz imaging systems have very low portability and extremely high cost (around US $25,000) [12, 25].
- **Electromagnetic Emission Sensing:** Studies find that e-devices transmit unintentional electromagnetic (UEM) radiations [51] when they are switched on. Many works [31, 57, 62] detect the existence of e-devices by analyzing their UEM waves. However, this technology is restricted and cannot be applied when the electronic device is powered off.

Therefore, we summarize that the current hidden e-devices recognition methods are either bulky, expensive or conditionally restrained, which cannot be directly applied in regular and large-scale public security check. Other alternative handheld scanners [9, 30] can only provide the existence detection rather than accurately recognize the device type.

9.2 mmWave Sensing

mmWave radars have been studied in a variety of domains based on the detection of an object's inherent movements (*e.g.*, cardiorespiratory measurements and gesture sensing [32, 36, 37]) in the last decade. Soli [35] is a 60GHz mmWave radar gesture sensing system, which can detect all kinds of hand motions for the human-computer interface. In [43], a 94GHz mmWave radar is deployed to extract features of cardiorespiratory movements based on the reflected mmWave signals. These mmWave sensing applications mainly rely on the Doppler motion of the objects and cannot be applied to sense the target under clothings or obstacles (*e.g.*, packages and luggages). Although there are some recent applications to explore "through-wall" and "through-obstacle" sensing via mmWave [17, 64, 66], these techniques can only be applied for the target with specific mmWave-absorption characteristics. According to the literature, *E-Eye* is the first mmWave sensing application to explore nonlinear effects for hidden electronics recognition.

10 CONCLUSION

In this paper, we proposed a hidden e-device recognition system *E-Eye*, to aid law enforcement and ensure security. We started from the basics characteristics of the e-device and cover material under the nonlinear effect. Then, we proposed a portable 24GHz mmWave probe and the e-device recognition module to accurately recognize the hidden e-device type. Furthermore, extensive experiments indicated that our *E-Eye* can achieve more than 99% accuracy in less than 20ms response time and centimeter level device physical size. Different levels of evaluation confirmed the effectiveness, reliability and robustness of our proposed system. The research findings are an essential step for understanding the *nonlinear response* of hidden e-device and their applications at large.

ACKNOWLEDGMENTS

We thank all anonymous reviewers for their insightful comments on this paper. This work was in part supported by the National Science Foundation under grant No. 1718375/1718483.

REFERENCES

[1] Accessed: 2018-1-11. IS turns hobby drones into remote-control bombs. https://nakedsecurity.sophos.com/2017/01/19/is-turns-hobby-drones-into-remote-control-bombs/.

[2] Accessed: 2018-1-11. ISM band. https://en.wikipedia.org/wiki/ISM_band.

[3] Accessed: 2018-1-21. ISIS' Online 'Training Manual' Teaches Sympathizers How to Disguise Themselves as Westerners and Build Bombs to Carry Out Attacks. https://www.christianpost.com/news/isis-training-manual-teaches-sympathizers-how-to-disguise-themselves-as-westerners-and-build-bombs-to-carry-out-terror-attacks-139253/.

[4] Accessed: 2018-1-21. Mobile-phone cheating in exams on the rise. https://www.cnet.com/news/mobile-phone-cheating-in-exams-on-the-rise/.

[5] Accessed: 2018-2-19. MSP430 Microcontrollers With CapTIvate Touch Technology. http://www.ti.com/lit/wp/slay044/slay044.pdf.

[6] Accessed: 2018-3-13. Sound card. https://en.wikipedia.org/wiki/Sound_card.

[7] Accessed: 2018-3-21. Bombs disguised as rocks in Yemen reportedly show Iran aid. https://www.defensenews.com/global/mideast-africa/2018/03/26/bombs-disguised-as-rocks-in-yemen-reportedly-show-iran-aid/.

[8] Accessed: 2018-3-22. International Telecommunication Union. https://www.itu.int/en/Pages/default.aspx.

[9] Accessed: 2018-3-23. Millimeter Scanning at Airports: Is It Worth the Cost? https://www.securitymagazine.com/articles/79508-millimeter-scanning-at-airports-is-it-worth-the-cost-1.

[10] Accessed: 2018-3-31. 5G mmWave: the next frontier in mobile broadband. https://www.qualcomm.com/invention/technologies/5g-nr/mmwave.

[11] Accessed: 2018-3-31. Digital Consumers Own 3.2 Connected Devices. https://blog.globalwebindex.net/chart-of-the-day/digital-consumers-own-3-point-2-connected-devices/.

[12] Accessed: 2018-3-31. Features of the Terahertz technology in security applications. http://terasense.com/news/thz-in-security/.

[13] Accessed: 2018-3-31. Geddes town supervisor's secretary faces felony for eavesdropping on co-workers. http://www.syracuse.com/crime/index.ssf/2016/12/geddes_town_supervisors_secretary_faces_felony_for_evesdropping_on_co-workers.html.

[14] Accessed: 2018-3-31. Package Explosion in Austin. https://www.washingtonpost.com/news/morning-mix/wp/2018/03/20/package-believed-to-be-bound-for-austin-explodes-at-texas-\fedex-facility-police-say/?utm_term=.8b593439781e.

[15] Accessed: 2018-3-31. Phone and Electronic Device Policy. https://collegereadiness.collegeboard.org/sat/taking-the-test/phone-electronic-device-policy.

[16] Accessed: 2018-3-31. Use of Cell Phones, Laptops, and Other Electronic Devices by Visitors. https://www.cadc.uscourts.gov/internet/home.nsf/Content/VL+-+Courthouse+-+Cell+Phones+Laptops+and+Other+Electronic+Devices.

[17] Fadel Adib and Dina Katabi. 2013. See through walls with WiFi! Vol. 43. ACM.

[18] Ruud M Bolle, Jonathan H Connell, Sharath Pankanti, Nalini K Ratha, and Andrew W Senior. 2013. Guide to biometrics. Springer Science & Business Media.

[19] Jamie Bullock and UCEB Conservatoire. 2007. Libxtract: a Lightweight Library for audio Feature Extraction.. In ICMC.

[20] Chedsada Chinrungrueng. 2003. Combining Savitzky-Golay filters and median filters for reducing speckle noise in SAR images. In Systems, Man and Cybernetics, 2003. IEEE International Conference on, Vol. 1. IEEE, 690–696.

[21] Seungjin Choi, Andrzej Cichocki, Hyung-Min Park, and Soo-Young Lee. 2005. Blind source separation and independent component analysis: A review. Neural Information Processing-Letters and Reviews 6, 1 (2005), 1–57.

[22] Federal Communications Commission and others. 2016. Use of spectrum bands above 24 GHz for mobile radio services. Fed Regist 81, 164 (2016), 58270–58308.

[23] Christine Connolly. 2008. X-ray systems for security and industrial inspection. Sensor Review 28, 3 (2008), 194–198. DOI: http://dx.doi.org/10.1108/02602280810882535

[24] Morten W Fagerland, Stian Lydersen, and Petter Laake. 2013. The McNemar test for binary matched-pairs data: mid-p and asymptotic are better than exact conditional. BMC medical research methodology 13, 1 (2013), 91.

[25] John F Federici, Brian Schulkin, Feng Huang, Dale Gary, Robert Barat, Filipe Oliveira, and David Zimdars. 2005. THz imaging and sensing for security applications: explosives, weapons and drugs. Semiconductor Science and Technology 20, 7 (2005), S266. http://stacks.iop.org/0268-1242/20/i=7/a=018

[26] Kevin G Gard, Lawrence E Larson, and Michael B Steer. 2005. The impact of RF front-end characteristics on the spectral regrowth of communications signals. IEEE Transactions on Microwave Theory and Techniques 53, 6 (2005), 2179–2186.

[27] Khaled M Gharaibeh. 2011. Nonlinear distortion in wireless systems: Modeling and simulation with MATLAB. John Wiley & Sons.

[28] Franco Giannini and Giorgio Leuzzi. 2004. Nonlinear microwave circuit design. John Wiley & Sons.

[29] U Gudaru and Vishal B Waje. 2012. Analysis of harmonics in power system using wavelet transform. In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on. IEEE, 1–5.

[30] S. Hantscher, B. Schlenther, M. Hagelen, S. A. Lang, H. Essen, A. Tessmann, A. Hulsmann, A. Leuther, and M. Schlechtweg. 2012. Security Pre-screening of Moving Persons Using a Rotating Multichannel W -Band Radar. IEEE Transactions on Microwave Theory and Techniques 60, 3 (March 2012), 870–880. DOI: http://dx.doi.org/10.1109/TMTT.2011.2181534

[31] J. Hertenstein and S. Jagannathan. 2013. Simulation and Detection of Unintended Electromagnetic Emissions From Super-Regenerative Receivers. IEEE Transactions on Instrumentation and Measurement 62, 7 (July 2013), 2093–2100. DOI: http://dx.doi.org/10.1109/TIM.2013.2248290

[32] M. C. Huang, J. J. Liu, W. Xu, C. Gu, C. Li, and M. Sarrafzadeh. 2016. A Self-Calibrating Radar Sensor System for Measuring Vital Signs. IEEE Transactions on Biomedical Circuits and Systems 10, 2 (April 2016), 352–363.

[33] Handan Ilbegi, Harun Taha Hayvaci, Imam Samil Yetik, and Asim Egemen Yilmaz. 2017. Distinguishing electronic devices using harmonic radar. In Radar Conference (RadarConf), 2017 IEEE. IEEE, 1527–1530.

[34] Jianhua Jia, Zi Liu, Xuan Xiao, Bingxiang Liu, and Kuo-Chen Chou. 2015. iPPI-Esml: an ensemble classifier for identifying the interactions of proteins by incorporating their physicochemical properties and wavelet transforms into PseAAC. Journal of theoretical biology 377 (2015), 47–56.

[35] 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. DOI: http://dx.doi.org/10.1145/2897824.2925953

[36] 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 (MobiCom '17). ACM, New York, NY, USA, 315–328.

[37] F. Lin, Y. Zhuang, C. Song, A. Wang, Y. Li, C. Gu, C. Li, and W. Xu. 2017. SleepSense: A Noncontact and Cost-Effective Sleep Monitoring System. IEEE Transactions on Biomedical Circuits and Systems 11, 1 (Feb 2017), 189–202.

[38] Hai-Bo Liu, Hua Zhong, Nicholas Karpowicz, Yunqing Chen, and Xi-Cheng Zhang. 2007. Terahertz spectroscopy and imaging for defense and security applications. *Proc. IEEE* 95, 8 (2007), 1514–1527.

[39] J Michael Lloyd. 2013. Thermal imaging systems. Springer Science & Business Media.

[40] Stephane G Mallat. 1989. A theory for multiresolution signal decomposition: the wavelet representation. IEEE transactions on pattern analysis and machine intelligence 11, 7 (1989), 674–693.

[41] Gregory J Mazzaro, Anthony F Martone, Kenneth I Ranney, and Ram M Narayanan. 2017. Nonlinear radar for finding rf electronics: System design and recent advancements. IEEE Transactions on Microwave Theory and Techniques 65, 5 (2017), 1716–1726.

[42] Gregory J Mazzaro and Kelly D Sherbondy. 2013. Combined linear and nonlinear radar: waveform generation and capture. Technical Report. ARMY RESEARCH LAB ADELPHI MD SENSORS AND ELECTRON DEVICES DIRECTORATE.

[43] 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. DOI: http://dx.doi.org/10.1109/TBME.2011.2111371

[44] 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.

[45] Amy Nordrum. 2016. Popular internet of things forecast of 50 billion devices by 2020 is outdated. IEEE Spectrum 18 (2016).

[46] J Pedro and N Carvalho. 2003. Intermodulation distortion in microwave and wireless circuits. Norwood, MA: Artech House. (2003).

[47] Zhengyu Peng, José-María 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.

[48] Adam C Polak, Sepideh Dolatshahi, and Dennis L Goeckel. 2011. Identifying wireless users via transmitter imperfections. IEEE Journal on selected areas in communications 29, 7 (2011), 1469–1479.

[49] 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.

[50] Lawrence R Rabiner and Bernard Gold. 1975. Theory and application of digital signal processing. Englewood Cliffs, NJ, Prentice-Hall, Inc., 1975. 777 p. (1975).

[51] C.J. Reddy. 1998. Control And Measurement Of Unintentional Electromagnetic Radiation. IEEE Antennas and Propagation Magazine 40, 2 (1998), 88–89.

[52] Matteo Rinaldi, Chiara Zuniga, Chengjie Zuo, and Gianluca Piazza. 2010. Super-high-frequency two-port AlN contour-mode resonators for RF applications. IEEE transactions on ultrasonics, ferroelectrics, and frequency control 57, 1 (2010).

[53] D. M. Sheen, D. L. McMakin, and T. E. Hall. 2001. Three-dimensional millimeter-wave imaging for concealed weapon detection. IEEE Transactions on Microwave Theory and Techniques 49, 9 (Sep 2001), 1581–1592. DOI: http://dx.doi.org/10.1109/22.942570

[54] Aditya Singh and Victor Lubecke. 2010. A heterodyne receiver for harmonic Doppler radar cardiopulmonary monitoring with body-worn passive RF tags. In Microwave Symposium Digest (MTT), 2010 IEEE MTT-S International. IEEE, 1600–1603.

[55] Satish Sinha, Partha S Routh, Phil D Anno, and John P Castagna. 2005. Spectral decomposition of seismic data with continuous-wavelet transform. Geophysics 70, 6 (2005), P19–P25.

[56] Chen Song, Aosen Wang, Kui Ren, and Wenyao Xu. 2016. Eyeveri: A secure and usable approach for smartphone user authentication. In Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on. IEEE, 1–9.

[57] C. Stagner, A. Conrad, C. Osterwise, D. G. Beetner, and S. Grant. 2011. A Practical Superheterodyne-Receiver Detector Using Stimulated Emissions. IEEE Transactions on Instrumentation and Measurement 60, 4 (April 2011), 1461–1468. DOI: http://dx.doi.org/10.1109/TIM.2010.2101330

[58] Colin Blake Stagner. 2013. Detecting and Locating Electronic Devices Using Their Unintended Electromagnetic Emissions. Doctoral Dissertations (2013). http://scholarsmine.mst.edu/doctoral_dissertations/2152

[59] J Svatoš, J Vedral, and P Nováček. 2012. Metal object detection and discrimination using Sinc signal. In Electronics Conference (BEC), 2012 13th Biennial Baltic. IEEE, 307–310.

[60] Serioja O Tatu and Ke Wu. 2013. Six-port technology and applications. In Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2013 11th International Conference on, Vol. 1. IEEE, 239–248.

[61] Phan Thanh Noi and Martin Kappas. 2017. Comparison of random forest, k-nearest neighbor, and support vector machine classifiers for land cover classification using Sentinel-2 imagery. Sensors 18, 1 (2017), 18.

[62] V. Thotla, M. J. Zawodniok, S. Jagannathan, M. T. A. Ghasr, and S. Agarwal. 2015. Detection and Localization of Multiple R/C Electronic Devices Using Array Detectors. IEEE Transactions on Instrumentation and Measurement 64, 1 (Jan 2015), 241–251. DOI: http://dx.doi.org/10.1109/TIM.2014.2331432

[63] Guochao Wang, Jose-Maria Munoz-Ferreras, Changzhan Gu, Changzhi Li, and Roberto Gomez-Garcia. 2014. Application of linear-frequency-modulated continuous-wave (LFMCW) radars for tracking of vital signs. IEEE Transactions on Microwave Theory and Techniques 62, 6 (2014), 1387–1399.

[64] 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.

[65] Ozgur Yilmaz and Scott Rickard. 2004. Blind separation of speech mixtures via time-frequency masking. IEEE Transactions on signal processing 52, 7 (2004), 1830–1847.

[66] 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.