2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)

2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT) | 979-8-3503-4649-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/DCOSS-IOT58021.2023.00050

Identification and Classification of Electronic Devices Using Harmonic Radar

Beatrice Perez
Department of Computer Science
Dartmouth College
Hanover, NH, USA

Timothy J. Pierson
Department of Computer Science
Dartmouth College
Hanover, NH, USA

Gregory Mazzaro
Department of Electrical & Computer Engineering
The Citadel, The Military College of South Carolina
Charleston, SC, USA

David Kotz
Department of Computer Science
Dartmouth College
Hanover, NH, USA

***Abstract*—Smart home electronic devices invisibly collect, process, and exchange information with each other and with remote services, often without a home occupants' knowledge or consent. These devices may be mobile or fixed and may have wireless or wired network connections. Detecting and identifying all devices present in a home is a necessary first step to control the flow of data, but there exists no universal mechanism to detect and identify all electronic devices in a space.**

In this paper we present ICED (Identification and Classification of Electronic Devices), a system that can (i) identify devices from a known set of devices, and (ii) detect the presence of previously unseen devices. ICED, based on harmonic radar technology, collects measurements at the first harmonic of the radar's transmit frequency. We find that the harmonic response contains enough information to infer the type of device. It works when the device has no wireless network interface, is powered off, or attempts to evade detection. We evaluate performance on a collection of 17 devices and find that by transmitting a range of frequencies we correctly identify known devices with 97.6% accuracy and identify previously unseen devices as 'unknown' with 69.0% balanced accuracy.

I. Introduction

Numerous projections assert that *billions* of Internet of Things (IoT) devices will be deployed over the next few years [1]. Many of these devices will collect and share information about their local environment. Because IoT devices may use invisible wireless networks or hidden wired connections, devices may collect and share data about people without the person's knowledge or consent, raising significant security and privacy concerns. A critical step towards protecting security and privacy is to detect and identify the set of devices present in a particular area. A related requirement is to discover the presence of unknown devices, which may have appeared after a prior inventory and may represent suspicious devices added to a personal space.

The literature proposes several methods for identifying electronic devices, with most of the work focusing on mobile phones as their target. Rather than relying on the contents of smartphones for identification (e.g., apps installed, songs played, sequence of apps used, configuration settings) [2], imperfections introduced during the manufacturing process [3], or the network and other characteristics of a device [4], the system introduced in this paper uses an unusual type of radar – *harmonic radar* – for device detection and identification.

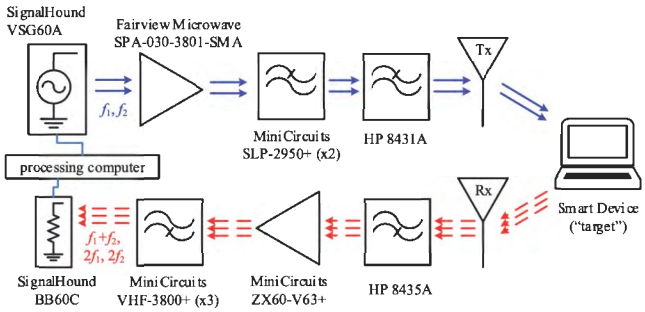


Fig. 1: Block diagram of the radar system designed for home consumer electronics. ICED uses separate transmit and receive chains to detect nearby electronic devices.

The key insight in our system, ICED (Identification and Classification of Electronic Devices), is that electronics distort radio frequencies before reflecting them. As in traditional radar systems, harmonic radar transmits radio frequency (RF) signals to obtain information about targets; however, when the transmitted RF interacts with the components in an *electronic* device, it generates a response at integer multiples (harmonics) of the transmitted signal. ICED leverages this characteristic to detect and classify devices, even if the devices are powered off or attempt to evade detection! Figure 1 shows an overview of the hardware components involved.

Although ICED is currently a prototype, we envision a handheld or easily portable device capable of detecting the presence of electronic devices located in an area (typically the same room). This system might be useful, for example, if a smart home containing dozens or even hundreds of devices is sold to a new owner. The new owner would be able to use ICED to catalog each device left behind by the previous

2325-2944/23/$31.00 ©2023 IEEE
DOI 10.1109/DCOSS-IoT58021.2023.00050

owner, perhaps as part of the pre-purchase home inspection. A second use case would be in a temporary living area such as AirBnB or in a shared working area such as Regus. ICED could alert the tenant to the presence of devices such as hidden cameras or microphones installed by the property owner.

Detection is different from identification. While prior work has shown harmonic radar can be used to *detect* the presence of electronic devices [5], in this paper we go further and attempt to not only detect devices, but also to *identify the type of device*. This work is also distinct in that it is a collaboration between electrical engineering and computer science. The radar theory and applications being developed within the scope of this work requires signal processing *and* machine learning to push our understanding of the technology further and its application towards commercial use. This work is novel in electrical engineering through its exploration of different (more common) targets, unexplored frequencies, and uncontrolled environments; it is novel in computer science in that it presents a universal solution to an open problem: the technology and methods available for the identification and classification of home electronics, particularly in its attempt to propose an encompassing solution for all types of devices. Moreover, these results can only be achieved at the edge of both disciplines – mathematical modeling and machine learning to make data usable, while building RF circuits and experimenting with different components to obtain detectable signals – then designing experiments to show the potential of the technology toward the objective. This paper positions harmonic radars as a serious contender in this space with promising results and interesting problems still to be explored.

In this paper, we make the following **contributions**:

- We build a prototype device that uses harmonic radar to detect and identify electronic devices from their response.
- We test 17 off-the-shelf consumer devices under four methods of identification.
- We use supervised classification algorithms and build models to identify the devices in our testbed, achieving an accuracy of 97.6%.
- We build a binary classifier that detects 'unknown' devices with balanced accuracy 69.0% and precision 65.8%.

II. Background

In this section we provide a brief primer on harmonic radars. We then describe our approach to uniquely fingerprint devices.

A. Harmonic radar primer

Harmonic radars are different from traditional radars. In a traditional radar, the system sends a pulse of RF energy toward a target and a portion of the energy reflects from the target at the same frequency transmitted (plus a small Doppler shift if the target is moving). A harmonic radar transmits RF signals that propagate through space like traditional radar systems, but when the signal strikes a target with *nonlinear* semiconductor components, such as the transistors and diodes found in electronic devices, a portion of the energy incident on the device is reflected as harmonics [6]. These harmonics occur at different frequencies from the original transmission. Naturally-occurring materials and most man-made materials, such as those found in a residence (e.g., drywall, furniture), are *linear*, i.e., they reflect only those frequencies transmitted to them. Therefore, reception of harmonics immediately indicates presence of objects with nonlinear electronic components. Perez et al. [3] give a description of the mathematics involved.

All electronic devices, from the simplest embedded systems to the most complex electronics, will respond harmonically to some (unknown) frequency [5]. Because this technique leverages reflections from transmitted RF striking nonlinear components, it detects electronic devices even if the device's battery is removed, if it is powered off, or simply idle and waiting for instructions.

B. Fingerprinting devices

Every type and model of device has a different set of components, in a different configuration. Consumer devices are also encased and shielded to limit RF leaks and RF interference; this shielding affects the way the device will receive and respond to an incident radar signal. If a device has an antenna, the natural path for reflecting the harmonics of a received tone is through the antenna; the geometry and design of each circuit determines the radiation pattern of re-radiated signals. ICED is predicated on the notion that these physical differences among devices – perhaps even between devices of identical make and model – lead to distinctive responses to a harmonic radar, allowing devices to be distinguished by a classifier trained to recognize these 'fingerprints'.

III. Implementation

ICED, shown in Figure 1, is a harmonic radar system built using commercial off-the-shelf components. The transmit chain, shown in blue, begins with a Signal Hound VSG60A signal generator capable of generating RF signals from 50 MHz to 6 GHz [7]. We chose this signal generator for its ability to transmit a broad spectrum. The generated RF is then passed to a Fairview Microwave SPA-030-3801-SMA-A power amplifier [8] to boost the signal strength. A series of low-pass filters remove any unwanted high frequency signals (i.e., two Mini Circuits SLP-2950 [9] and an HP 8431A) before the clean output signal is transmitted toward a target device by a directional Ettus Research LP-0965 log-periodic antenna [10].

The receive chain, shown in red in Figure 1, begins with a matching Ettus Research LP-0965 log-periodic antenna placed outside the transmit antenna's radiation pattern. The antenna is followed by high-pass filters (i.e., Mini Circuits VHF-3800+ [11] and HP 8435A) designed to filter the lower frequency corresponding to the transmitted signal, leaving only the higher frequency harmonic signal. Next a Mini Circuits ZX60-V63+ [12] amplifier boosts the faint received signal before sending it to another Mini Circuits VHF-3800+ for final filtering. Last, a Signal Hound BB60C [13] spectrum analyzer processes the received signal.

Previous work shows that the harmonic response of devices is likely to be stronger around frequencies at which devices are designed to operate [14]. We designed our prototype with Wi-Fi and Bluetooth devices in mind; they tend to operate around 2.4 GHz. Although the signal generator and spectrum analyzer together can support frequencies from 50 MHz to 6 GHz, we selected high-pass and low-pass filters to limit the frequency range for the probe signal to the lower end of the S band, that is, between 2 and 2.8 GHz. We controlled the signal generator and spectrum analyzer using their Python API. We used Python and scikit-learn [15] to process and evaluate the data.

IV. Approaches

We explore three approaches for device identification. The first approach transmits a single tone (frequency) and listens for a response at the first harmonic (e.g., two times the transmitted frequency). The second approach sweeps a single tone over a range of frequencies while listening at two times each transmitted frequency. The third approach transmits two tones simultaneously, purposely generating intermodulation distortion, and listens over a range of frequencies. We briefly describe each of these approaches in more detail next.

A. Single tone

In this approach ICED transmits a single tone at 2.328 GHz. We choose this frequency because it is close to the operating frequency of the Wi-Fi and Bluetooth devices in our collection (see Table I for a list of devices) and because prior research suggests devices tend to respond well at this frequency [5]. We measure the response at the first harmonic of 4.656 GHz.

B. Swept range of tones

In this approach ICED steps through a sequence of tones from 2.0 GHz to 2.8 GHz, in 10 MHz increments. At each step it transmits a single tone, pauses, then listens for a response at the corresponding first harmonic (from 4.0 GHz to 5.6 GHz).

C. Simultaneous tones

In this approach ICED transmits two tones simultaneously, purposefully creating *intermodulatation distortion* (IMD), that is, signals with multiple tones on the same wave. Specifically it creates mixing products (in addition to the normal harmonics) at $2\omega_1 - \omega_2$ and $2\omega_2 - \omega_1$. The system measures the response over the mixing products of the tones. In this way, ICED acts similarly to an IMD radar [14].

In this approach, we use only two tones a with a commonly used spacing of 1 MHz between the two frequencies to generate the cross-modulated harmonics [16]. Here, the limiting factor is the Signal-to-Noise Ratio of the response. Compared to the power of the reflected signal of a single-tone harmonic, the reflection of each tone in a multi-tone signal is scaled down by a factor proportional to the number of tones. In other words, by transmitting more than one tone (but the same total power) the power of the response of the single-tone harmonic gets distributed across all transmitted (and thus received) frequencies.

TABLE I: Device list and manufacturers.

Device Category	Manufacturer	Label
Light Control	Linkind	B
Wi-Fi Smart Plug	D-Link	C
Wi-Fi Smart Plug	SmartThings	D
Smart Tag	SmartThings	E
Smart Tag	Tile	F
Smart Tag	Samsung Galaxy	G
Smart Thermostat	Ecobee3	H
Smart Thermostat	Govee	I
Smart Camera	Yi	J
Smart Camera	SmartThings	K
Smart Camera	Blink	L
Thermometer	Kinsa	M
Thermometer	Kinsa	N
Pedometer	Polar	O
Pedometer	Polar	P
Pedometer	Zephyr	Q
Oxymeter	iHealth	R

V. Evaluation

We collected data at a single residential location in a metropolitan city with the background RF noise one might expect in an urban apartment complex. We positioned ICED's transmit and receive antennas at a fixed position in front of the target device at a range of approximately 45 cm and fixed the power of the transmitted signal.

For an open-air line-of-sight measurement as in this paper, in the far field of the antennas, the received signal strength at all harmonic and multitone frequencies is proportional to $1/R^6$ where R is the distance between the antennas and the target.[1] In other words, less incident power-on-target generates less baseline power received from that target, but it does not change its unique pattern of frequencies. At longer distances, the target's fingerprint is unchanged but that fingerprint is simply received at a lower power level.

As targets, we experimented with a collection of 17 off-the-shelf 'smart' devices, listed in Table I. The set includes both Wi-Fi and Bluetooth devices, with a range in sizes and capabilities. In choosing devices, we considered multiple devices from a category. For example, in the *Smart Tags* and *Smart Cameras* categories we included three models of each. Smart Tags are similar in size and shape to the pedometers but have different use (and therefore different components) and we include two pedometers of the same manufacturer and model and attempt to differentiate between separate instances of the device.

We evaluate the success of each method using the average *accuracy*, that is, the fraction of cases for which the classifier correctly identifies a specific device based on its response to the transmitted frequency. For our collection of 17 devices, a simple random-guessing classifier would achieve accuracy 0.059 ($= 1/17$), less than 6%.

[1] Assuming the nonlinear junction(s) activated at the target are not saturated by incident power, which is a safe assumption for practical targets [14].

TABLE II: Summary of the metrics obtained for the three variations of the classification task.

Approach	Accuracy	Precision	Recall	F1-Score
Single Tone	0.376	0.266	0.376	0.305
Swept Range	0.976	0.973	0.971	0.970
Multiple Tones	0.353	0.342	0.353	0.330

VI. Device Identification

The results for the three approaches described in Section IV are summarized in Table II. For each approach, we conducted 10 experiments where we transmitted a signal toward a target device and listened on the first harmonic of the transmitted signal. We then performed 10-fold cross validation where we created classifiers repeatedly using 9 experiments as training data and evaluated the system on the 10th. Importantly, for these experiments the orientation of the device relative to the transmit and receive antennas of ICED was fixed. We relax that restriction in Section VII and consider identification of devices at different orientations.

Additionally, while we computed results using three classifiers (Random Forests, Support Vector Machines, and Gradient Boost algorithms), we found that Random Forests provided the best results for all classification tasks, so we report only the Random Forest results here. The configuration parameters for the Random Forest were selected through a grid search and ultimately, each forest was comprised of 300 estimators with a maximum depth of 90 and at least 5 samples per leaf.

A. Single tone

We collected 170 measurements (10 measurements per device for 17 devices), each comprised of 412 signal strength readings over a 1 MHz window centered on the first harmonic of the 2.328 GHz transmitted signal. Figure 2a presents an illustrative response collected for Device R. Other devices had similar patterns with a spike at the harmonic frequency, but different nonlinear electrical components within each device resulted in different amplitudes.

We use these results as as starting point to explore the fingerprinting abilities of harmonic radar. Figure 3a shows the confusion matrix for identifying a specific device using a Random Forest classifier. The cross-validated accuracy of this approach is 0.376. Compared to the random-choice baseline, fingerprinting devices from the harmonic response is already improving the classification accuracy by a factor of 6. Grouping devices by the categories indicated in Table I (e.g., identifying the device as a Polar Pedometer instead of identifying it as Polar Pedometer number 2) results in an accuracy of 0.429. While these results are not definitive, they build confidence that other approaches might have better performance.

B. Swept range of tones

In the second approach, we transmit probe signals with frequencies in steps of 10 MHz from 2–2.8 GHz for a total of 160 readings. We collect the response, one at a time, at the first harmonic of the transmitted frequency (i.e., $2f_{Tx}$). Figure 2b presents, as an example, the response recorded for Device G. As expected, however, the exact shape of the plot varied between devices. The full dataset contains 10 measurements per device for 17 devices for a total of 170 measurements each with 160 readings of the amplitude of the monitored frequencies.

Table II and Figure 3b present near-perfect classification results for identifying each specific device (including differentiating between Polar Pedometer 1 and Polar Pedometer 2). These results show, with an accuracy of 0.976, that the use of a wide range of transmit frequencies generates a distinct fingerprint across devices in the our collection. Strangely, this approach resulted in a drop in accuracy for determining device categories (e.g., identifying Polar Pedometers) compared with identifying device categories. With eight device types (Light Control, Wi-Fi Smart Plug, Smart Tag, Smart Thermostat, Smart Camera, Thermometer, Pedometer, and Oxymeter from Table I), the classification accuracy declined to 0.733. We suspect this is due to device orientation, a topic we explore further in Section VII.

It is worth noting that while this approach is less accurate when identifying device types compared with its performance when identifying specific devices, it is still the most successful of the three approaches.

C. Simultaneous tones

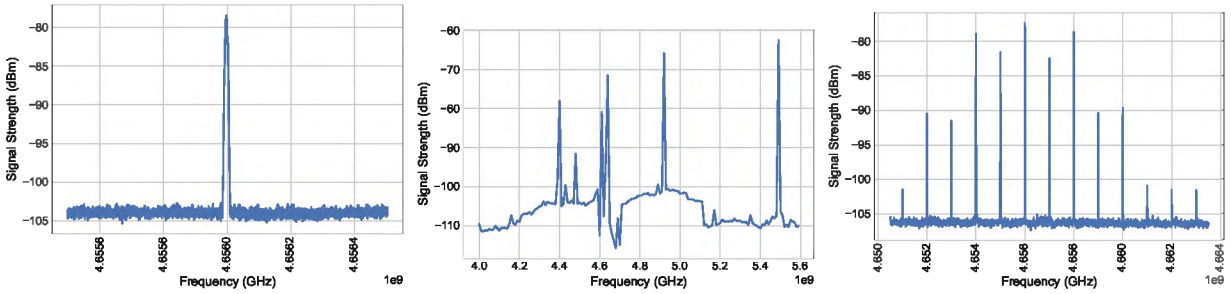
In this approach, we transmitted two simultaneous frequencies at 2.328 GHz $\pm$1 MHz. As discussed in Section IV-C, when two narrow tones are transmitted simultaneously, we expect a response at the harmonic of each tone and the mixing product of both tones. To capture the finer resolution, the dataset for this approach contains 10 measurements per device for 17 devices where each measurement is comprised of 5,336 signal strength readings in a window of 14 MHz. Figure 2c shows, as an example, Device M.

Table II shows the accuracy for identifying a specific device for this approach was 0.353. The challenge is that compared to a single tone, even with more data, devices and device types are more similar to each other using two tones. Figure 3c shows the confusion matrix for this approach.

VII. Device Orientation

The experiments above indicate that the most accurate approach for identification is the response from a swept range of tones. In a real-world deployment, however, it may not always be possible to probe a device at the same orientation angle for which the classifier was trained. Indeed it is unlikely the device will be in the same orientation in the field. The simplest solution is to scan a device from multiple angles during training (building a more robust fingerprint from different perspectives).

The scientific question of orientation remains: how does changing the angle of the incident signal alter the harmonic response of a device? Our hypothesis is that at different

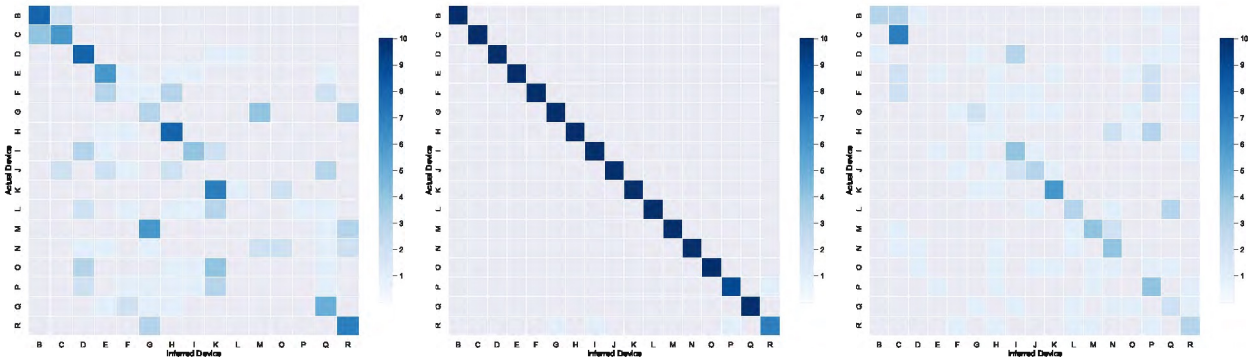


(a) Device R harmonic response from a single transmitted frequency at 2.328 GHz.

(b) Device G harmonic response to swept tones transmitted from 2.0 – 2.8 GHz.

(c) Device M harmonic response to two tones +/- 1 MHz around 2.328 GHz.

Fig. 2: Spectrum frequency responses at different configurations.



(a) Single tone confusion matrix. (b) Swept range of tones confusion matrix. (c) Simultaneous tones confusion matrix.

Fig. 3: Confusion matrices for different configurations. Darker shades of blue indicates a higher number; grey indicates zero.

orientations, the transmitted signal will likely be re-radiated by a different set of nonlinear device components which should result in a different received signal. We thus designed an experiment to test the robustness of the swept range of tones method to changes in angle of the probe signal. In this experiment, each device was placed on a graduated turntable and scanned at intervals of 30°. We captured high-resolution spectral data around 10 evenly spaced frequencies. Figure 4 shows the example of Device B at 60°.

The final dataset contains 10 measurements per device for 17 devices and each measurement contains 12 observations for angles in steps of 30°. Using the swept range of tones, we computed the accuracy of the method by leaving out one angle at a time over all 10 measurements training on 11 angles of 9 measurements and testing on all 10 measurements of the removed angle plus the full data of the 10th measurement (i.e., the one left out). Figure 5a presents the confusion matrix for identifying a specific device.

The combined accuracy of all tests (i.e., just over 2,000 experiments: 12 angles, 10 measurements per device, 17 devices) is 0.808. When identifying a device at the same angle from which it was measured we are successful in choosing the right device with an accuracy of 0.976. If instead, we receive a measurement from an angle previously unknown, we can identify the correct device with an accuracy of 0.808.

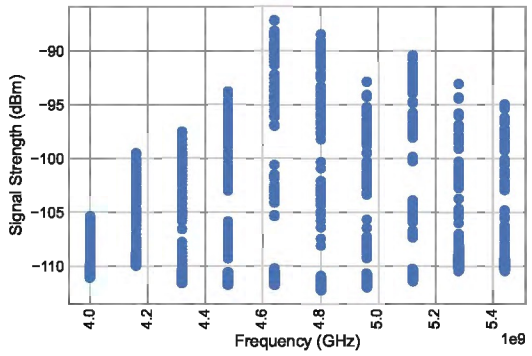
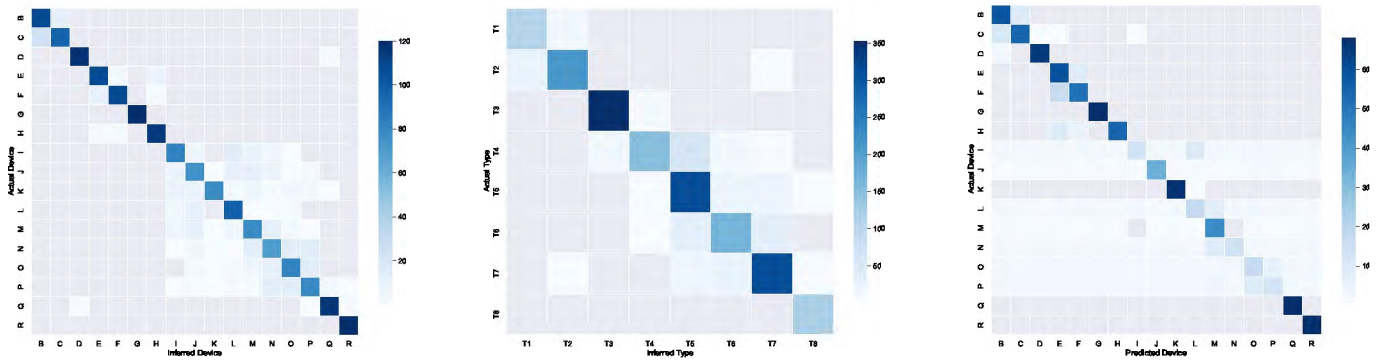


Fig. 4: Spectrum frequency response for Device B from a single tone at 2.328 GHz.

Taking it one step further, we shift our attention from identifying the device to determining the type (or category) of the device; for this task the accuracy increased to 0.853. Figure 5b presents the confusion matrix for identifying the device category.

These results suggest that ICED is able to correctly identify devices with high probability using the swept range of tones approach, even if the devices are at a different orientation from which the classifier was trained.



(a) Leave-one-angle-out classification for identifying specific devices.

(b) Leave-one-angle-out classification for identifying device categories.

(c) Binary classification (known vs. unknown) by class.

Fig. 5: Confusion matrices for device rotation and unknown device detection.

VIII. Detecting Unknown Devices

We now consider a different, but related problem to identifying *unknown* devices from a set of devices. There are many contexts where it may be important to determine whether the device being tested belongs to the set of '*known*' devices, i.e., to discover the arrival of a new device that needs to be added to the known inventory, or to determine whether the new device may have been placed (or replaced) by an adversary. This is a binary classification task where each device is labeled either as 'known' or 'unknown'. We test the ability of ICED to detect unknown devices by creating a two-stage classifier; in the first stage, our classifier outputs a probability of a target device being in each one of the $N = 17$ 'known' classes; in the second stage, the classifier outputs 'known' if the probability for the output class is above a predetermined threshold (ultimately set at 0.35), and 'unknown' if no class achieves that threshold probability.

For this scenario, we train the multi-class classifier by excluding one device at a time. We use all examples of the excluded device and four of the ten measurements for the remaining devices in the testing set. Finally, we repeat this process for all devices and aggregate the results. Because of the imbalance of the classes in the testing set, we compute the *balanced accuracy* for all test observations rather than accuracy.

Primary results are presented in Table III. From the combined count of all experiments, we find that the binary classifier has a sensitivity of 63.6% and a specificity of 74.4% which results in a balanced accuracy of 69%. The confusion matrix in Figure 5c shows that 12 of the 17 devices were correctly labeled (i.e., known and unknown were assigned appropriately). Most importantly though, both the figure and the confusion matrix show that the binary classifier had good performance when classifying known devices (i.e., low false negative rate) with a failure rate of 7.52%.

Finally, we trained the binary classifier for the task of assigning 'known' and 'unknown' to device *categories*. We found that while the threshold changed, the balanced accuracy (not shown) remained the same.

TABLE III: Confusion matrix for the binary classifier. Numbers are the count of training observations.

		Actual Class		
		Known	Unknown	Total
Inferred Class	Known	519	87	606
	Unknown	297	253	550
	Total	816	340	1156

IX. Discussion

The three different approaches in this paper are neither competing nor mutually exclusive. From the confusion matrices that display the results, we see that devices are more (or less) recognizable depending on the approach for identification. Ultimately, a deployed system could potentially integrate all three approaches.

X. Related Work

Researchers have proposed many methods for discovering devices present in an area. Solutions tend to fall into one of several categories: (1) sniffers, (2) discovery protocols, (3) traditional radar technologies, and (4) other harmonic radar approaches. We briefly discuss each of these approaches in this section. None, however, accomplish our goal of detecting *all* devices in an area, let alone distinguishing (identifying) them.

A. Sniffers

One of the most basic ways to discover devices is to simply sniff their communications. With this approach, a sniffer listens for device communications and attempts to identify the device based on the characteristics of the transmissions, such as a MAC address in a packet header.

There are several shortcomings to sniffing. First, the sniffer must speak the same protocol the device speaks. For example, a Wi-Fi sniffer would not discover Bluetooth or Zigbee devices, even though they share the same radio spectrum. Second, the sniffer must monitor the correct frequencies. Wi-Fi, for example, has two bands, 2.4 GHz and 5 GHz, with each band comprising several channels. A sniffer listening on one

Wi-Fi channel would not discover devices transmitting on another channel. Third, some devices might use analog communications (such as older cordless phones). These would not be detected by a digital sniffer, even if the sniffer were capable of monitoring and decoding all common digital communication protocols. Comprehensively monitoring all frequencies for all communication modalities is a tall task indeed. Furthermore, while sniffers can detect some transmitting devices, they cannot detect devices that do not transmit (such as a camera or microphone that stores data on removable media). They are also incapable of detecting devices that communicate on wired network connections (such as Ethernet or landline telephone). Finally, by design, some malicious devices may use communication techniques deliberately designed to evade detection by sniffers [17].

Sniffers have many serious shortcomings if the goal is to detect all smart devices. ICED can find and identify devices regardless of their communication protocol – even if they do not transmit or are powered off.

B. Device discovery protocols

Numerous device-detection protocols have been proposed by researchers. Cabrera et al. provide a survey of many of these types of discovery protocols [18]. Discovery protocols, however, typically require devices to cooperate. They expect that, given some query by a discovery device, other target devices will respond to the query with truthful information about their identity and capabilities. Two problems prevent this approach from meeting our goal of discovering *all* devices in an area. First, devices must be aware of the discovery protocol; legacy devices may not be aware of the new discovery protocols. Second, malicious devices may attempt to evade detection by ignoring discovery queries, or perhaps worse, may masquerade as legitimate devices.

Our harmonic radar approach does not suffer from these drawbacks. It can discover and identify devices without their cooperation.

C. Traditional radar

In an application of traditional radars, ultra-high frequencies (UHF), generally in the range of 300 MHz to 3 GHz, propagate efficiently through ground and walls. The upper part of this spectrum corresponds to wavelengths narrow enough to form visible images of environments inside of which disturbances are discernible [19]. Ground-penetrating radars use UHF to find landmines, pipes, and other targets which are buried or otherwise obscured [20]. Typically, these responses are not recognized by the naked eye; feature extraction and target recognition are accomplished in post-processing [21] using signal-processing techniques. Over short ranges (less than 10 m) and with minimal penetration (under 1 cm), higher frequencies may be used to form images with resolution fine enough for a trained operator to recognize particular classes of targets [22]. An example of this sensor is the millimeter-wave technology implemented in airports to detect hazards carried by travelers, either hidden in luggage or carried under clothing [23]. These approaches, however, rely on detecting known shapes and do not generalize well to detecting electronic devices that may take any form. In contrast, ICED, can detect devices by comparing against the background noise and, if the task is identification, it matches devices to a library of known fingerprints.

D. Harmonic radar

Literature in the topic of harmonic radars can be grouped into one of three categories: the design of the radar and its components [6], [24]–[28], the detection of non-linear circuits and the mathematical modeling and analysis of this behavior [6], [29]–[33], and applications in which this technology is useful [34]–[39].

Our work most closely resembles the second area: the detection of non-linear targets. The relevant literature is focused on countersurveillance applications. This area is exactly where our work fits: we are detecting unwanted electronics in a space. Our main contribution is that we focus on *identifying* electronics rather than simply *detecting* them. Like some detection approaches [5], [6], our identification technique probes devices using frequencies to which they are likely to respond with harmonics. Most published work, in terms of identification, detects individual semiconductors (e.g., a PCB, integrated circuit, RFID tag); in reality these are components of more complex electronics. One gap in the literature, which we begin to address, is demonstrating the effectiveness of non-linear responses when the devices are shielded and when the signal is passing through multiple (i.e., millions) non-linear junctions, as is the case in out-of-the-box electronics [40].

XI. Conclusion

A robust method for detection and identification of electronic devices is a difficult, open problem, especially when requiring (as we do) the solution to detect unpowered, non-communicating devices. In this paper we leverage the non-linear response that electronics exhibit to radio waves as a means to produce a device fingerprint. Our main challenge is to develop and test the boundaries technology in tandem with the methods for analysis and classification. The paper uses a collection of 17 devices and three different fingerprinting methods to verify the identity of a device among a set of devices 'known' to the classifier. We also measure the ability of the system to detect an *unknown* device, that is, to determine that a target device is not one of the devices known to the classifier. Our results show that using a wide-range frequency sweep we were able to classify devices with an accuracy of 0.976 and, in the binary problem of flagging unknown devices, the number of false negatives was only 7.5%.

We view these results as a first step toward accurately identifying *all* electronic devices in an environment, even if the devices are powered off or try to evade detection!

Acknowledgements

This research results from the SPLICE research program, supported by a collaborative award from the SaTC Frontiers

program at the the National Science Foundation under award numbers CNS-1955805, and under Grant 2030859 to the Computing Research Association for the CIFellows Project. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors. Any mention of specific companies or products does not imply any endorsement by the authors, by their employers, or by the sponsors.

REFERENCES

[1] F. Dahlqvist and M. Patel, "Growing opportunities in the Internet of Things — McKinsey & Company,," Online at https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things.

[2] A. Das, M. Degeling, D. Smullen, and N. Sadeh, "Personalized privacy assistants for the internet of things: Providing users with notice and choice," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 35–46, Jul. 2018, DOI 10.1109/MPRV.2018.03367733.

[3] B. Perez, M. Musolesi, and G. Stringhini, "Fatal attraction: identifying mobile devices through electromagnetic emissions," in *Proceedings of the Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*. ACM, 2019, pp. 163–173.

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

[5] B. Perez, G. Mazzaro, T. J. Pierson, and D. Kotz, "Detecting the presence of electronic devices in smart homes using harmonic radar technology," *Remote Sensing*, vol. 14, no. 2, p. 327, 2022.

[6] H. Aniktar, D. Baran, E. Karav, E. Akkaya, Y. S. Birecik, and M. Sezgin, "Getting the bugs out: A portable harmonic radar system for electronic countersurveillance applications," *IEEE Microwave Magazine*, vol. 16, no. 10, pp. 40–52, 2015.

[7] Signal Hound, "VSG60A 6GHz Vector Signal Generator," Online at https://signalhound.com/products/vsg60a-6-ghz-vector-signal-generator.

[8] Infinite Electronics International, Inc., "SPA-030-38-01-SMA," Online at https://www.fairviewmicrowave.com/medium-power-amplifier-1watt-38db-spa-030-38-01-sma-p.aspx.

[9] Mini Circuits, "SLP-2950+," Online at https://www.minicircuits.com/WebStore/dashboard.html?model=SLP-2950\%2B.

[10] Ettus Research, "LP0965," Online at https://www.ettus.com/all-products/lp0965/.

[11] Mini Circuits, "VHF-3800," Online at https://www.minicircuits.com/WebStore/.

[12] Mini Circuits , "ZX60-V63+," Online at https://www.minicircuits.com/WebStore/dashboard.html?model=ZX60-V63.

[13] Signal Hound, "BB60C Real Time Spectrum Analyzer," Online at https://signalhound.com/products/bb60c/.

[14] G. J. Mazzaro, A. F. Martone, and D. M. McNamara, "Detection of RF electronics by multitone harmonic radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 50, no. 1, pp. 477–490, 2014.

[15] Scikit-learn Developers, "Scikit-learn," Online at https://scikit-learn.org/stable/whats_new/v0.23.html.

[16] J. C. Pedro and N. B. Carvalho, *Intermodulation distortion in microwave and wireless circuits*. Artech House, 2003.

[17] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," *IEEE Access*, vol. 4, pp. 2621–2648, 2016.

[18] C. Cabrera, A. Palade, and S. Clarke, "An evaluation of service discovery protocols in the Internet of Things," in *Proceedings of the Symposium on Applied Computing (SAC)*. ACM, 2017, pp. 469–476.

[19] B. R. Phelan, K. I. Ranney, K. A. Gallagher, J. T. Clark, K. D. Sherbondy, and R. M. Narayanan, "Design of ultrawideband stepped-frequency radar for imaging of obscured targets," *IEEE Sensors Journal*, vol. 17, no. 14, pp. 4435–4446, 2017.

[20] D. Shaw, K. C. Ho, K. Stone, J. M. Keller, M. Popescu, D. T. Anderson, R. H. Luke, and B. Burns, "Explosive hazard detection using mimo forward-looking ground penetrating radar," in *Proceedings of the SPIE*, 2015, pp. 94 540Z–1–94 540Z–14.

[21] K. Ranney, D. Liao, T. Dogaru, C. Tran, and L. Nguyen, "Buried target radar imaging with an ultra-wideband, vehicle-mounted antenna array," in *Proceedings of the SPIE*, 2013, pp. 87 140K–1–87 140K–11.

[22] R. Knipper, A. Brahm, E. Heinz, T. May, G. Notni, H. G. Meyer, A. Tunnermann, and J. Popp, "THz absorption in fabric and its impact on body scanning for security application," *IEEE Transactions on Terahertz Science and Technology*, vol. 5, no. 6, pp. 999–1004, 2015.

[23] D. M. Sheen, D. L. McMakin, and T. E. Hall, "Three-dimensional millimeter-wave imaging for concealed weapon detection," *IEEE Transactions on Microwave Theory and Techniques*, vol. 49, no. 9, pp. 1581–1592, 2001.

[24] T. Harzheim, M. Mühmel, and H. Heuermann, "A SFCW harmonic radar system for maritime search and rescue using passive and active tags," *International Journal of Microwave and Wireless Technologies*, pp. 1–17, 2021.

[25] G. J. Mazzaro and K. D. Sherbondy, "Filter selection for wideband harmonic radar," in *SoutheastCon*. IEEE, 2019, pp. 1–6.

[26] B. G. Colpitts and G. Boiteau, "Harmonic radar transceiver design: Miniature tags for insect tracking," *IEEE Transactions on Antennas and Propagation*, vol. 52, no. 11, pp. 2825–2832, 2004.

[27] J. Kiriazi, J. Nakakura, K. Hall, N. Hafner, and V. Lubecke, "Low profile harmonic radar transponder for tracking small endangered species," in *International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, 2007, pp. 2338–2341.

[28] I.-h. Kim, K.-s. Min, J.-h. Jeong, and S.-m. Kim, "Circularly polarized tripleband patch antenna for non-linear junction detector," in *Asia-Pacific Microwave Conference (APMC)*, 2013, pp. 140–142.

[29] K. A. Gallagher, G. J. Mazzaro, A. F. Martone, K. D. Sherbondy, and R. M. Narayanan, "Derivation and validation of the nonlinear radar range equation," in *Radar Sensor Technology XX*, vol. 9829. International Society for Optics and Photonics, 2016, p. 98290P.

[30] K. A. Gallagher, R. M. Narayanan, G. J. Mazzaro, K. I. Ranney, A. F. Martone, and K. D. Sherbondy, "Moving target indication with nonlinear radar," in *Radar Conference (RadarCon)*. IEEE, 2015, pp. 1428–1433.

[31] H. Ilbegi, H. T. Hayvaci, I. S. Yetik, and A. E. Yilmaz, "Distinguishing electronic devices using harmonic radar," in *Radar Conference (RadarConf)*. IEEE, 2017, pp. 1527–1530.

[32] A. F. Martone, K. I. Ranney, K. D. Sherbondy, K. A. Gallagher, G. J. Mazzaro, and R. M. Narayanan, "An overview of spectrum sensing for harmonic radar," in *International Symposium on Fundamentals of Electrical Engineering (ISFEE)*. IEEE, 2016, pp. 1–5.

[33] G. Mazzaro, K. Gallagher, K. Sherbondy, and K. Salik, "Detecting nonlinear junctions using harmonic cross-modulation," in *SoutheastCon*. IEEE, 2021, pp. 1–7.

[34] V. Viikari, M. Kantanen, T. Varpula, A. Lamminen, A. Alastalo, T. Mattila, H. Seppa, P. Pursula, J. Saebboe, S. Cheng *et al.*, "Technical solutions for automotive intermodulation radar for detecting vulnerable road users," in *VTC Spring Vehicular Technology Conference*. IEEE, 2009, pp. 1–5.

[35] A. Singh and V. M. Lubecke, "Respiratory monitoring and clutter rejection using a CW doppler radar with passive RF tags," *IEEE Sensors Journal*, vol. 12, no. 3, pp. 558–565, 2011.

[36] T. Aballo, L. Cabria, J. Garcia, T. Fernandez, and F. Marante, "Taking advantage of a Schottky junction nonlinear characteristic for radio frequency temperature sensing," in *European Microwave Conference (EuMC)*. IEEE, 2006, pp. 318–321.

[37] B. Kubina, J. Romeu, C. Mandel, M. Schüßler, and R. Jakoby, "Design of a quasi-chipless harmonic radar sensor for ambient temperature sensing," in *SENSORS*. IEEE, 2014, pp. 1567–1570.

[38] H. M. Aumann and N. W. Emanetoglu, "A wideband harmonic radar for tracking small wood frogs," in *Radar Conference (Radar Conf)*. IEEE, 2014, pp. 0108–0111.

[39] Z.-M. Tsai, P.-H. Jau, N.-C. Kuo, J.-C. Kao, K.-Y. Lin, F.-R. Chang, E.-C. Yang, and H. Wang, "A high-range-accuracy and high-sensitivity harmonic radar using pulse pseudorandom code for bee searching," *IEEE Transactions on Microwave Theory and Techniques*, vol. 61, no. 1, pp. 666–675, 2012.

[40] G. J. Mazzaro, K. A. Gallagher, K. D. Sherbondy, and A. F. Martone, "Nonlinear radar: a historical overview and a summary of recent advancements," in *Radar Sensor Technology XXIV*, vol. 11408. International Society for Optics and Photonics, 2020, p. 114080E.