# Evaluating the practical range of harmonic radar to detect smart electronics

Beatrice Perez*, Cesar Arguello†, Timothy J. Pierson†, Gregory Mazzaro‡, David Kotz†

*Riverside Research, Lexington, MA
†Dartmouth College, Hanover, NH
‡The Citadel, The Military College of South Carolina, Charleston, SC

MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM) | 979-8-3503-2181-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/MILCOM58377.2023.10356371

***Abstract*—Prior research has found that harmonic radar systems are able to detect the presence of electronic devices, even if the devices are powered off. These systems could be a powerful tool to help mitigate privacy invasions. For example, in a rental property devices such as cameras or microphones may be surreptitiously placed by a landlord to monitor renters without their knowledge or consent. A mobile harmonic radar system may be able to quickly scan the property and locate all electronic devices. The effective range of these systems for detecting consumer-grade electronics, however, has not been quantified. We address that shortcoming in this paper and evaluate a prototype harmonic radar system. We find the system, a variation of what has been proposed in the literature, is able to reliably detect some devices at a range of about two meters. We discuss the effect of hardware on the range of detection and propose an algorithm for automated detection.**

## I. Introduction

The Internet of Things (IoT) has embedded computation and communication abilities into everyday objects. Ranging from smart light bulbs to smart refrigerators, increasing numbers of these devices are deployed in homes [4]. This trend does not appear to be stopping any time soon; new devices come to market on an almost daily basis. The presence of many devices in an area, however, raises numerous privacy concerns. If each device is able to sense some portion of the environment, in aggregate, many devices deployed in an area may be able to infer subtle information about the area's occupants that would have otherwise been private. Additionally, some devices such as cameras and microphones may be surreptitiously placed in an area. Prior research has found harmonic radar is able to detect the presence of consumer electronics [13], [14], but the effective range of these systems has not been quantified. We address that shortcoming in this paper and discuss how harmonic radar might be used to help protect privacy.

While we focus on discovering electronic devices in a smart home, the same techniques can be applied to offices or secure areas such as Sensitive and Compartmentalized Information Facilities (SCIFs). If information leaks from those facilities via electronic devices, grave damage may result. Harmonic radar may be a way to mitigate those threats.

### A. Inventorying devices

A first step toward protecting privacy is to simply determine what devices are present. While keeping an accurate inventory of devices was an easy task in the past, a typical household today might contains dozens of devices. In the near future it will likely contain even more. For example, today is common for people to have a laptop, cell phone, tablet, and possibly other devices such as fitness trackers or smart watches that are not shared with other family members. In a family of four, that already raises the number of devices to well over a dozen. Designers have imagined other smart personal devices such as jewlry [3] and gloves [6]. These devices have not yet gained market traction, but they might in the near future. If they do, they would further increase the number of devices in a home. Additionally, the home itself might have devices such as smart lightbulbs, door locks, refrigerators, and themostats that do not belong to a particular resident, but instead provide services to all residents. Other designers have envisioned intelligent every day items such as smart forks [7] that would be used by all residents. If this trend continues, keeping an accurate inventory of devices present in a home will become increasingly difficult. It would be easy for residents to be overwhelmed by the sheer number of devices and it would be easy to forget about smart devices brought into an environment long ago.

### B. Difficult to detect devices

Aside from the sheer numbers of devices expected to be present in homes, another factor that makes creating an accurate inventory of devices in an area difficult is that some IoT devices appear to be their 'dumb' counterparts. Smart door locks, for example, may look like an ordinary door lock until their enhanced functionality is activated. Figure 1 shows an example of one such smart lock that could easily be mistaken for an ordinary lock [12]. A visual search for these types of devices will be time consuming and error prone.

In some cases, devices may be purposely hidden to learn information about home residents without their knowledge or consent. For example, there have been numerous cases where a landlord has installed hidden cameras or microphones in rental properties such as AirBnB or hotels [10]. Other hidden devices may be less ominous. For example, a landlord might install a water leak detector to alert if a pipe bursts. Monitoring water flow, however, has been shown to disclose a surprising amount of information about the habits of home occupants [11]. While we consider hidden devices an important topic, in this paper

Fig. 1: A Level Lock smart lock that appears to be an ordinary lock and might not be noticed as a smart device [12].

we are interested in quantifying the *maximum* detection range so we do not occlude devices (e.g., we do not hide them behind dry wall). We consider occlusion an area for future work.

### C. Contributions

Detecting *all* devices present in a home is becoming an increasingly daunting challenge. In this paper we examine harmonic radar in detail and make the following **contributions**:

- We explore the tradeoff between power and noise by measuring a harmonic radar system detecting devices in ideal and real-world environments.
- We explore one and two antenna configurtions and quantify the range of detection of these configurations.
- We build an automated detection algorithm that responds to changes in the noise of the system.

In Section II we discuss common device discovery methods and why harmonic radar is a good choice for detecting devices. In Section III we briefly review the fundamentals of how harmonic radars work. In Section IV we discuss our experimental set up and in Section V we discuss the practical range of harmonic radar for detecting consumer-grade electronics. Finally, we summarize our findings in Section VI.

## II. Device discovery

Researchers have proposed many methods for discovering devices present in an area. Solutions tend to fall into one of two categories: sniffers and discovery protocols. We briefly discuss each of these approaches in this section. Neither, however, accomplishes our goal of detecting *all* devices in an area.

### A. Sniffers

One way to discover devices is to 'sniff' their communications. With this approach, a sniffer device listens for network transmissions and attempts to identify the device of origin 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 or AM/FM bugs). 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). Wireless sniffers are also incapable of detecting devices that communicate on wired network connections (e.g., Ethernet, landline telephone). Finally, by design, some malicious devices may use communication techniques deliberately designed to evade detection by sniffers such as encrypting and bursting or spreading their communication across the radio spectrum [9].

Sniffers have many serious shortcomings if the goal is to detect all smart devices. In Section III we discuss how harmonic radar can detect devices regardless of their communication protocol – even if they are on standby 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 [2]. Typically, discovery protocols require devices to cooperate. They expect devices to respond to a discovery inquiry 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 respond to the protocol. Second, malicious devices may attempt to evade detection by ignoring discovery queries or may masquerade as legitimate devices.

Harmonic radar does not suffer from these drawbacks. It can discover devices without their cooperation.

## III. Harmonic radar principles

In this section we provide a brief primer on harmonic radars and discuss why this technique is well suited for device discovery. For a more detailed description of the mathematics behind harmonic radar see Perez et al. [14].

### A. Harmonic radar primer

Traditional radar transmits an RF signal towards a target and a portion of that signal is reflected from the outer portion or the encasing of the target. Assuming an otherwise empty environment, reflection indicates target detection and the time delay between TX (transmission) and RX (reception) is used to compute the range from the radar to the target. Traditional radar is linear; the set of frequencies reflected from the target is the same as frequencies transmitted, except for a slight difference imparted by relative motion between

the target and the radar (the Doppler shift). These radars, however, are not well suited to detecting electronic devices in a cluttered environment such as a home, hotel room, or office. In those environments, the reflection of small electronics will be inter-mixed with reflections from walls, furniture, and people, among other obstacles. Detecting an electronic device, particularly if small and stationary, is extremely difficult due to the clutter and the motion of irrelevant objects.

Harmonic radars are different from traditional radars. A harmonic radar transmits RF signals at frequency $f_0$ that propagates 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 [1]. These harmonics occur at different frequencies from the original transmission (primarily $2f_0$). Naturally-occurring materials and most man-made materials, such as those found in a residence or office (e.g., drywall, furniture, and so forth), 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. As shown in prior work, all electronic devices, from the simplest embedded systems to the most complex electronics, will respond harmonically to some frequency [14]. Because this technique leverages reflections from transmitted RF striking nonlinear components, it detects electronic devices even if the device's battery is removed, if the device is powered off, or is simply idle. Unlike a sniffer, it does not require the device to transmit, and unlike a device discovery inquiry, it does not require the device to cooperate.

### B. Harmonic radar device discovery in a home setting

Imagine a stationary harmonic radar system deployed to discover all electronic devices present in a home. To be practical, this system must have two characteristics: (1) enough range to cover the whole home (and possibly other areas such as a garage or outside deck), and (2) the ability to differentiate devices at different angles and distances from the harmonic radar. In Section V we discuss the range of the harmonic radar with the chosen setup. Our results suggest that a single harmonic radar tasked with monitoring an entire home (from a single location) is not practical. One solution might be to deploy multiple harmonic radars around the home, each covering a small area. Another solution would be a portable harmonic radar that is used to periodically 'sweep' a residence room-by-room. We ultimately adopt the sweep approach.

## IV. Methods

While prior research showed harmonic radar can be used to reliably detect consumer-grade electronic devices [14], our goal is quantify the range of this approach to detect real devices. We test our system with a set of six electronic IoT devices and two non-electronic items (an empty soda can and a piece of cork). We measure signal strength at twelve distances in steps of 2.5 cm to get fine grained measurements of the area we expect a response and four more distances

Fig. 2: Setup for all test devices inside the chamber. The photo shows a smart plug at 60 cm.

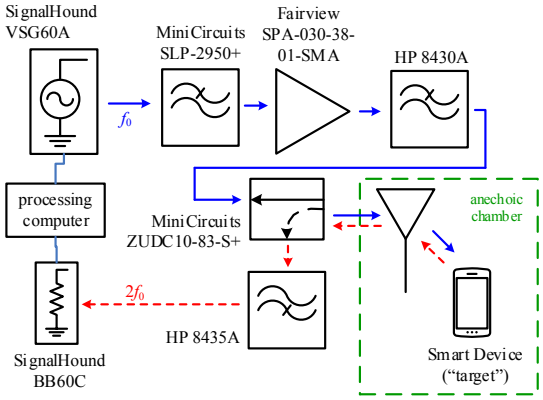



Fig. 3: Experimental setup for a single-antenna RF circuit serving both TX and RX channel.

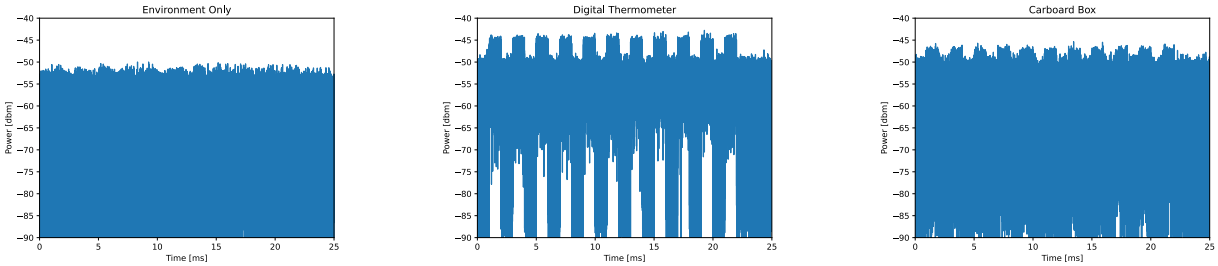
in steps of 7.5 cm to make sure that the trend is sustained. Once the response signal drops below the total noise (noise generated within the system itself, and the noise present in the environment), the target becomes undetectable.

### A. Anechoic chamber

To establish ground truth we experiment in an anechoic chamber. The benefit is that we eliminate interference from multi-path and other transmissions in the environment. Ideal conditions in the chamber guarantee that the radar captures all emissions (at the correct signal strength) for a given set of conditions (i.e., distance, components, and power settings). The maximum experimental range is bounded by the dimensions of the chamber. Our chamber is approximately 2.1 m by 1.5 m. Figure 2 shows a photo of the inside of the chamber. The device under test in the photo is a Wi-Fi smart plug.

### B. Hardware components

Figure 3 shows the block diagram for the system used to test all devices. The (independent) system variable is the transmit frequency. Previous work shows that, in general, the strongest harmonic response will be detected at a frequency at which the device being tested is designed to operate. Most IoT devices are designed to receive (RX) and transmit (TX) information




(a) Environmental Measurements (b) Digital Thermometer (c) Cardboard Box

Fig. 4: Noise present in harmonic measurement. A 1 ms pulsed wave is transmitted and the response of the first harmonic is recorded under different conditions: (a) no object placed in front of the radar, (b) a digital thermometer placed in front of the radar, (c) a cardboard box placed in front of the radar. One can observe that only background noise is present in (a) while the 1 ms pulse is present (with a small amplitude) in (c) due to the linear reflections of the system-generated harmonics leaving the transmitter; the higher amplitude of the 1 ms pulse in (b) emerges from the interference of the linear reflection of the system-generated harmonics with the harmonic response from the device's semiconductors.

at Wi-Fi or Bluetooth frequencies. To this end, we set the transmit frequency $f_0 = 2.328$ GHz.

The transmit frequency constrains the hardware choices for the system. On the TX path, we begin with a SignalHound VSG60A signal generator capable of generating frequencies up to 6 GHz, well above our target $f_0$ frequency. A MiniCircuits SLP-2950low-pass filter then reduces (and an ideal circuit would completely remove) harmonics created by the signal generator. Next a Fairview SPA-030-38-01-SMA power amplifierboosts the filtered signal. A Hewlett Packard HP 8430A bandpass filteragain reduces unwanted signal components, this time induced by the power amplifier, before sending the signal to a MiniCircuits ZUDC10-83-S+ couplerand ultimately to an Ettus Research LP0965 log-periodic antenna [5] for transmission.

On the RX path, the Ettus Research LP0965 log-periodic antenna receives any harmonics and passes them to the Mini-Circuits ZUDC10-83-S+ coupler. Because we are detecting at $2f_0 = 4.656$ GHz, a HP 8435A high-pass filter [8] reduces the base frequency $f_0$ before the harmonic signal reaches a BB60C spectrum analyzer [15].

### C. Sources of noise

RF measurements, such as those collected with a harmonic radar system, contain background signals from the environment and system-generated noise created by the radar's hardware components. Both types of noise need to be accounted for and the mitigation techniques for each are different. Figure 4 provides some insight into both types of noise. These measurements were collected using the same setup: a tripod with two grips to hold a target in place with two antennas aligned to the target (triangle placement). The change between the three measurements is the target in the grips. In Figure 4a, the grip is empty and the antennas are pointed at empty space in an open-space laboratory. The figure shows what we might expect — random noise with a floor around -50 dBm as a response to a transmitted sequence of eleven pulses.

Step two captures the response of the system with a target (i.e., a digital thermometer) in the grips. The transmit signal is a sequence of eleven pulses within the first 25 msec. The response, shown in Figure 4b, shows a one-to-one correspondence with the transmitted signal (with max value around -42 dBm) followed by environmental noise. This is the expected harmonic response at work!

The third step in the sequence replaces the digital thermometer with a cardboard box of the same size and shape as the thermometer. If the radar's hardware components successfully filtered all system-generated noise, we would expect to see the same result as Figure 4a because the cardboard box contains no nonlinear elements. Although we use several filters to eliminate noise from hardware components, we see in Figure 4c that there is still some leakage at $2f_0$ that gets transmitted. The transmit path (i.e., the components between the signal generator and the antenna) are electronic and have nonlinearities. It is the job of the low pass filters to attenuate and ideally eliminate any high-frequency components in the transmit signal. However, as in step two, the transmitted signal is a sequence of eleven pulses and Figure 4c shows that there is a non-neglegible portion that gets transmitted. The (non-electronic) cardboard box is not responding at the harmonic of the transmit frequency but rather it is responding linearly to the harmonic frequency being inadvertently emitted by the antenna (with a max value around -45 dBm). We deal with this noise using Algorithm 1 below.

### D. Antenna configuration

We use two configurations for the placement of the antennas and the targets: a linear and a triangle configuration. In the linear configuration we have one antenna that transmits and receives the signal and the target is placed directly in front of the antenna. In this configuration, a coupler separates the TX and RX paths. The coupler (Mini Circuits ZUDC10-83-S+) forces a 10 dBm loss on the system, which reduces detection range. In this paper, the distance reported in linear experiments

is the one-dimensional distance between the tip of the antenna and the front casing of the device.

The triangle configuration uses two antennas (one for RX, one for TX) placed in the vertices of an isosceles triangle. The target device makes up the third vertex. The distance reported in these measurements is the height of the triangle (from the device being tested to the side joining the antennas). The two antenna configuration is experimentally more error prone as it requires maintaining the angle between the antennas and the target constant as the range of the device is tested.

### E. IoT testbed

We use six COTS devices and two dummy targets to measure distance. Covering a range of sizes and functions, we use: two smart plugs (different brands), a blood oximeter, a thermometer, a smart thermostat, and a Bluetooth pedometer. The two dummy targets are a cork top and an empty can.

## V. Results

We explore the range of detection of the system given the limitations inherent to the hardware. We present two types of results: the harmonic signal strength over a range of distances and the output of an automated detection algorithm based on probability distributions.

### A. Harmonic signal strength

Figure 5 shows a sample of the harmonic frequency (e.g., $2f_0 = 4.656\ GHz$) signal strength collected for each target at different distances using the aforementioned linear antenna configuration in the anechoic chamber. The green dashed line is a measurement of the environmental noise taken just before transmitting a signal. The blue line is the measured (return) signal once the signal generator is transmitting a continuous wave. This value is comprised of the system-generated noise (defined in Section IV-C) plus harmonic signals re-radiated by the target device. The right-most column of the figure shows the dummy targets: cork and can. As with the cardboard box in Figure 4c, both cork and can show a small but detectable response ($\mu = -133.8$ dBm $\pm 0.86$ for the cork and $\mu = -133.9$ dBm $\pm 0.72$ for the can). While greatly reduced, tests inside the chamber show a linear response from the system-generated noise. In Section V-B, we use the system generated noise (i.e., the shift between the green line and the blue line) to improve the detection algorithm and avoid false positives.

### B. Automated detection

We expect a harmonic signal returned from an electronic device to be separable from noise. To differentiate between noise and signal, we compute the mean $\bar{x}$ and standard deviation $s$ for the environmental noise data comprised of 1,515 RX measurements collected while the system was not transmitting. Then, we calculate the standard error of the mean $\sigma_{\bar{x}}$, which shows that $\bar{x}$ is within one percent of the true mean $\mu$. We use these measurements to represent the environmental noise as a normal distribution with probability density $f(z|\bar{x}, s^2)$.

To address the system-generated noise, we correct the environmental noise with a translation in the y axis. We take as reference the readings collected from one dummy device. Conceptually, we raise the dashed green lines in Figure 5 to the solid blue lines. Practically, we approximate the shift in the environmental noise distribution by the arithmetic mean of one dummy target.

After correcting the distribution for the system-generated noise, we expect with 95% confidence that noise measurements in our setup satisfy $f(z) \geq \lambda = 0.0377$, where $\lambda$ is the probability density at the boundary of the selected confidence interval (95%)—used as threshold. Given any RX measurement $m$, it is highly probable that a target is present when $f(m) < \lambda$. Algorithm 1 shows our method for detection.

**Algorithm 1** Automated Detection Algorithm

**Input:** Rx measurements $m_1, m_2, ..., m_n$
  **for** all $m_i$ **do**
    **if** $f(m_i) < \lambda$ **then**
      return **DETECTED**
    **else**
      return **NOT DETECTED**
    **end if**
  **end for**

As a robustness and accuracy test, Algorithm 1 was applied to a dataset containing 170 RX measurements per IoT device in our test bed and 130 RX measurements of dummy targets (in the anechoic chamber with the system in the linear configuration); the results are summarized in Figure 6. The algorithm accurately rejects the dummy targets with an average 5% false positive rate. Moreover, all devices were correctly detected 100% of the time out to 5 cm. Some devices such as the Wi-Fi Plug(2) and the Pedometer are discovered more than half of the time up to 60 cm with average detection rates of 67.06% and 82.35% respectively. Hence, a harmonic-radar aided by Algorithm 1 could be effective in situations where a manual 'sweep' with a portable radar system is plausible. We also see, however, that some devices such as the Thermometer are only detected at short ranges.

One thing to note is that since $\lambda$ is dependent on the confidence level, it serves as a "sensitivity gauge". Selecting a lower confidence level (i.e., higher $\lambda$), increases the detection range at the cost of also increasing the number of false positives. Thus, the trade-offs should be evaluated before selecting an appropriate $\lambda$. Figure 7 shows the detection rates for devices in our testbed using Algorithm 1 with three values of $\lambda$ corresponding to 85%, 90%, and 95% confidence levels. As expected, we see the false positive rate for the cork and can increase slightly, but the detection ranges for the IoT devices increases significantly.

Finally, one limitation of the methodology is that the correction for system-generated noise is both linear and based on the dummy targets. In a deployed system the correction could include measurements from more linear targets accounting for variations in size, shape, and material. An ideal system would

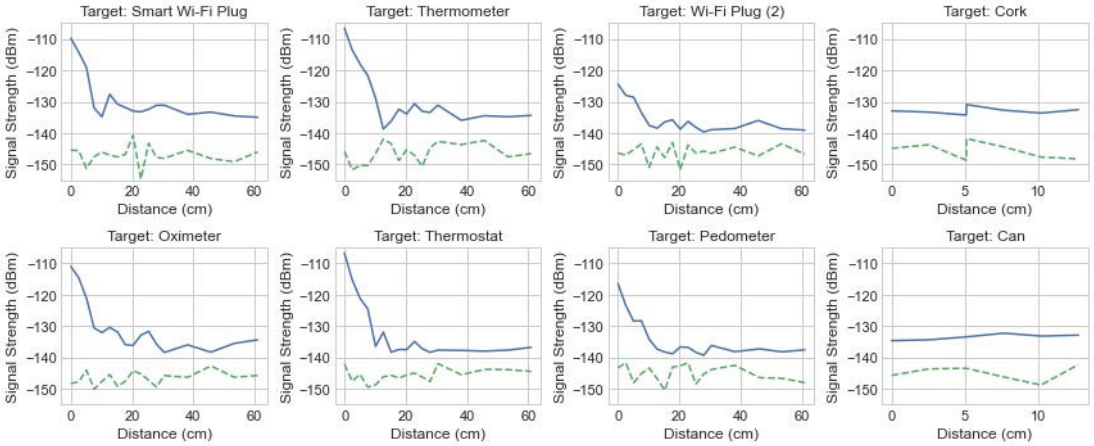



Fig. 5: Measurements per device. The green (dashed) line shows the environmental noise at the time of collection. The blue line shows the received signal strength. The blue line combines the response from the target and the system-generated noise.

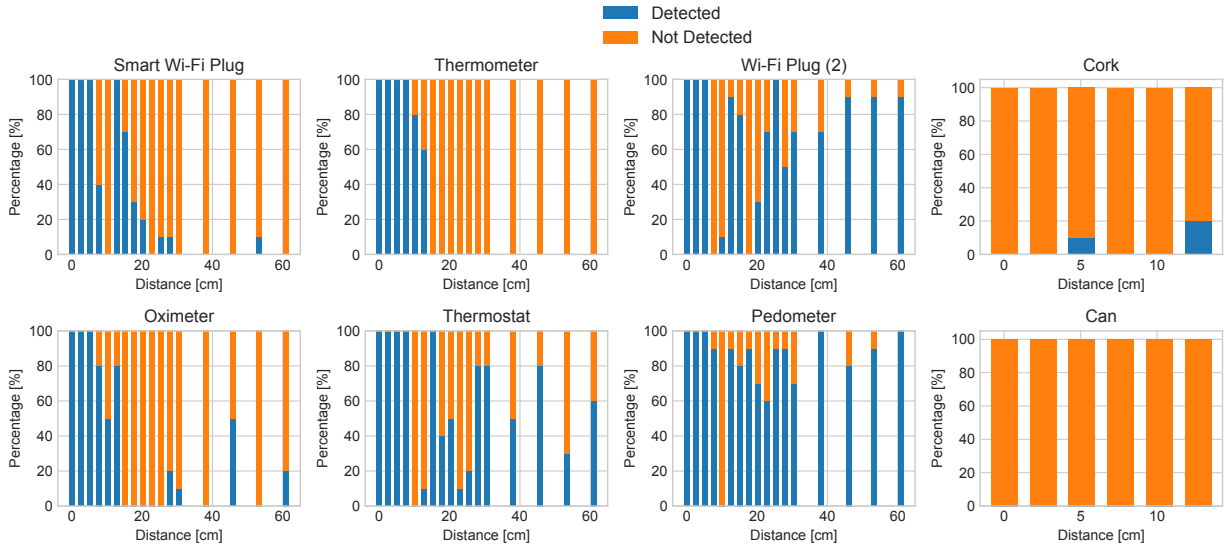



Fig. 6: Automated detection results from Algorithm 1 applied to RX measurements of all targets.

detect the shape of a target and find a correction function that matches the target's characteristics.

### C. Maximum system range

Following the linear configuration experiments for detecting small IoT devices (see Section IV-D for the different configurations), we next considered the maximum possible range for our system inside the chamber. The block diagram in Figure 9 shows the components used in the triangle configuration of this second round of experiments. Now, we use higher gain antennas, no coupler (and thus no 10 dBm penalty), and a laptop as the target device. The laptop has a more complex circuit (in terms of the number of semiconductors) than small IoT devices and we expect this complexity to increase the detection range of the system.

Transmitting at 900 MHz to the laptop inside the anechoic chamber, we see greatly increased harmonic signal strength in Figure 8. With this setup we detected the presence of the laptop to a range of 2 m – the farthest distance we could explore inside the chamber! We note, however, that even with the two antennas and a more powerful amplifier, the harmonic signal is rapidly attenuating and suspect there would not be a great deal more detection range, even with a larger chamber.

### D. Detection in the real world

Experiments in an anechoic chamber help to determine the behaviour of the harmonic radar system in ideal situations. The next step is to explore system performance in 'normal' operation, where it faces challenges like multi-path reflections and interference from other signals at and around the transmit frequency. Figure 10 shows the block diagram for this second

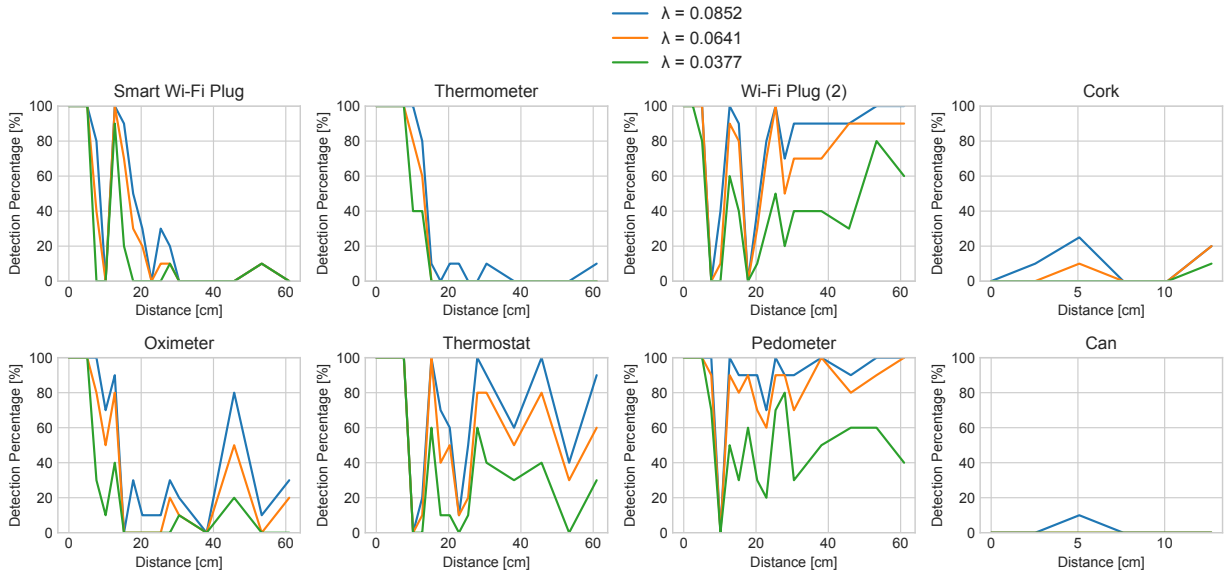



Fig. 7: Automated detection results from Algorithm 1 with $\lambda$ = 0.0852, 0.0641, and 0.0377, derived from confidence level 85%, 90% and 95% respectively.

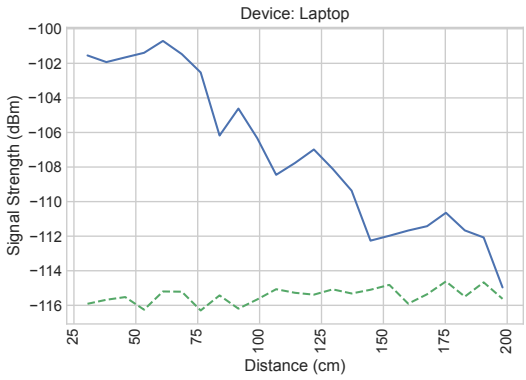



Fig. 8: Signal strength measurements for a laptop inside the chamber for the maximum distance of 2 m.

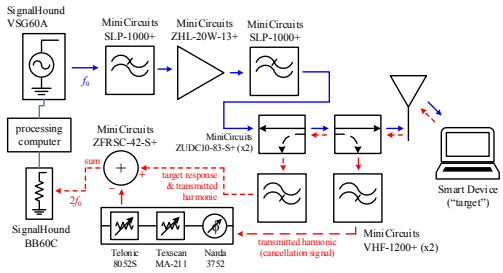



Fig. 10: Block diagram for the experimental setup in the outside detection experiment.

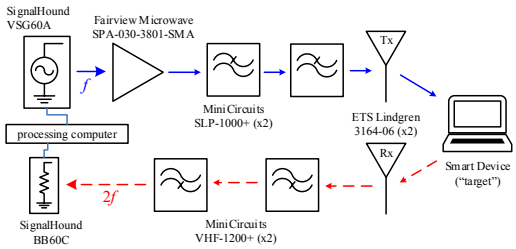



Fig. 9: Block diagram for the two-antenna harmonic radar system at 900MHz. This configuration detected the laptop inside the anechoic chamber to a range of 2 meters.

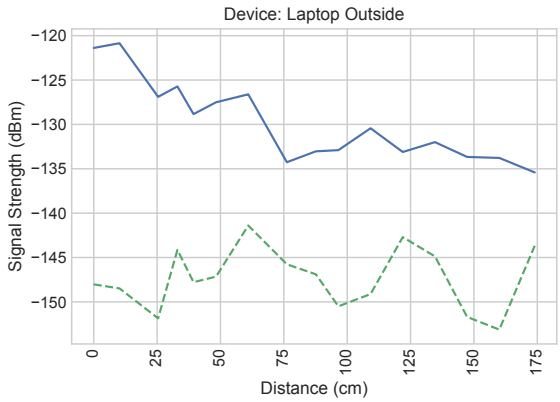



Fig. 11: Distance measurements for a laptop in open air for a maximum distance of 1.74 m

setup. The main difference from our earlier experiment is the use of a different power amplifier. The MiniCircuits ZHL-20W-13+ has a gain of approximately 50 dB (compared to the 37dBm of the SPA-030-38-01). Maintaining a clean signal at this power required the addition of the negative feedback loop composed of two couplers, the variable attenuator, and the phase shifter. In this setup, the harmonics generated by the nonlinear components of the system cancel themselves out by shifting the phase of the noise signal and adding it through the feedback loop creating destructive interference. These results are shown in Figure 11.

### *E. Power and range*

It might appear like increasing the range of detection requires simply augmenting the strength of the transmit signal – higher power leading to higher range. Experimentally (and in the literature), this is not the case. Increasing the power that flows through components has two undesirable consequences: first, the active components in the circuit (like the power amplifiers) saturate and their performance becomes unstable; and second, the noise generated by the system (which is proportional to power) stifles any response from the targets.

Similarly, initial consideration of a harmonic radar system might give the impression that range is dependant upon the target being studied. This is, again, only partially correct. For traditional radars, the area of the cross-section that reflects the signal alters the strength of the response. With harmonic radar, to detect a target the power of the transmitted signal needs to exceed an 'activation threshold' that triggers nonlinearities.

We use multiple configurations and components to automate measurements and make experiments repeatable. We add (and vary) the types of filter and amplifiers to transmit the cleanest signal possible. The main contribution of the work is to evaluate the range of a harmonic radar system, but a real-world system must deal with system-generated noise. We explored the possible software and hardware mitigation techniques that deal with that noise.

## VI. Conclusion

In this paper we experimented in a controlled environment to understand the range of a harmonic radar's ability to discover electronic devices. We saw that hardware components played a key role in determining range. Choosing two antennas (vs. one), or indeed more powerful amplifiers and filters, extend the range. With our setup, we observed a range of at least 2 meters for detecting a laptop computer (perhaps more but we were limited by the size of our chamber).

We envision a real system designed to detect electronic devices in a residential, office, or secure setting such as a Sensitive and Compartmentalized Information Facility (SCIF). One approach is to install a set of localized harmonic radars, each assigned to cover a 2 meter circular area. A more practical approach would be a portable device for making periodic sweeps of the area in search of missing or unknown devices. We believe a harmonic radar system might be invaluable in the near future, where the facilities may contain dozens (or hundreds) of devices. In this case *all* devices can be quickly discovered, even if they do not transmit or are powered off.

## Acknowledgements

This research results from the SPLICE research program, supported by a collaborative award from the SaTC Frontiers program at 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 representing the official policies, either expressed or implied, of the sponsors. Mention of specific companies or products does not imply endorsement by the authors, by their employers, or sponsors.

## References

[1] Huseyin Aniktar, Dursun Baran, Enes Karav, Eren Akkaya, Y Serdar Birecik, and Mehmet Sezgin. Getting the bugs out: A portable harmonic radar system for electronic countersurveillance applications. *IEEE Microwave Magazine*, 16(10):40–52, 2015.

[2] Christian Cabrera, Andrei Palade, and Siobhán Clarke. An evaluation of service discovery protocols in the Internet of Things. In *Proceedings of the Symposium on Applied Computing (SAC)*, pages 469–476. ACM, 2017.

[3] Hang Cai, Tianlong Yun, Josiah Hester, and Krishna K Venkatasubramanian. Deploying data-driven security solutions on resource-constrained wearable IoT systems. In *IEEE International Workshop on Internet of Things Computing and Applications (IoTCA 2017)*, pages 199–204. IEEE, 6 2017.

[4] Fredrik Dahlqvist and Mark Patel. Growing opportunities in the Internet of Things, https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things. Accessed: 2023-01-22.

[5] Ettus Research. Ettus Research, https://www.ettus.com/all-products/lp0965/.

[6] Cristian Gyozo Haba, Liviu Breniuc, Romeo Cristian Ciobanu, and Ioan Tudosa. Development of a wireless glove based on RFID sensor. In *2018 International Conference on Applied and Theoretical Electricity (ICATE)*, pages 1–6, 2018.

[7] Hapifork.com. Hapifork bluetooth-enabled smart fork. https://www.hapilabs.com/product/hapifork. Accessed: 2023-01-22.

[8] Hewlett Packard, Inc. Hewlett Packard HP 8435A, https://www.torontosurplus.com/hp-8435a-agilent-8435a-bandpass-filter-4-to-8-ghz-in-stock.html. Accessed: 2023-04-02.

[9] Georges Kaddoum. Wireless chaos-based communication systems: A comprehensive survey. *IEEE Access*, 4:2621–2648, 2016.

[10] Kim Komando. How to check for hidden cameras in Airbnb, VRBO, or vacation rentals. https://www.usatoday.com/story/tech/columnist/komando/2022/06/23/how-check-hidden-cameras-airbnb-vrbo-vacation-rentals/7652726001, 2023. Accessed: 2023-01-22.

[11] Alexia Dini Kounoudes, Georgia M. Kapitsaki, Ioannis Katakis, and Marios Milis. User-centred privacy inference detection for smart home devices. In *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, pages 210–218, 2021.

[12] Level Lock. Level Lock Smart Door Lock. https://level.co/shop/level-lock-touch-edition. Accessed: 2023-04-02.

[13] Gregory Mazzaro, Kyle Gallagher, Kelly Sherbondy, Alex Bouvy, Beatrice Perez, Timothy J. Pierson, and David Kotz. Harmonic response vs. target orientation: a preliminary study of the effect of polarization on nonlinear junction detection. In *Radar Sensor Technology XXVI*, volume 12108, pages 11–31. SPIE, 2022.

[14] Beatrice Perez, Gregory Mazzaro, Timothy J. Pierson, and David Kotz. Detecting the presence of electronic devices in smart homes using harmonic radar technology. *Remote Sensing*, 14(2):327, 2022.

[15] Signal Hound. Signal Hound, https://signalhound.com/products/bb60c. Accessed 2023-04-02.