Replicating Human Immune System via Harmonic Radar: A Framework and Preliminary Results in Thwarting Cyber-physical Attacks

Nathanael Denis, Roberto Di Pietro

Abstract—Cyber-physical attacks target the intersection of digital systems and physical infrastructure. To mitigate such threats, we introduce a methodology based on harmonic radar and image classification, inspired by the human immune system's self and non-self discrimination mechanism. We evaluate our framework with a use case focusing on authentication at the physical layer of USB devices—these latter devices being a common vector for cyber-physical attacks. Our approach achieves an average F1-score of 0.945 without requiring physical contact or activation to distinguish self from non-self devices. The results demonstrate the feasibility of the framework for reducing the attack surface in cyber-physical environments. This work lays the foundation for broader applications of harmonic radar in intrusion detection and hardware authentication.

Index Terms—Harmonic radar, Cyber-physical systems, Hardware security, Wireless security, USB, Bio-inspired security.

1 Introduction

Cyber-physical systems (CPS) are integrated systems that combine software and physical components. CPSs have experienced rapid growth over the past decade in fields such as telemedicine, smart manufacturing, autonomous vehicles, the Internet of Things, industrial control systems, and smart power grids [1]. As CPSs are integrated with network infrastructures, they are vulnerable to cyberattacks and network faults, but also to physical vulnerabilities and physical attack vectors [2]. These vectors are numerous, including widely used USB devices [3], [4]. The possibility of evading detection using obfuscation techniques, as well as the possibility of damaging the equipment used for malware detection, calls for an adapted threat detection method to mitigate cyber-physical threats.

Physical layer authentication (PLA) and fingerprinting leverage the inherent characteristics of hardware components to uniquely identify devices. These techniques use variations in power consumption, electromagnetic emissions, or signal reflections to create distinct fingerprints for devices [4], [5]. Wireless PLA is also known as radio fingerprinting when referring to the challenge of extracting features from the received signal and attributing a fingerprint, which can uniquely identify the transmitting source [6]. Physical layer approaches have been widely applied in wireless security, enabling robust authentication without reliance on higher-layer protocols.

Harmonic radar is a technology that leverages the non-linear response of a target to solicitation in the RF domain. Specific use cases include detection for electronics, but also tracking using RFID tags, e.g., to locate hornet nests [7]. In particular, when such a target receives a signal at a fundamental frequency f_0, it radiates a non-linear response which is a multiple of the original frequency; that is, non-linear targets will reflect back an infinite set of frequencies multiple of the received one: $2f_0, 3f_0$.... Due to the physical limits, higher frequencies are not easily detectable and the signal power exponentially decreases as the harmonic number grows. As a consequence, the first harmonic is usually used for detection and tracking [8]. The intuition here is that not only do the harmonic signals enable the detection of electronics, but they also their classification, hinting at a unique harmonic fingerprint for every device [9]. The devices' fingerprints collected with the harmonic radar can be used to classify electronic components.

Intrusion detection systems (IDS) based on the human immune system's (HIS) offer an innovative approach by mimicking the HIS ability to differentiate between *self* and *non-self*. By establishing a baseline self for legitimate devices, the IDS can identify deviations — non-self — indicative of cyber-physical threats, such as modified or malicious electronics. Artificial immune systems have been implemented to mitigate cybersecurity threats, such as attacks against drones [10] and ransomware detection [11]. This principle aligns with harmonic radar's capabilities. Signals at harmonic frequencies generated by electronic components can be used to create a unique fingerprint for each device and establish the HIS-inspired self of the system. Devices whose harmonic signature is not known are considered non-self, malicious, and quarantined, thus possibly preventing attacks on the cyber-physical system.

Contributions. In this paper, we aim to present the cybersecurity impacts of harmonic radar technology and bio-inspired threat detection. We detail a novel cyber-physical threat classification method leveraging the harmonic radar technology and claim the following contributions:

- We leverage harmonic radar and bio-inspired threat

Corresponding author: nathanael.denis@kaust.edu.sa
This document is a preprint. The final version will appear in DSN2025 DISRUPT Track.

detection to provide a wireless classification of electronic devices.
- The proposed methodology does not require the activation of the fingerprinted devices.
- We demonstrate the feasibility of the proposed methodology by applying it to the classification of USB sticks. It can differentiate self and non-self USB sticks with a minimum F1-score of 0.9373.

Outline. This paper is organized as follows. Section 2 introduces the background on bio-inspired models and electronic classification using harmonic radar. Section 3 details the experimental setup and presents the proposed methodology based on self and non-self classification. Section 4 explores applications in USB security, demonstrating how the methodology can detect cyber-physical threats. Section 4.2 presents experimental results, including self vs. non-self classification performance, before concluding in Section 5.

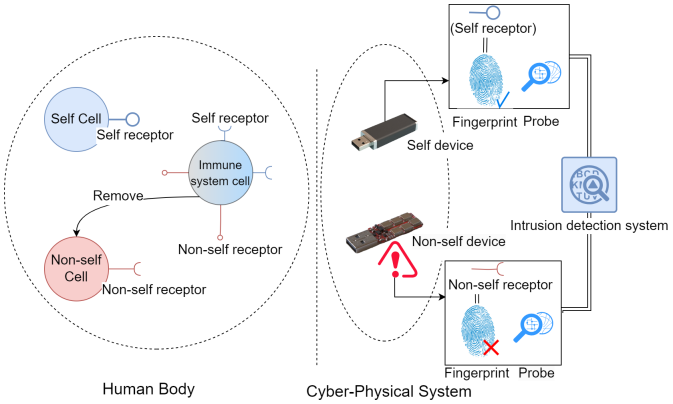


Fig. 1: Comparison of self/non-self discrimination in the human immune system and cyber-physical intrusion detection. Biological self-cells and non-self cells are represented as self-events (legitimate) and non-self events (malicious)

2 Background

2.1 Bio-inspired model

Bio-inspired model based on the human immune system (HIS) mechanisms have been successfully applied in information security for solving various challenges [12]. The immune system is a system of structures in a living body that differentiates foreign pathogens from its own cells and defends the human body against them. The unique features of self and non-self discrimination, self-organization, and parallel management, make it an ideal candidate for various applications in cybersecurity. Models inspired by the human immune systems are generally split into: 1) self and non-self discrimination; and, 2) approaches based on danger theory [12]. The latter is applied to network architectures, while the former is applied to anomaly detection [13], [14].

2.1.1 Self and non-self

Self and non-self-discrimination are based on a universal set of patterns called $\mathcal{U}$, composed of two subsets $\mathcal{S}$ and $\mathcal{N}$ such that $\mathcal{U} = \mathcal{S} \cup \mathcal{N}$. The universal set of pattern $\mathcal{U}$ is the union of the set of self-patterns $\mathcal{S}$ and the set of non-self patterns $\mathcal{N}$. By extension to the cyber-physical world, $\mathcal{S}$ can represent legitimate and acceptable events, while $\mathcal{N}$ represents illegitimate events. The resulting detection system is $\mathcal{D}(\phi, \mu)$ where ϕ represents a classification function and μ a set of selected patterns from $\mathcal{U}$ called the memory of the classification system. ϕ maps a memory set μ to a selected pattern $s \in \mathcal{U}$, with two possible boolean values *True* or *False* for normal and abnormal events, respectively [12]. Figure 1 depicts the human immune system self and non-self, as well as its extension to the cyber-physical world. In this article, we extend the principles of self and non-self-determination to detect cyber-physical threats. The self-patterns $\mathbf{S}$ contain all the normal device representations from the physical world, while the set $\mathbf{N}$ represents all the devices that are abnormal and may have been maliciously modified.

2.2 Harmonic radar

Radars are remote detection systems with a transmitter (TX) that emits an RF wave at a specific frequency f_0 and phase ϕ, and a co-located receiver (RX) that detects reflections at this frequency. The transmitted wave travels through the air, striking objects in its path; part of this energy reflects back to the receiver. A detected signal at the transmitted frequency indicates a target is within the radar's range. This type of behavior, where the return signal matches the transmitted frequency, is known as a linear response. Harmonic radars work differently, by detecting harmonic frequencies that are multiples of the fundamental frequencies, i.e., $f_1 = 2f_0, ..., f_n = (n+1)f_0$. Some objects generate harmonics when struck by the radar signal, which is known as non-linear behavior. Harmonic radar has been used in a diversity of use cases, including insect tracking [7], battery cell detection [15], or vital signs detection [16].

2.2.1 Electronics detection and classification

Objects that exhibit non-linear behavior are rare in natural environments and are most likely man-made objects, such as metal-to-metal junctions inside semiconductors. This makes harmonic radar an attractive technology for electronic detection in indoor environments. Perez *et al.* [8], [9] introduce ICED, a system that enables: 1) the identification of devices from a predefined set; and, 2) the detection of previously unknown devices. Leveraging harmonic radar technology, ICED captures signals at the first harmonic of the radar's transmit frequency, revealing fingerprints to classify electronics such as smart cameras and smart tags, even when devices lack a network interface or are powered off. In the cited paper, the evaluation on a dataset of 17 devices shows ICED achieves 97.6% accuracy when identifying known devices and 69.0% balanced accuracy when classifying unknown devices as unknown.

3 Testbed and Methodology

In this section, we describe how we processed the harmonic signal samples resulting from our data collection to classify and authenticate electronic devices. The testbed used in the experiments is provided in Section 3.1. The methodology is provided in the following Section 3.2.

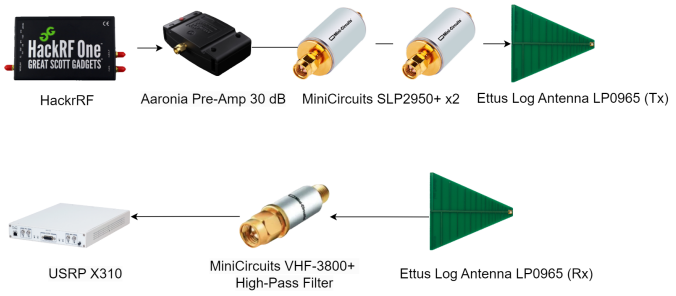


Fig. 2: Experimental setup. A HackRF signal is amplified and filtered before being transmitted to the electronics under scrutiny. The receiving side filters out the fundamental frequency and the URSP receives and amplifies the first harmonic

3.1 Testbed

A second log antenna LP0965 (RX), listens to $2f_0$. A high-pass filter removes the fundamental frequency f_0 from the collection and retains only the received harmonics components. Finally, the general-purpose software-defined radio Ettus X310 USRP amplifies and processes the signals. To process the harmonic signals, we used the open-source GNU Radio software radio ecosystem.

The implementation of the Convolutional Neural Network (CNN) was designed using Python 3.12.3 and Pytorch 2.3.0+cu118 open-source machine learning frameworks. The training, validation, and testing were carried out on a node belonging to a high-performance cluster. The GPU node used for the experiments features 4 Nvidia V100 GPUs (32 GB each) and 256GB RAM.

3.2 Methodology

The proposed methodology aims to identify the unique signature derived from the harmonic signals produced by electronics when exposed to an amplified signal. To leverage to the fullest the capabilities of computer vision algorithms, we convert the IQ samples collected by the software-defined radio to grayscale images. To this end, we compute the frequency spectrum of the samples using the Fast Fourier Transform. The Fast Fourier Transform has different sizes; the higher the size, the higher the sampling rate. Additionally, we stack several FFT samples to enrich the information inside the image.

3.2.1 Training

We train the convolutional neural network using images derived from the harmonic responses IQ samples. The resulting images are split into three datasets: the training dataset $\mathcal{D}_{tr}$, the validation dataset $\mathcal{D}_{val}$, and the testing dataset $\mathcal{D}_{test}$. The training dataset $\mathcal{D}_{tr}$ is composed of randomly shuffled images derived from the data collection and makes up 60% of the total dataset. The training is calibrated using the validation dataset $\mathcal{D}_{val}$, also generated with randomly shuffled images. $\mathcal{D}_{val}$ accounts for 20% of the total data. The training phase is run 10 times to ensure the consistency of the results. The metrics provided are the average of the 10 training rounds, the maximum, and the minimum. This reflects both the performance of the model as well as its consistency.

Once trained, the model can attribute a collection of IQ samples to a device, with an accuracy that will be determined during the following testing phase. The self of the device is determined by all the IQ samples that belong to the corresponding class, while all the harmonic signals belonging to other classes compose the non-self. For each device and its corresponding class $c \in C$ — where C is the set of all existing classes, the model is able to determine its self $\mathcal{S}_C$ and its non-self $\mathcal{N}_C$, where:

$$U = S \cup N = \bigcup_{c \in C} (S_c \cup N_c) \tag{1}$$

3.2.2 Testing

The testing dataset $\mathcal{D}_{test}$ is also generated from randomly shuffled images from the original dataset and comprises 20% of the total data generated. We define our primary evaluation metric, the F1-score, as follows:

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{2}$$

The F1-score balances precision and recall, serving as a comprehensive metric when false positives and negatives carry significant consequences [17]. After the training phase, we compute these metrics on the entire $\mathcal{D}_{test}$ dataset, which was not used during training. Here, the trained model attempts to attribute samples — converted into images — to the corresponding device. In addition to accuracy, we analyze the model's performance through precision, recall, and F1-score, which provide insights into the model's ability to correctly establish the 'self' classes and its robustness in managing class imbalances.

4 Digital Immune System: These are not my USBs

In this section, we apply the proposed methodology to fingerprint USB devices and create a self and non-self harmonic signal database, to detect potentially harmful devices such as USB Killers.

4.1 Reference scenarios

To illustrate the potential applications of this methodology, we propose two reference USB device scenarios where our methodology could provide an additional layer of security. We then experiment on the second scenario to validate the feasibility of such an approach.

4.1.1 Industrial production line monitoring

In industrial settings, maintaining the integrity of production inputs is critical. The proposed methodology could serve as a quality control tool on the production line, enabling wireless verification of USB devices without any device activation. The proposed methodology can detect non-linear features of devices and verify that each USB stick meets manufacturing specifications without excessively diverting from a reference harmonic signature. Such an application would streamline production processes, enhance

security by preventing unauthorized modifications, and potentially reduce costs associated with manual inspection. Harmonic radar monitoring in this context would ensure that only conform devices reach the consumer.

4.1.2 Cyber-physical threat detection in industry settings

Cyber-physical systems, which integrate physical processes with digital control, are vulnerable to attacks exploiting this interconnection. USB devices are a common vector for cyber-physical threats, enabling malicious actors to compromise both the digital and physical domains of secure systems. Without requiring activation or physical contact, the harmonic radar can identify potentially dangerous devices, notably USB Killers [3]. This wireless capability aligns with stringent cybersecurity protocols, offering an added layer of protection to detect cyber-physical attacks without taking the risk of destroying the sandbox used for testing.

4.2 Experimental Results

We tested the methodology with a set of 76 devices related to 19 different USB stick models. It is worth considering we investigated devices from the same brand with very similar designs, e.g., Sandisk Cruzer Blade 16GB, 32GB, and 64GB. A USB stick model refers to a specific design or version of a USB flash drive, defined by its manufacturer, features, and specifications, such as storage capacity, form factor, and supported technologies, e.g., USB 3.0. The USB sticks were never activated during the experiments. To ensure consistency, devices were placed at the same distance from the radar and in the same orientation if they belonged to the same stick model. This was to ensure that the modified distance introduced no bias.

4.2.1 Parameters

The experiments reported in this section are conducted with a fundamental frequency $f_0 = 2.5GHz$. USB 3.0 operates at a frequency of 5 gigabits per second. Harmonic signals are expected to be stronger at the frequency at which the devices operate [8]. Picking a frequency of $f_0 = 2.5GHz$ results in the first harmonic $f_1 = 5GHz$, maximizing the strength of the harmonic response. To generate the images to be fed to the CNN, we apply Fast Fourier Transform with 4096 as the FFT size and stacked 128 spectra, crafting waterfall images. The resulting images are input into Resnet34. ResNet-34 is lighter compared to deeper variants like ResNet-50 or ResNet-101, reducing computational costs and the risk of overfitting [18]. While ResNet-18 is an even lighter alternative, ResNet-34's additional depth allows for more nuanced feature extraction, making it particularly suitable for capturing the subtle patterns in harmonic radar signals. Each USB device has been illuminated by the transmitter for 15 minutes, resulting in a 1-hour collection for each class of devices.

4.2.2 Self and non-self classification

In this scenario, we aim to distinguish between self and non-self USB devices based on their harmonic signatures. The binary classification task consolidates all self devices into a single class and non-self ones into another class, reflecting practical security requirements where the primary concern is in identifying threats. In particular, we train the model to identify USB Killers, which can destroy a sandbox when powered on [3]. This experiment provides insights into the classifier's ability to generalize and differentiate between legitimate and not-legitimate categories. In this scenario, the classifier behaves as an HIS-inspired intrusion detection system where the devices whose signatures are known are considered as part of the *self*. The proposed methodology achieved an average F1-score of 0.945 (cf. Table 1). The F1-score ranges from 0.9373 to 0.9493, with an average of 0.9450. The F1-score is therefore consistent through the different rounds of training. The CNN classifier is very effective at identifying *non-self targets* and hence possibly preventing cyber-physical attacks.

Metric	Minimum	Maximum	Average
F1-score	0.9373	0.9493	0.9450

TABLE 1: F1-score metrics for self and non-self classification, with 16 USB Stick models included in the self and 3 considered non-self (76 USB sticks in total).

5 Conclusion

This paper introduced a novel bio-inspired methodology leveraging harmonic radar for wireless classification and authentication of electronic devices. By applying the human immune system's self and non-self discrimination paradigm, this approach provides a non-invasive method for detecting cyber-physical threats. Experimental results run over a PoC aiming at differentiating among USB drivers validate the methodology's effectiveness. In particular, in the self vs. non-self classification scenario, the system achieved an average F1-score of 0.945. This methodology disrupts traditional security paradigms by enabling passive, activation-free device authentication, significantly reducing the attack surface in cyber-physical environments.
Given its novelty and the preliminary outstanding results, we believe our proposed methodology has the potential to pave the way for next-generation authentication mechanisms.

References

[1] N. Jeffrey, Q. Tan, and J. R. Villar, "A review of anomaly detection strategies to detect threats to cyber-physical systems," *Electronics*, vol. 12, no. 15, 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/15/3283

[2] H. Harkat, L. M. Camarinha-Matos, J. Goes, and H. F. Ahmed, "Cyber-physical systems security: A systematic review," *Computers & Industrial Engineering*, vol. 188, p. 109891, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360835224000123

[3] N. Nissim, R. Yahalom, and Y. Elovici, "Usb-based attacks," *Computers & Security*, vol. 70, pp. 675–688, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404817301578

[4] O. A. Ibrahim, S. Sciancalepore, G. Oligeri, and R. D. Pietro, "MAGNETO: fingerprinting USB flash drives via unintentional magnetic emissions," *ACM Trans. Embed. Comput. Syst.*, vol. 20, no. 1, pp. 8:1–8:26, 2021. [Online]. Available: https://doi.org/10.1145/3422308

[5] R. Spolaor, H. Liu, F. Turrin, M. Conti, and X. Cheng, "Plug and power: Fingerprinting usb powered peripherals via power side-channel," in *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications*, 2023, pp. 1–10.

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

[7] R. Maggiora, M. Saccani, D. Milanesio, and M. Porporato, "An innovative harmonic radar to track flying insects: the case of vespa velutina," *Scientific Reports*, vol. 9, 08 2019.

[8] 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, 2022. [Online]. Available: https://www.mdpi.com/2072-4292/14/2/327

[9] B. Perez, T. J. Pierson, G. Mazzaro, and D. Kotz, "Identification and classification of electronic devices using harmonic radar," in *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, 2023, pp. 248–255.

[10] M. Shivers, C. Llanes, and M. Sherman, "Implementation of an artificial immune system to mitigate cybersecurity threats in unmanned aerial systems," in *2019 IEEE International Conference on Industrial Internet (ICII)*, 2019, pp. 12–17.

[11] O. I. Falowo, L. Edinam Botsyoe, K. Koshoedo, and M. Ozer, "Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response," *IEEE Access*, vol. 12, pp. 123 811–123 822, 2024.

[12] U. Rauf, "A taxonomy of bio-inspired cyber security approaches: Existing techniques and future directions," *Arabian Journal for Science and Engineering*, vol. 43, 02 2018.

[13] K. Saleem, G. M. Alabduljabbar, N. Alrowais, J. Al-Muhtadi, M. Imran, and J. J. P. C. Rodrigues, "Bio-inspired network security for 5g-enabled iot applications," *IEEE Access*, vol. 8, pp. 229 152–229 160, 2020.

[14] A. O. David and U. J. Joseph, "A novel immune inspaired concept with neural network for intrusion detection in cybersecurity," *International Journal of Applied Information Systems*, vol. 12, no. 30, pp. 13–17, 2020.

[15] C. Arguello, B. Perez, T. J. Pierson, and D. Kotz, "Detecting battery cells with harmonic radar," in *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2024, Seoul, Republic of Korea, May 27-29, 2024*, Y. Kim, J. Kim, F. Koushanfar, and K. Rasmussen, Eds. ACM, 2024, pp. 231–236. [Online]. Available: https://doi.org/10.1145/3643833.3656137

[16] F. Zhu, K. Wang, and K. Wu, "A fundamental-and-harmonic dual-frequency doppler radar system for vital signs detection enabling radar movement self-cancellation," *IEEE Transactions on Microwave Theory and Techniques*, vol. 66, no. 11, pp. 5106–5118, 2018.

[17] O. Rainio, J. Teuho, and R. Klén, "Evaluation metrics and statistical tests for machine learning," *Scientific Reports*, vol. 14, no. 1, p. 6086, 2024.

[18] J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, B. Shuai, T. Liu, X. Wang, G. Wang, J. Cai, and T. Chen, "Recent advances in convolutional neural networks," *Pattern Recognition*, vol. 77, pp. 354–377, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0031320317304120