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

Nathanael Denis and Roberto Di Pietro
nathanael.denis@kaust.edu.sa





King Abdullah University of Science and Technology

June 25, 2025 DSN2025

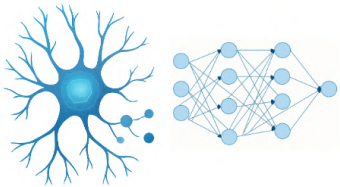
Introduction

- Bio-inspired technologies
- Replicating the Human Immune System
  - Conceptual aspects
  - Digital Immune System
- Implementation using Harmonic Radar
  - Principles
  - Results

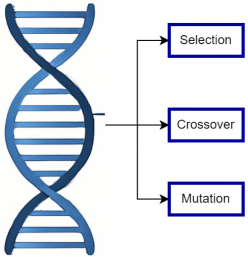
Bio-inspired technologies

Biology has inspired major discoveries in the digital world:

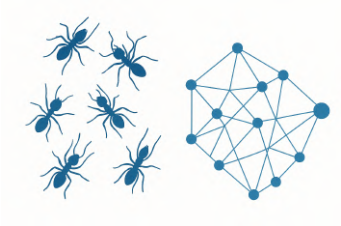
- Neural networks
- Genetic algorithms - Optimization
- Swarm intelligence - Routing



(a) Neural networks



(b) Genetic algorithm



(c) Swarm intelligence



Can biology also inspire the way we defend cyber-physical systems?

Applying human biology to cyber-physical systems

Replicating the Human Immune System

The Human Immune System (HIS) is based on self and non-self discrimination:

- Cells have receptors
- Immune system cells remove cells whose receptors are known to be non-self, e.g., T cells
- Immune system cells also remove cells with unknown receptors, e.g., Natural killers (NK)

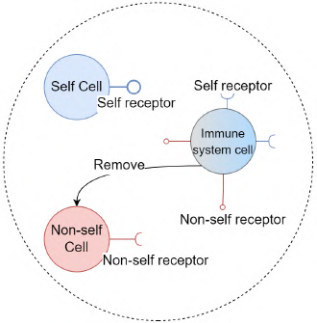


Figure 3: Human Immune System - Conceptualized

A digital HIS replicates the human immune system by attributing receptors to events or objects:

- Legitimate events or items have a known fingerprint, used as a receptor
- Known illegitimate events or unknown events are deemed suspicious.

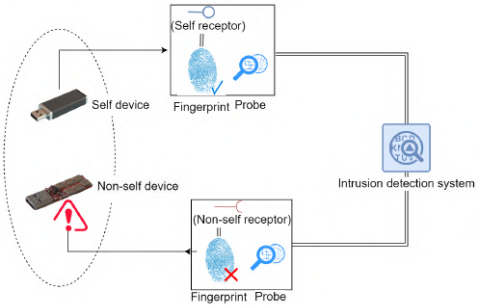


Figure 4: Digital Immune System



How to implement a digital immune system for cyber-physical systems?

Creating the fingerprints and the probe

- Radar is usually used to locate targets, emitting and listening at the same frequency f_0
- Harmonic radar instead emits at f_0 and listens to the multiple frequencies, i.e., $2f_0, 3f_0 \ldots$

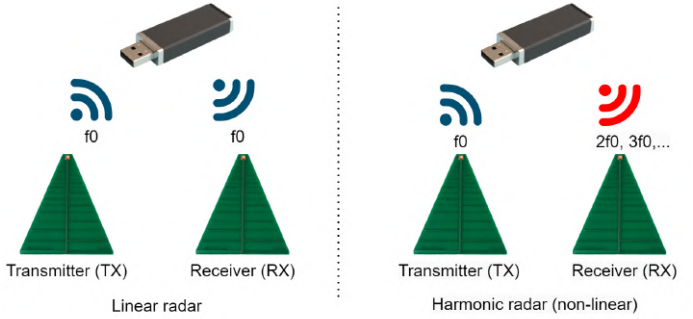


Figure 5: Comparison between linear and harmonic radar

- Only specific items re-emit at multiple frequencies, e.g., semiconductors.

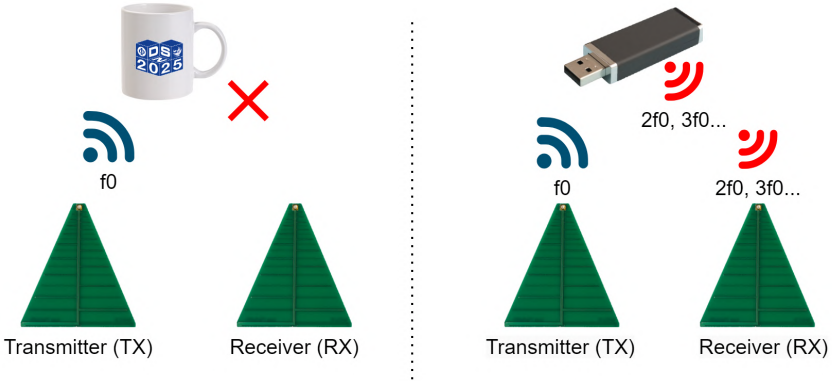


Figure 6: Detection of non-linear objects with harmonic radar

Implementation using Harmonic Radar

- Signals are unique to each class of device
- It is possible to turn the resulting signals at $2f_0$ into spectrograms
- Spectrograms are classified using convolutional neural networks

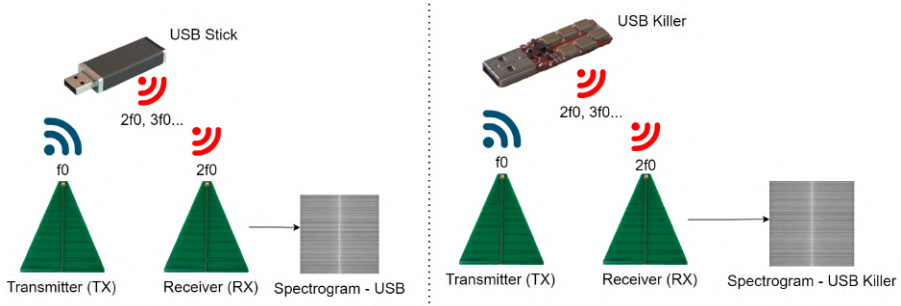
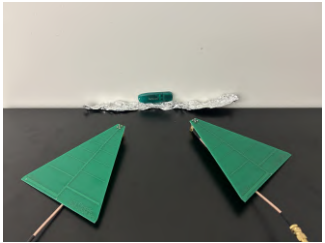
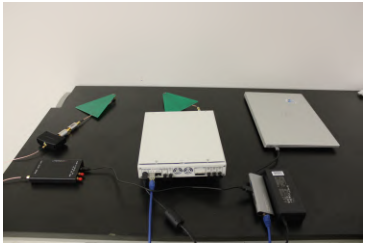


Figure 7: Detection of non-linear objects with harmonic radar

Implementation using Harmonic Radar



(a) USB stick in direct line-of-sight



(b) Harmonic radar - Setup



(c) USB sticks used for experimental campaign

Results

- **Goal**: Distinguish *self* (legitimate) vs. *non-self* (USB Killer) devices by their harmonic signatures.
- Trained on **16** self models vs. **3** non-self models (76 sticks total).
- Consistently high performance across rounds:
  - **Average F1-score**: **0.945**
  - Range: 0.9373 – 0.9493
- Classifier is effective at flagging potentially destructive devices **before power-up**.

Metric	Min.	Max.	Avg.
F1-score	0.9373	0.9493	0.9450

Open research questions



The proposed instance of a digital immune system raises several questions and research directions:

- How to handle an unknown device class?
  - Distance-based approach
  - Autoencoders
- How to handle a misclassification?
  - Multi-layer security

Conclusion



- Applied human immune system to cyber-physical systems
- Created fingerprints from harmonic radar spectrograms
- Classified spectrograms using convolutional neural networks
- Detected and flagged malicious (non-self) devices based on the fingerprints



Questions ?