The Day-After-Tomorrow: On the Performance of Radio Fingerprinting over Time

Saeif AlHazbi
Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University
Doha, Qatar

Savio Sciancalepore
Eindhoven University of Technology
Eindhoven, Netherlands

Gabriele Oligeri
Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University
Doha, Qatar
What is Radio Frequency Fingerprinting? (1/2)

Identification of the transmitter at the physical layer

- Two identical transmitters DO not exist
- The hardware differences of the transmitters are reflected into the over-the-air signal
- The receiver detects the differences in the signals and identify the transmitter
What is Radio Frequency Fingerprinting? (2/2)

Data collection

• Data from radio spectrum is collected in the form of I-Q samples.

Data processing – Deep learning

• Data preparation
• Training
• Testing
Challenges of Radio Frequency Fingerprinting (1/3)

Impact of channel noise (multipath) in the RFF process

- Amplitude
- Phase
- ... fingerprint
Challenges of Radio Frequency Fingerprinting (2/3)

Impact of the channel in the RFF process

Current state of the art

Impact of the channel in the RFF process

Current state of the art
Challenges of Radio Frequency Fingerprinting (3/3)

One missing important factor

We define **power cycle** as the process involving the software and hardware (re-)initialization of the radio. This takes place by applying the power-off/power-on of the radio.
Measurement set-up

The power cycle effect

We tested our assumption against a wired and wireless link

We considered 5 transmitters and 1 receiver
- USRP X310

Datasets:

<table>
<thead>
<tr>
<th>Link</th>
<th>Sample Rate [Mps]</th>
<th>Duration [Days]</th>
<th>Runs</th>
<th>Samples per Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS1</td>
<td>Wired</td>
<td>1</td>
<td>3</td>
<td>144M+</td>
</tr>
<tr>
<td>DS2</td>
<td>Wired</td>
<td>0.256</td>
<td>18</td>
<td>33B+</td>
</tr>
<tr>
<td>DS3</td>
<td>Radio</td>
<td>1</td>
<td>4</td>
<td>144M+</td>
</tr>
</tbody>
</table>

Run: the sequence of 6 consecutive measurements where the receiver is the same while the transmitter changes every time among all the available ones (no power-cycle).
Analysis plan

1. **Experiment E3**
   - Cable link: multipath does not exist
   - Proof that the power cycle affects measurements taken close in time (standard RFF approach)

2. **Experiment E4**
   - Proof that measurements taken in different days (no power cycle) experience high classification accuracy (standard RFF approach)

3. **Analysis of E3 to mitigate the power-cycle effect**
   - Finding a mitigation strategy for the power-cycle

4. **A real case study with the wireless link**
Experiment E3

- Power cycle affects classification accuracy
- Measurements taken one after the other
- Cable: No multipath
- Dataset DS1
Experiment E4

Measurements taken in different days experience high classification accuracy **when radio are not power-cycled**

- Cable: No multipath
- Dataset DS2
Mitigating the power cycle effect

We propose an alternative technique to classify data:

- Avoid using raw IQ samples (standard RFF approach)
- We generate images from IQ samples
- We use the images as input for Convolutional Neural Networks
Experiment E3… with mitigation strategy

Translating IQ samples into images boosts the performance

When the number of runs is high enough, our solution reaches accuracy level close to 100%
A real case study with the wireless link

Let us consider a real wireless scenario

- TX-RX distance of 10 meters
- No Line of Sight
- Office environment
- People moving around in the close proximity

Image-based classification achieves better performance than raw IQ samples (standard RFF approach)

- ResNet50
- 100,000 samples per image (1/10 of second)
Conclusions

Power-cycle has major impact in RFF

The problem can be mitigated but there are still open challenges to address

Image-based RFF classification turns out to be effective to boost RFF performance