## 

Proposal

**manifetch**

İrem Onaran

Merve İçkilli

Sacide Sena Filiz

Şevval Neva Varol

## Topic #

### 1. Project Title

**RF Fingerprinting System for Spoofing Detection with Real-Time Dashboard**

### 2. Problem Definition & Objectives

* **Problem Definition:** Wireless systems are vulnerable to spoofing attacks where attackers forge software identifiers such as MAC addresses. RF fingerprinting can detect such attacks by analyzing physical-layer characteristics. However, existing solutions often lack user-friendly interfaces. A combined approach that both detects spoofing and presents results in an intuitive dashboard can provide a practical and demonstrable security solution.
* **Objectives:**
* Capture RF signals and extract device fingerprints using SDRs.
* Detects spoofed identities by comparing fingerprints with reported identifiers.
* Design a real-time dashboard to visualize active devices, spoofing alerts, and device statistics.
* Deliver a demonstrable prototype that highlights both technical and usability aspects.

### 3. Scope

### Develop spoofing detection models based on RF fingerprints.

### Implement visualization dashboard for real-time monitoring.

### Proof-of-concept with 3–5 devices under controlled spoof scenarios.

### 4. User Profile

* **Target Users:**
  + Network security professionals.
  + IoT administrators.
  + Wireless research labs.

### 5. Anticipated Challenges & Constraints

* **Technical hurdles**
  + Achieving real-time spoofing detection accuracy.
  + Integrating ML pipeline outputs into a responsive dashboard.
* **Time/resources limits**
  + Limited SDR hardware.
  + Project restricted to one semester.
* **Ethical or regulatory considerations**
* Passive reception only, no active transmissions.
* Spoofing limited to test devices owned by the team.

### 6. Data Sources

### I/Q datasets collected via SDR.

### Controlled spoofing attack data (altered MAC identifiers).

### Dashboard input = model outputs + metadata.