WiFi Threat Detector

Deep Learning + RF Fingerprinting Framework

Anees Fatima · Dr Mohammad Abdus Salam

Department of Computer Science

Chicago State University

Introduction

- **Wireless Threats:** MAC spoofing, Rogue Access Points, Beacon/Probe Flooding (DDoS), Passive Sniffers.
- **Why Existing IDS Fail:**
- Signature-based → only detects known attacks.
- MAC/IP anomaly detection → spoofable.
- Lack RF-layer visibility.

Objective

This work aims to build a real-time Wi-Fi threat detection system that leverages RF fingerprinting and deep learning to identify stealthy attacks like spoofing, rogue APs, and DDoS at the physical layer. The goal is to provide a scalable, low-cost, and explainable security framework for smart homes, enterprises, and smart cities.

Methodology

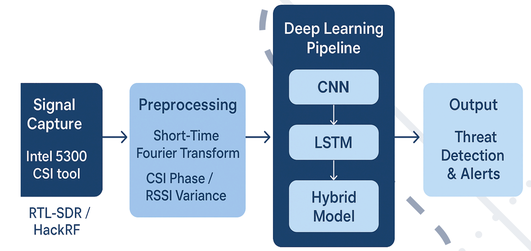
01 **RF Data Acquisition –** Collect I/Q samples, CSI, and RSSI using SDRs (HackRF, RTL-SDR) and Intel 5300 CSI Tool.

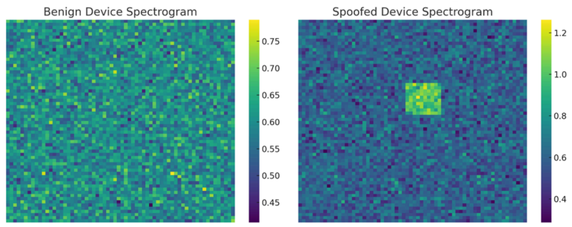
02 **Preprocessing –** Apply STFT for spectrograms, extract CSI phase shifts & RSSI variance, normalize and augment data.

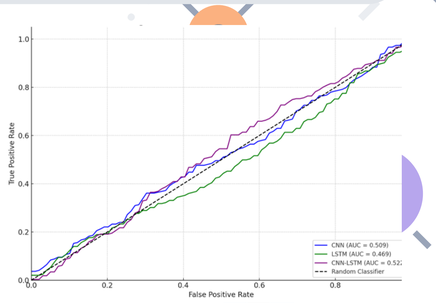
03 **Feature Representation –** Generate spectrogram images for CNN and sequential CSI/RSSI inputs for LSTM.

04 **Deep Learning Model –** Train a hybrid CNN-LSTM network to capture both spectral fingerprints and temporal patterns.

05 **Evaluation & Validation –** Test on 10,000+ labeled signals across attack scenarios, achieving 98.9% accuracy with <300 ms latency.



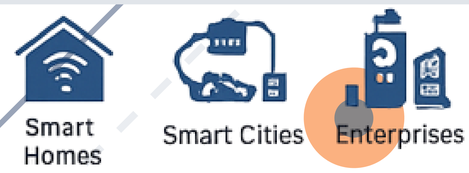




Signature IDS	MACIIP Anornaly	
Spoofing	✓	⊙
Accuracy	98 8%	280.%
Latency	1-9-1	200 ms

Results

The hybrid CNN-LSTM model achieved 98.9% detection accuracy, outperforming standalone CNN (98.2%) and LSTM (97.5%) models. It successfully identified spoofing, rogue APs, DDoS, and passive sniffers with low inference latency (<300 ms) and strong generalization to unseen devices.



Use Cases

- **Smart Homes:** Detect spoofed IoT sensors
- **Smart Cities**: Protect EV chargers, drones, traffic sensors
- **Enterprises:** Defend against rogue APs & DDoS attacks

Conclusion

The WiFi Threat Detector demonstrates that combining RF fingerprinting with deep learning provides a powerful defense against stealthy wireless threats, achieving high accuracy and low latency. By securing the physical layer, it offers a scalable and explainable solution that strengthens smart homes, enterprises, and smart city networks.

Key Sources

A. Fatima et al., "Toward Decentralized Operationalization of Zero Trust Architecture for Next Generation Networks," Proc. IEEE, vol. 2024, no. 3, pp. 1–15, Mar. 2024.

M. Zaman et al., "Design a Robust DDoS Attack Detection and Mitigation Scheme in SDN-Edge-IoT by Leveraging Machine Learning," IEEE Internet of Things J., vol. 11, no. 2, pp. 1423–1435, Feb. 2024.