

Adversarial Attacks against Wifi Based Sensing

Oskar Iwaniuk and Brian Chacon
Mentors: Dr. Minsung Kim & Dr.
Byungjun Kim

Team

Landscape

Opportunities

Timeline

The Team



Oskar Iwaniuk



Brian Chacon



Dr. Minsung Kim

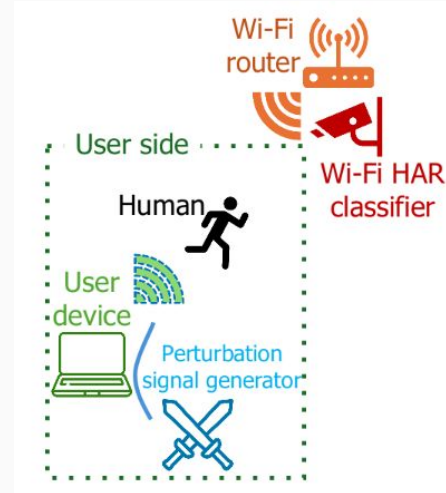
Mentor



Dr. Byungjun Kim

Mentor

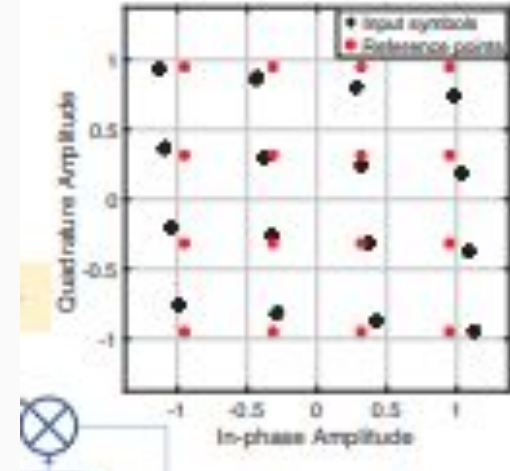
- Research Wifi Based Sensing
- Explore Adversarial Attacks



Wifi Fingerprinting

Wifi Fingerprinting

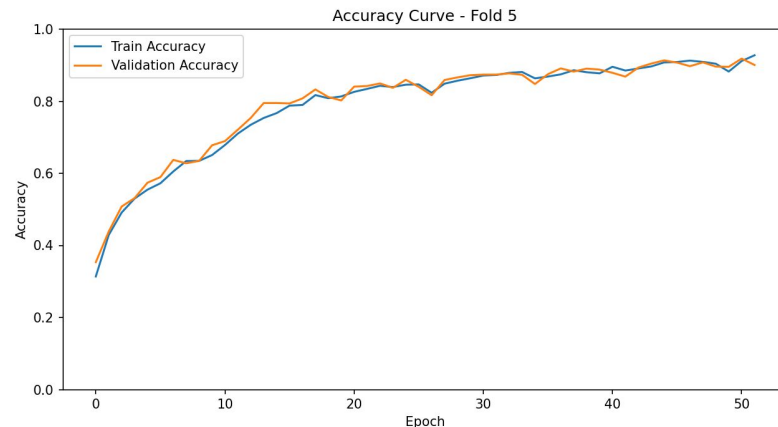
- Uses hardware imperfections to detect Carrier Frequency Offset



Wifi Human Activity Recognition

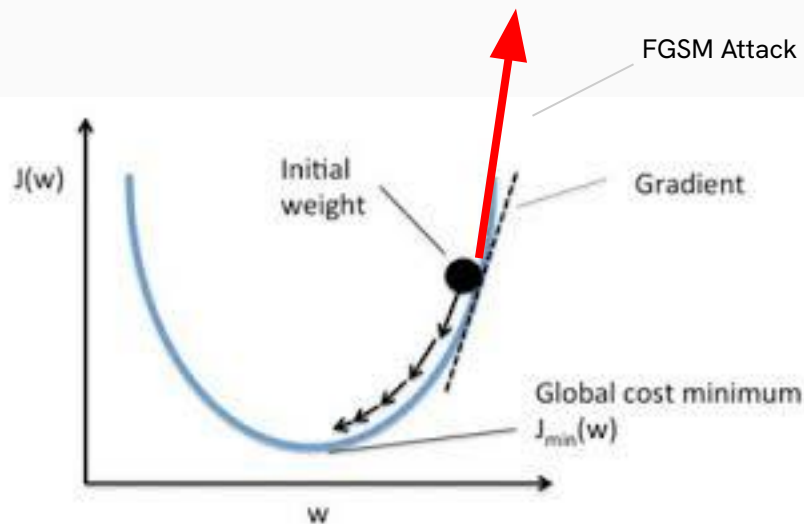
Wifi HAR

- WiFi-based HAR detects human activity
- WiFi signals reflect off people moving between devices and the router.



Fast Gradient Sign Method (FGSM)

$$x^{adv} = x + \varepsilon \cdot \text{sign}(\nabla_x J(x, y_{true})),$$

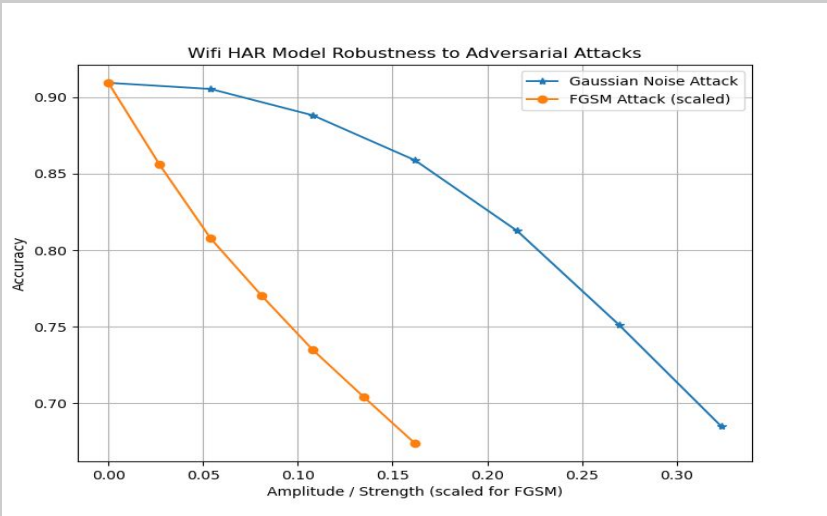


Gaussian Random Signal Noise

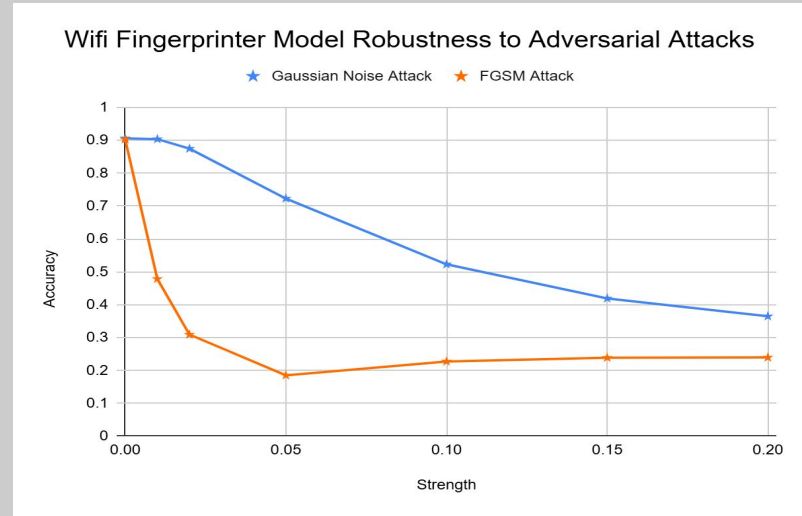
$$x_{noisy} = x_{original} + N(\mu, \sigma^2)$$



Project results



Wif HAR



Wifi Fingerprinter

Thank you!
