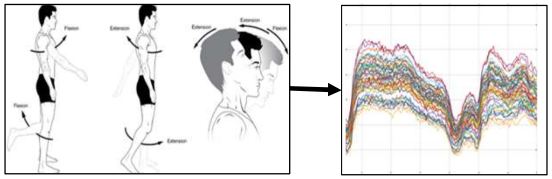
RUTGERS
WINLAB | Wireless Information Network Laboratory

Mobile Sensing System

Ethan Lung (HS), Damon Lin (UG), Rut Mehta (UG), Jacob Morin (UG)
Advisors: Prof. Yingying Chen

Background

- Channel State Information (CSI) based application
  - WiFi channel response varies according to human movements
  - CSI can be used to train deep learning model for classification



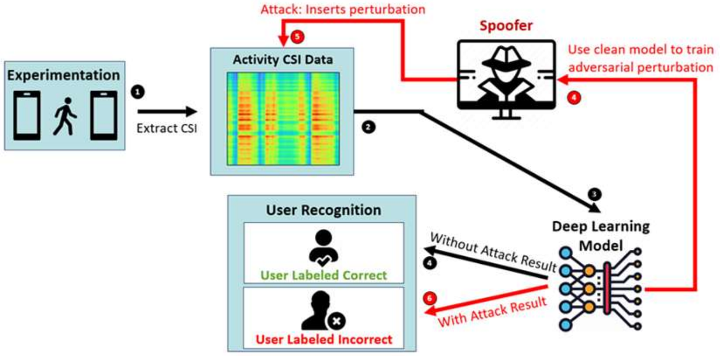
- Adversrial attack against WiFi sensing
  - CSI sample can be modified by adversarial perturbation to deceive the DNN model
  - Targeted universal perturbation: Users do kicking, but the model only recognize as walking

Objective

- Study the Security of WiFi sensing systems under adversarial attack
- Utilize mobile device to extract channel state information (CSI) to train deep learning model for recognition tasks
  - Human Activity Recognition and User Authentication
- Develop a type of adversarial attack algorithm to generate perturbation that can deceive the deep learning model

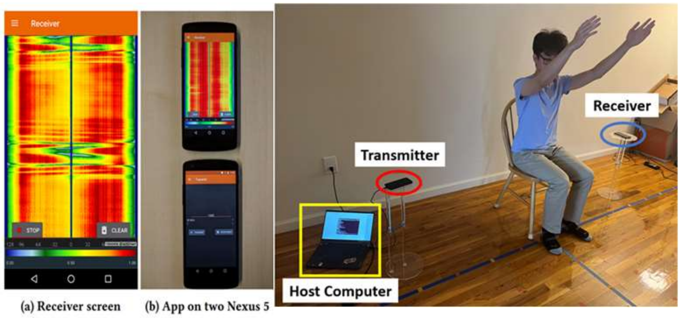
Main Challenges

- Extracting CSI from Mobile Devices
  - Nexus phones were not connecting to Wi-Fi
- Building an efficient and robust model trained by input CSI
- Generating an effective adversarial attack against the model



Experiment Procedure

- Set up mobile phones on Linux system, and enable the ability to extract Channel State Information (CSI)
- Used two mobile phones to transmit and receive WiFi packet
  - Receiving Nexus 5 extracts CSI data from the kernel
  - Performed daily movements such as: Walking, squatting, raising arms, kicking, sitting

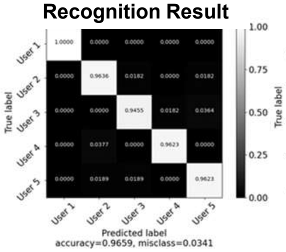


(a) Receiver screen (b) App on two Nexus 5

Results

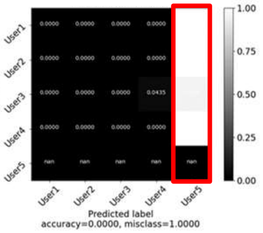
- Clean Model Recogniton Result
  - Model is able to achieve recognition accuracy at 96% for User authentication
- Attack result on User Authentication
  - Overall attack success rate can reach to 80%

Clean Model Recognition Result



accuracy=0.9659, misclass=0.0341

Attack Result for User 5



accuracy=0.0000, misclass=1.0000

Future Work

- Run more experiments on other humans to increase user authentication accuracy
- Attack testing on Human Activity Recognition

Acknowledgements

We would like to thank our advisor Dr. Yingying Chen and our mentors Changming Li, Honglu Li, and Tianfang Zhang for their support throughout this project.

Reference

[1]Carlini, Nicholas, and David Wagner. "Towards evaluating the robustness of neural networks." 2017 ieee symposium on security and privacy (sp). Ieee, 2017.

WINLAB

This work was supported by the NSF REU program