Security in Artificial Intelligence

Week 7

Ethan, Damon, Rut, Jacob

what to add/include

background slides for new people (1-2 slides)

- basic info

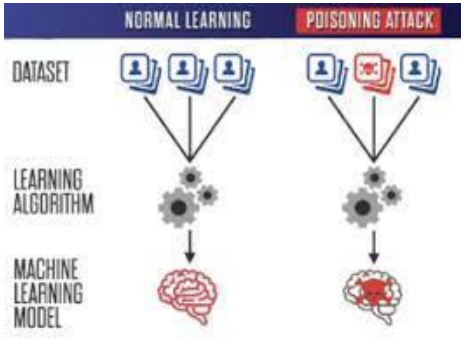
progress:

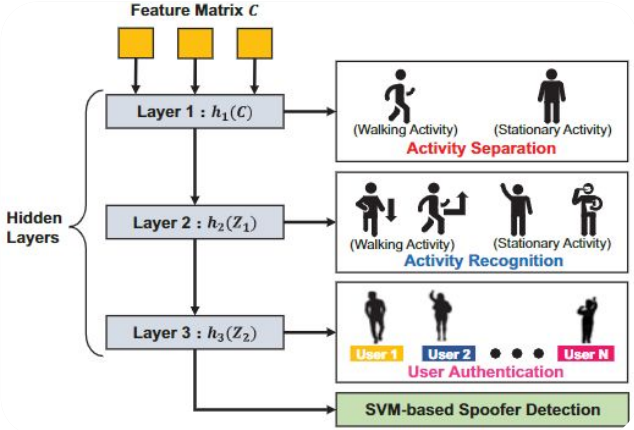
- obtained two new phones from last week (Nexus 4 + 5)
- Nexus 4 was incompatible with nexmon
- Nexus 5 is insanely buggy (screen flickers and dies + good boot up attempt every ~30 tries)
- set up firmware on both Nexus 5's
- attempting to collect data (7/18)

Project Overview

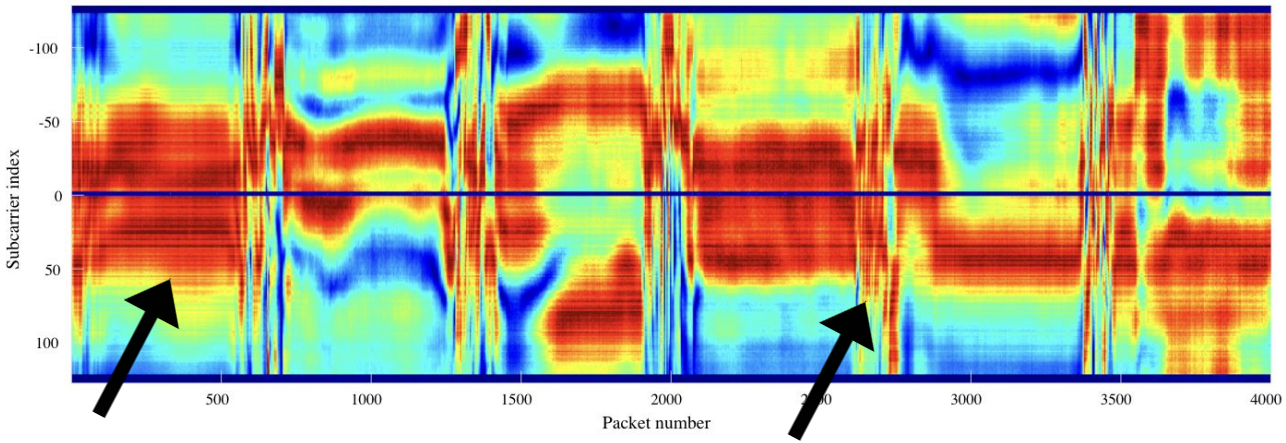
- The project aims to study methods of user authentication through IoT Channel State Information (CSI Data)

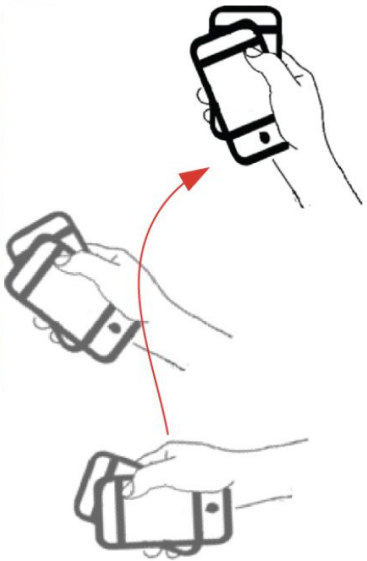
- The project also focuses on developing techniques to mitigate backdoor attacks and enhance the security of AI-enabled mobile and IoT devices.





CSI Amplitudes





Steady phone
- Stable wireless channel

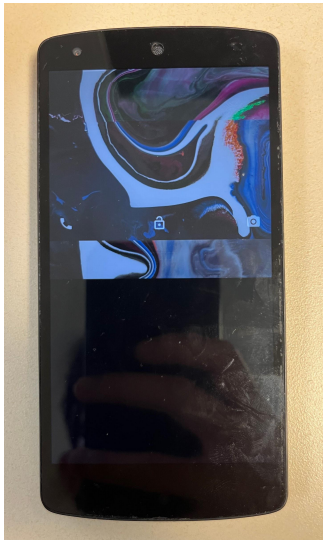
Shaking device
- Rapid fluctuations in CSI

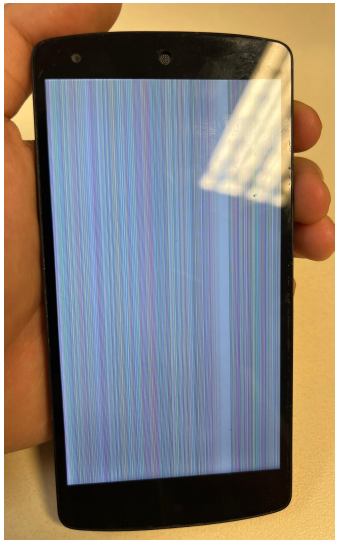
Expectations

=

Reality

≠





Annoying data

```
hammerhead:/ # nexutil -Iwlan0 -m1
hammerhead:/ # tcpdump -i wlan0 -c 50 -vv dst port 5500 -w /sdcard/csi.pcap
tcpdump: listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 b
ytes
^C0 packets captured
17 packets received by filter
0 packets dropped by kernel
23 packets dropped by interface
```

t... / Human-Activities-Gestures-Recognition-using-Channel-State-Information-CSI-of-IEEE-802.... Type / to search

Code | Issues 3 | Pull requests | Actions | Projects | Security | Insights

Human-Activities-Gestures-Recognition-using-Channel-State-Information-CSI-of-IEEE-802.11n Public

Watch 8 | Fork 14 | Star 40

master | 1 branch | 0 tags | Go to file | Add file | Code

tahmidzbr Update README.md 095269c on Sep 19, 2021 13 commits

README.md	Update README.md	2 years ago
extract_time_information.m	Update extract_time_information.m	5 years ago

README.md

Human Activities, Gestures and Fall detection using Channel State Information (CSI) of IEEE-802.11n Devices

This repository is to make the dataset collected for Human activities using the Channel State information (CSI) of IEEE 802.11n devices. As of this time, we are waiting for our papers to be published.

UPDATE (2021-09-19): If you are interested in our dataset please contact me at tahmidzbr@ece.ubc.ca

(i) Our first paper has been published using preliminary results: WiHACS: Leveraging WiFi for human activity classification using OFDM subcarriers' correlation https://ieeexplore.ieee.org/document/8308660

(ii) The thesis outlining details can be found here: Using Wi-Fi channel state information (CSI) for human activity recognition and fall detection https://open.library.ubc.ca/cIRcle/collections/ubctheses/24/items/1.0365967

About

This is a data-set for Human Activities & Gestures Recognition (HAGR) using the Channel State information (CSI) of IEEE 802.11n devices

machine-learning | deep-neural-networks | deep-learning | signal-processing | wi-fi | human-activity-recognition | time-frequency | channel-state-information | intel-5300

Readme
Activity
40 stars
8 watching
14 forks
Report repository

Releases

No releases published

Plan for Next Week

- Fix Wifi connectivity issue with mentors
- Run Nexmon on Nexus 5's
- Collect CSI Amplitudes data
- Generate Artificial Data