

# **Misbehavior Detection System for Cellular Vehicle-to-Everything Networks**

---

## **Final Critical Design Review**

Customer: Dr. David Starobinski

Grad Advisor: Stefan Gvozdenovic

Michael Aliberti, Max Ellsworth, Jason Inirio,  
Samuel Krasnoff, Julia Zeng, and Yixiu Zhu

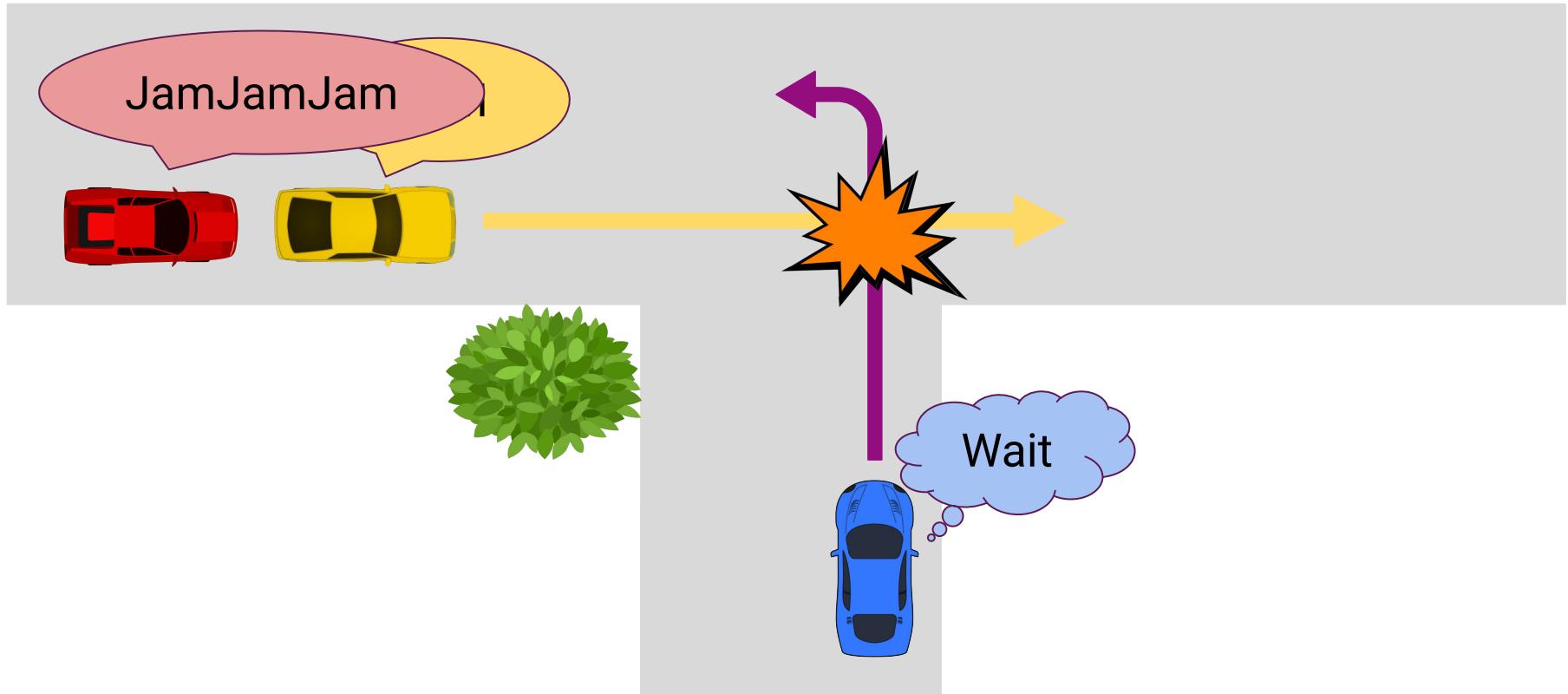


# Overview

- Problem Statement
- Requirements
- C-V2X Protocol
- Experimental Setup
- Software Libraries
- Demo:
  - Cellular Bitrate Tests
  - C-V2X Transmit
- Signal Analysis
- Progress
- Gantt Chart



# A Quick Visual

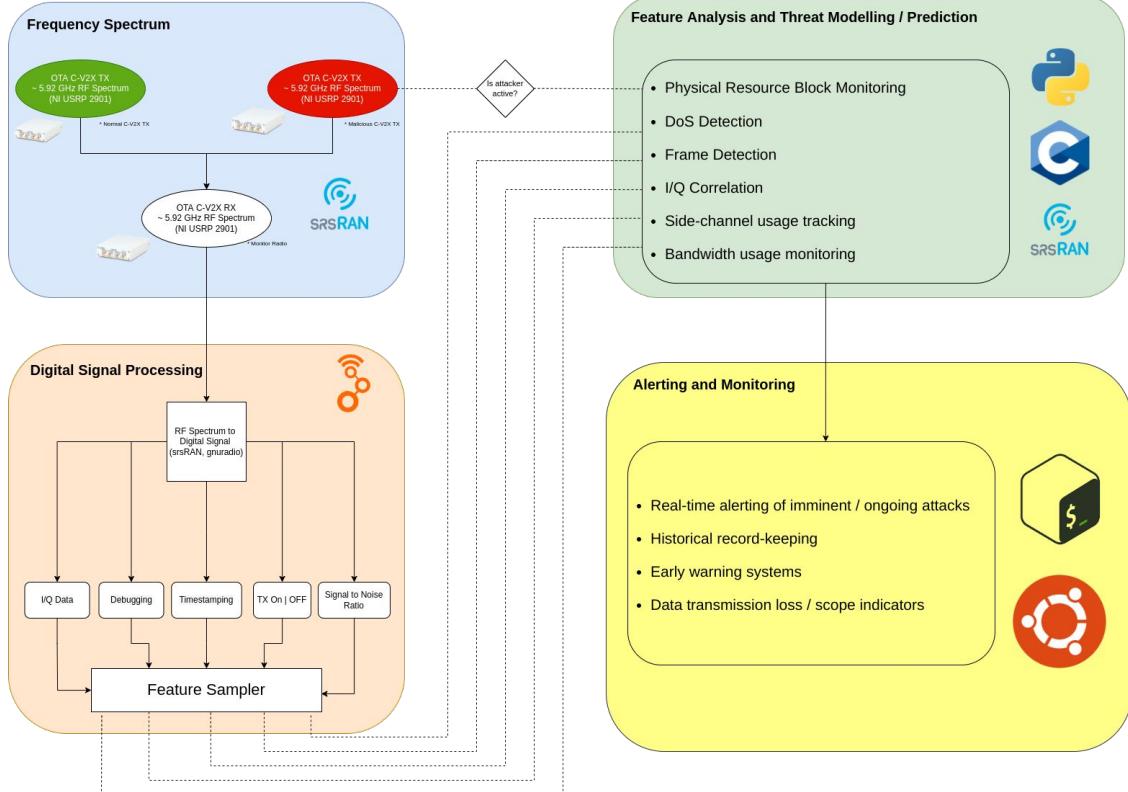


# Problem Statement

To thoroughly understand the effectiveness of the C-V2X standard, we must analyze physical layer attacks on nodes in the network.



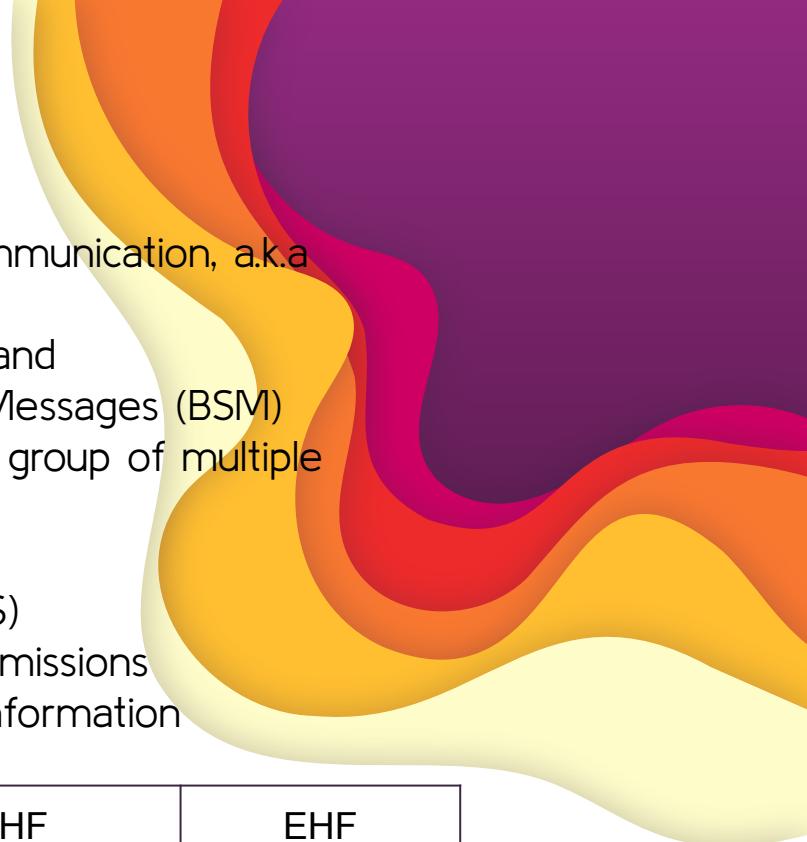
# Project Components



# C-V2X Protocol

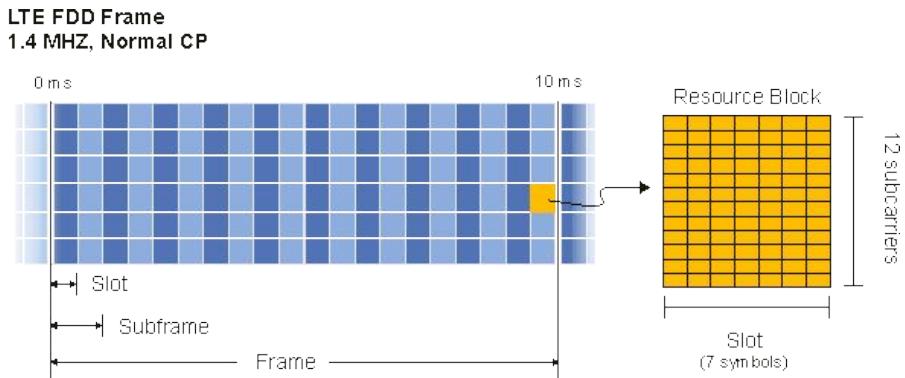
- A cellular network protocol that uses sidelink communication, a.k.a direct, peer-to-peer communication
- Based on LTE and operates in the 5.9 GHz ITS band
- Vehicles communicate via periodic Basic Safety Messages (BSM)
- Bandwidth is divided into subchannels which is a group of multiple resource blocks
- Mode 4: autonomous resource selection
- Sensing-Based Semi-Persistent Scheduling (SB-SPS)
  - Frequency hop after some number of transmissions
  - Sensing: energy, PSCCH decoding, priority information

HF	VHF	UHF	SHF	EHF
30 MHz	300 MHz	3 GHz	30 GHz	

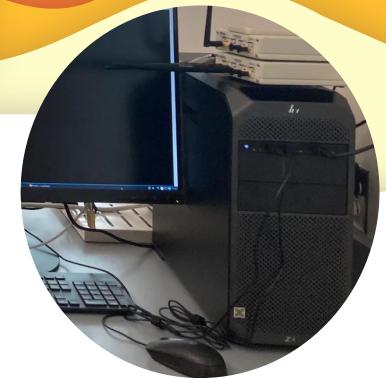


# Resource Blocks

- The LTE physical layer frequency allocation can be visualized with resource blocks.
  - Each frame spans 10 ms and is subdivided into 1 ms subframes each of which is capable of carrying at most one transmission.
  - A transmission can use one or more resource blocks within a subframe.

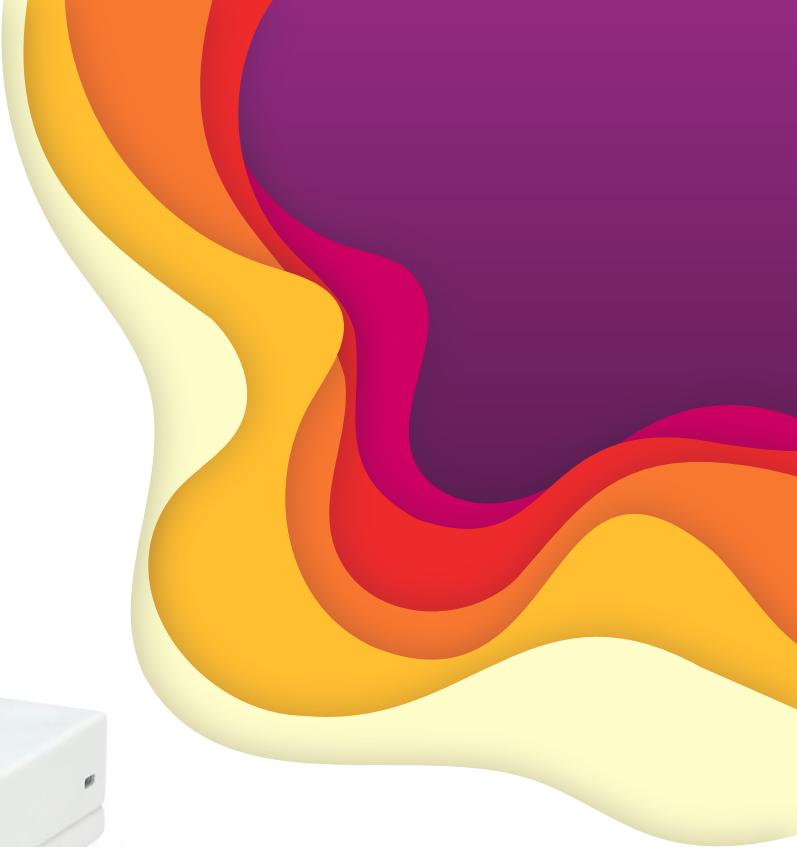


# Experimental Setup



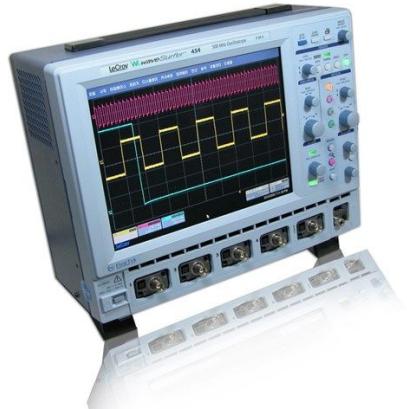
# Experimental Setup

- National Instruments Universal Software Radio Peripheral 2901
  - (NI USRP 2901)
- 70 MHz to 6 GHz
- 56 MHz Bandwidth



# Experimental Setup

- Keysight 33550B Waveform Generator
  - 10 MHz sine, 10 dBm
  - 1 Hz sine, 10 dBm
- LeCroy Wavesurfer 442 Oscilloscope
  - Verification



# Software Libraries

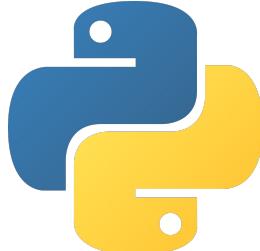


## Cellular Vehicle-to-Everything Traffic Generator

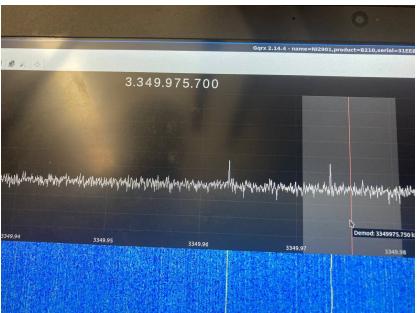
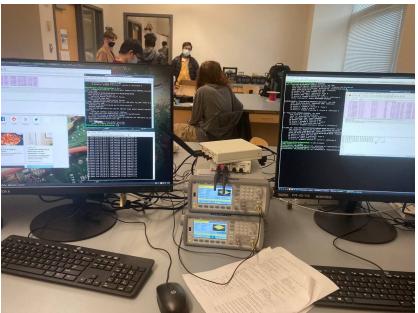
An SDR-based C-V2X Traffic Generator based on [srsLTE](#).



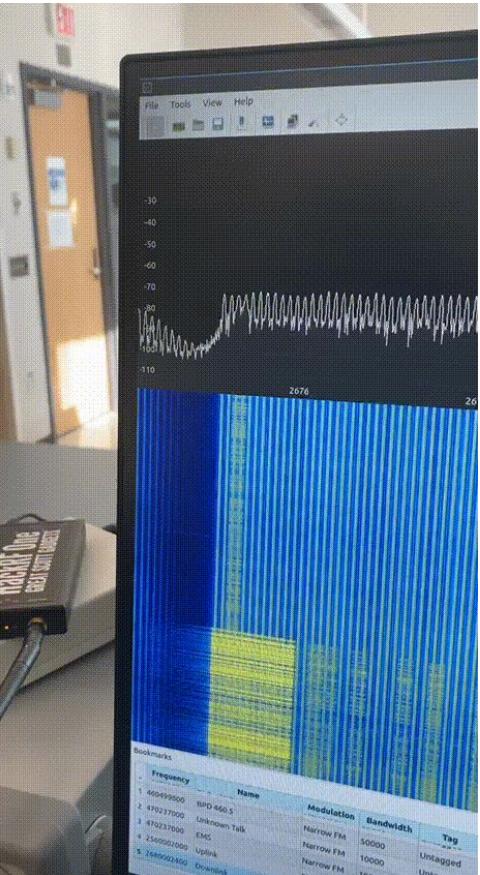
Funded by  
**DFG** Deutsche  
Forschungsgemeinschaft  
German Research Foundation



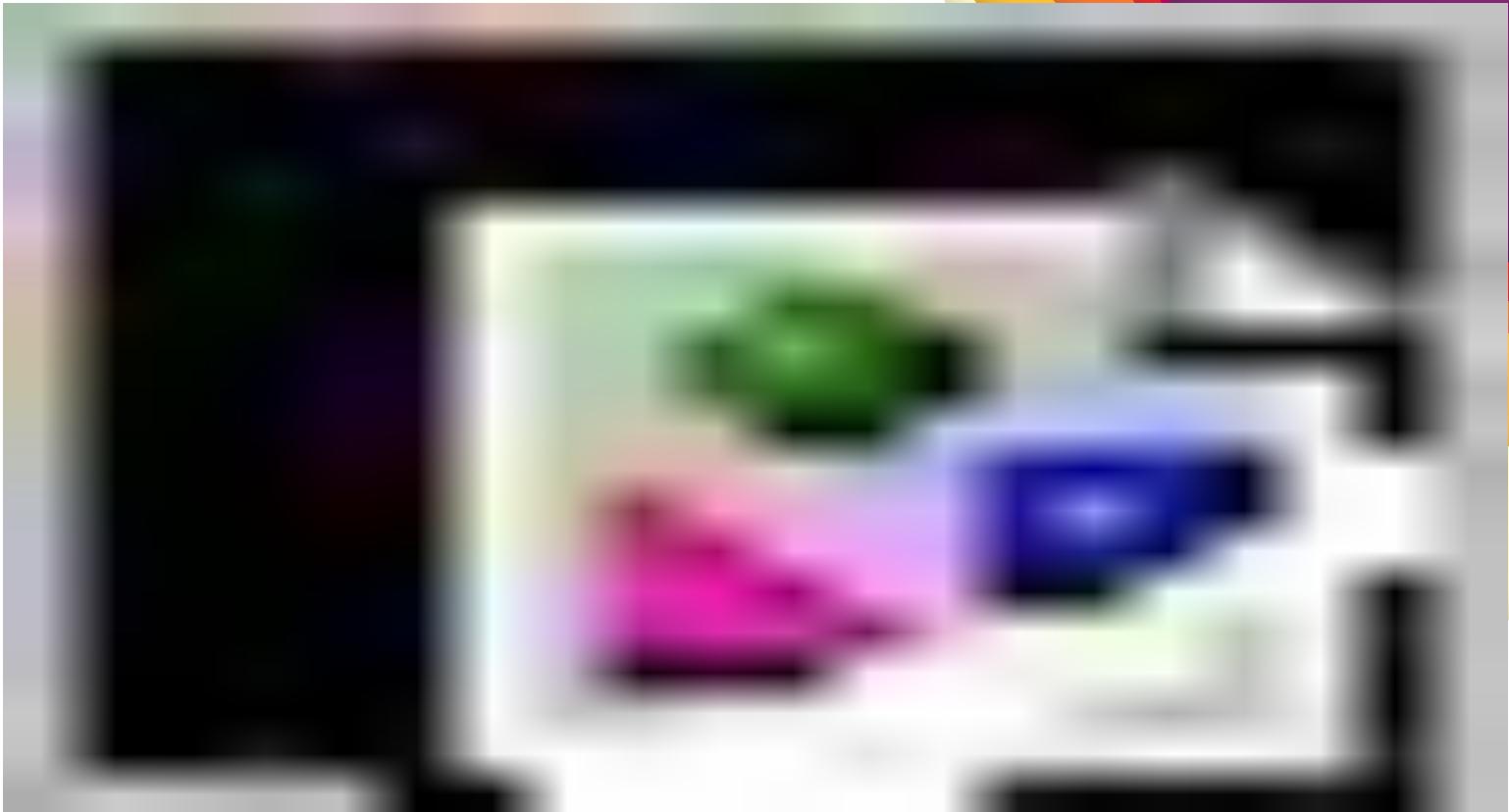
# Demo: Cellular Bitrate Test



```
dragon@dragon-a-z4-G4-Workstation:~$ lperf -c 172.16.0.1 -w 2m -t 30s
Invalid value of '1s' for -t interval
-----
Client connecting to TCP port 5001
TCP window size: 2.00 MByte (WARNING: requested 1.91 MByte)
-----
[ 3] local 172.16.0.5 port 37700 connected with 172.16.0.1 port 5001
[ 10] Interval Transfer Bandwidth
[ 3] 0.0- 0.5 sec 4.00 MBbytes 2.00 Mbit/sec
[ 3] 1.0- 2.0 sec 2.62 MBbytes 22.0 Mbit/sec
[ 3] 2.0- 3.0 sec 2.75 MBbytes 23.1 Mbit/sec
[ 3] 3.0- 4.0 sec 2.12 MBbytes 17.8 Mbit/sec
[ 3] 4.0- 5.0 sec 2.75 MBbytes 23.1 Mbit/sec
[ 3] 5.0- 6.0 sec 2.62 MBbytes 22.0 Mbit/sec
[ 3] 6.0- 7.0 sec 1.18 MBbytes 9.89 Mbit/sec
[ 3] 7.0- 8.0 sec 0.00 MBbytes 0.00 Mbit/sec
```

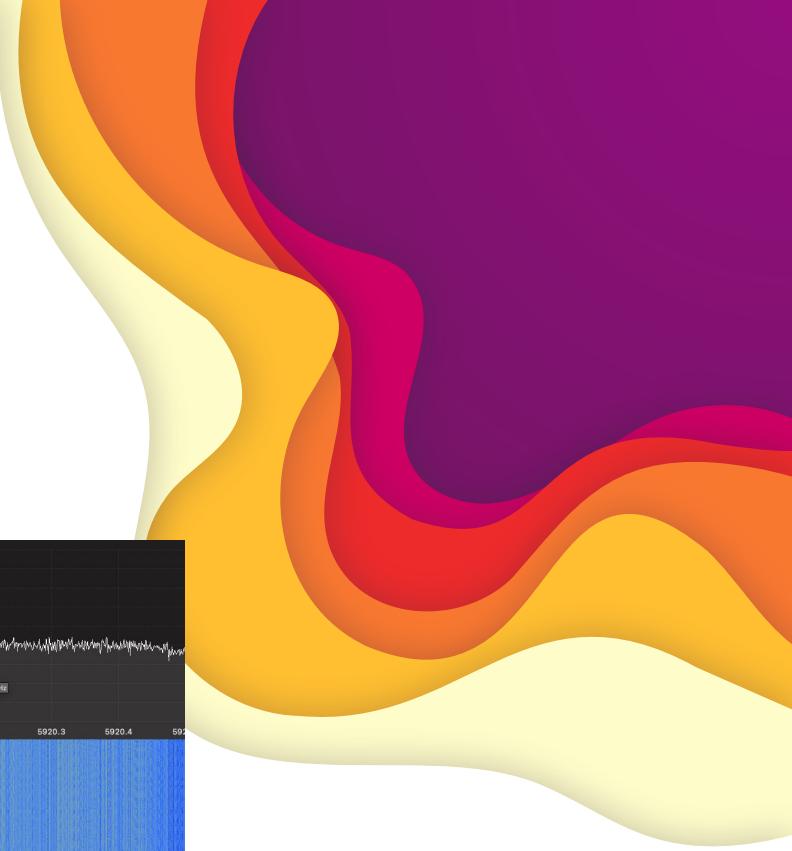
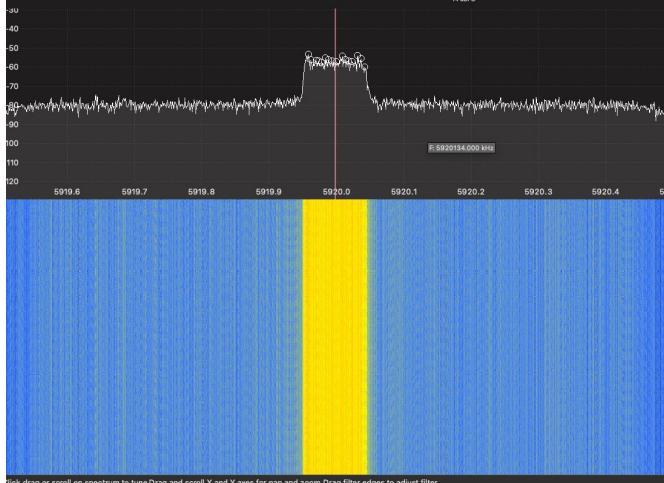


# Demo: C-V2X Capture



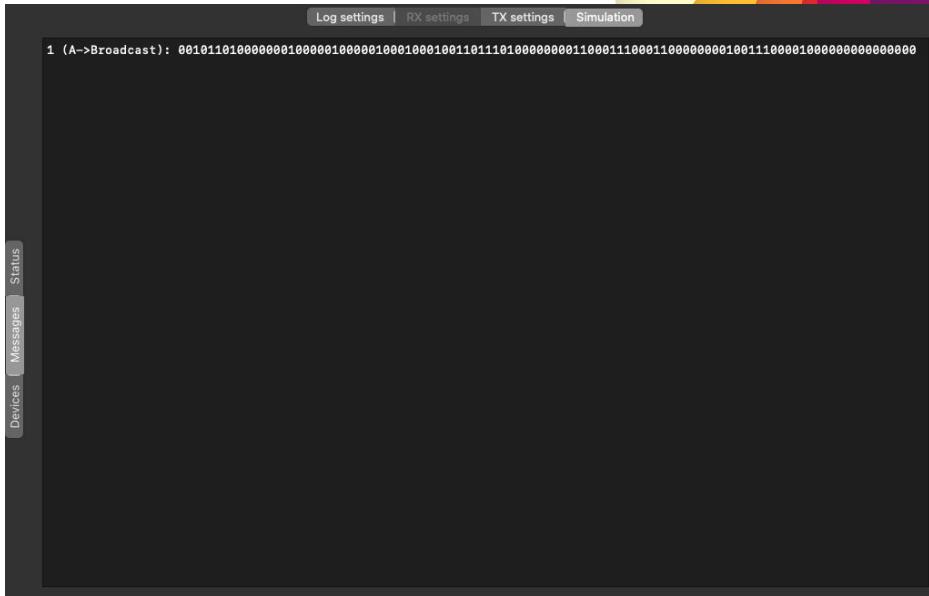
# Signal Analysis

gqrx: big-picture analysis of frequency



# Signal Analysis

# Universal Radio Hacker: granular analysis



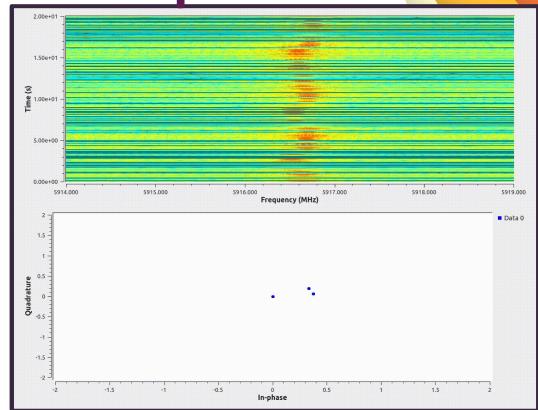
# Teams

- Hardware Team
  - Radio setup
  - Jammer design
- Data Team
  - Data extraction
- Machine Learning
  - Algorithmic jammer detection
- Cross-Team
  - Written deliverables

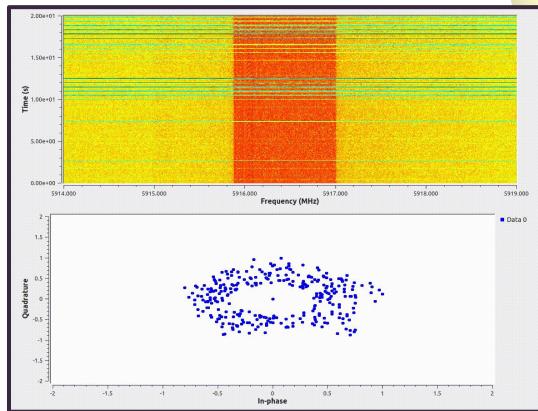


# Hardware Team: Complete

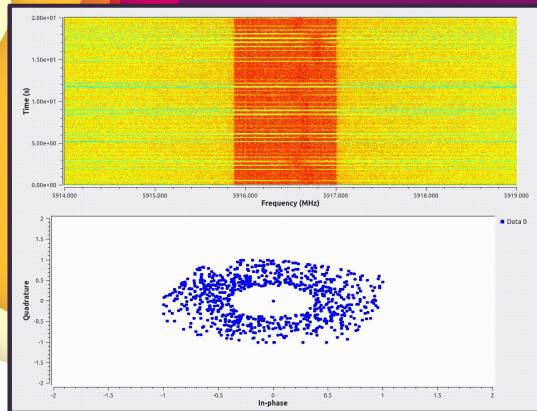
- Set up radio infrastructure
- Sync USRPs with signal generators
- Verify OTA communication through ping tests
- Generation of V2X signal
- Modification of jammer code
- Creation of combined-receiver for jammer and V2X-TX



+



=



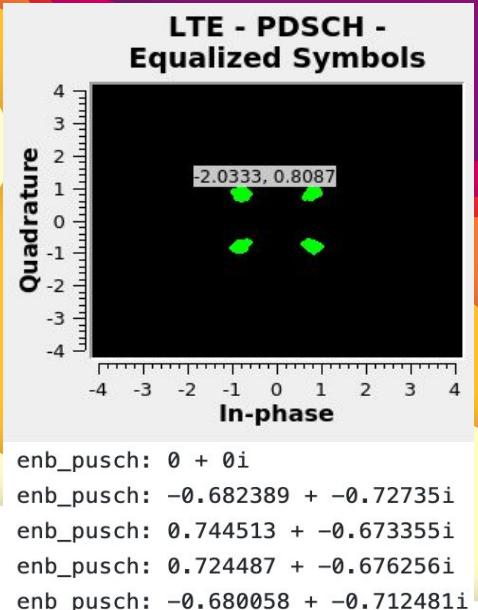
# Hardware Team: Todo

- Create GNURadio file to transmit both signals to modified srsRAN receiver created by data team
- Iterate on jammer code/possibly transition to pattern matching



# Data Team: Complete

- Identify classes in SrsRAN containing IQ data and resource block information
- Design probing function to circumvent config disabling print statements
- Extract time-stamped IQ data from SrsRAN
- Extract resource block group allocation array from SrsRAN



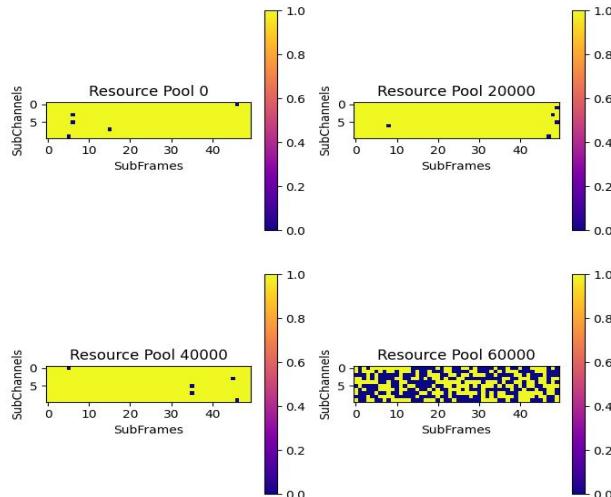
# Data Team: Todo

- Data collection IQ data using GNURadio and the WPI jammer for the non-jammed and jammed states
- Labelling and pre-processing of the data for use in the machine learning model
- SrsRAN C-V2X reception



# Machine Learning: Complete

- Prototype CNN Model for testing jammed RBGs detection
- Deep learning model with 3 methods
  - CNN with more tunded layers
  - ResNet (Residual Network)
  - CLDNN (Convolutional Long-Short Term Deep Neural Network)



# Machine Learning: Todo

- Final model selection and evaluation  
(do the validation and testing based on  
our own GNU generated datasets)
- Further feature engineering for better  
jammed block recognition.



# Cross-Team: Complete

- Preliminary Design
- PDRR slides and report
- First prototype test plan and report
- Second prototype test plan
- CDR slides
- Air Force Research Lab reports
  - Interim progress report
  - Final design showcase and report



# Cross-Team: Todo

- Second prototype test report
- Final prototype test plan and report
- User Manual draft and final
- Customer installation
- AFRL Conference?
- ECE Day poster



# Gantt Chart (2021)

## C-V2X: Misbehavior Detection

### Planning

- First Client Meeting
- Preliminary Design
- PDRR Writing
- PDRR Presentation
- PDRR

### Research

- C-V2X Protocol Overview
- Attack Detection Overview
- Library Selection
- C-V2X Simulation Software
- GPSDO vs. Signal Generation
- Sidelink Channels
- Time Synchronization

### Hardware Acquisition

- Provisioned 1st PC with DragonOS
- Deployed 2x USRP
- Deployed 2x Waveform Generator
- Provisioned 2nd PC with DragonOS
- Deployed 3rd USRP

### ENB-UE Communication

- Virtual Machine Setup
- ZeromQ Virtual Network
- ZeromQ Network Tests
- SrsRAN Hardware Configuration
- First OTA Communication
- OTA Testing
- Prototype Testing

### C-V2X Communication

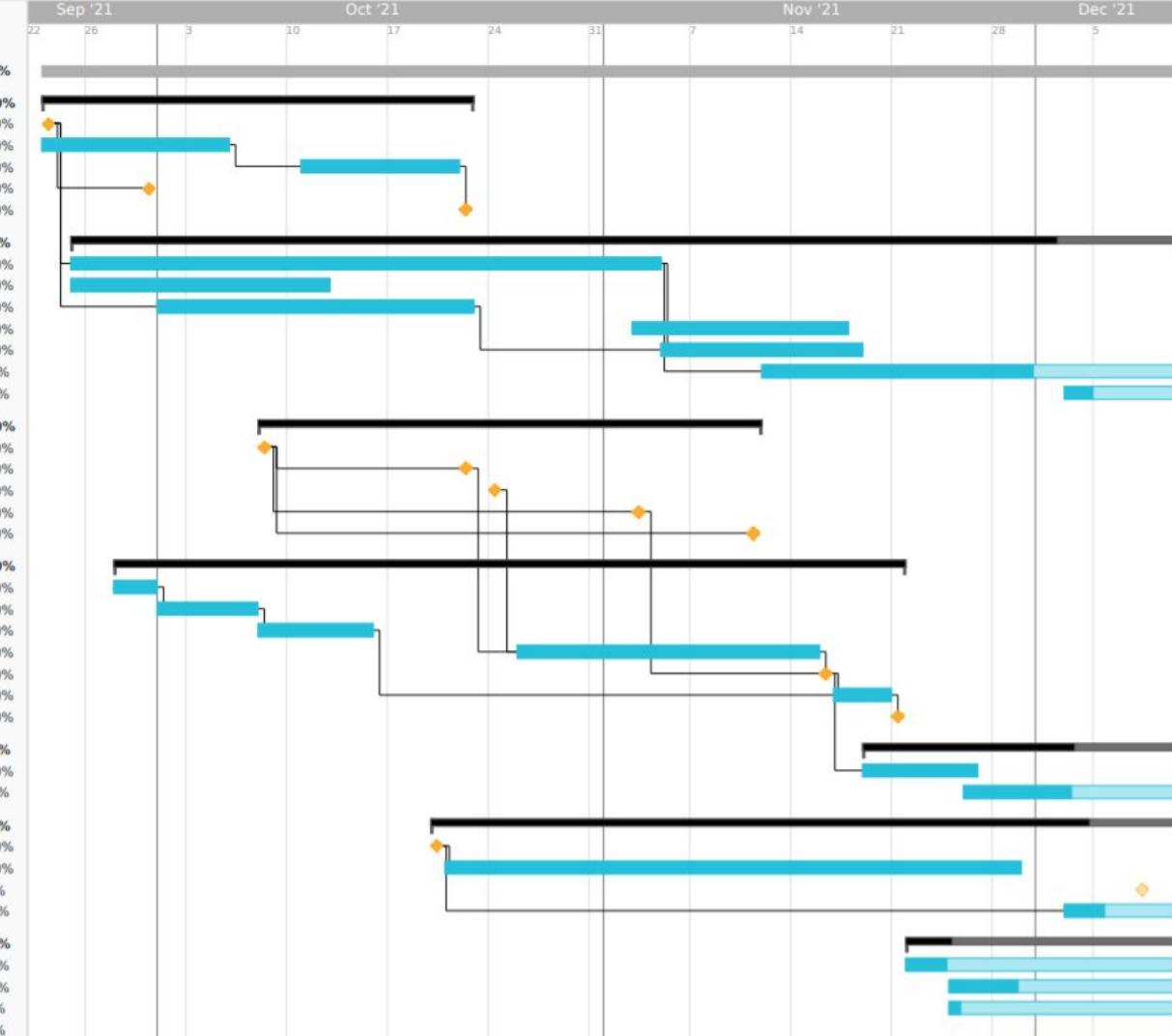
- C-V2X OTA transmission
- C-V2X OTA reception

### AFRL Challenge

- Kickoff Meeting
- Team Fact Sheet
- End-of-Year Review
- Interim Progress Report

### Future Work

- DoS Attack Implementations
- Defense Strategy Implementations
- ML Attack Detection Mechanism
- Web API



# Gantt Chart (2022)

## C-V2X: Misbehavior Detect...

### Hardware Team

- GNU Radio Jammer Research
- Virtual C-V2X IQ Capture
- Jammer Python Implementation
- OFDM Jammer Implementation
- OTA Jammed C-V2X IQ Capture
- Jammer Pattern Matching

### Data Team

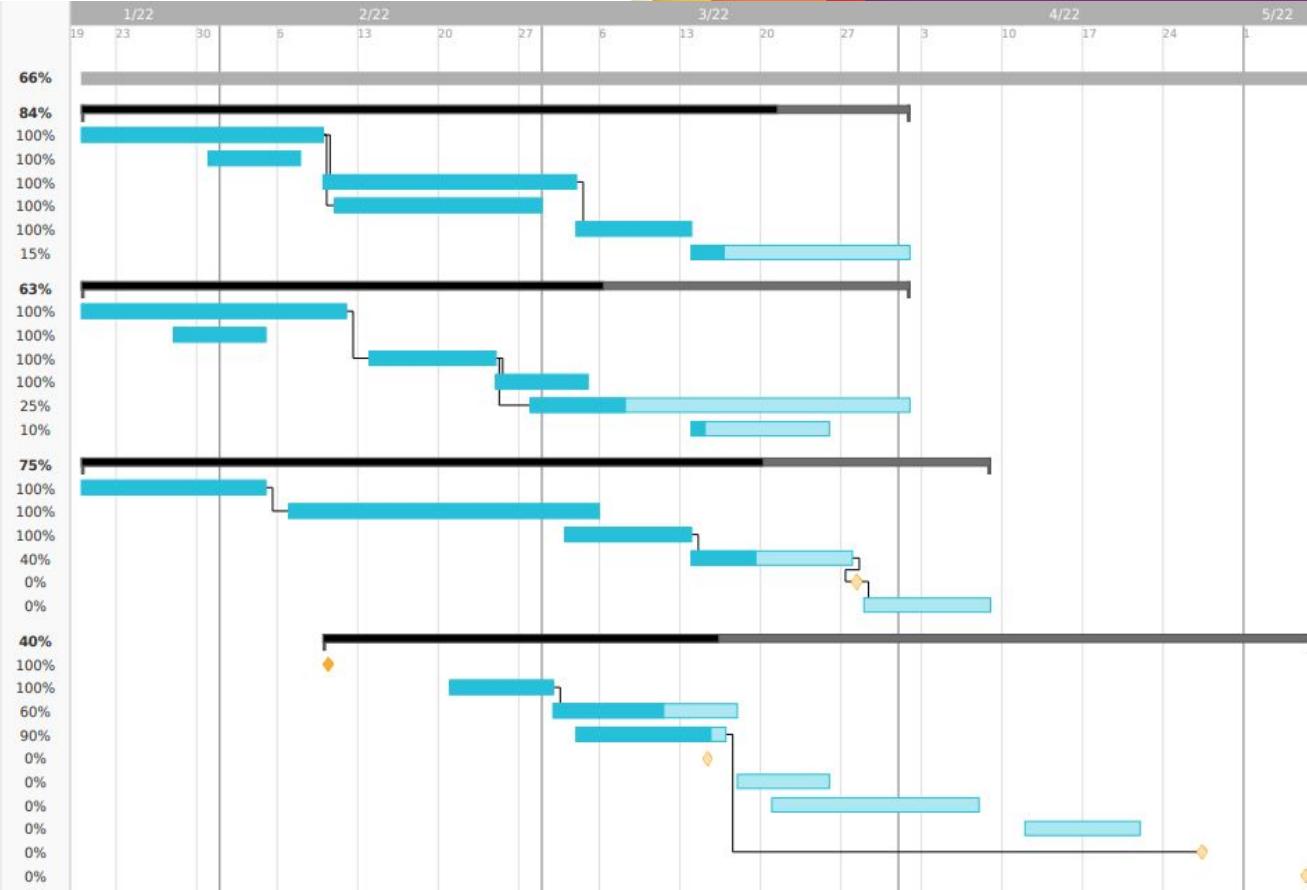
- SrsRAN Class Research
- SrsRAN IQ Data Extraction
- SrsRAN Probe Design
- SrsRAN RBG Extraction
- IQ Dataset Creation
- SrsRAN C-V2X Reception

### Machine Learning Team

- Data Simulation
- RBG CNN Model
- Prototype IQ Deep Learning Model
- Final Model Evaluation
- Final Model Selection
- Deep Learning Model Tweaks

### Cross-team

- AFRL Final Design Showcase
- Second Prototype Test Plan
- Second Prototype Test Report
- AFRL Final Design Report
- Critical Design Review
- User Manual (Draft)
- Final Prototype Test Plan and Report
- Customer Installation
- AFRL Conference
- ECE Day



**Thank you!**

# Questions?