Misbehavior Detection System for Cellular Vehicle-to-Everything Networks

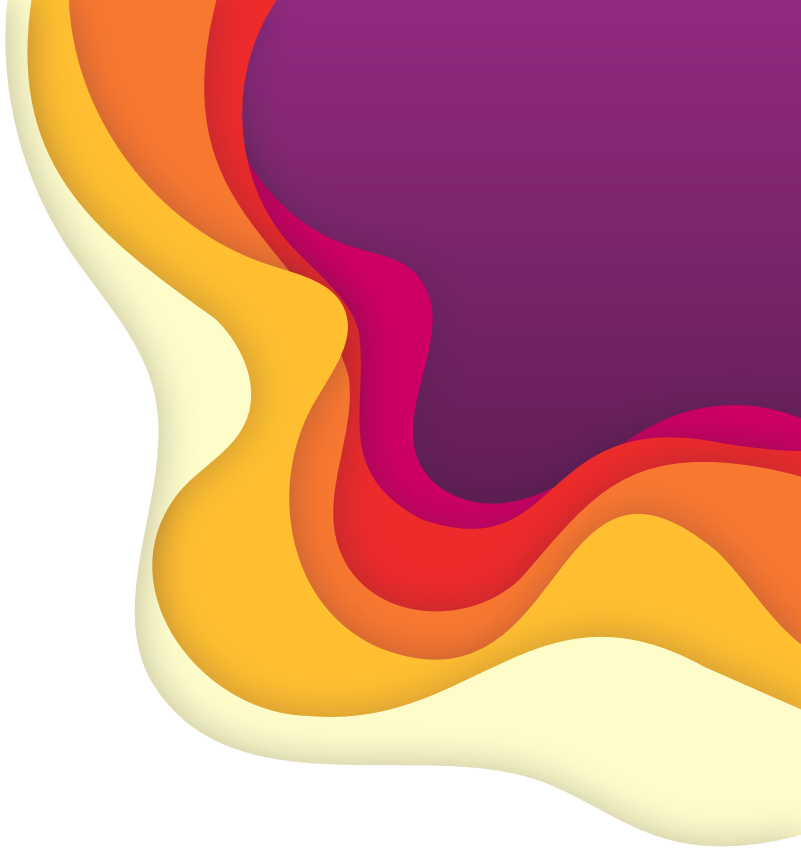
Preliminary Design Review

Grad Advisor: Stefan Gvozdenovic

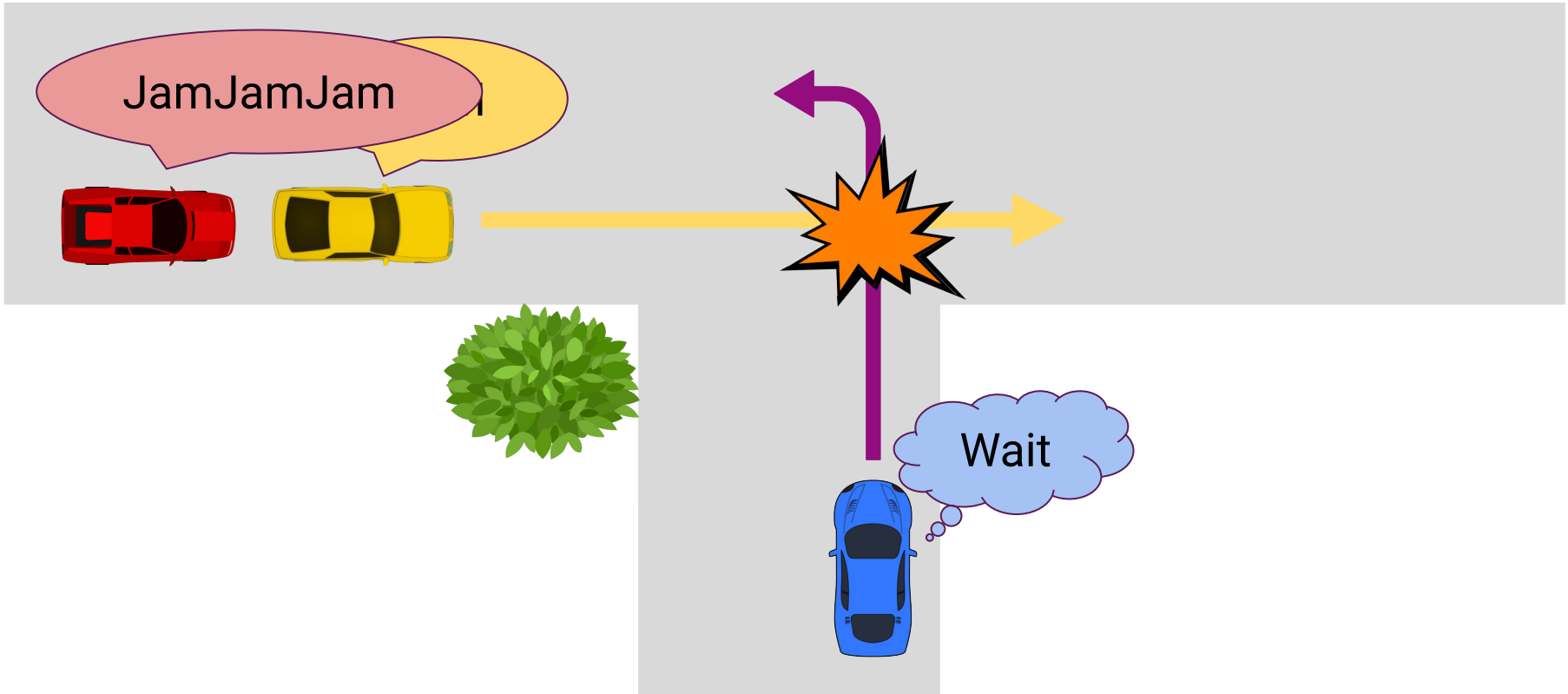
Michael Aliberti, Max Ellsworth, Jason Inirio, Samuel Krasnoff, Julia Zeng, and Yixiu Zhu

Overview

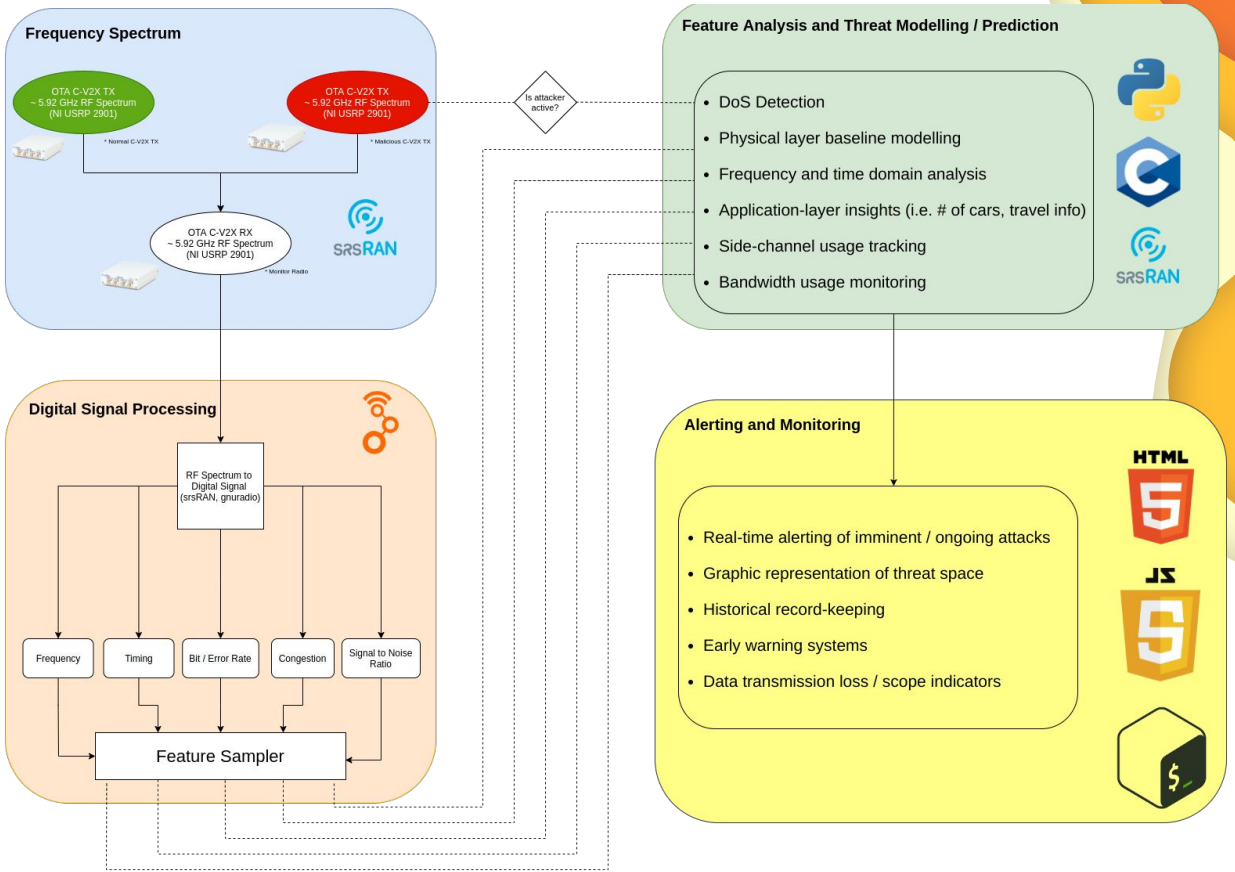
- Problem Statement
- Requirements
- C-V2X Protocol
- Experimental Setup
- Software Libraries
- Demo:
  - Cellular Bitrate Tests
  - C-V2X Transmit
- Signal Analysis
- Gantt Chart
- Future Work



A Quick Visual



Project Update

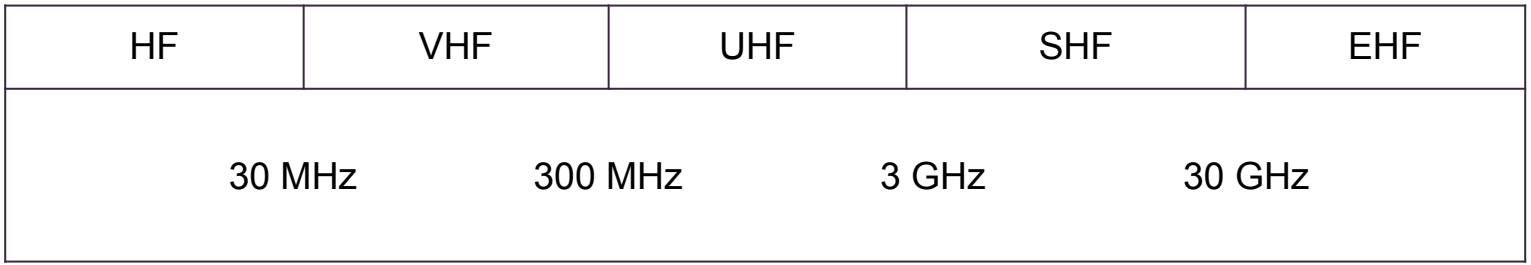


Problem Statement

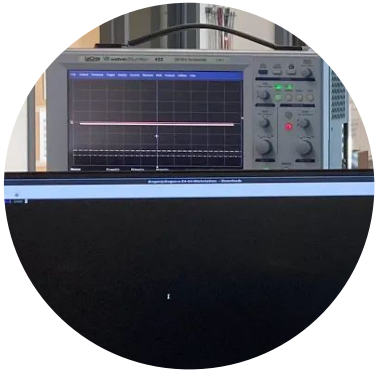
To thoroughly understand the effectiveness of the C-V2X standard, we must analyze physical layer attacks on nodes in the network.

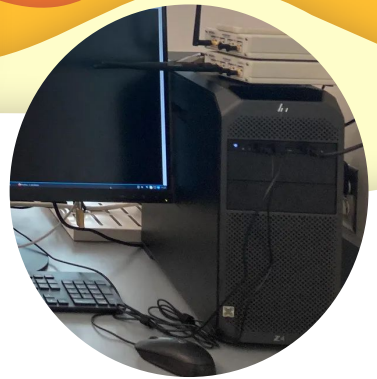
C-V2X Protocol

- 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-Base Semi-Persistent Scheduling (SB-SPS)
    - Frequency hop after some number of transmissions
    - Sensing: energy, PSCCH decoding, priority information



Experimental Setup

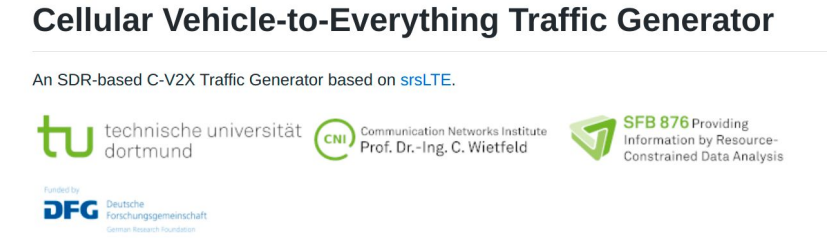




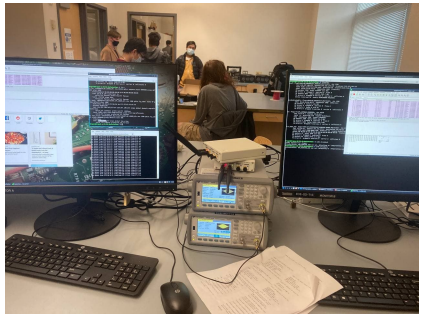
Experimental Setup

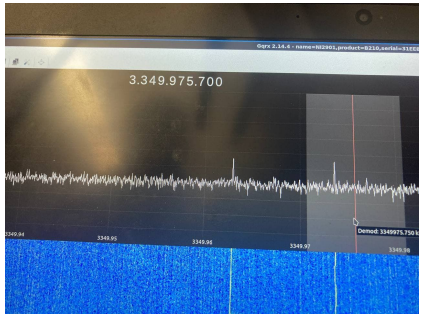
- National Instruments Universal Software Radio Peripheral 2901
  - (NI USRP 2901)
- 70 MHz to 6 GHz
- 56 MHz Bandwidth

Software Libraries

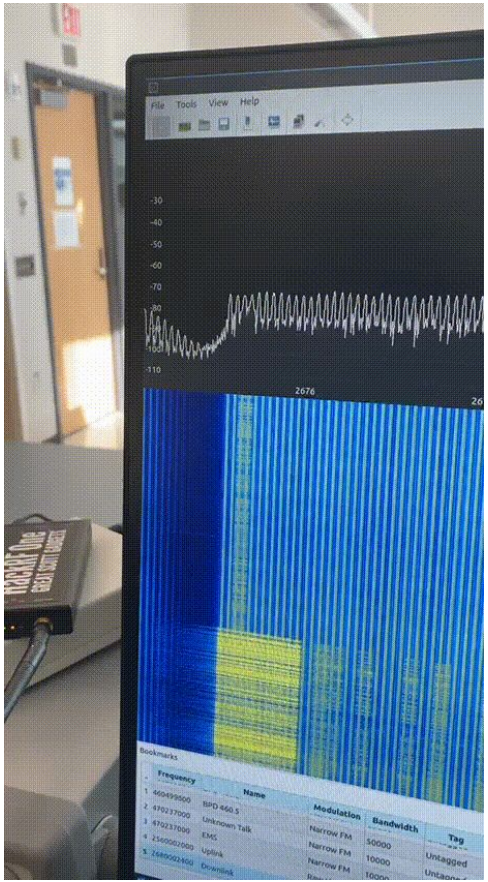


Demo: Cellular Bitrate Test

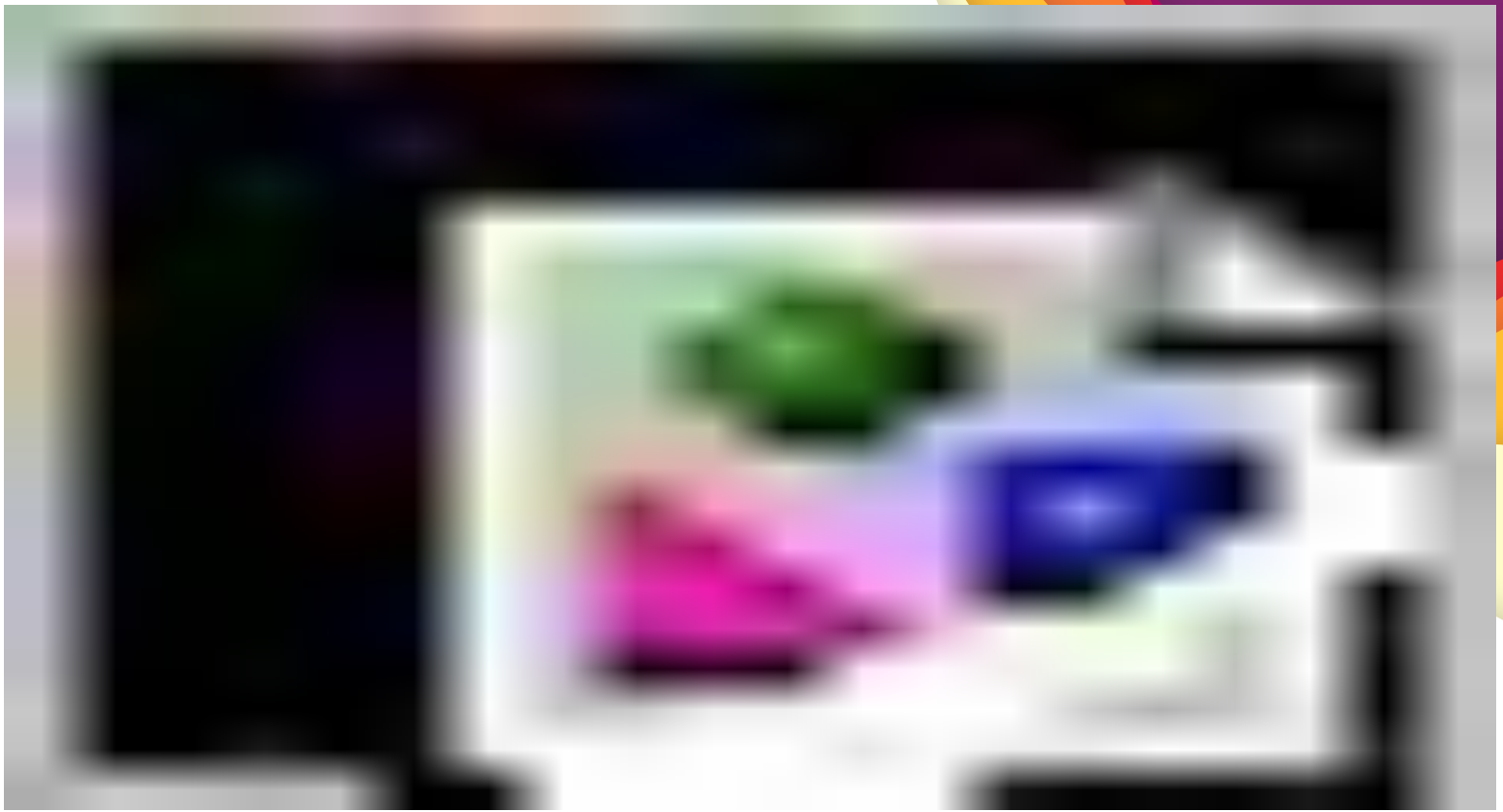





```
dragon@dragon-a-Z4-G4-Workstation:~$ iperf -c 172.16.0.1 -w 2m -t 30s
Invalid value of '1s' for -i interval
------------------------------------------------------------
Client connecting to 172.16.0.1, TCP port 5001
TCP window size: 2.00 MByte (WARNING: requested 1.91 MByte)
------------------------------------------------------------
[  3] local 172.16.0.5 port 37700 connected with 172.16.0.1 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec  4.12 MBytes  34.6 Mbits/sec
[  3]  1.0- 2.0 sec  2.62 MBytes  22.0 Mbits/sec
[  3]  2.0- 3.0 sec  2.75 MBytes  23.1 Mbits/sec
[  3]  3.0- 4.0 sec  2.12 MBytes  17.8 Mbits/sec
[  3]  4.0- 5.0 sec  2.75 MBytes  23.1 Mbits/sec
[  3]  5.0- 6.0 sec  2.62 MBytes  22.0 Mbits/sec
[  3]  6.0- 7.0 sec  1.18 MBytes  9.89 Mbits/sec
```

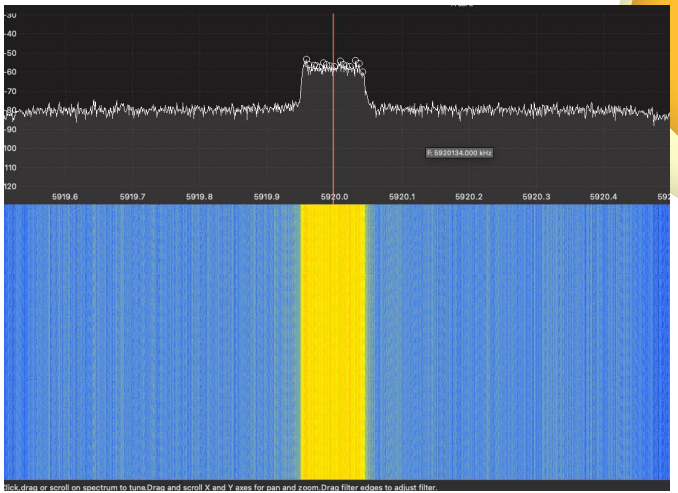


Demo: C-V2X Capture



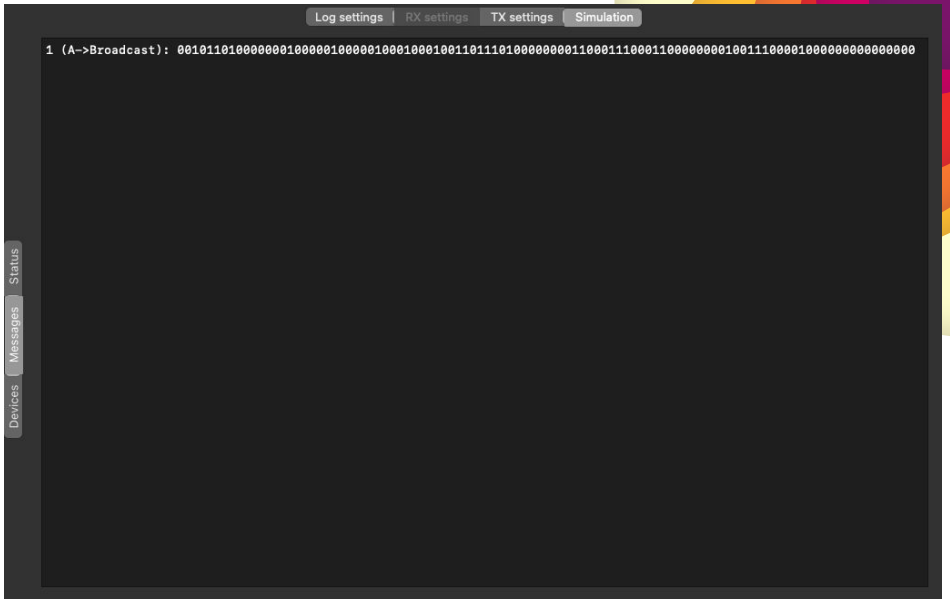
Signal Analysis

gqrx: big-picture analysis of frequency

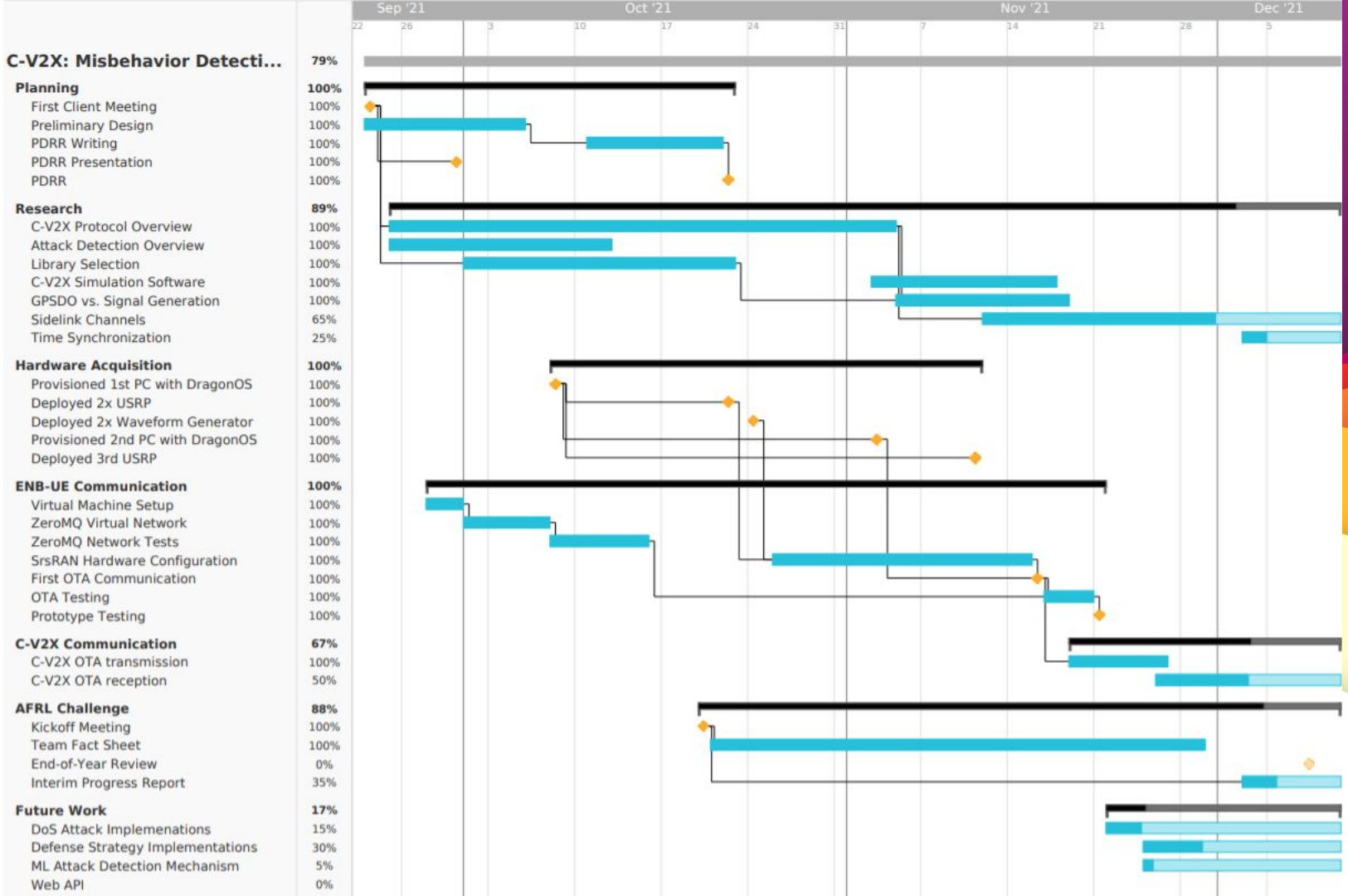


Signal Analysis

urh: granular analysis



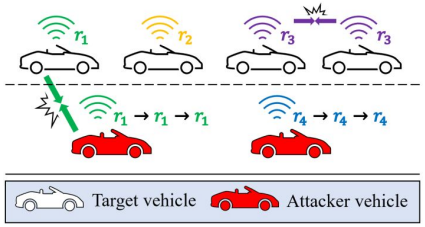
Gantt Chart

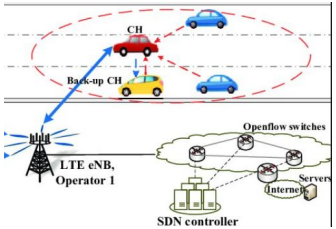


C-V2X: Misbehavior Detecti...	**79%**
Planning	**100%**
First Client Meeting	100%
Preliminary Design	100%
PDRR Writing	100%
PDRR Presentation	100%
PDRR	100%
Research	**89%**
C-V2X Protocol Overview	100%
Attack Detection Overview	100%
Library Selection	100%
C-V2X Simulation Software	100%
GPSDO vs. Signal Generation	100%
Sidelink Channels	65%
Time Synchronization	25%
Hardware Acquisition	**100%**
Provisioned 1st PC with DragonOS	100%
Deployed 2x USRP	100%
Deployed 2x Waveform Generator	100%
Provisioned 2nd PC with DragonOS	100%
Deployed 3rd USRP	100%
ENB-UE Communication	**100%**
Virtual Machine Setup	100%
ZeroMQ Virtual Network	100%
ZeroMQ Network Tests	100%
SrsRAN Hardware Configuration	100%
First OTA Communication	100%
OTA Testing	100%
Prototype Testing	100%
C-V2X Communication	**67%**
C-V2X OTA transmission	100%
C-V2X OTA reception	50%
AFRL Challenge	**88%**
Kickoff Meeting	100%
Team Fact Sheet	100%
End-of-Year Review	0%
Interim Progress Report	35%
Future Work	**17%**
DoS Attack Implemenations	15%
Defense Strategy Implementations	30%
ML Attack Detection Mechanism	5%
Web API	0%

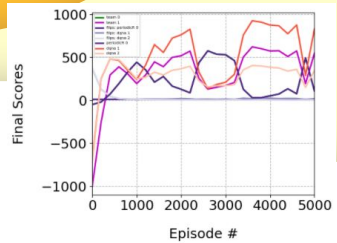
Future Work

- Dos Attack Implementations
- ML-based attack detection mechanism
- Web Visualization API
- Defence Strategy implementations





Categories	Classes of Strategies	
Non-adaptive (NA)	Exponential	Periodic
	Renewal	
	General non-adaptive	
Adaptive (AD)	Last move (LM)	
	Full history (FH)	



Thank you!

Questions

Experimental Setup

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