Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

CYD CYBER DEFENCE CAMPUS



Passive and Active Attacks on TPMS systems

Threats of Long-term surveillance and fast attacks to Tire Pressure Monitoring Systems

09 08 2025

Yago Lizarribar

Introduction

whoami

Researcher at CYD Campus in Switzerland

Working at the intersection of AI and Cybersecurity

Experience in Spectrum Sensing Networks and Localization

Also worked with Autonomous vehicles



What are we talking about?

- **Tire Pressure Monitoring Systems (TPMS):**
  - Designed to increase vehicle safety
  - Have been mandatory for more than a decade
- Cars have complex software stacks:
  - **Cyberattacks** on them are very common nowadays
  - Since **July 2022**: Europe requires cybersecurity certificates
  - Against attacks that: reveal identity, location, and so on
  - TPMS not included in this



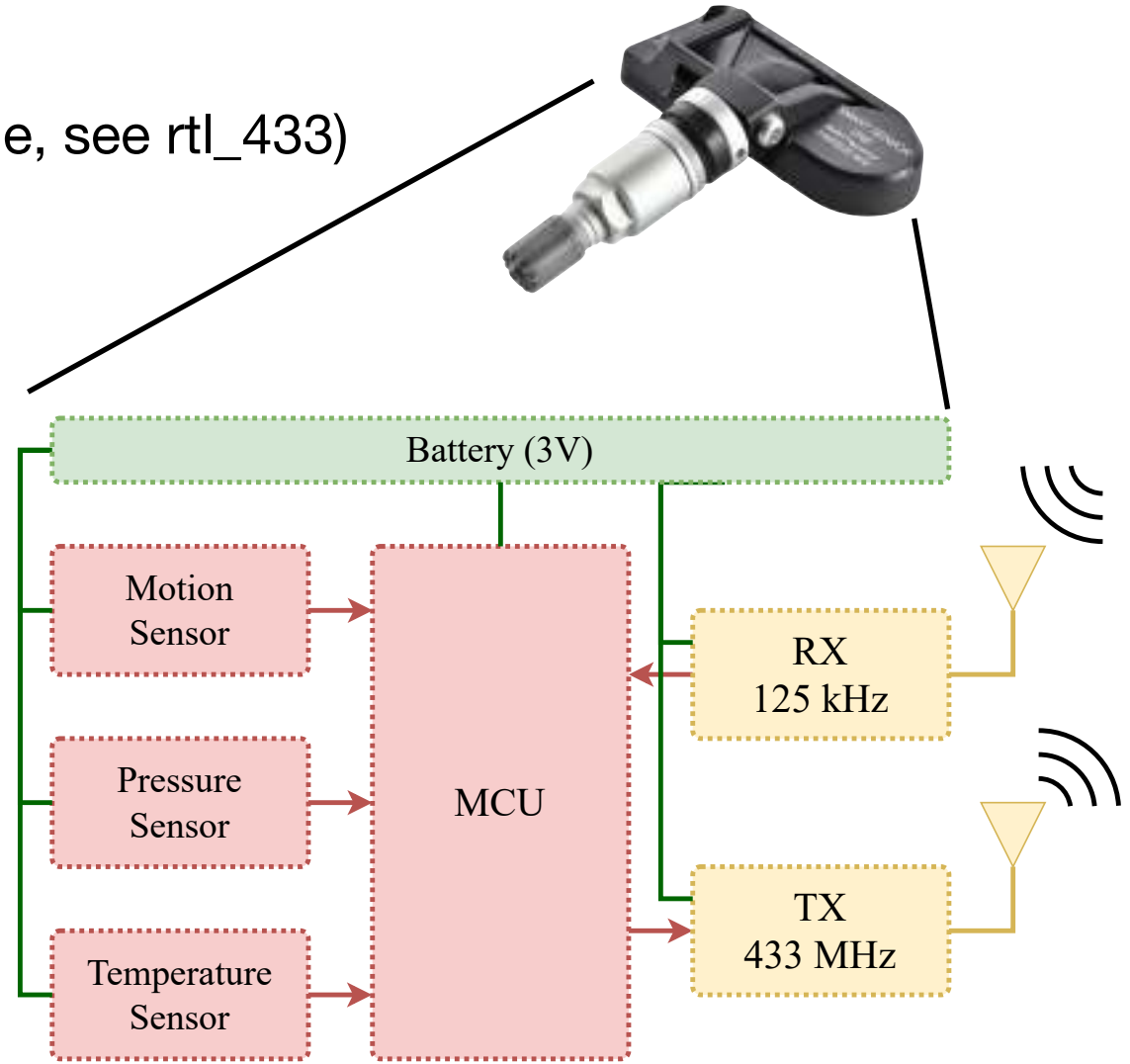
TPMS Families

- **Indirect TPMS (iTPMS):**
  - Based on rotation of wheel
  - Less accurate
  - Favored by: VW Group, GM
- **Direct TPMS (dTPMS):**
  - Pressure and Temperature
  - More accurate
  - Favored by: Toyota, Ford, OEM
- **Other:**
  - Bluetooth-based
  - More accurate
  - Favored by: Tesla, Pirelli

Direct TPMS Primer

- On the **inside** of a TPMS sensor:
  - Battery-powered devices
  - Protocols are proprietary (but easily reversible, see rtl_433)
  - Simple modulations (ASK/FSK @ 433 MHz)

- They have **different modes** of operation:
  - In theory, many only transmit when car movement starts. Then every 30-60 seconds
  - When parked they should not transmit
  - By sending a 125 kHz signal, it is possible to trigger a transmission

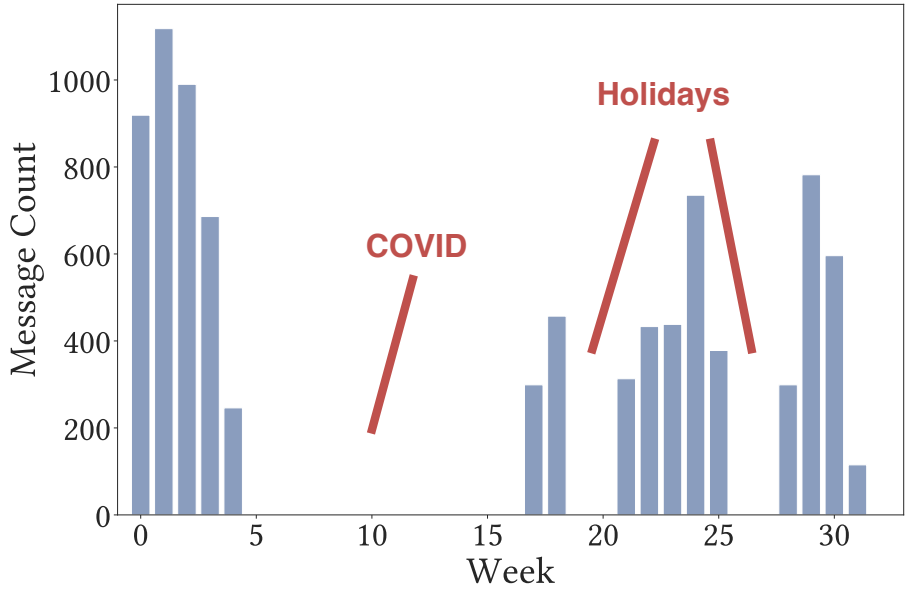


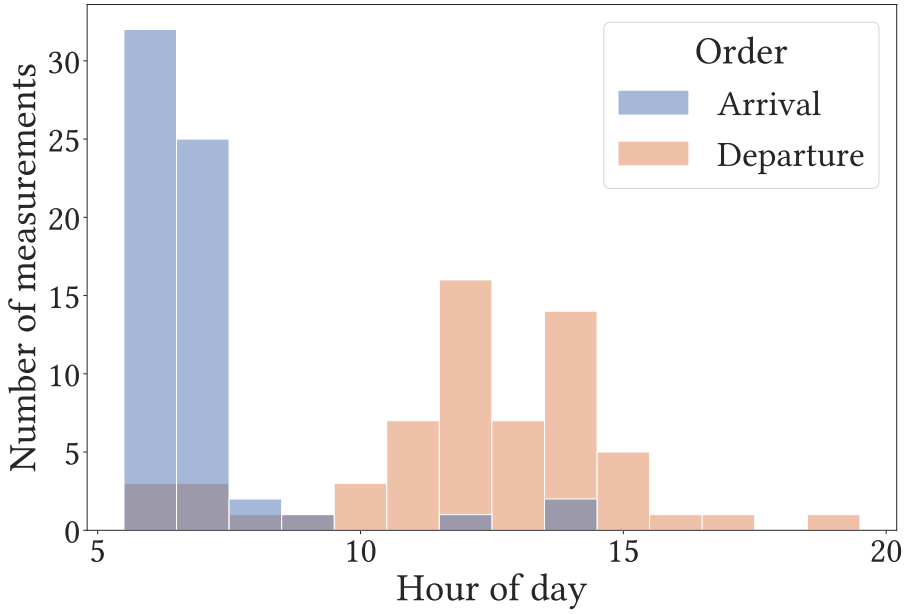
Sensor ID (32 bit) | Pressure (kPa) | Temperature (C)

From Passive Monitoring…

Why did we start with this

- IT Director and a Toyota
- Doing unrelated measurements we noticed some things:
  - We could easily track our director's schedule
  - After some time, we could learn when he had holidays, random absences, …
- We asked ourselves:
  - Is it actually feasible to track cars with dTPMS?
  - What patterns can we learn?

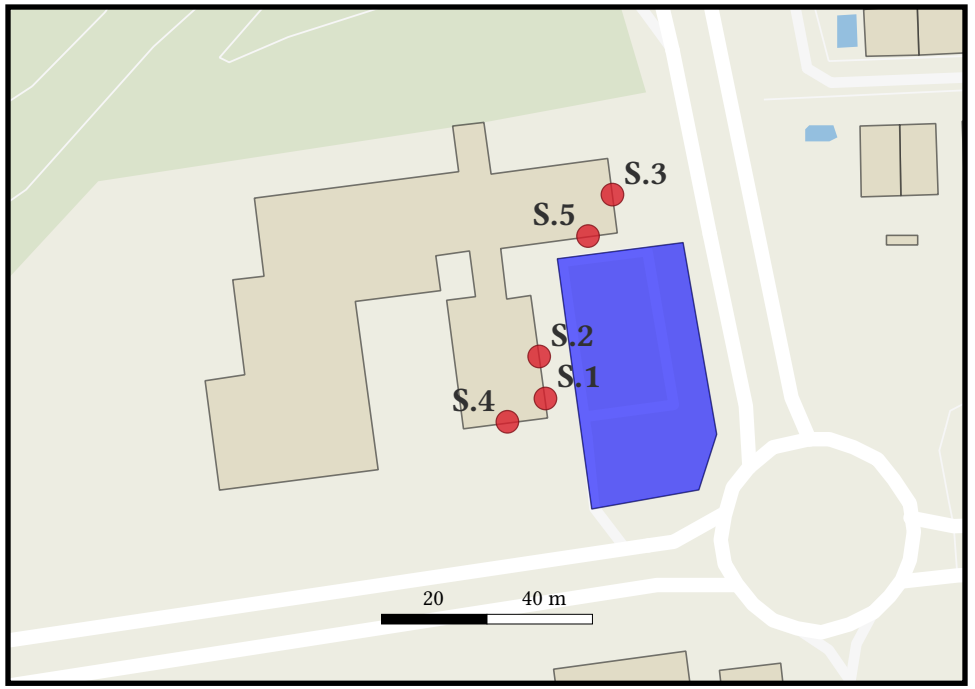




Setup

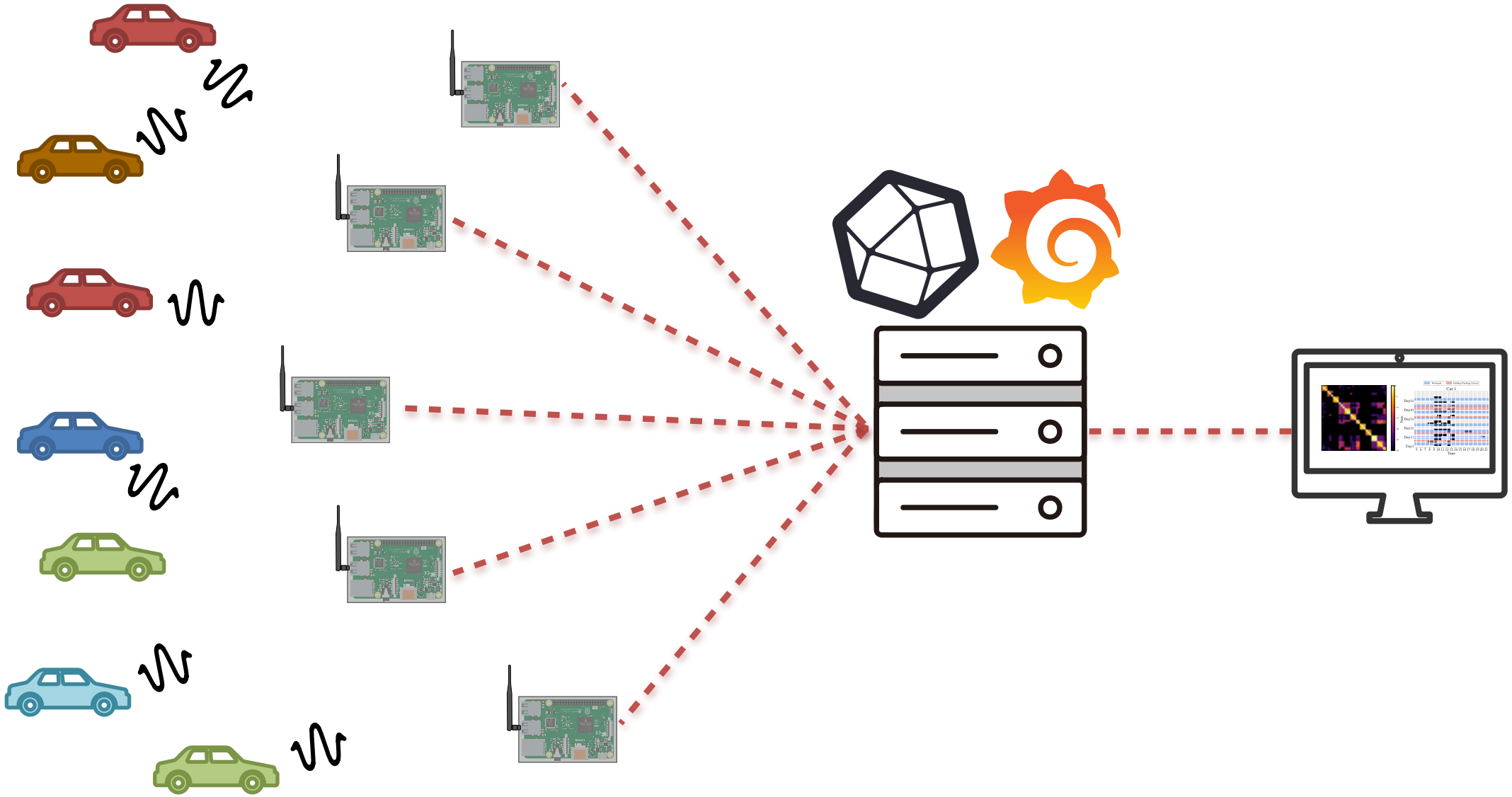
- Hardware:
  - RTL-SDR + 433 MHz Antenna
  - Raspberry Pi
  - Internet Connectivity + Power
- Software:
  - **rtl_433** + custom modules
- Infrastructure:
  - Sensors send data to Database
- We can now capture millions of messages





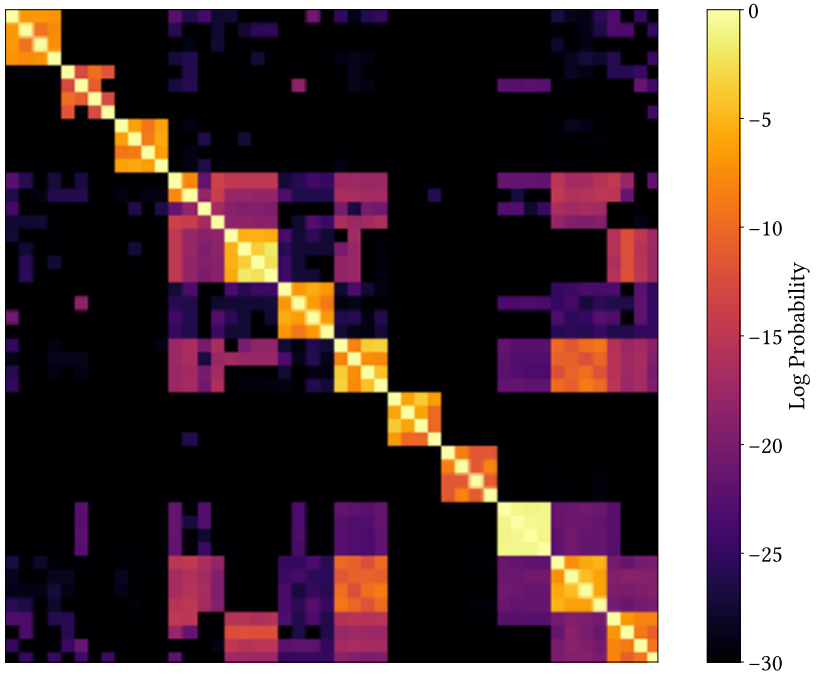
Site name	Recording Hours	Measured IDs	Recorded IDs
Receiver 1	655	476248	17621
Receiver 2	655	412905	22706
Receiver 3	655	514484	3230
Receiver 4	653	753327	7708
Receiver 5	362	356526	24123

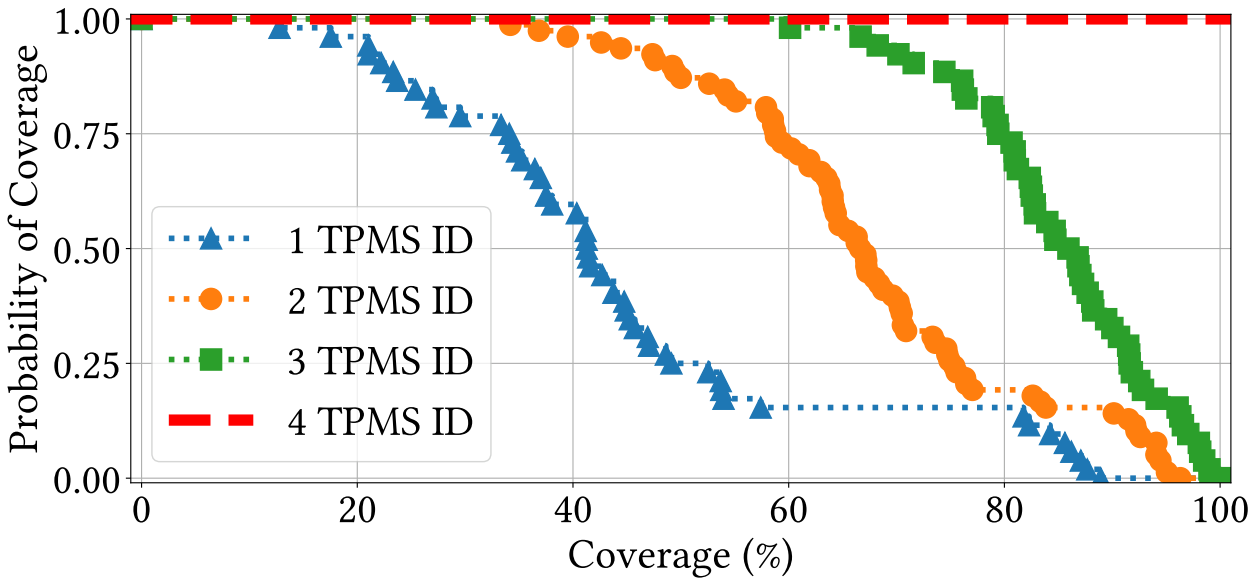
Infrastructure



Car Matching

- If we just capture a single ID:
  - We cannot capture all the times a car passes by
- We develop methods to correlate IDs of same car:
  - Cross-Correlation
  - **Jaccard Index**
- We design a robust matching:
  - To capture transitivity between IDs
  - Even in narrow time windows we capture cars

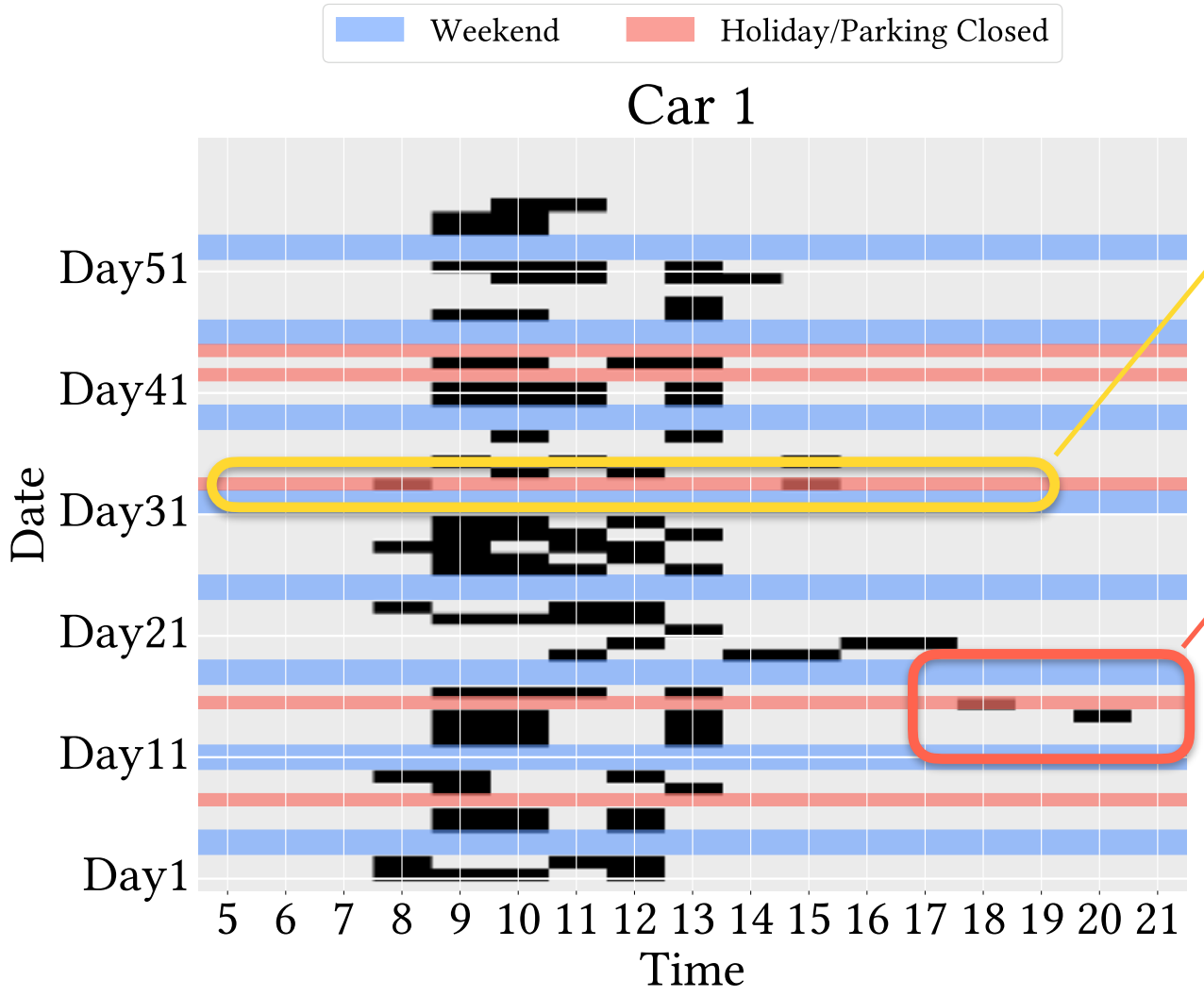




Method	Agg. (s)	Naive Match	Robust Match	Comp. Time (s)
Xcorr	5 sec.	5	9	2.0970
	10 sec.	6	10	1.5616
	30 sec.	8	11	1.1017
	1 min.	8	12	0.8708
	2 min.	10	12	0.6534
Jaccard	5 sec.	7	10	34.1570
	10 sec.	9	12	23.7702
	30 sec.	10	12	21.1729
	1 min.	11	12	19.1987
	2 min.	11	12	18.2871

Long-Term Patterns (I)

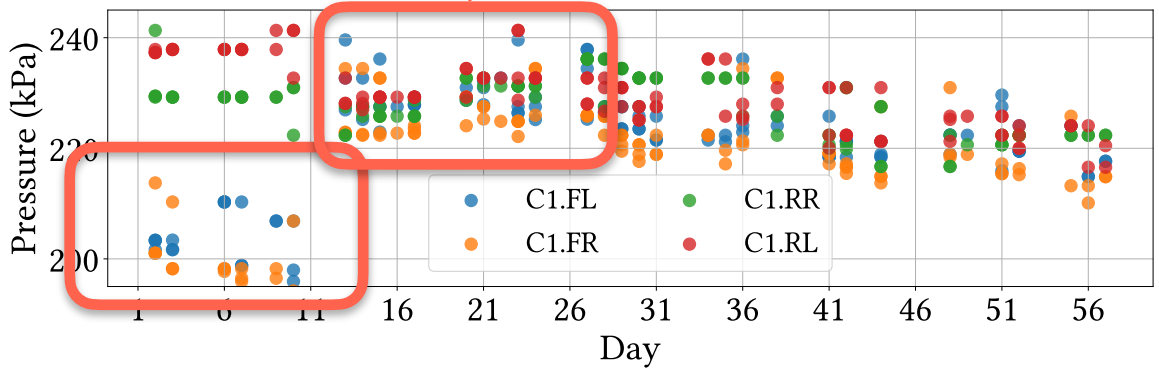
- Car 1: Part-Time Student



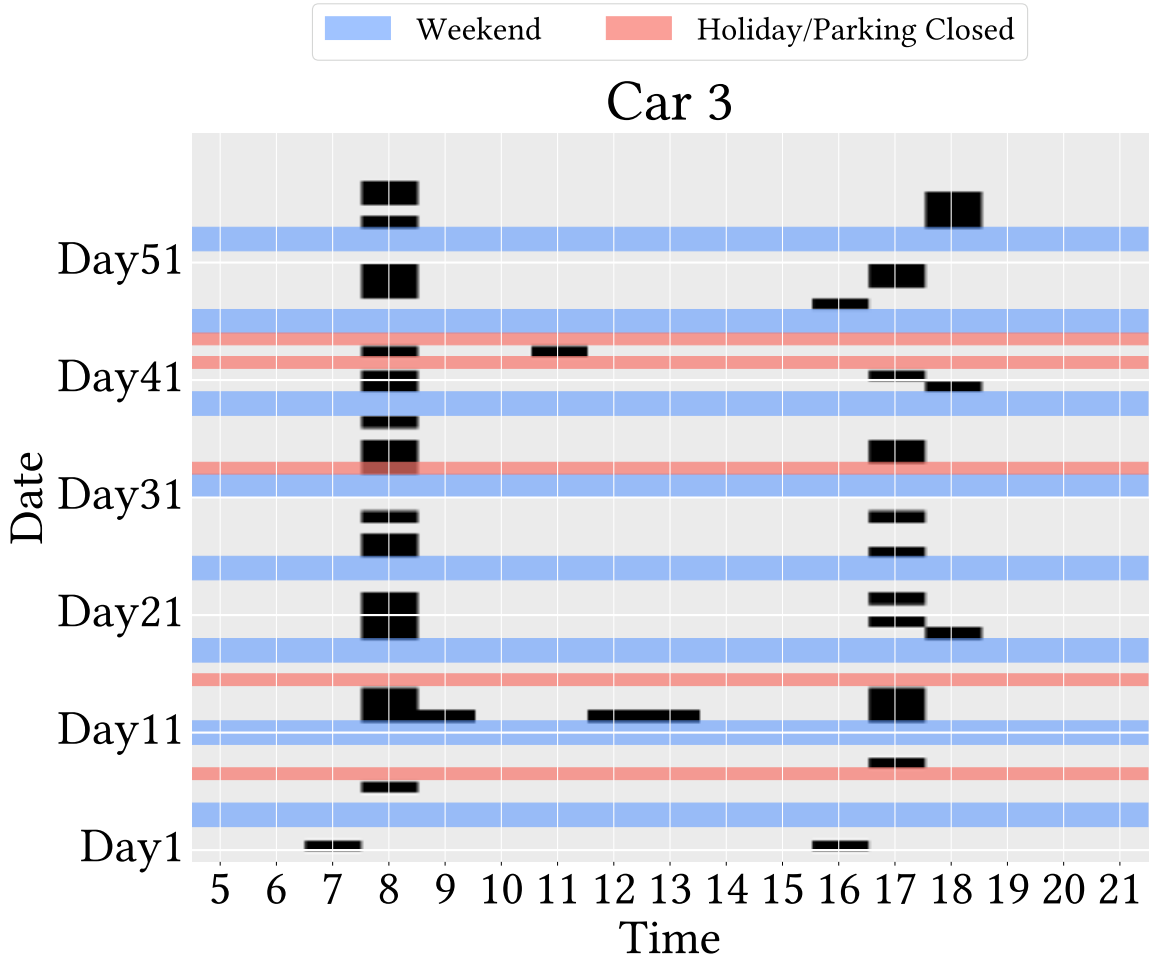
No Holidays

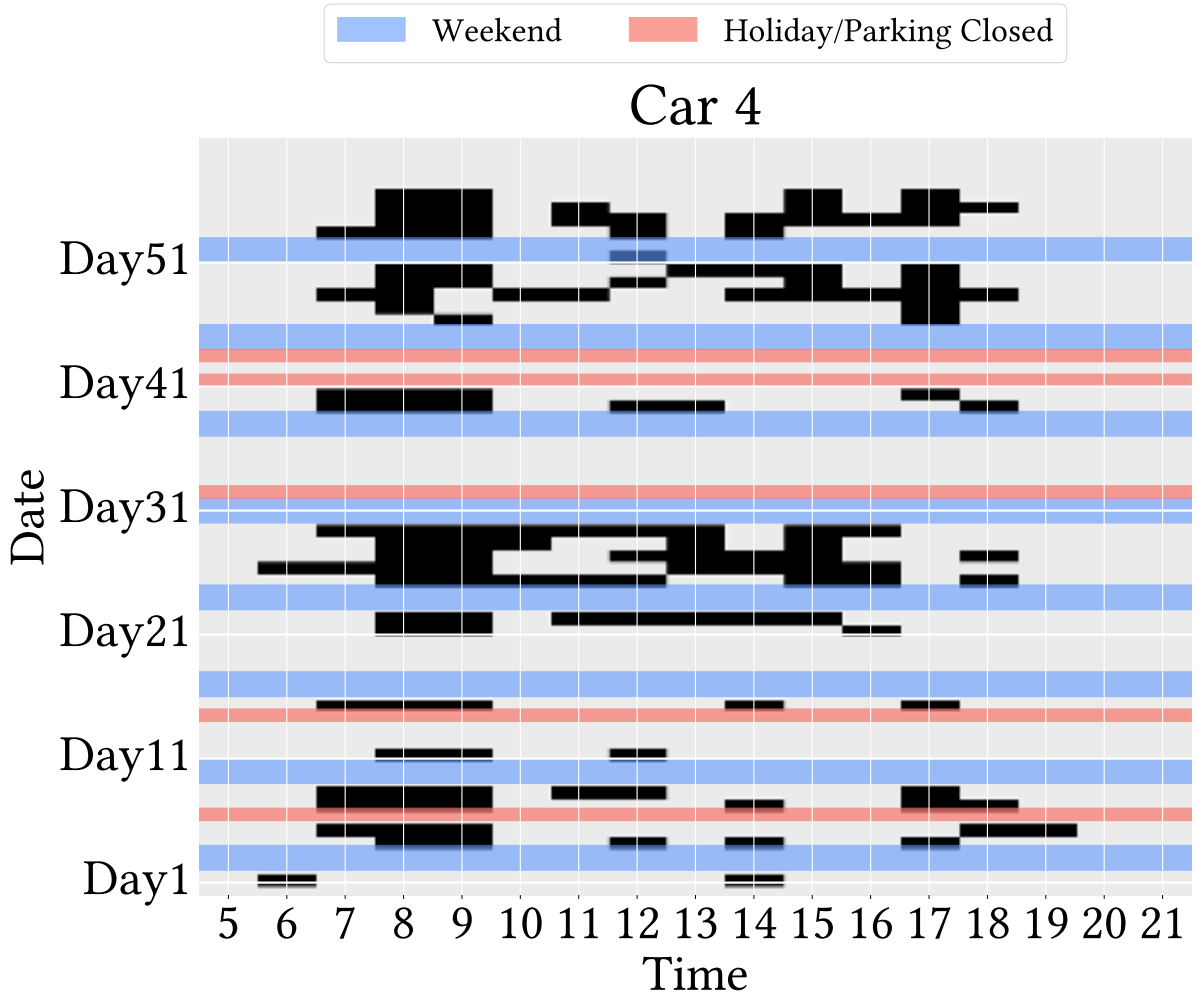
University Course

Taking care of our participants



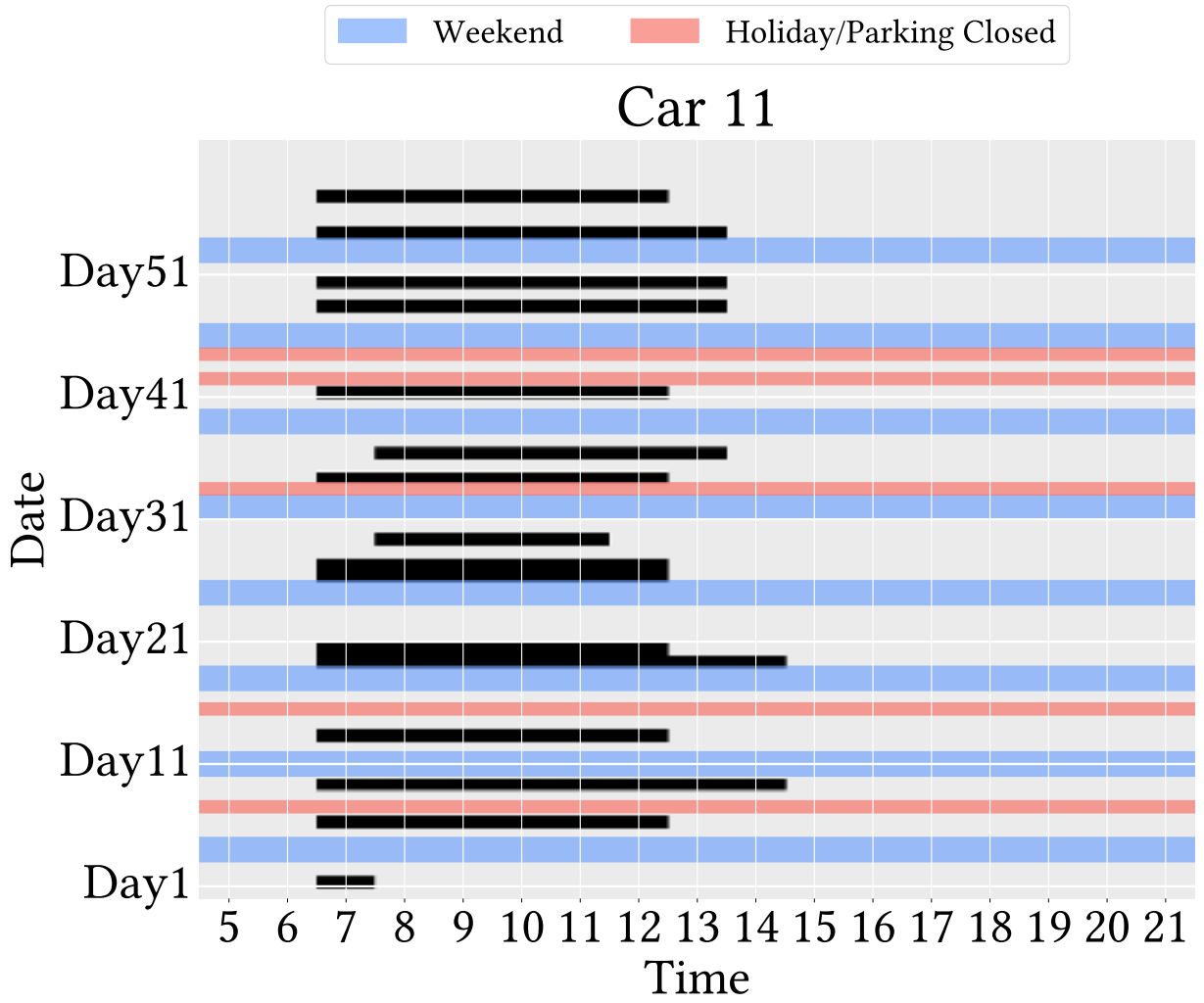
Long Term Patterns (II)





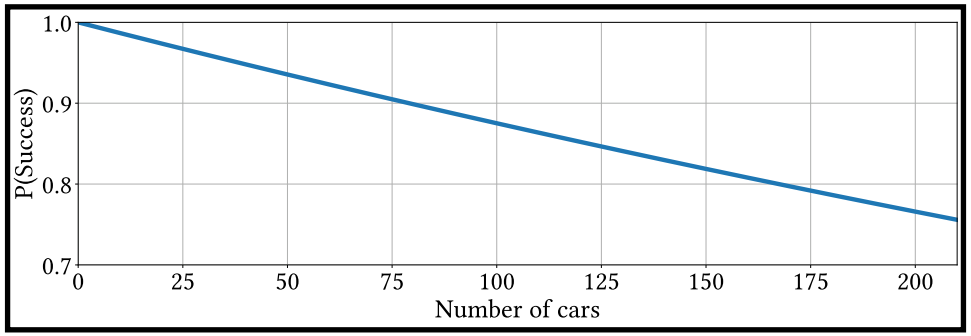
Long-Term Patterns (III)

- Some brands are chattier than others:
  - Some sensors only transmit when the car starts moving
  - Others transmit from time to time even when stopped
  - The last type transmits at all times in regular time periods
- In our research:
  - All Toyotas that we looked into transmit at least every 15 min even when stopped
  - High-Transmit power as well

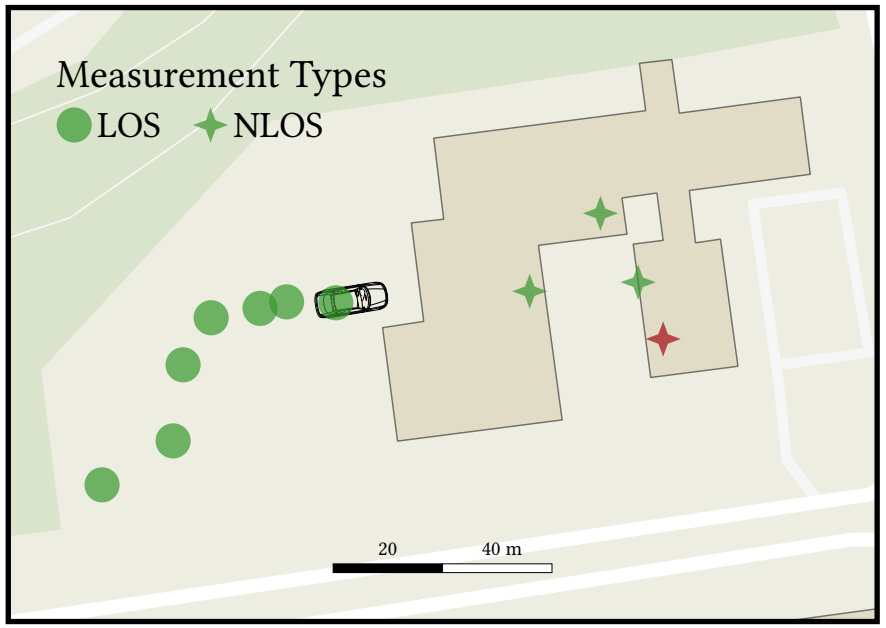


What happens with more/moving/faraway cars

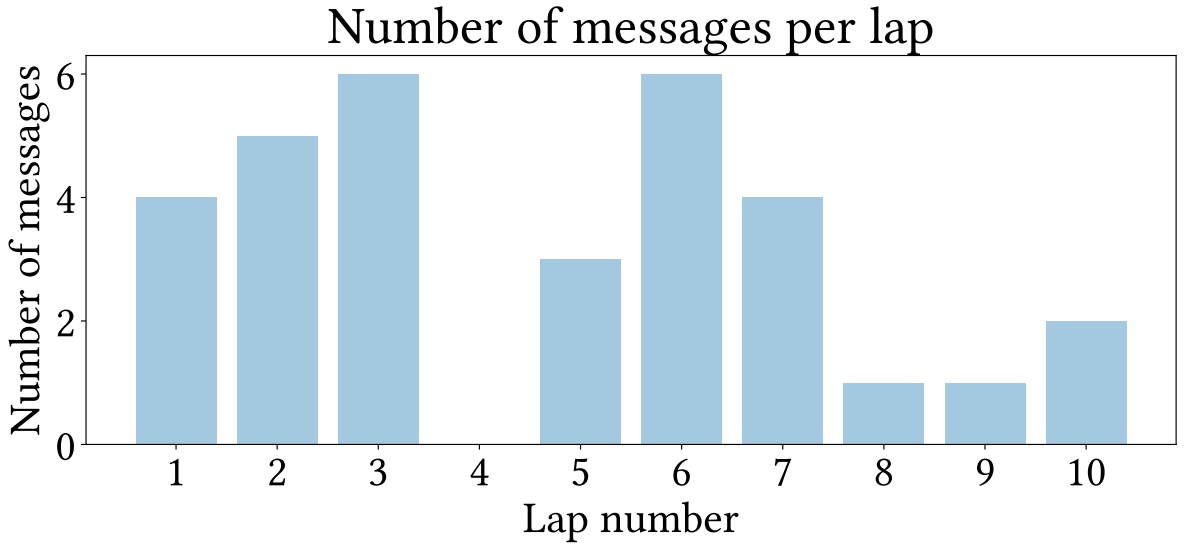
- We estimate that 1 sensor can track:
  - Around 200 cars can be tracked in 30 second windows



- We estimate that 1 sensor can track:
  - Much more than 60 m even in NLOS



- Up to 50 kph:
  - We can capture messages ‘easily’



…To active attacks

Study: Renault ZOE (2021)



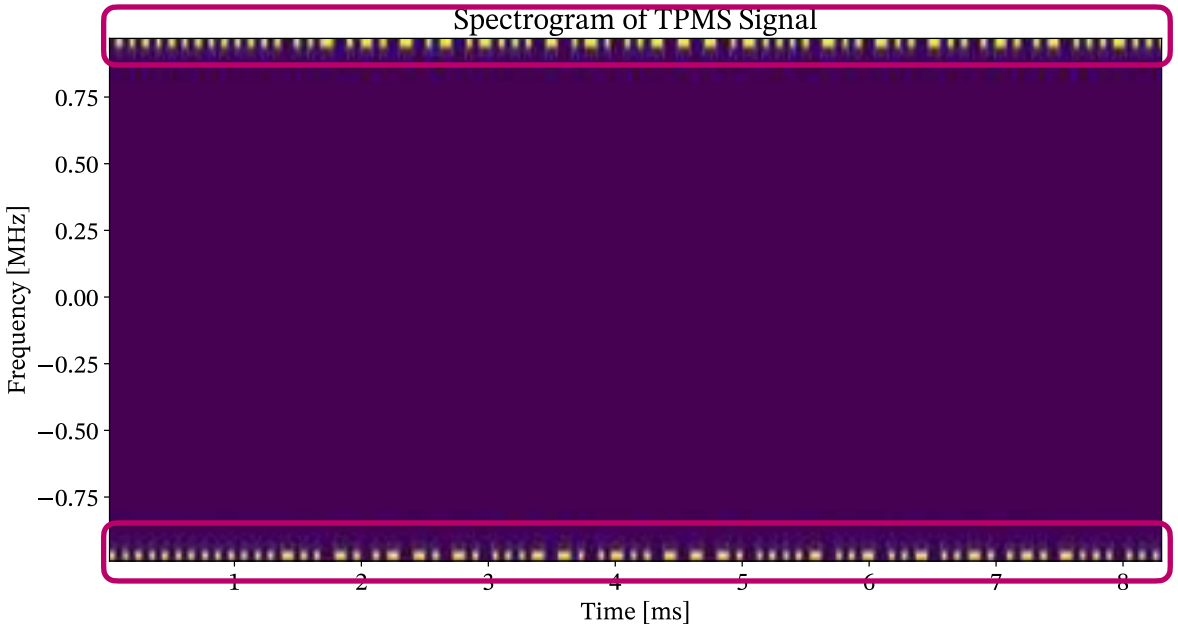
- **Renault** uses **dTPMS** technology:
  - Modulation is widely known
  - We build a signal spoofer to test how the car responds to different messages
- Some of the characteristics:
  - Frequency: 433 MHz
  - Modulation: 2-FSK + PWM
  - Manchester Encoding
  - Bit duration: 52 µs
  - Main fields:
    - Flags (1 byte)
    - ID (3 bytes)
    - Pressure (2 bytes)
    - Temperature (1 byte)
    - Unknown (2 byte)

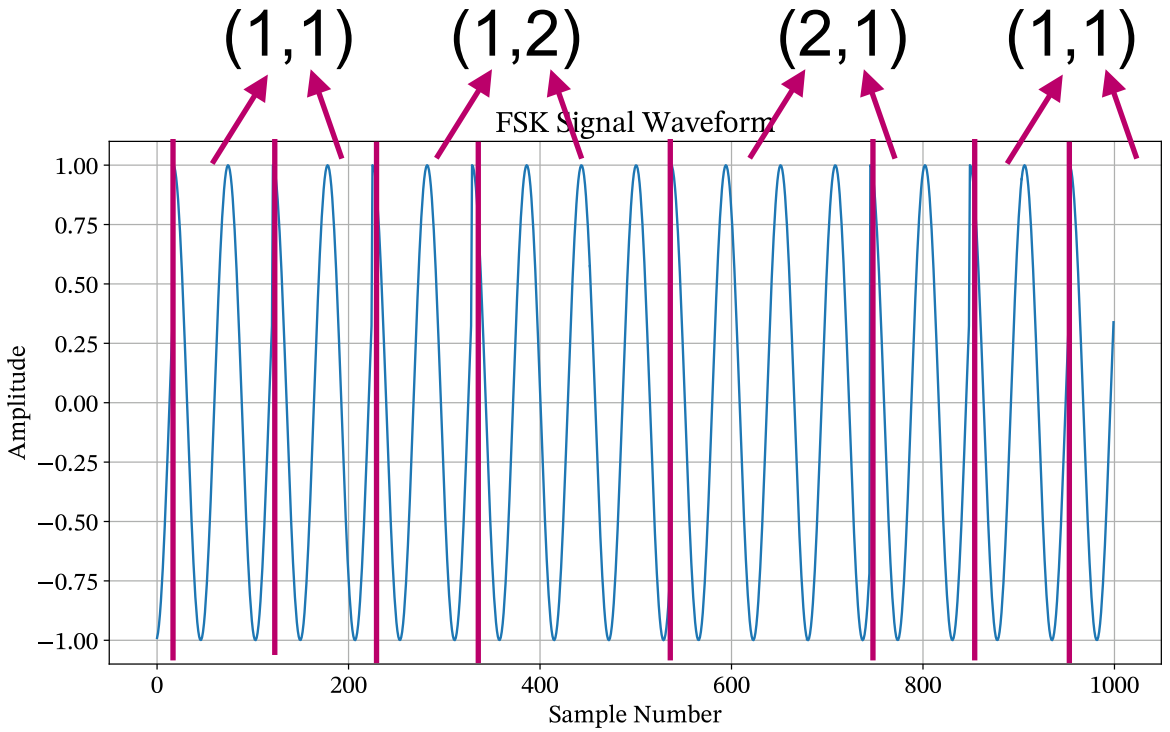
Toolset: SDR with RX/TX capabilities



From PHY to Pulses

- 2-FSK generates a sequence of pulse-gaps:
  - We decode FSK and generate tuples





From Pulses to the message

From a sequence of tuples:
[(1,1),(1,2),(2,1),(1,1),…]

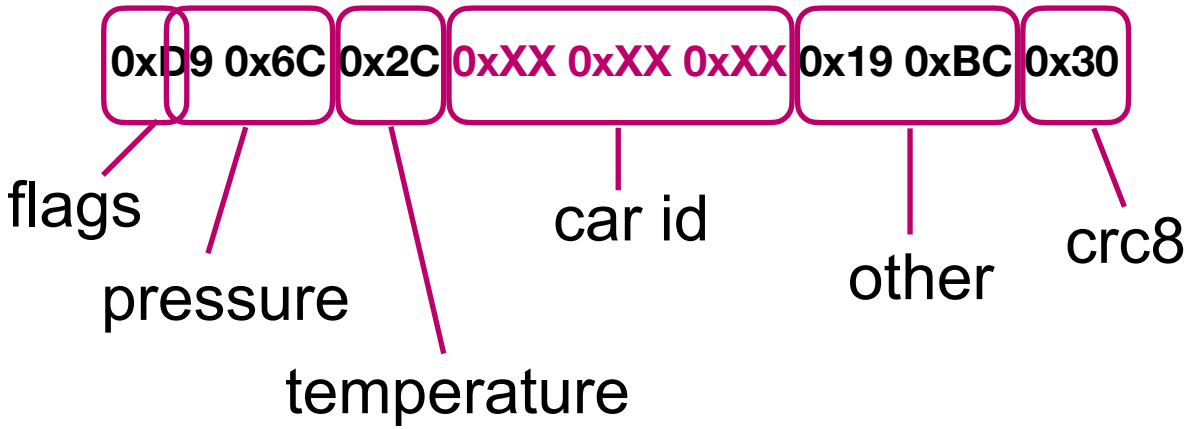
We generate a sequence of bits:
1010011010…

We invert the sequence:
0101100101…

Manchester Decoding:
11011…

We find the preamble:
For Renault cars, it is **0xaa, 0xa9**

Final Message



How to Transmit?

We reverse the flow 😊

Producing Errors



Wrapping up…

What are the conclusions?

- dTPMS systems are widely vulnerable to all sorts of attacks:
  - Given the current status of SDR hardware attacks that combine passive monitoring and active spoofing are quite feasible
- Passive Monitoring can affect some brands (Toyota) more than others
- What solutions exist:
  - Ditch dTPMS (not feasible for all cars in the streets)
  - Add rolling IDs (same as car key fobs)
  - Add encryption (research has shown it is possible)
- We provide 2 repositories to replicate this research

tpms-analysis



tpms-tools



Follow us on...



LinkedIn

Website

cydcampus.admin.ch

CYD | CYBER DEFENCE CAMPUS