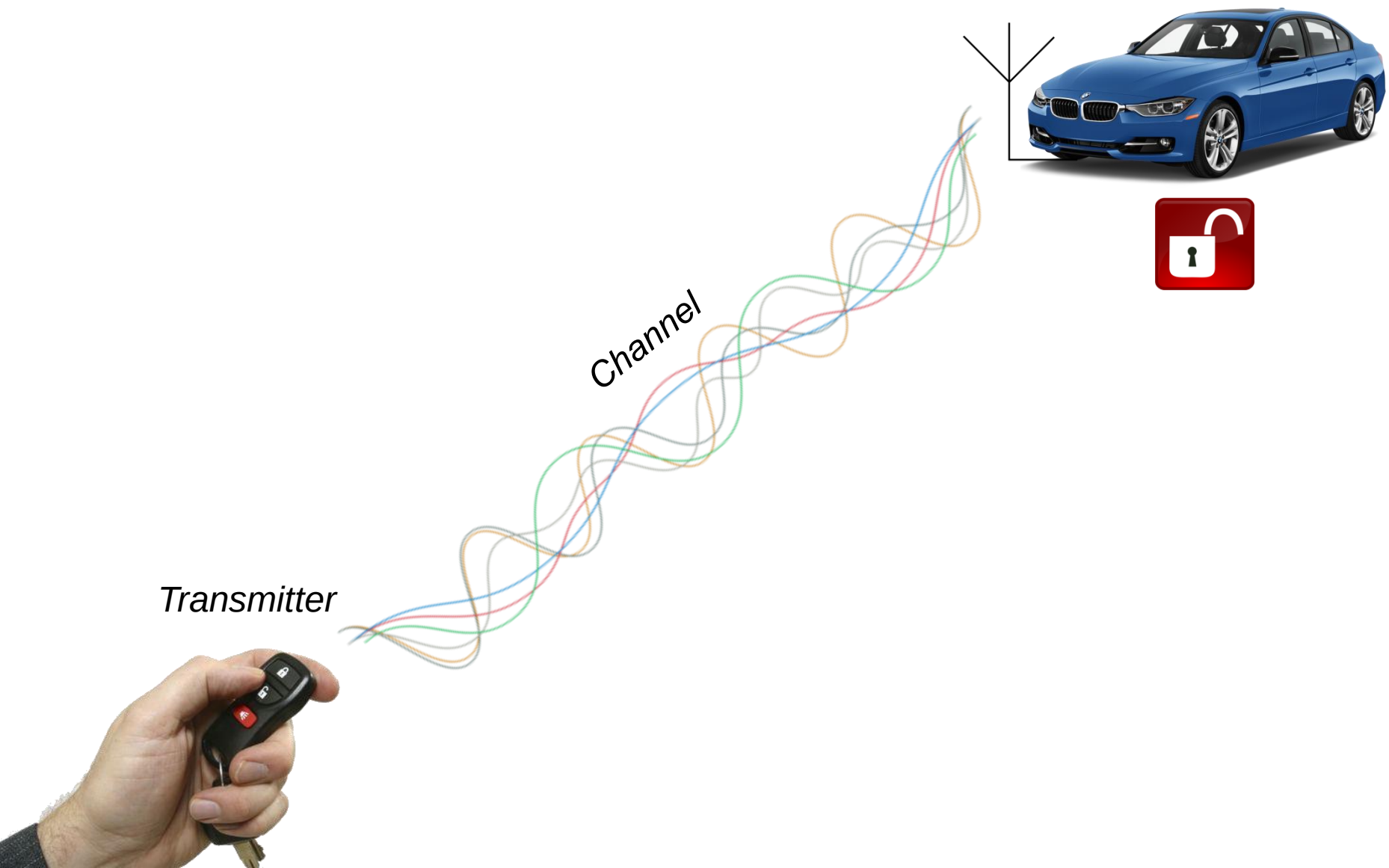
CAR KEY JAMMING DETECTION

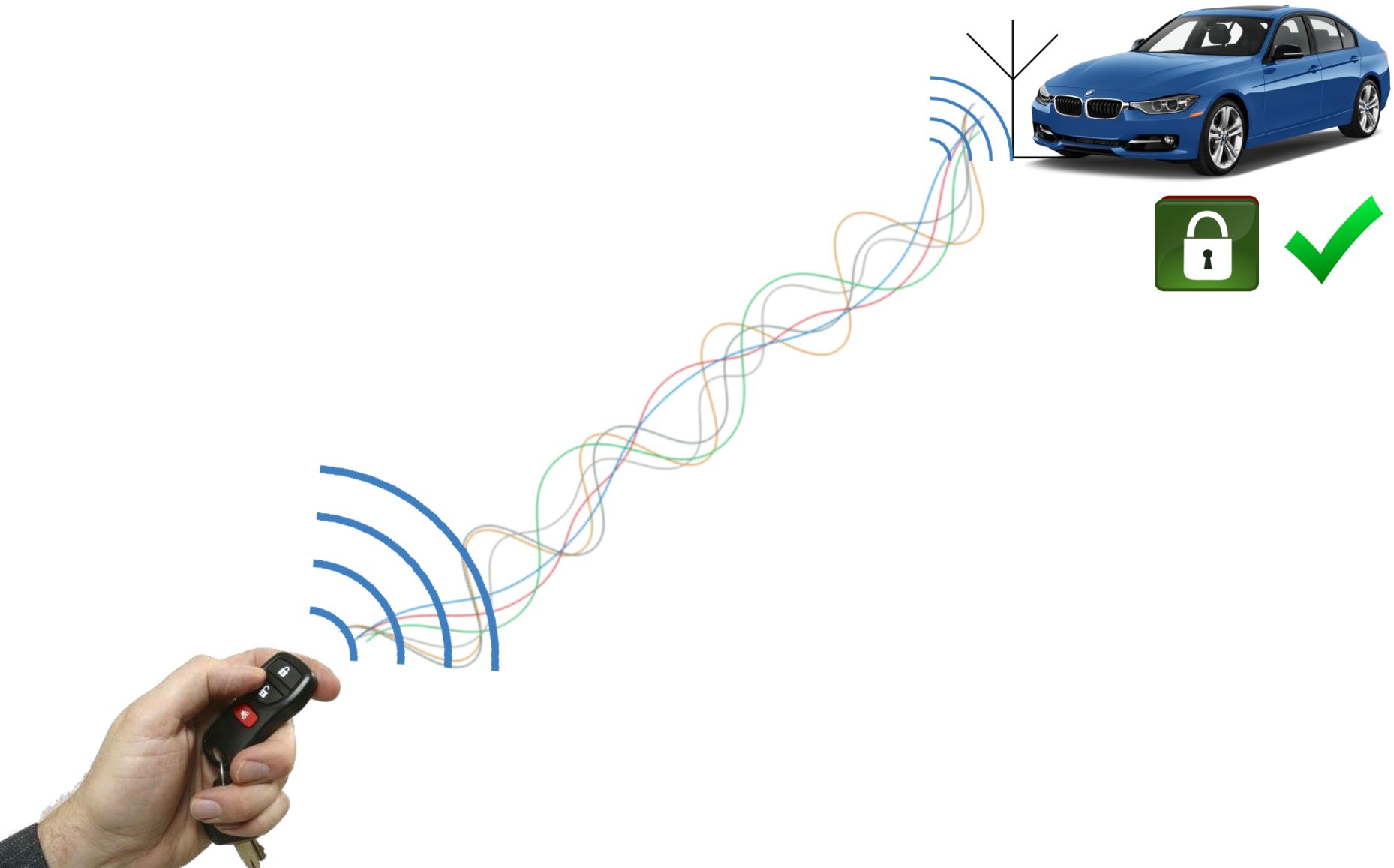
By Khodor Safa

17th August 2017

How does Jamming Work?



No Jammer



What happens when you introduce a jammer?

With Jammer

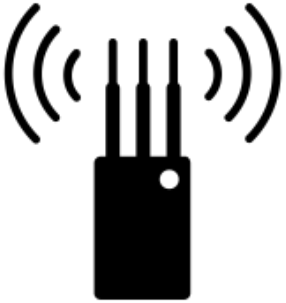
How to prevent against jamming attacks?

Use a Physical lock

Check car doors

Install a jamming detector

Project Process



Car Key Signal Detection

- Testing Different Keys
- Testing Range

Signal Jamming

- Investigate Jamming Techniques

Jammer Detection

- Investigate Jamming Detection methods

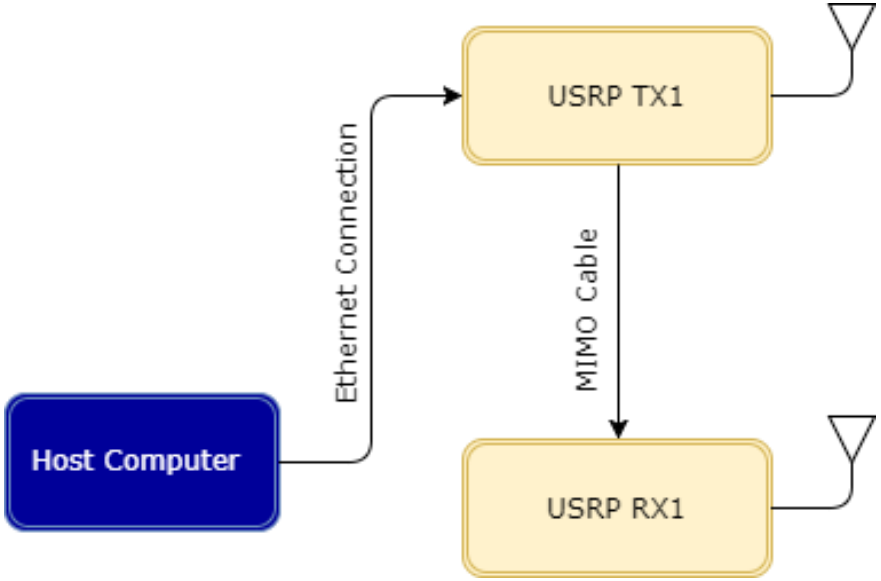
Project Setup

USRP 2920

VERT2450 Antenna

Ethernet Cable

MIMO Cable



Car Key Signal Detection

I. Car key fobs operate at 315MHz or 433MHz frequencies

II. A total of 6 available keys have been tested on:
    1. Three Mercedes keys
    2. One Mazda key
    3. Two KIA keys

III. The testing parameters:
    Distance and Power

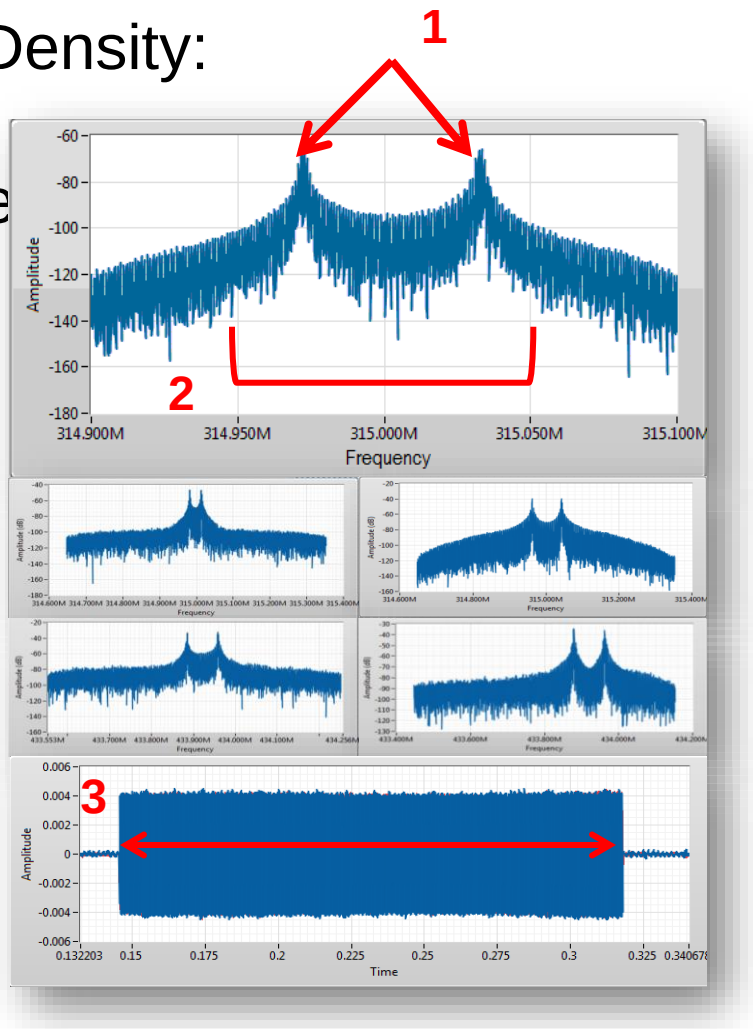
Car Key Signal Testing - Results

Looking at the Power Spectrum Density:

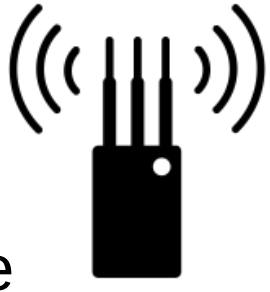
1. We notice that we always have two peaks representing distinct frequencies.

2. The bandwidth for these results does not exceed 200KHz

3. The transmission time is very short



Signal Jamming



Based on the previous three results, we can conclude these minimal Jammer requirements

- Centered at 315/433MHz
- The bandwidth can be fixed to 200KHz
- It should be running *before* activating the key signal

Types of Jammers

Reactive Jamming

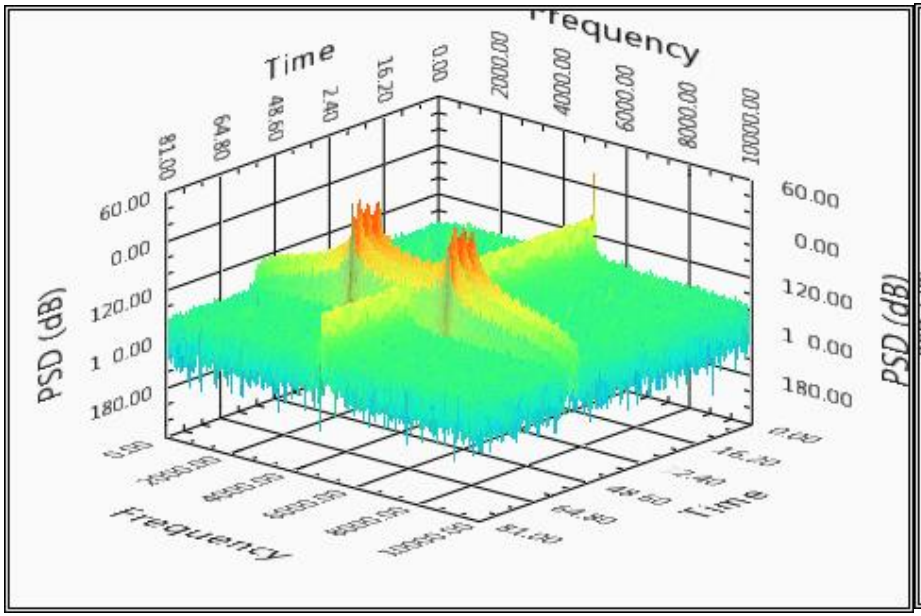
- Waits until there is transmission over the channel to start jamming

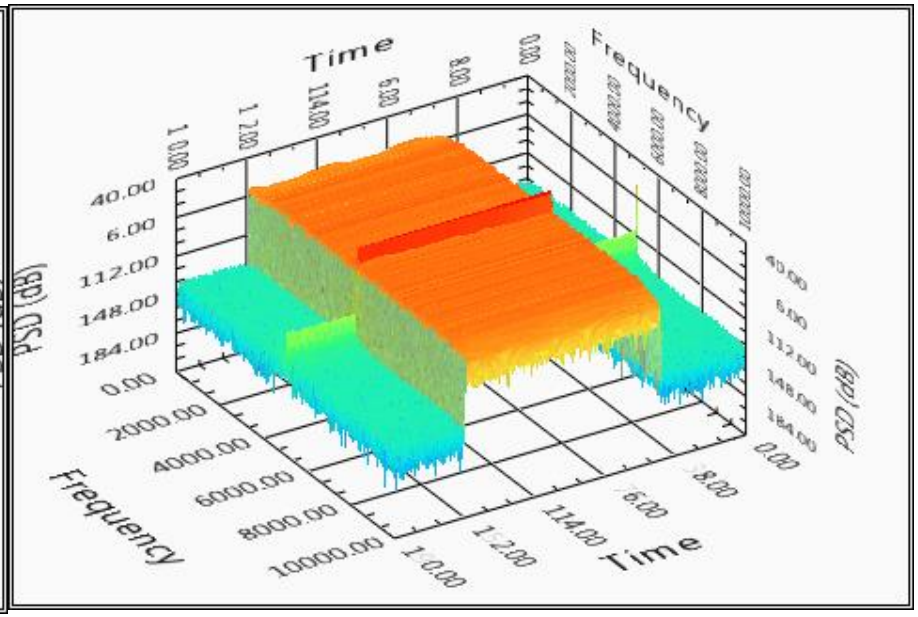
Proactive Jamming

- Transmits data regardless if there is a communication link

Jamming Techniques

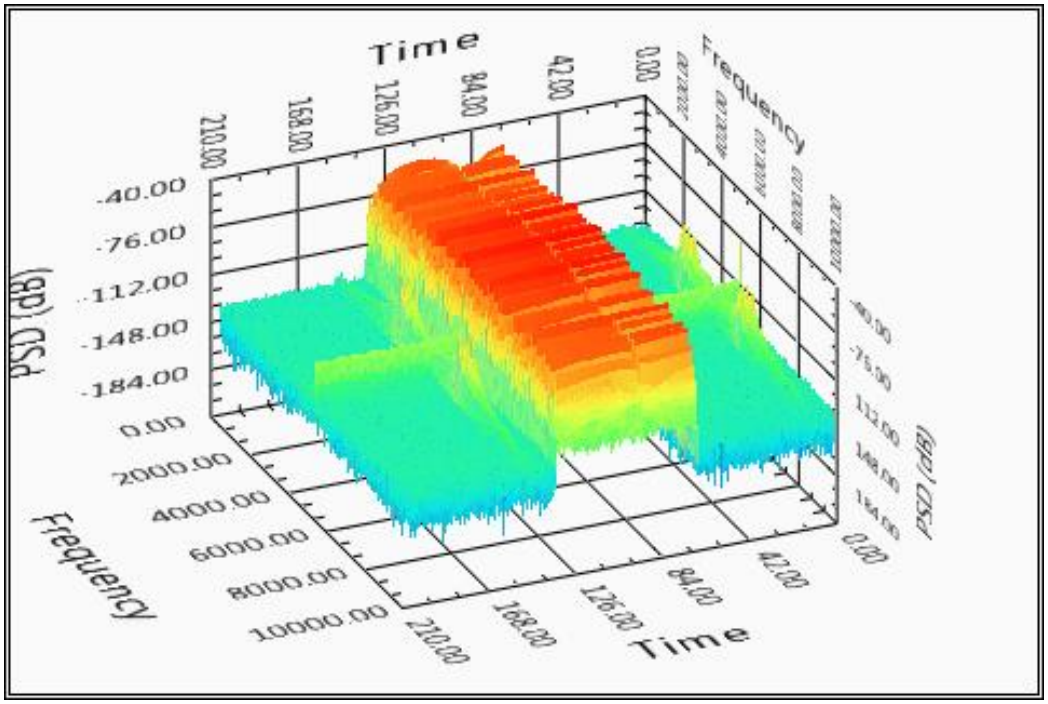
Increasing the noise floor (White Noise Jamming): transmitting random data with *high power*, to *drown* the message signal or cause enough *interference* to distort it





Jamming Techniques

Single or Multi-tone Jamming: transmit at a single or multiple frequencies at a higher power to jam the targeted message.



Pros and Cons

White Noise Jamming

Pros: high jamming efficiency

Cons: high power consumption

Multi-tone Jamming

Pros: low power consumption

Cons: lower jamming efficiency

Jamming Detectors Scope

Industrial Scope

Commercial Scope

Commercial Product

Device Description:

Installed inside of the car

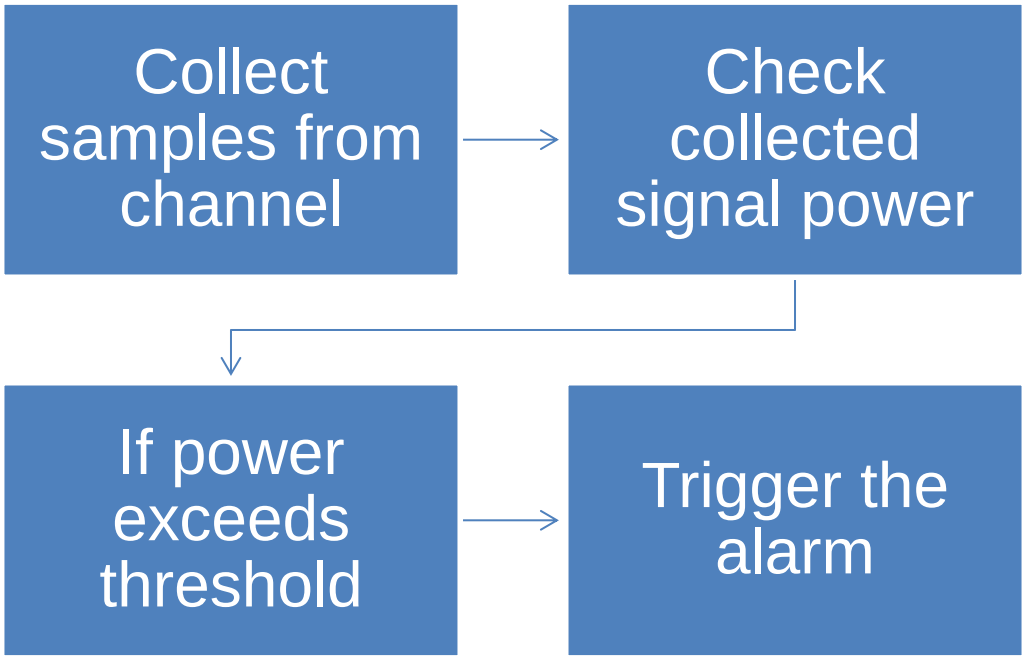
Connected to the car battery for power

Scans environment for any undesirable signal that might interfere with the message

Jamming Detection Methods

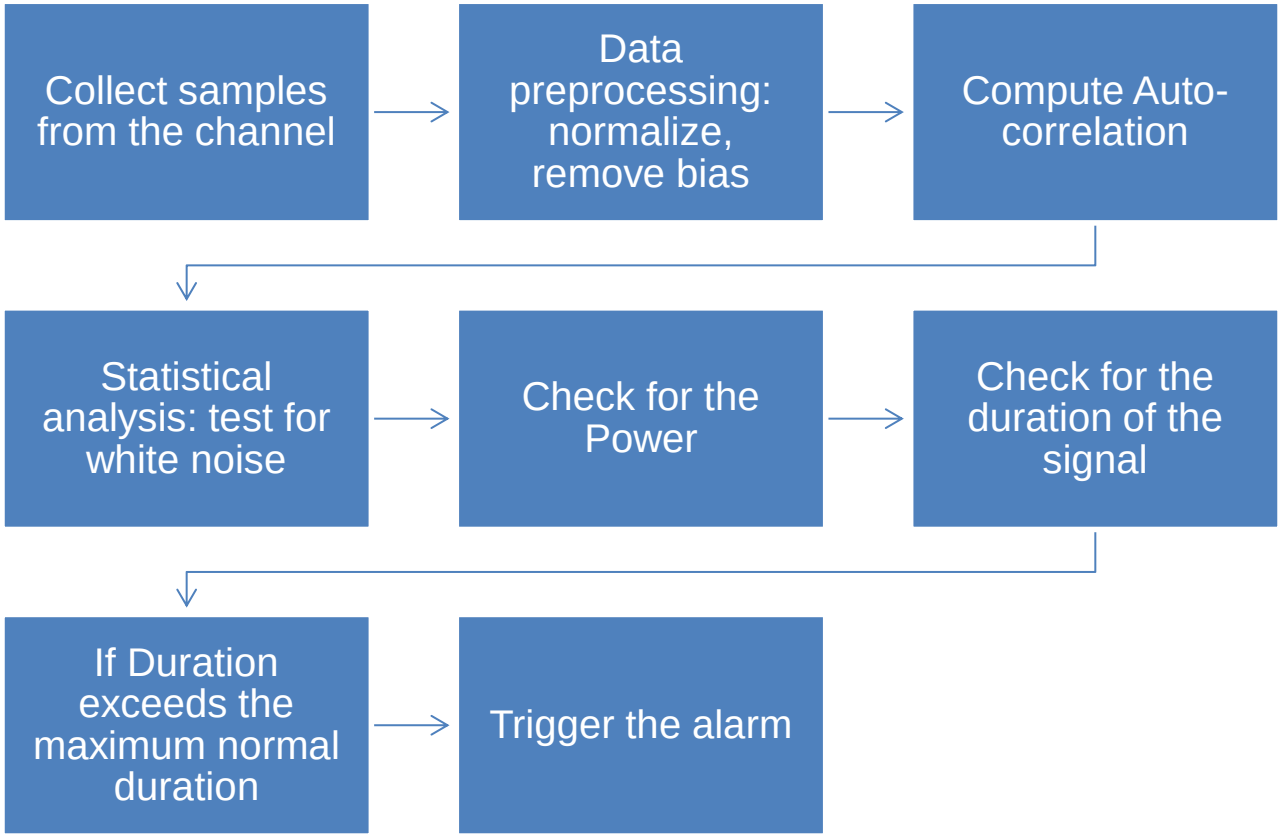
Define the parameters for the following method: ***power*** of detected signals and their **duration** (**time)**.

Method 1: threshold monitoring



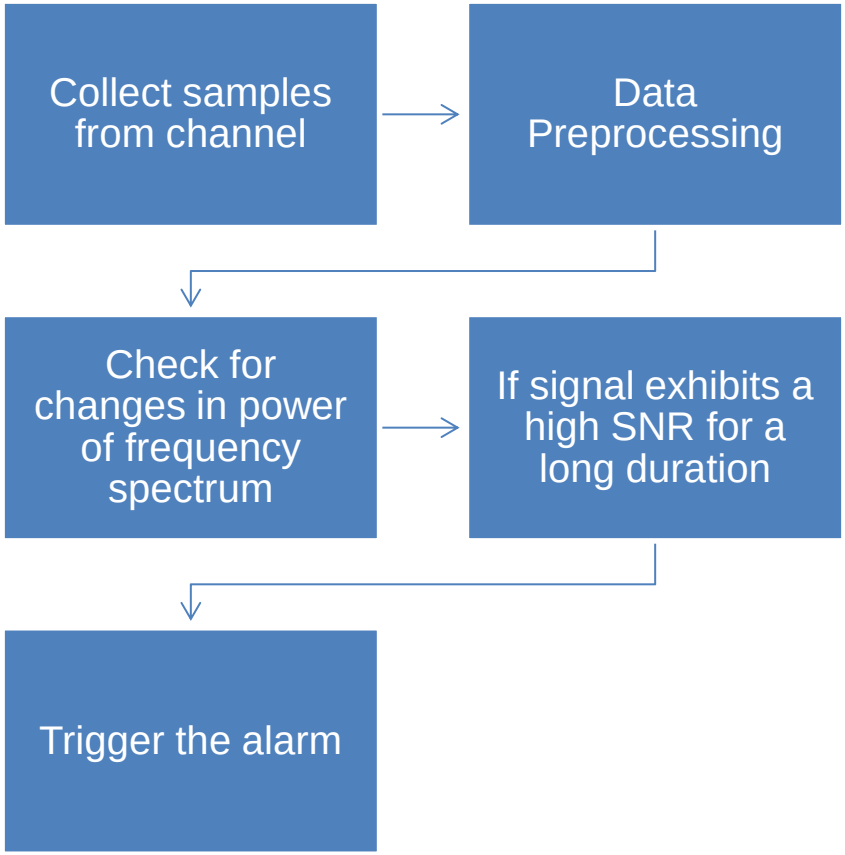
Jamming Detection Methods

Method 2: Noise Floor monitoring

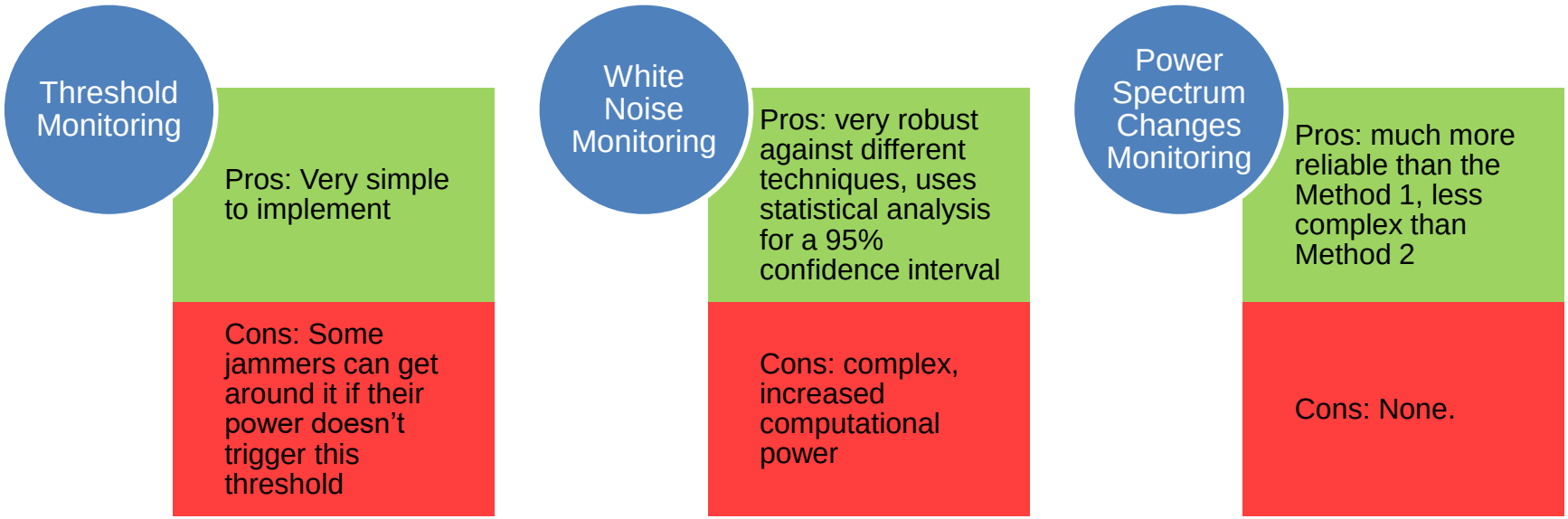


Jamming Detection Methods

Method 3: Spectrum changes monitoring



Jamming Detection Methods



Current Solutions: Sanji ZX JamAlert

1. Can be installed to any type of vehicle
2. It is activated when the ignition is off, then starts monitoring the environment for any jamming signal
3. It sounds an alarm when it detects any remote jamming signal

SANJI INTELLICA

Observed Problems with this solution

The device is activated when it senses that the ignition is off. We can infer that it does not take into account the cases when the car is being locked and unlocked without triggering the ignition, which in turn does not trigger the security system rendering it useless against attackers.

The description specifies that it detects remote jamming with no indication if it is adaptable to different types of jammers, which raises questions concerning its robustness and reliability.

Challenges

Student Mindset

Constructing a solid framework

Lack of specific documentation

References

1. http://www.sanji.co.za/zx%20jamalert.htm
2. https://www.iol.co.za/motoring/cars/hyundai/protect-your-hyundai-from-remote-jammers-2010311
3. http://www.carmag.co.za/news_post/hyundais-anti-car-jammer-device/
4. http://www.news24.com/Video/Motoring/watch-how-to-prevent-your-car-from-getting-signal-jammed-20160307
5. Grover, Kanika, Alvin Lim, and Qing Yang. "Jamming and anti–jamming techniques in wireless networks: a survey." *International Journal*
6. *of Ad Hoc and Ubiquitous Computing* 17.4 (2014): 197-215.
7. Li, Mingyan, Iordanis Koutsopoulos, and Radha Poovendran. "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks." *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, 2010, pp. 1119-1133.

Questions & Answers

Acknowledgements

Special thanks to:

- National Instruments
- Ramzi Mourtada – Internship Program Mentor
- Samah Chazbeck – Project Mentor
- BDD Community

Contacts details:
E-mail: khodor.m.safa@gmail.com
Phone Number: +96171396944