Defending Ultrasonic Sensors Against Spoofing in Autonomous Vehicles

EECS 452 – Digital Signal Processing Design Lab

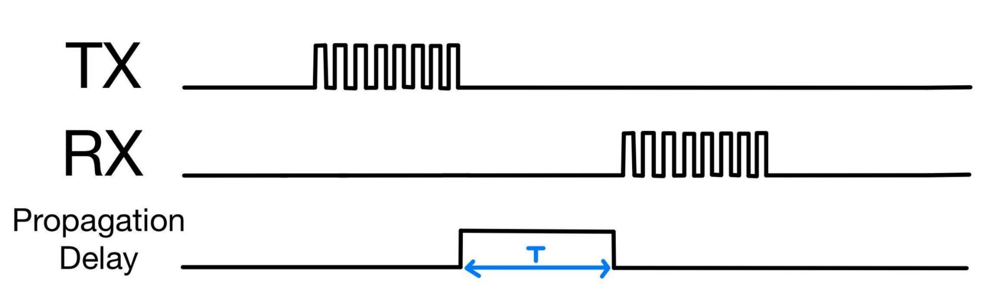
Jack Brady, Leela Mukherjee, Ian Steele

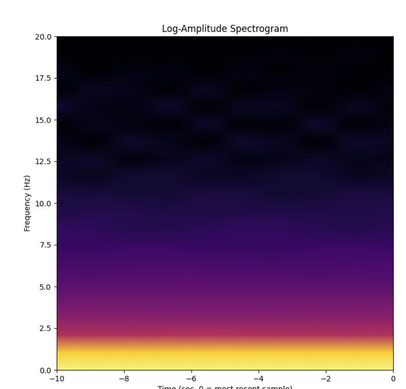
Background & Intro

Ultrasonic sensors are used in autonomous vehicles (AVs) for close-range tasks like parking, blind spot detection, and other ADAS functions, offering a low-cost alternative to LiDAR.

Although rare, attacks can cause serious failures, like missing an obstacle or false detection, leading to accidents. Given this semester's focus of Privacy & Security, we investigated and replicated how these sensors can be attacked.

An ultrasonic sensor determines the distance from objects by sending out a burst of pulses, which bounce off from the object and are received again. The distance from the object is calculated by taking the time difference.

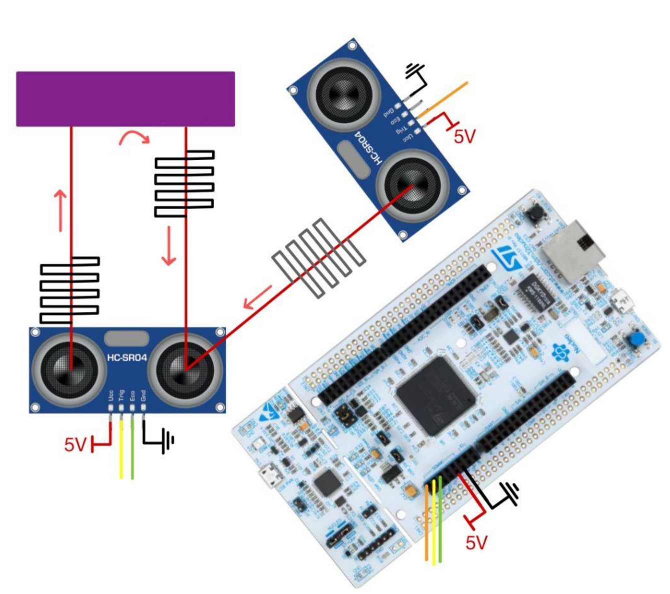




STFT shows overall lower values

Design Choices

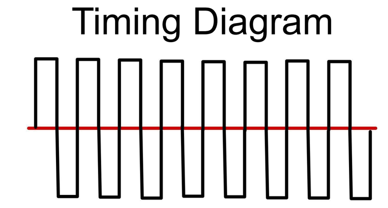
- Two HC-SR04 U/S sensors
  - Attacker - Sends interference pulses
  - Defender - Measures distance of closest object
- Sensor Limitations
  - Susceptibility to signal deflection, absorption by soft materials, and blind zones
  - Analog processing on-chip (i.e no easy way to read raw signal)
  - Lack of documentation
- Comparison with other ultrasonic sensors
  - AV-grade sensors offer improved resolution, longer range, and narrower field of view (FOV), minimizing crosstalk
  - Built-in filtering capabilities and digital outputs (CAN, LIN)

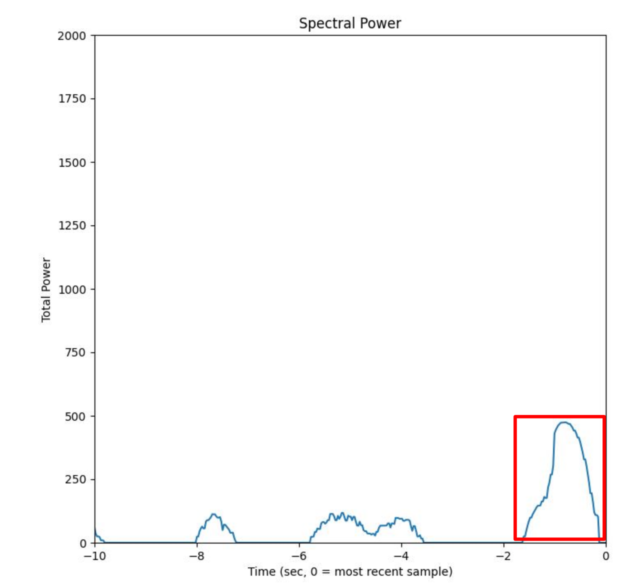


Attack Signals and Processing

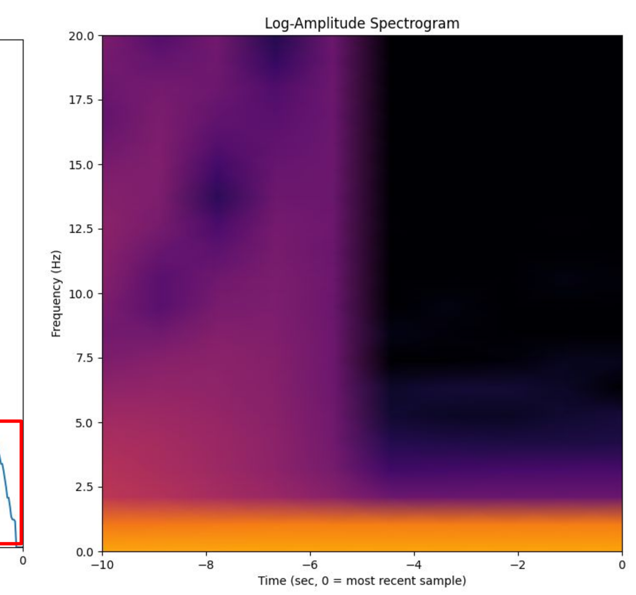
Jamming Attack

Timing Diagram





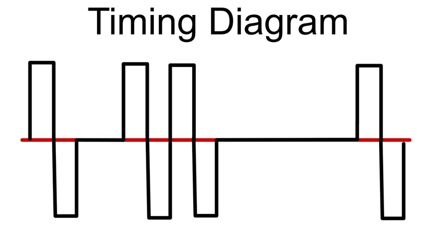
Spectral power jumps, then drops incredibly low - very quiet signal

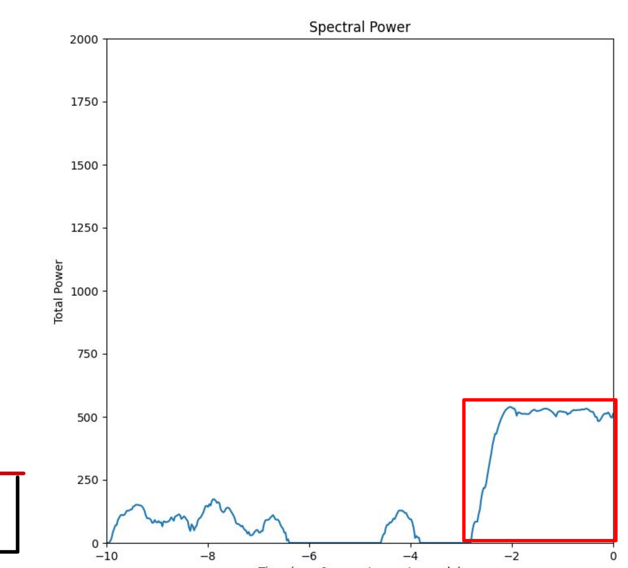


STFT shows a sharp increase in certain higher freq., then only DC

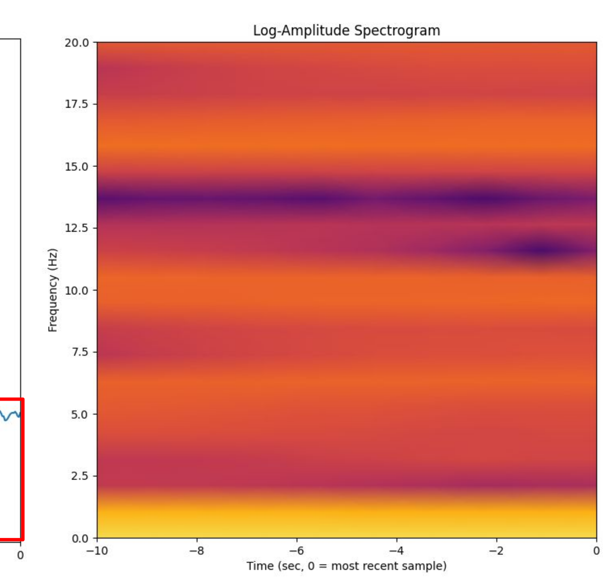
Random Spoofing Attack

Timing Diagram



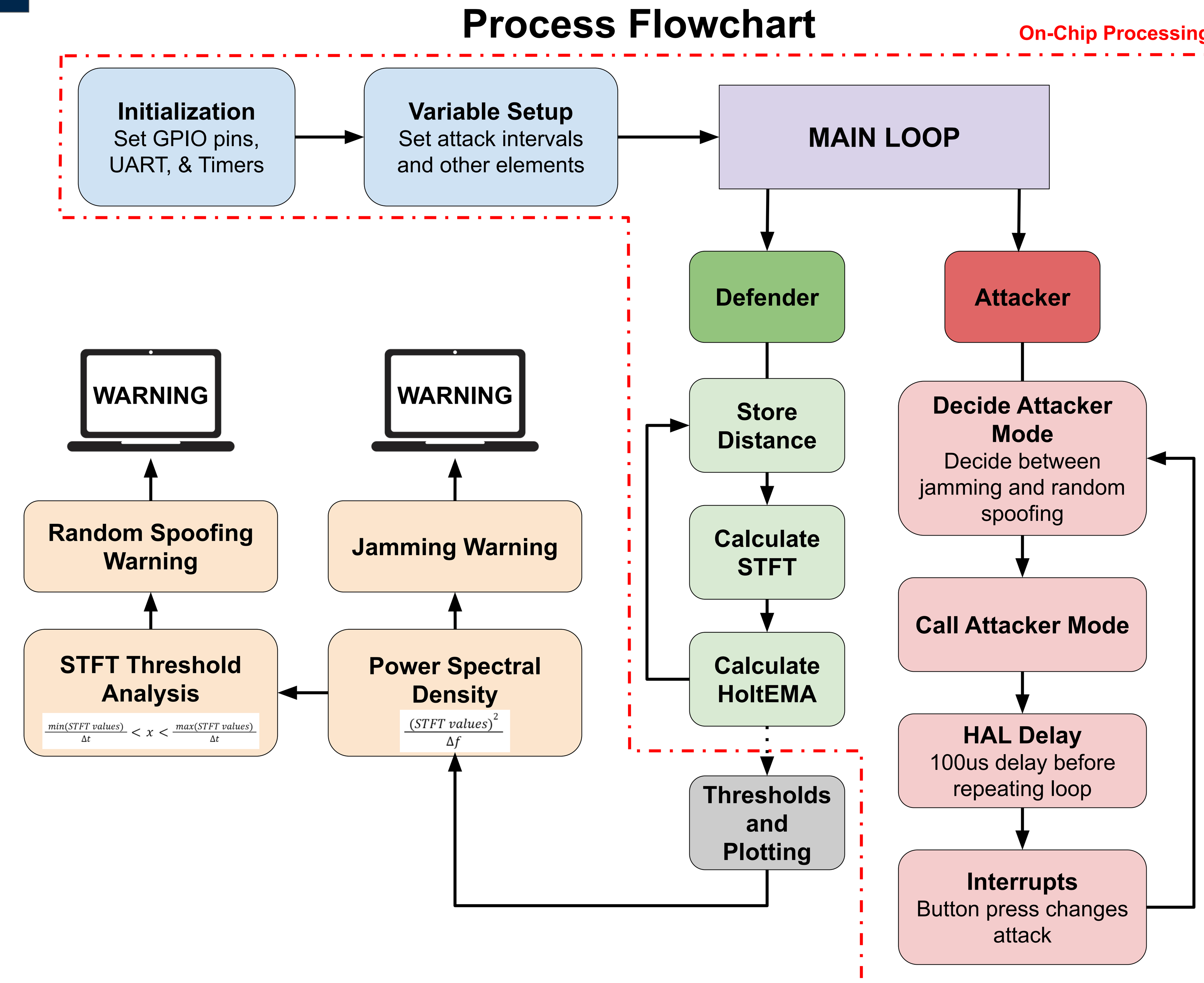


Spectral power jumps up and stays high - lots of freq. content



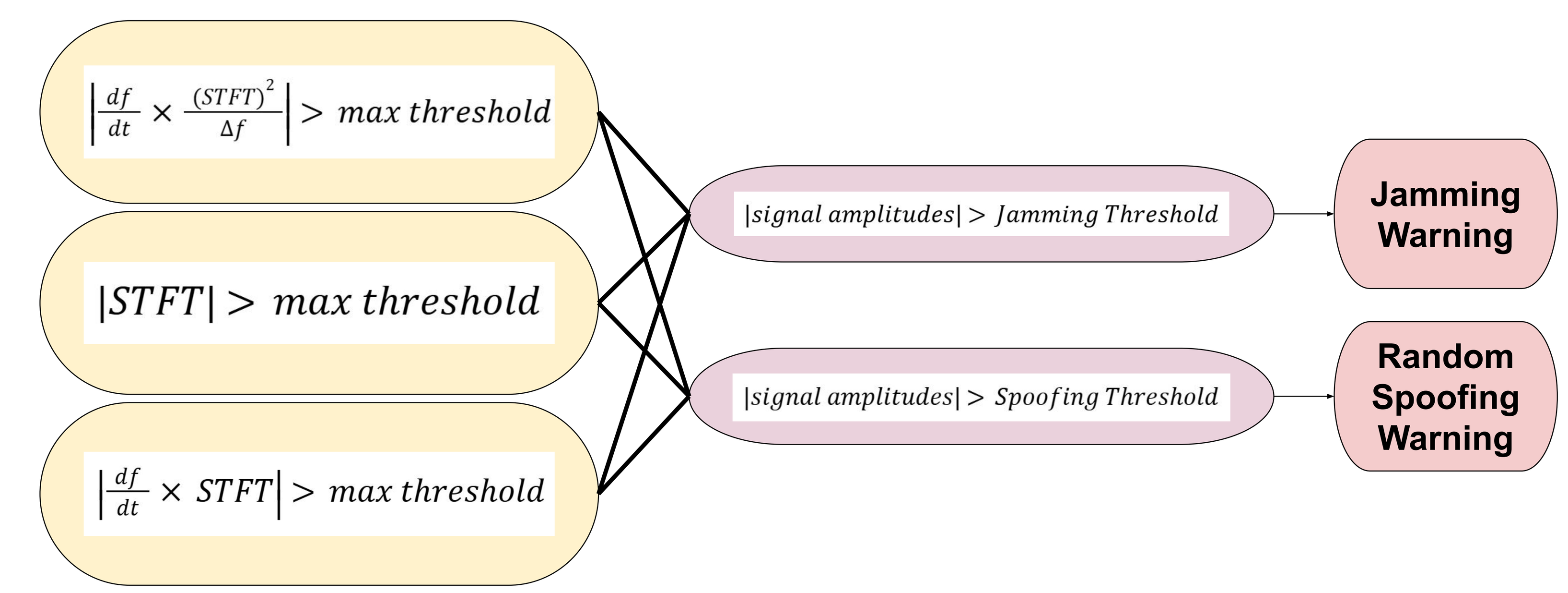
STFT shows higher values, including lines on certain freqs.

Process Flowchart



Anti-Spoofing Algorithm

- Successfully detects attacks and sends a warning
  - STFT looks for repeated anomalies in frequency
  - Spectral power analysis looks sudden changes in frequency components of the signal
- We weren't able to clean the signal
  - Relied on a Holt exponential moving average to smooth the data under normal operation
  - Consumer AVs typically ignore sensor data rather than clean it, so our approach makes sense



Conclusions

- Attacking a single sensor is relatively straightforward, especially the HC-SR04
- With our sensor limitations, cleaning data in real time poses significant technical challenges
- Individual sensors are prone to eventually fail
- Need redundancy in sensor type and placement, along with intelligent systems to recognize failures
- As implemented in industry, sensor fusion is the best way to ensure safety in autonomous vehicles

References & Acknowledgements

We would like to thank Professor Revzen, Marion Anderson and Daphne Zhou for their guidance throughout the semester.

References:

1. Lou et al., 2021, "SoundFence: Securing Ultrasonic Sensors in Vehicles Using Physical Layer Defense", IEEE Xplore
2. Islam et al., 2024, "A review of cyber attacks on sensors and perception systems in autonomous vehicles", Journal of Economy and Technology
3. Xu et al., 2018, "Analysing and Enhancing the Ultrasonic Sensors Security for Autonomous Vehicles and its Enhancement", IEEE Xplore