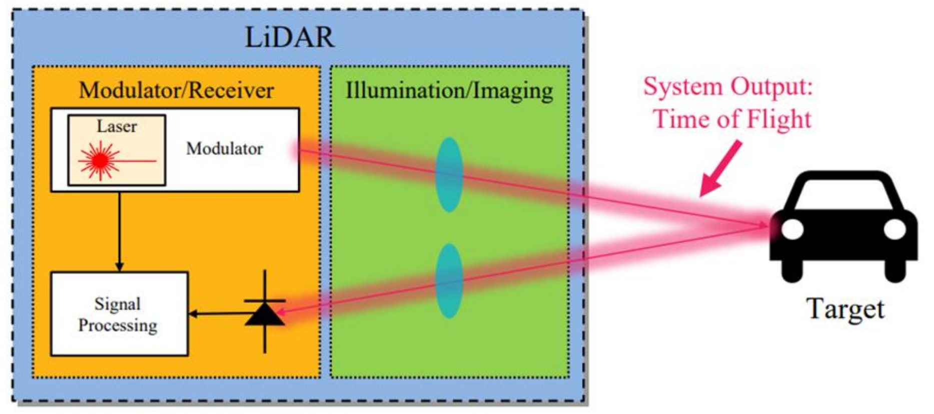
Secure Frequency Encryption FMCW LiDAR System

Marziyeh Rezaei, Liban Hussein

01

Background

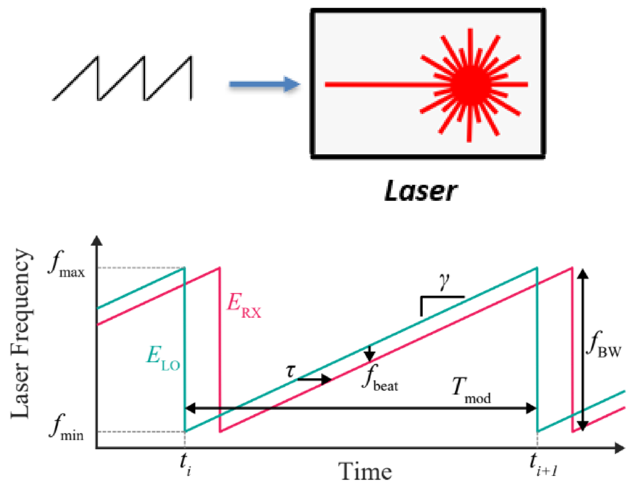
- Robust and secure sensing and imaging capabilities are necessary for future autonomous vehicles
- LiDAR is a major 3D imaging technology used for accurate range and velocity measurement
- Typical LiDAR system can have security vulnerabilities that pose threats to human safety
- This work investigates:
  - Different security vulnerabilities of LiDAR systems using MATLAB Simulink
  - Frequency encrypted beam-steering frequency modulated continuous wave (FMCW) LiDAR systems
- Frequency encryption (FE) technique makes LiDAR systems robust against possible attacks



[Kim, Berkeley]

FMCW Beam-Steering LiDAR

- Most promising LiDAR architecture from performance and security perspectives
- Laser frequency is linearly modulated with a ramp signal
- There is a constant frequency difference between Tx and Rx signals known as *beat frequency*, which is linearly proportional to Time of Flight (TOF)
- At the receiver, RX and TX lights beat together and beat frequency is calculated
- By measuring the beat frequency, **the distance to the object can be determined**

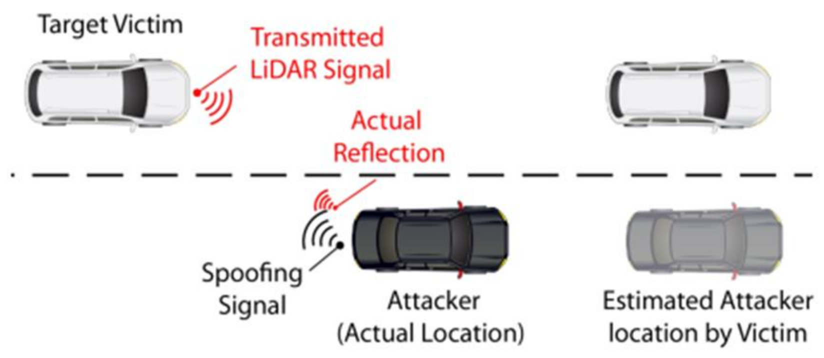


$$\gamma = f_{BW}/T_{meas}$$
$$\Delta f = \gamma\tau_{TOF}$$

Adversarial LiDAR System Attacks

The most spiteful types of attacks are:

- ***Jamming***
  Attacker transmits light (incoherent with victim's laser) with high power to saturate victim's receiver
- ***Spoofing*** *(Most Detrimental)*
  Attacker can lock its laser frequency to the victim's LiDAR and overwrite the actual reflected signal with its spoofing signal



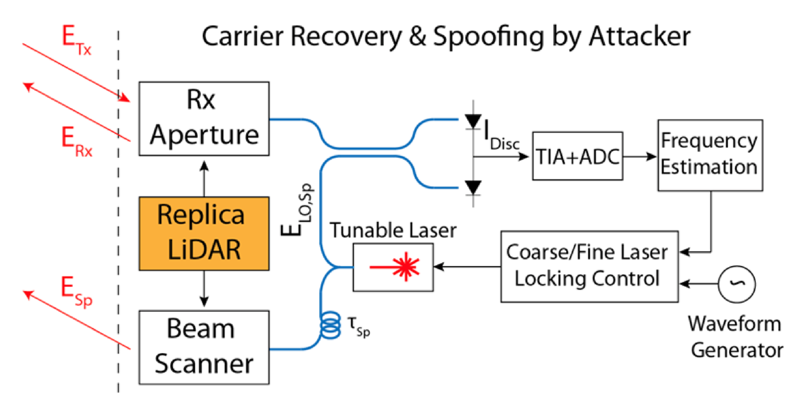
Spoofing Attack Architecture

- Attacker has a replica LiDAR, Optical Phased Locked Loop (OPLL) and Frequency Estimation blocks.
- The proposed attacking scenario has 3 steps:

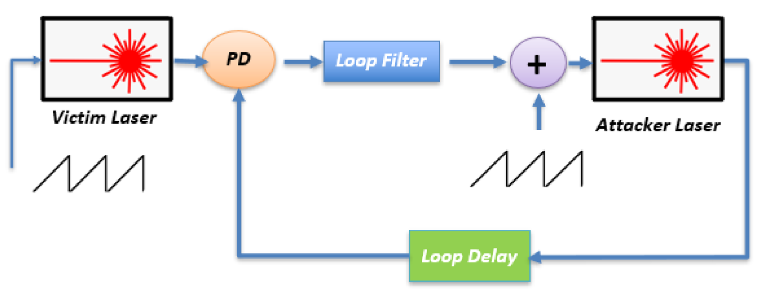
1. Coarse Tuning:
Decreases the wavelength offset between attacker's laser and victim's laser to be in the range of photodetector BW.

2. Fine Tuning (using the OPLL):
Attacker locks its laser frequency to the victim's laser using OPLL and finds the chirp rate (The locking time of the OPLL is higher than the attack requirement, so another step is required).

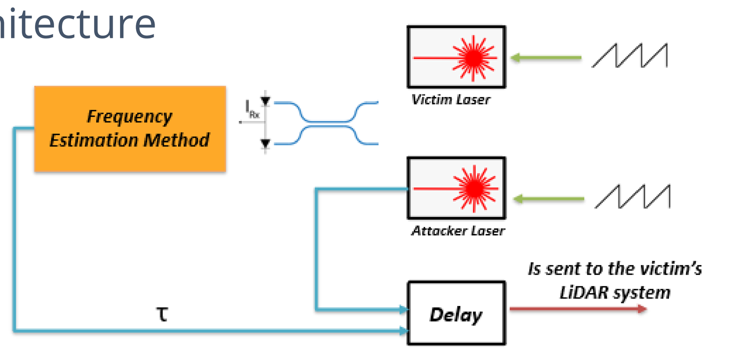
3. Time Tuning (using zero-crossing method):
Attacker finds the delay between its laser and the victim's laser, then it delays its output signal and sends it to the victim receiver to fool it.



Attacker Architecture



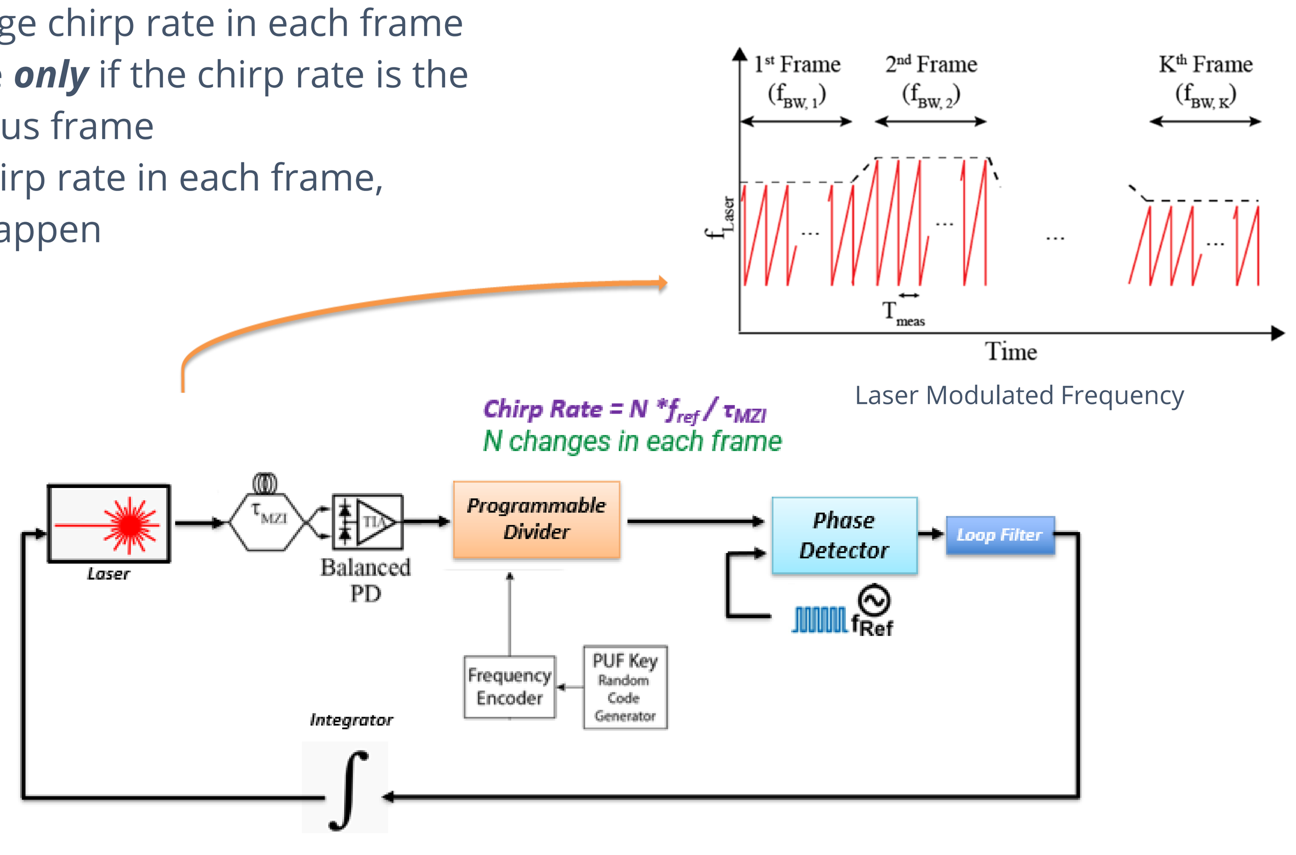
Attacker OPLL



Attacker Frequency Estimation Architecture

FE-FMCW LiDAR using Electro-Optical Synthesizer

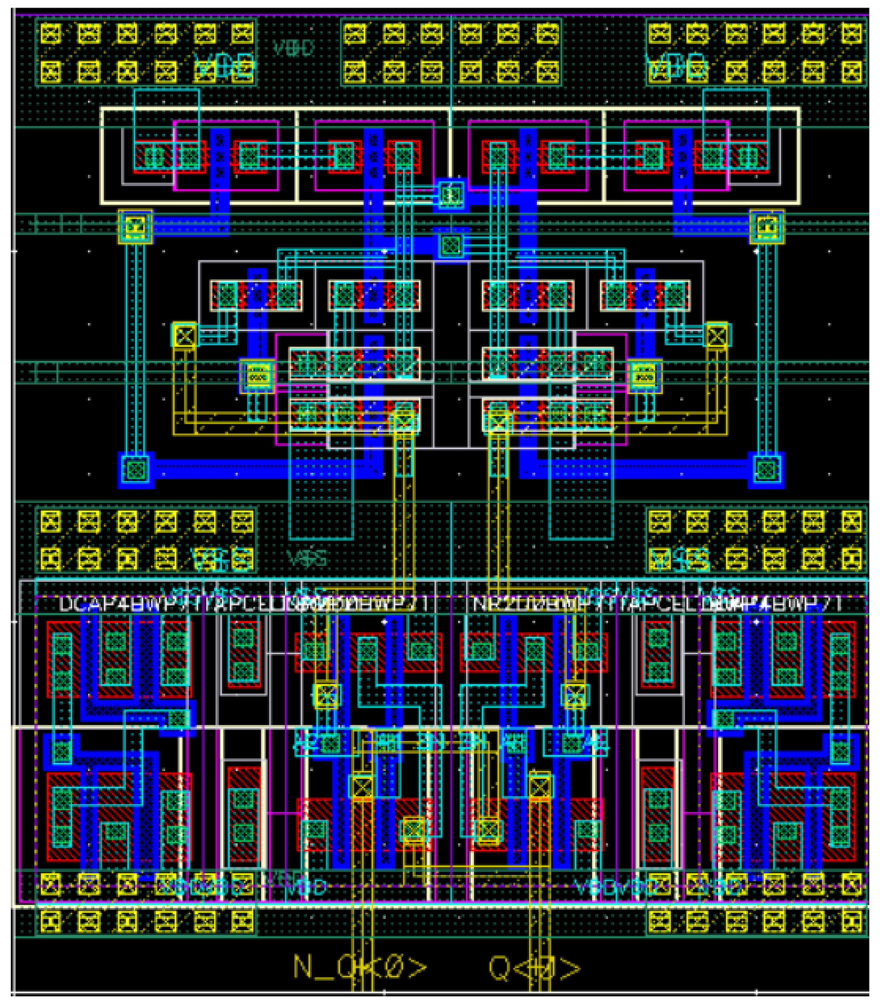
- The idea is to change chirp rate in each frame
- Step 3 can be done ***only*** if the chirp rate is the same as the previous frame
- By changing the chirp rate in each frame, attacking cannot happen



EO-Synthesizer

Frequency Encryption: Physically Unclonable Functions (PUF)

- Known chirp rate provides attacker with information necessary to attack LiDAR system
- Randomizing this chirp rate for each frame makes the system impossible to hack
- Implemented using physically unclonable function (PUF)
- Inherent variations in devices generate "unique" ID to be assigned for chirp rate generation
- SRAM topology used in conjunction with SR latch for random bitstream generation



References

Kim T (2019) Realization of Integrated Coherent LiDAR. Phd Thesis

ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY of WASHINGTON

ADVISOR: Sajjad Moazeni

SPONSOR: ELECTRICAL & COMPUTER ENGINEERING DEPARTMENT, UNIVERSITY OF WASHINGTON