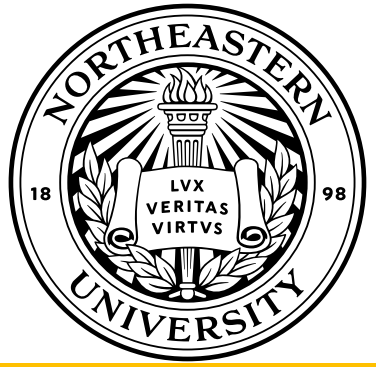
mmSpoof: Resilient Spoofing of Automotive Millimeter-wave Radars using Reflect Array

Rohith Reddy Vennam[1], Ish Kumar Jain[1], Kshitiz Bansal[1], Joshua Orozco[1], Puja Shukla[1], Aanjhan Ranganathan[2], Dinesh Bharadia[1]

[1] *University of California San Diego, La Jolla, CA*

[2] *Northeastern University, Boston, MA*



mmWave Radars in automotive vehicles (ADAS)

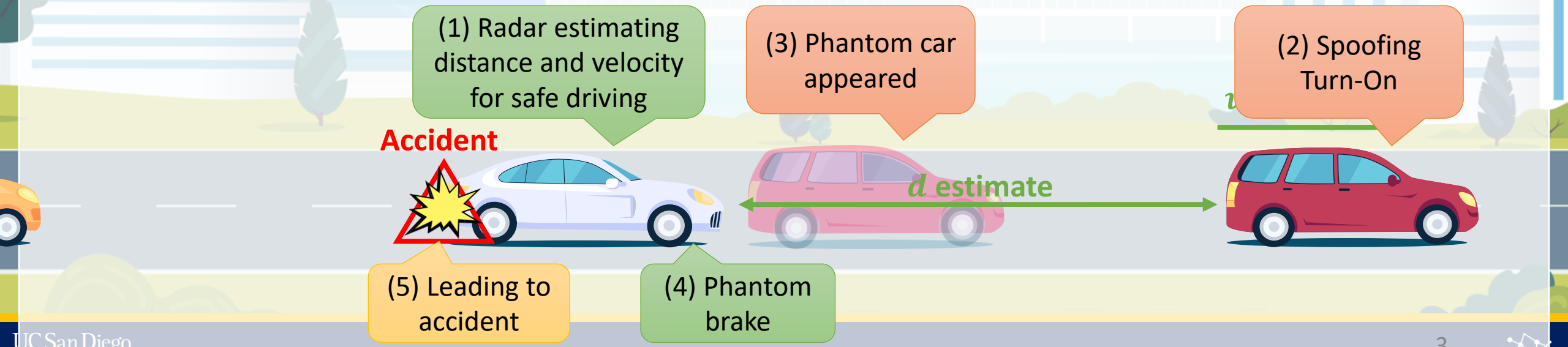
Ultrasound | Camera | Short/Medium Range radar | Radar / Lidar | Long Range radar

Are these mmWave Radars secure enough?

Spoofing mmWave Radars

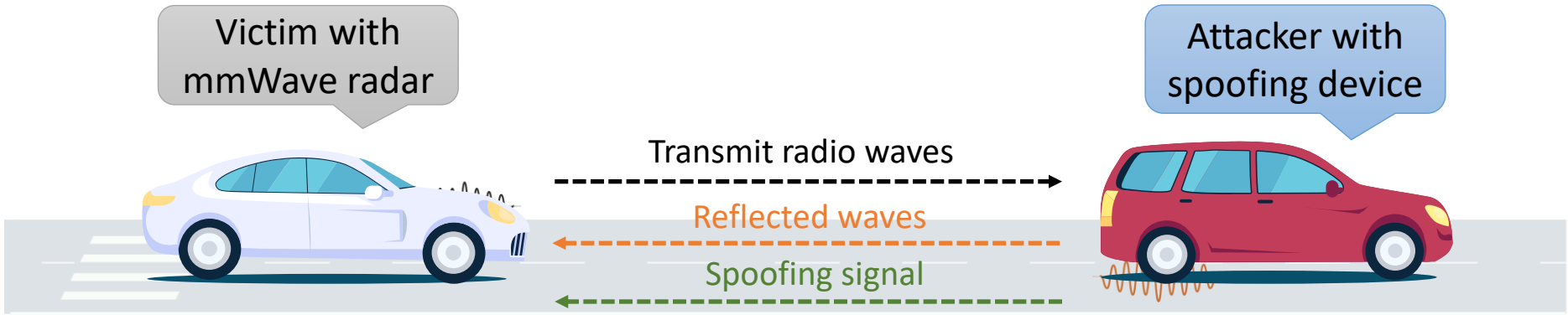
Radar Spoofing: Manipulating radar measurements with a desired quantity
for instance, changing distance (d) and velocity (v) measured by the radar with a controllable value.

These attacks are highly effective due to their ability to spoof both distance and velocity on radar.



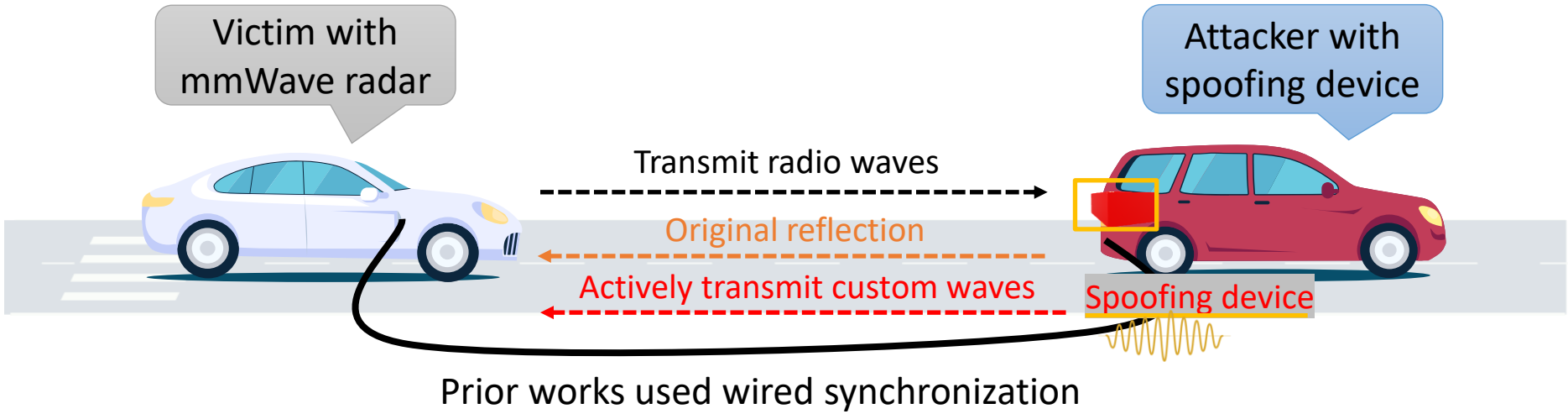
Attack model

Goal: Attacker should independently spoof victim radar's distance and velocity



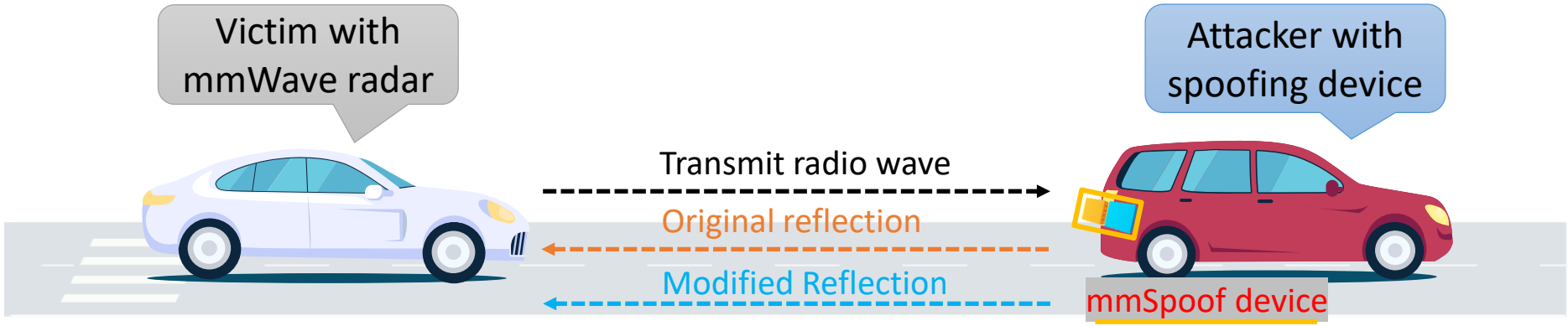
Current spoofing attacks are not feasible

- ✗ Active transmission
- ✗ Requires synchronization



mmSpoof: Resilient spoofing of mmWave radars using reflect array

- No active transmission
- No synchronization

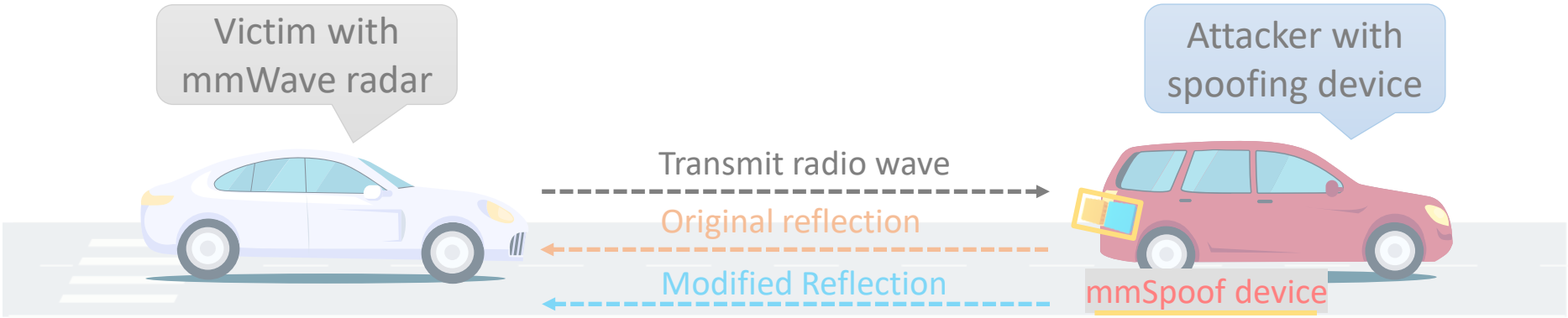


mmSpoof does not require any synchronization between attacker and victim

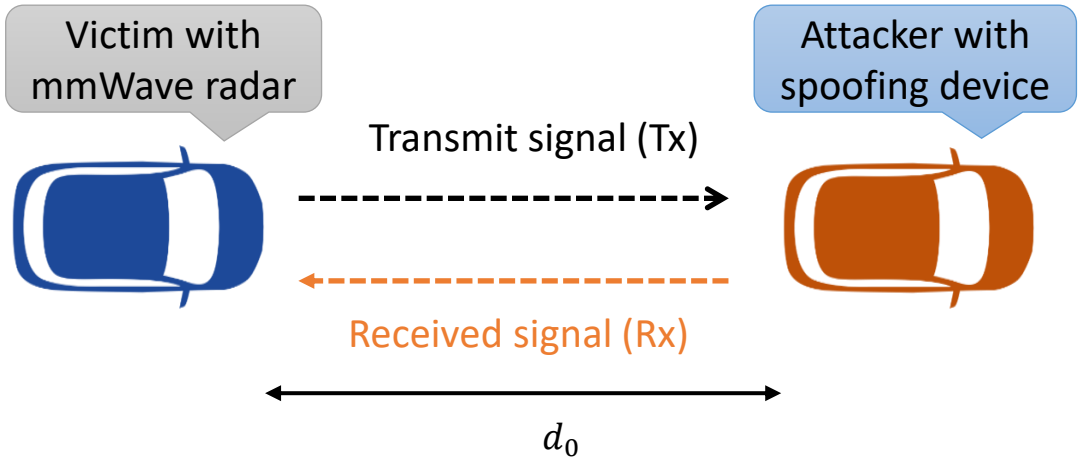
mmSpoof: Contributions

Further in talk, we discuss the following key contributions

- Independent distance and velocity spoofing
- mmSpoof prototype with COTs Hardware
- Realtime victim radar parameter estimation

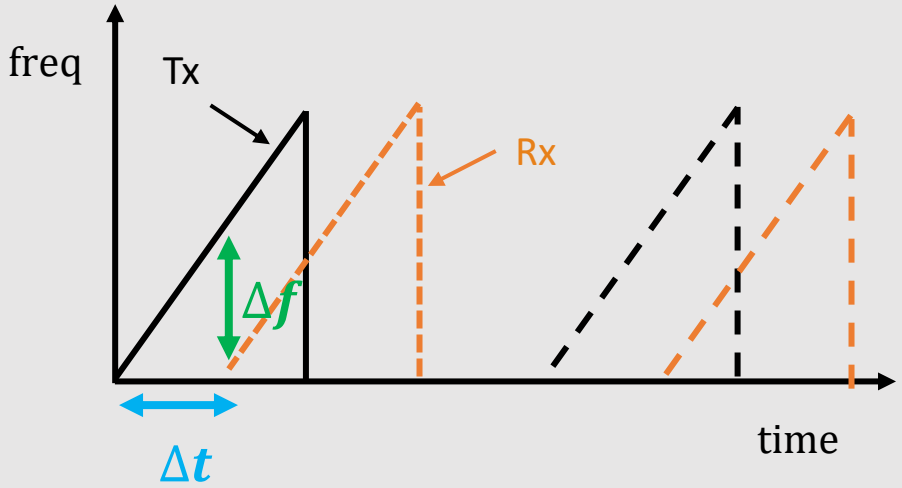


Distance estimation by radar



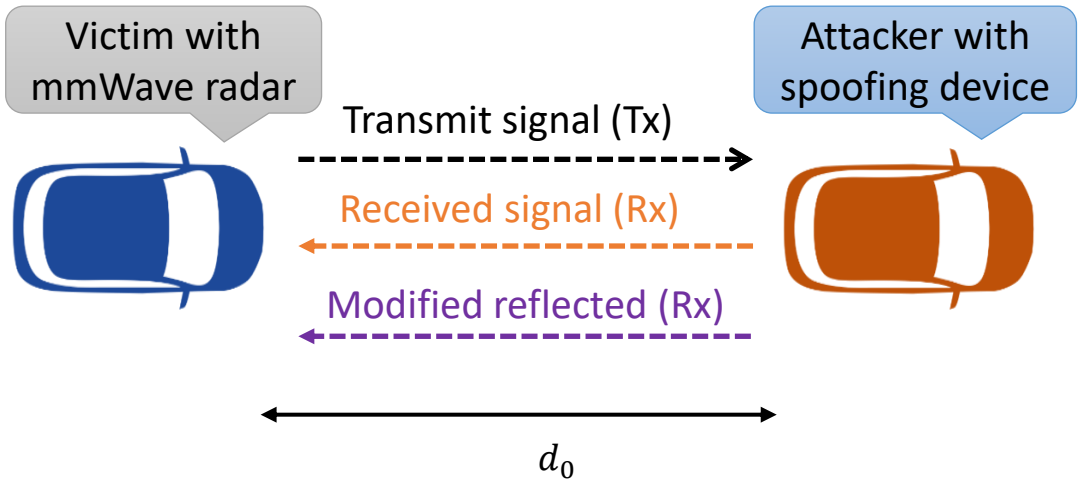
Radar estimated

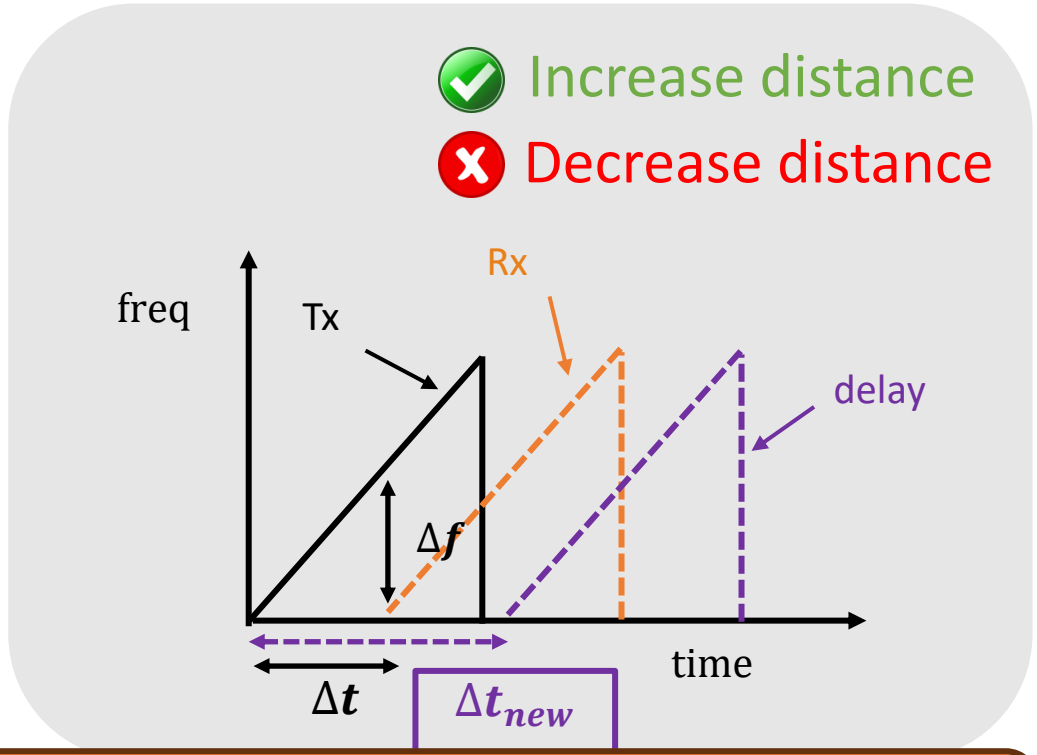
$$\text{distance} = \frac{c}{2}\,\Delta t = \frac{c}{2}\frac{\Delta f}{slope}$$



$$\Delta t = \frac{\Delta f}{slope}$$

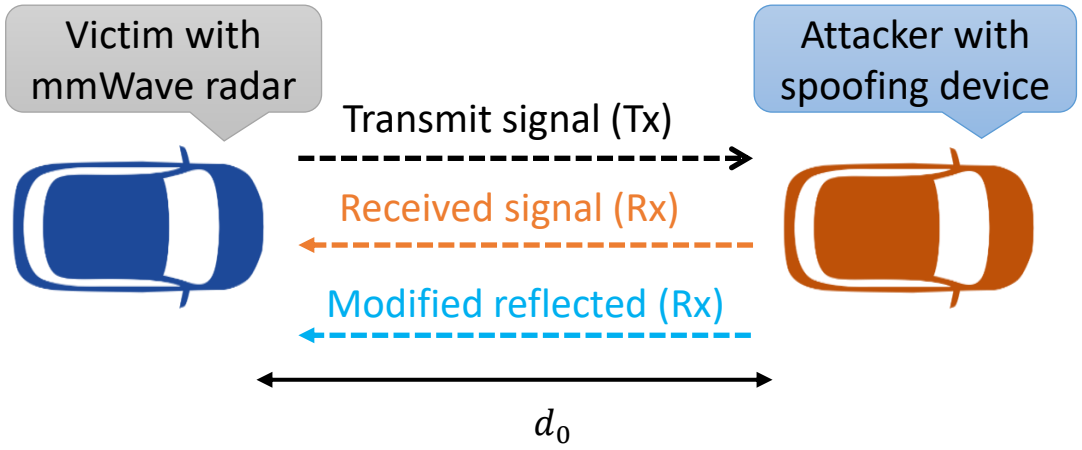
Spoofing distance: Naive solution



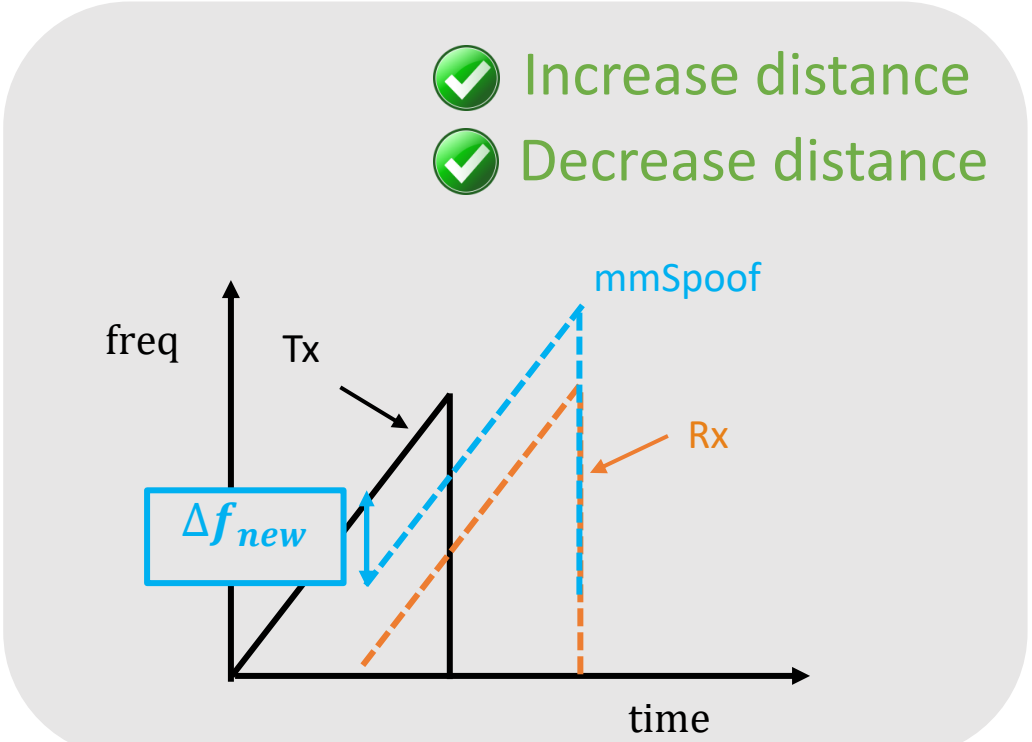


Positive delays increase distance, but we cannot create negative delays, which leads to a failure in spoofing shorter distances.

Spoofing distance: mmSpoof's approach

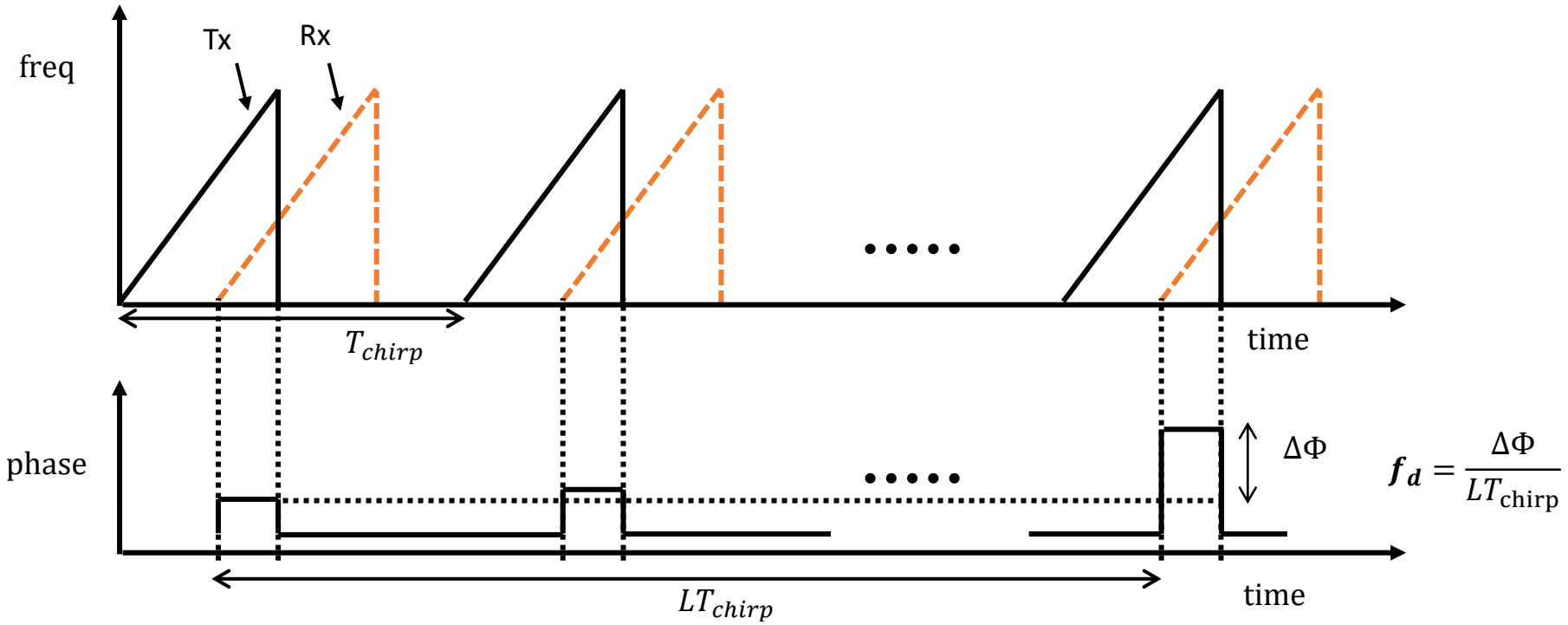


Radar estimated distance $= \frac{c}{2}\frac{\Delta f_{new}}{slope}$



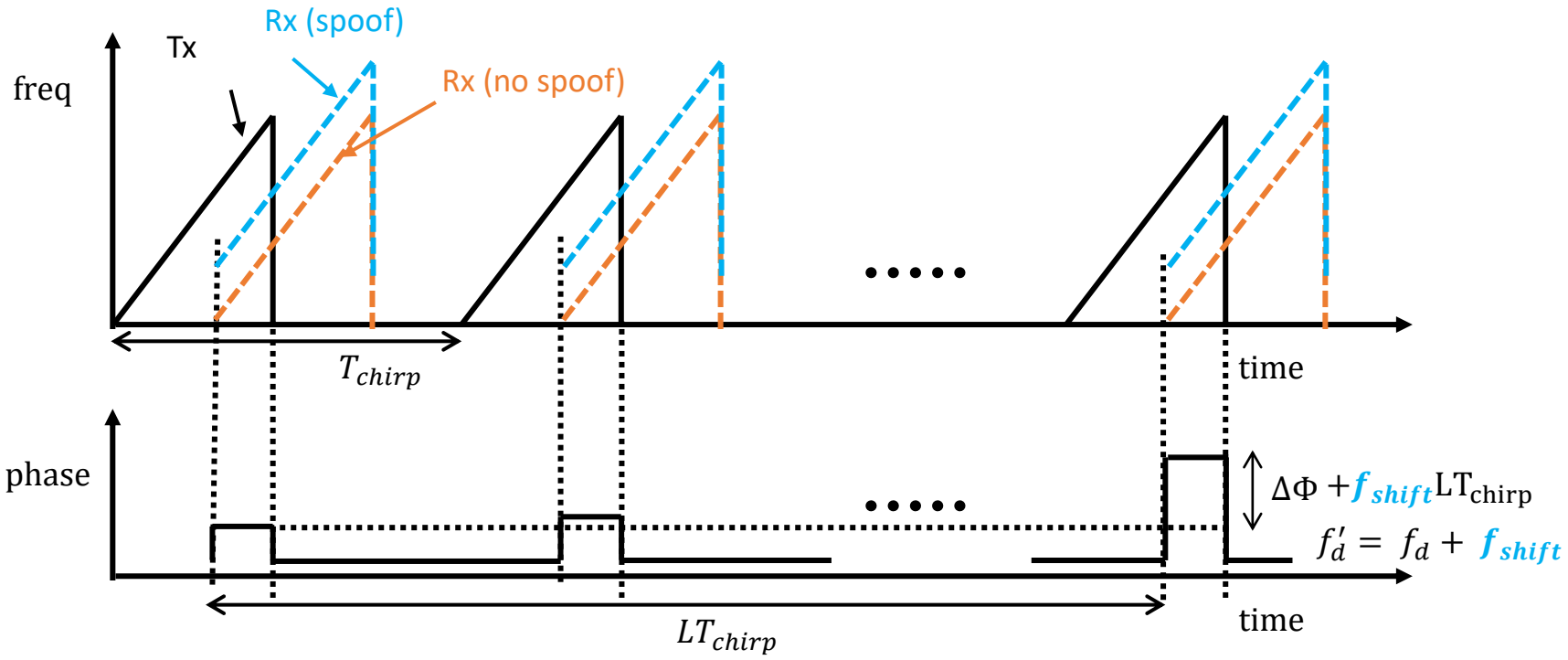
Frequency shift at reflect array spoof distance measured at radar

Velocity estimation by radar



Radar estimated velocity $= \frac{c}{2f_0} f_d$

Spoofing velocity: mmSpoof's approach

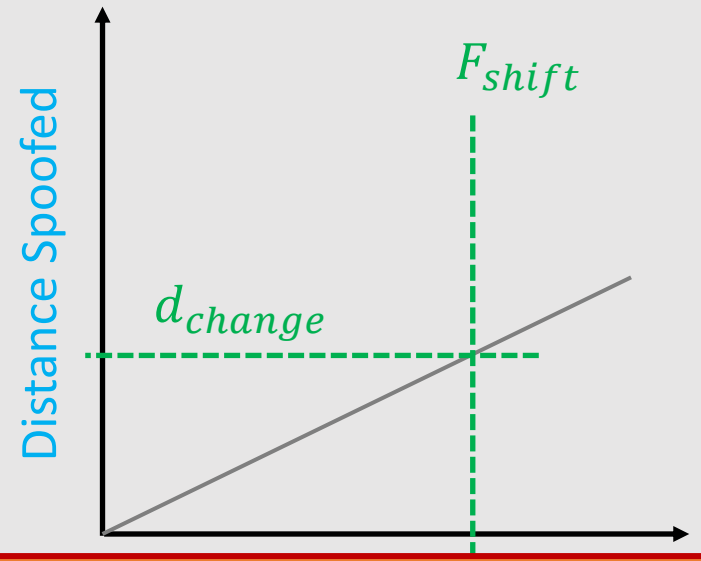


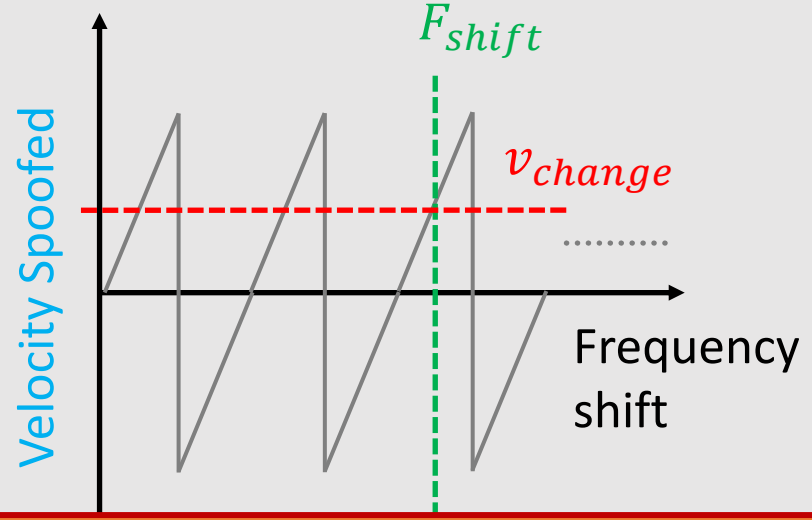
Radar estimated velocity $= \frac{c}{2f_0}(f_d + f_{shift})$

mmSpoof: Coupling between distance and velocity spoofing

$$d_{est} = d_0 + \frac{c}{2k} f_{shift}$$

$$v_{est} = v_0 + \frac{c}{2f_0} f_{shift}$$

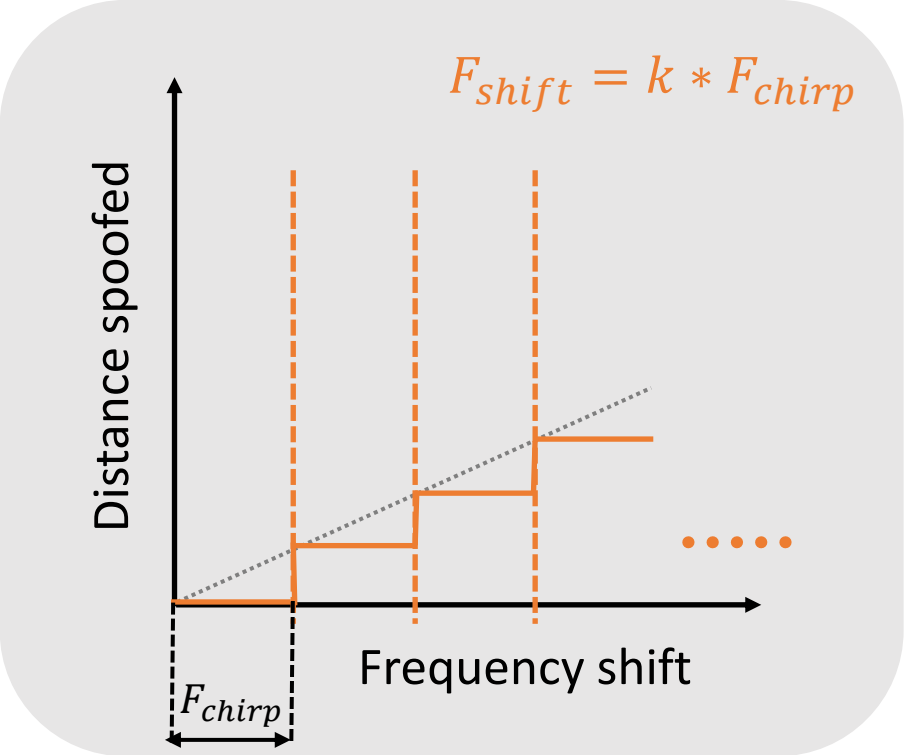


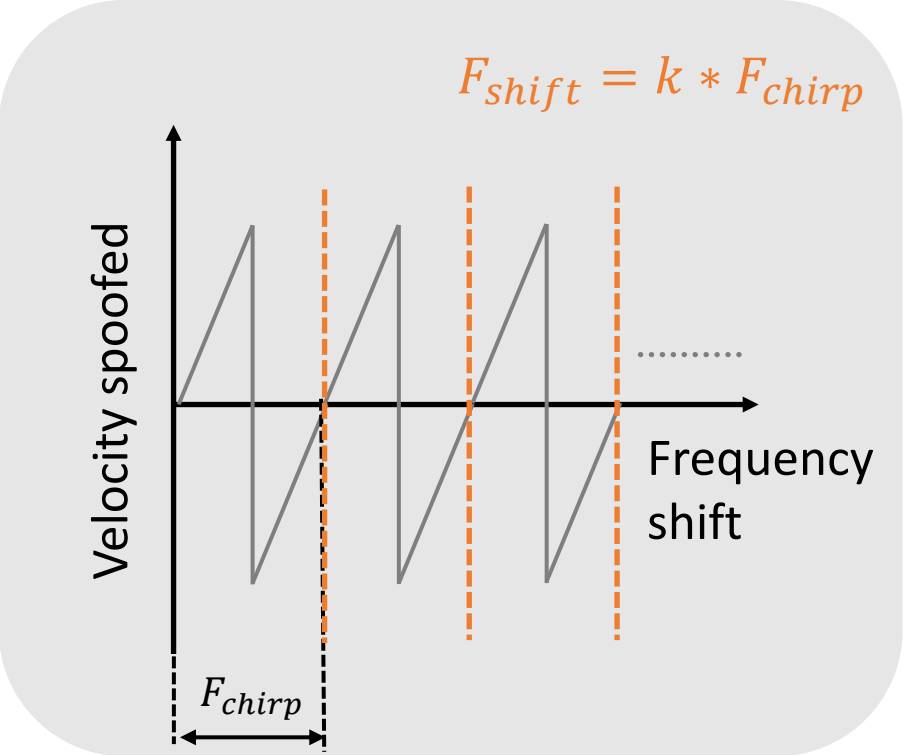


We cannot spoof distance and velocity independently due to coupling issue.

De-coupling distance and velocity spoofing: Changing only distance

Periodicity in velocity spoofing

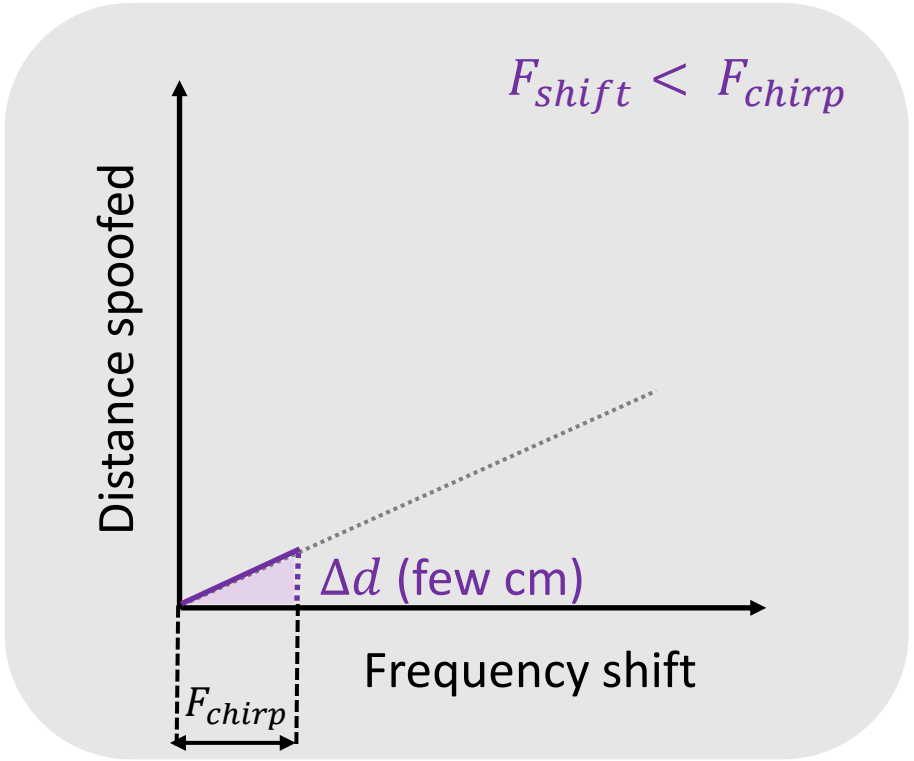


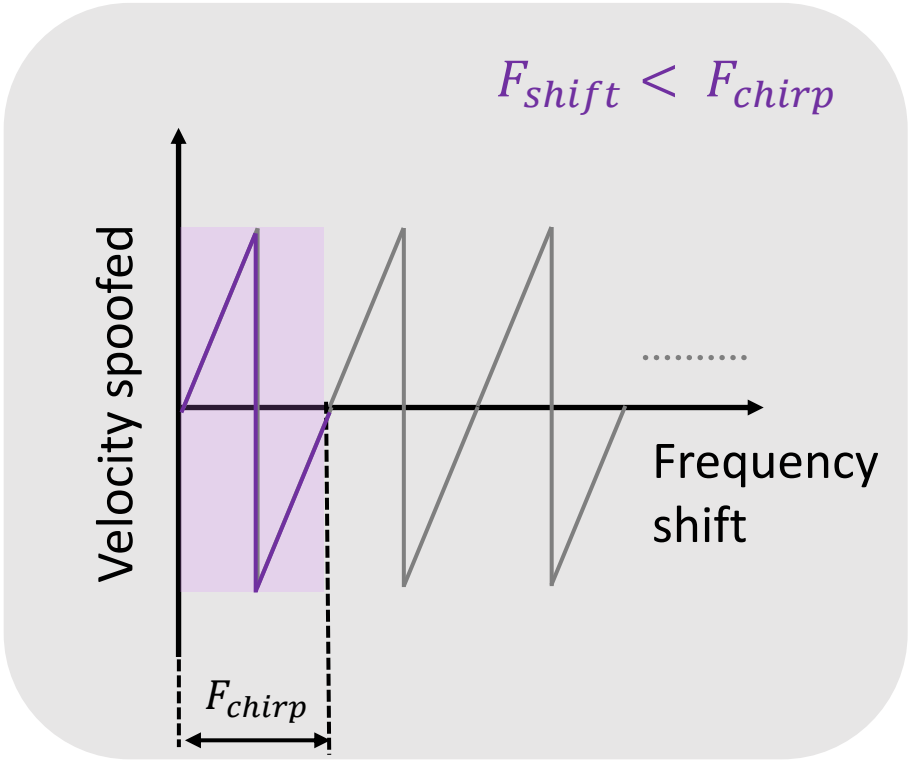


Frequency shifts in steps of F_{chirp} only changes distance while keeping the velocity constant

De-coupling distance and velocity spoofing: Changing only velocity

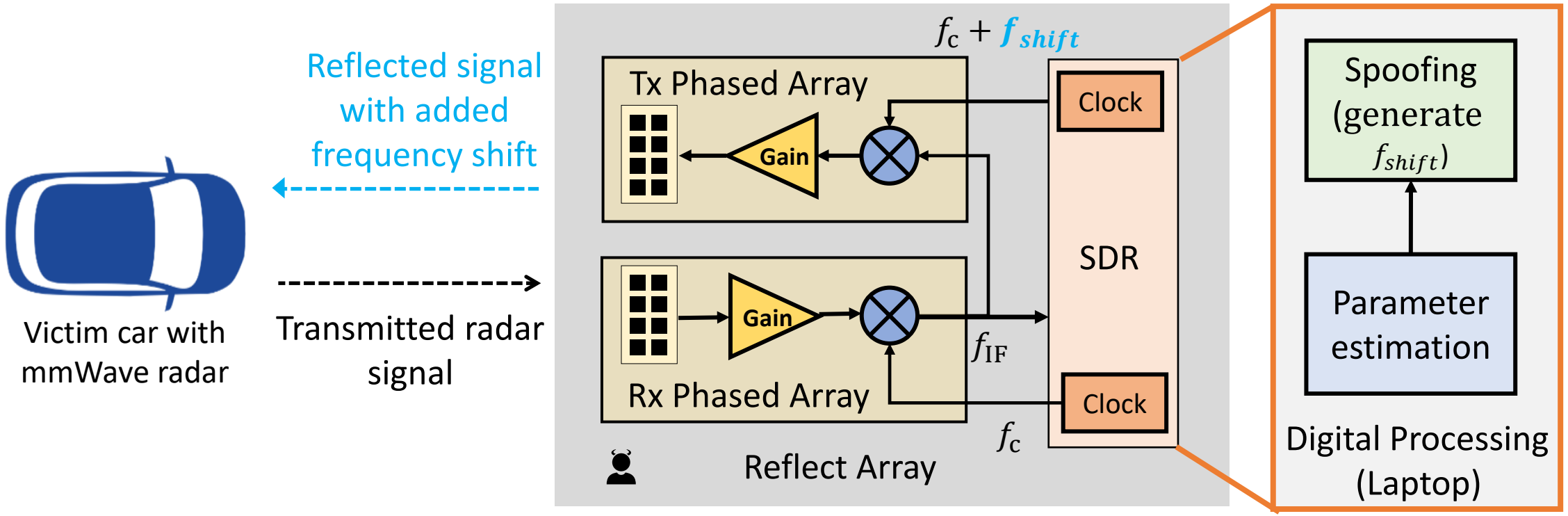
Negligible distance change for small frequencies





Small frequency shifts $< F_{chirp}$ only changes velocity

mmSpoof: Architecture design of reflect array
(Two phased arrays and SDR)

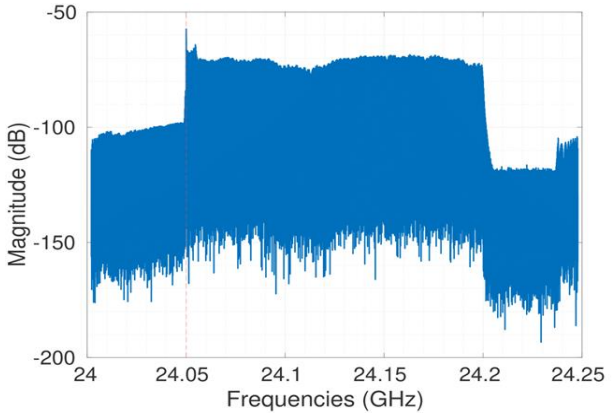


Hardware feasibility: A prototype can easily build with 2 phased arrays and SDR

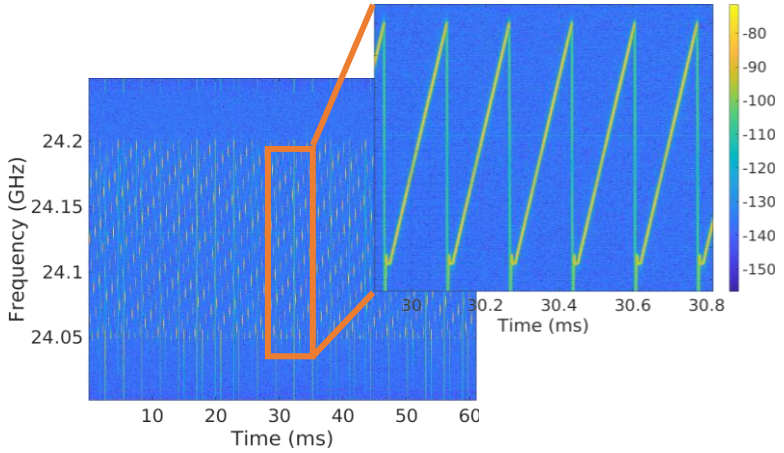
Demonstrating radar parameter estimation with real radar data

Parameter estimation (T_{chirp}, f_c, k)

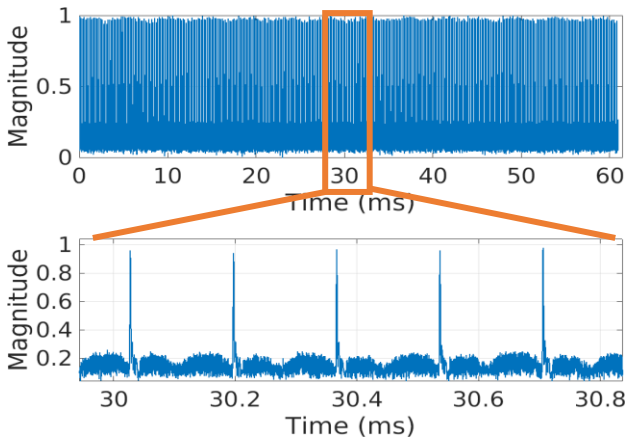
Digital Processing



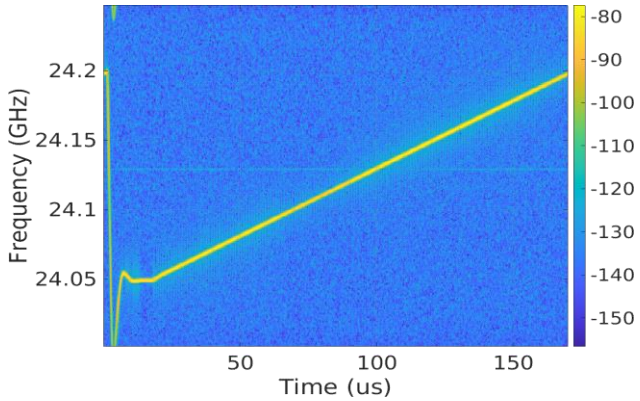
Step1: Start frequency estimation



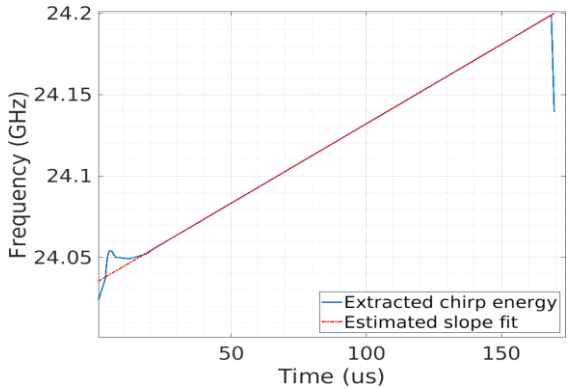
Step2: Extracting FMCW chirps



Step3: Chirp time estimation

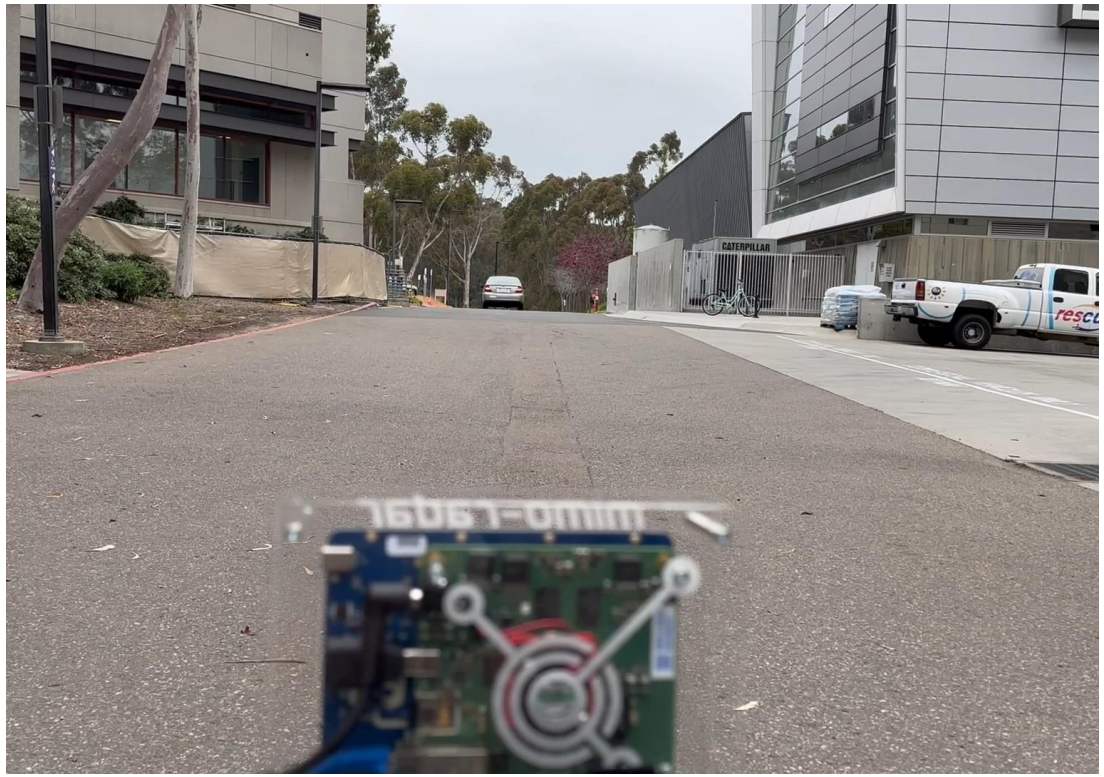


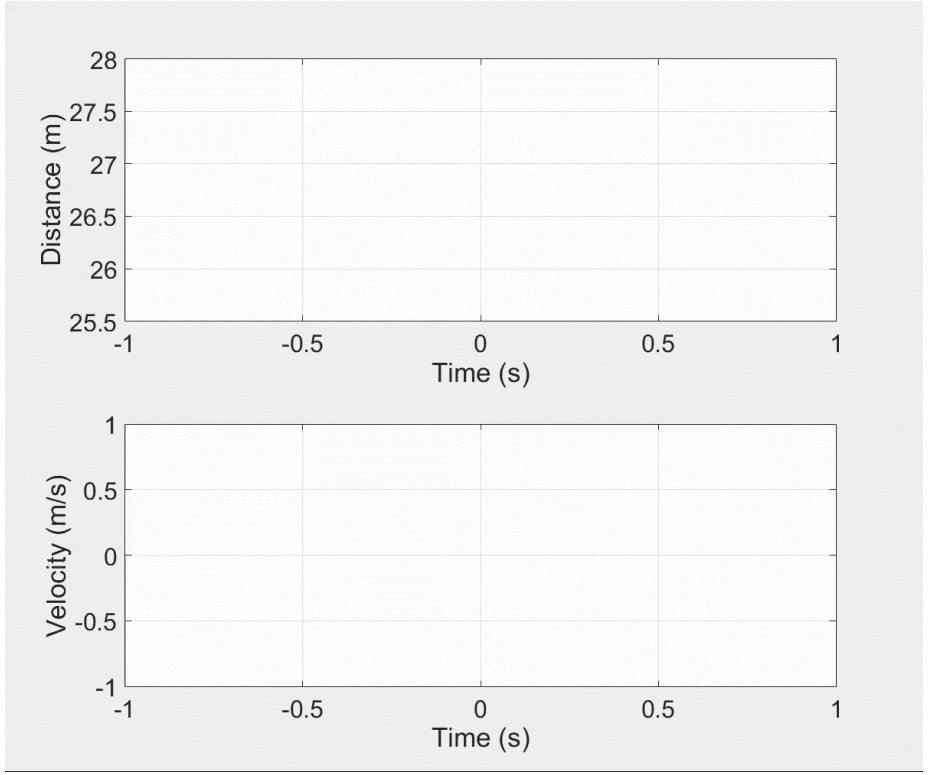
Step4: Extraction of single chirp



Step5: Slope Estimation

Attack demonstration: Radar measurements when car ahead is approaching closer to it

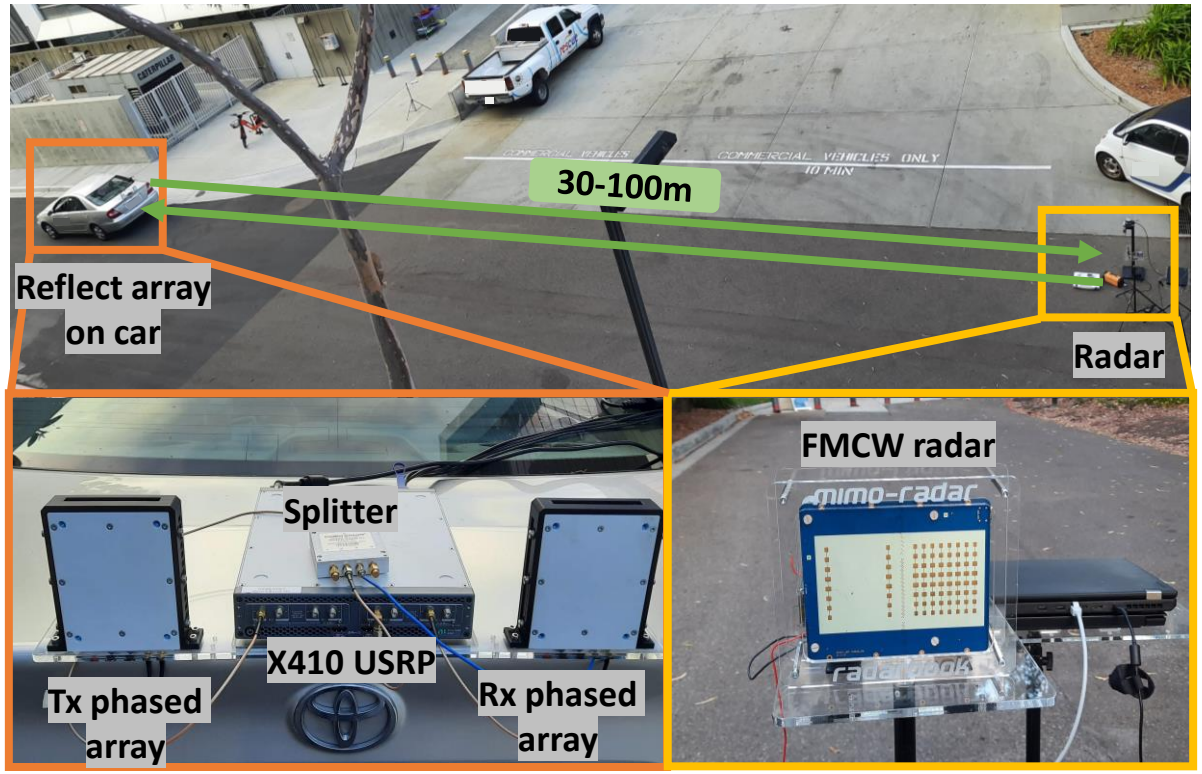




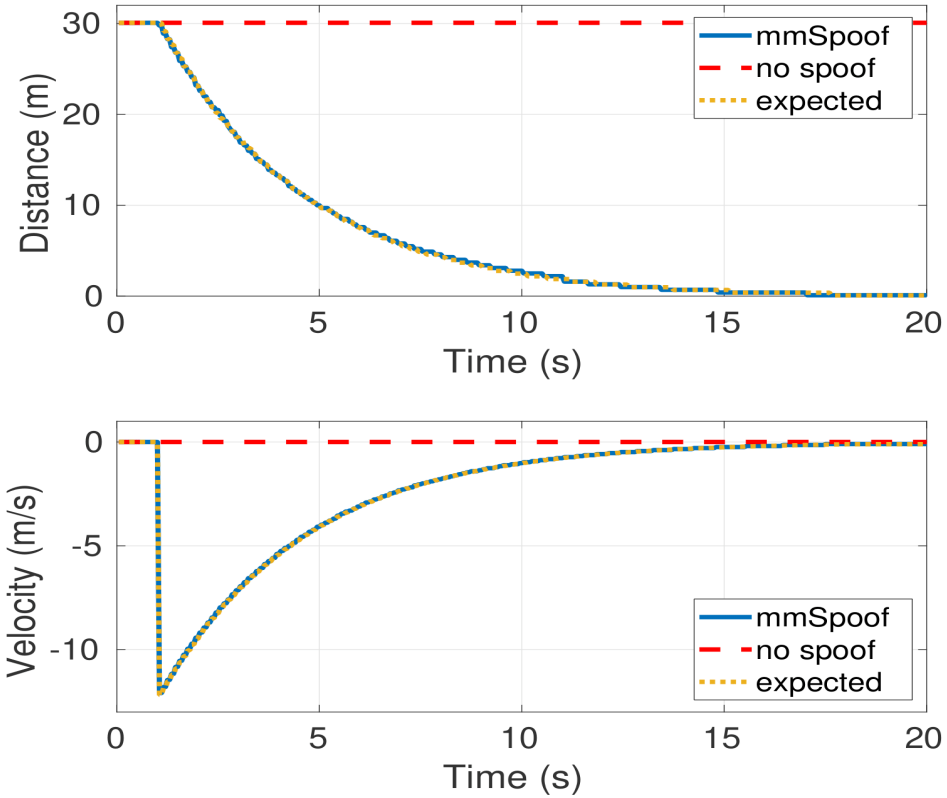
Attack goal: spoof radar to mimic this scenario with phantom car

Attack demonstration: Static scenario

when there is *no relative velocity* between attacker and victim



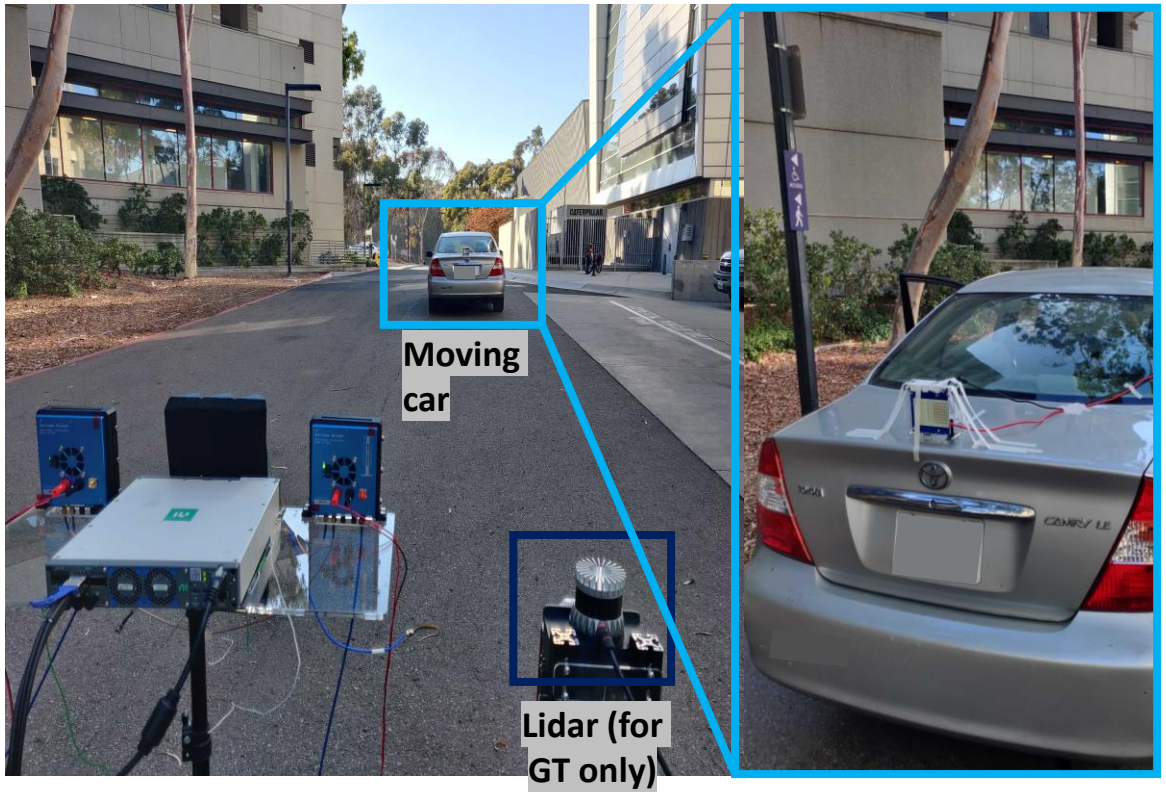
Static scenario: Evaluation setup with COTs hardware



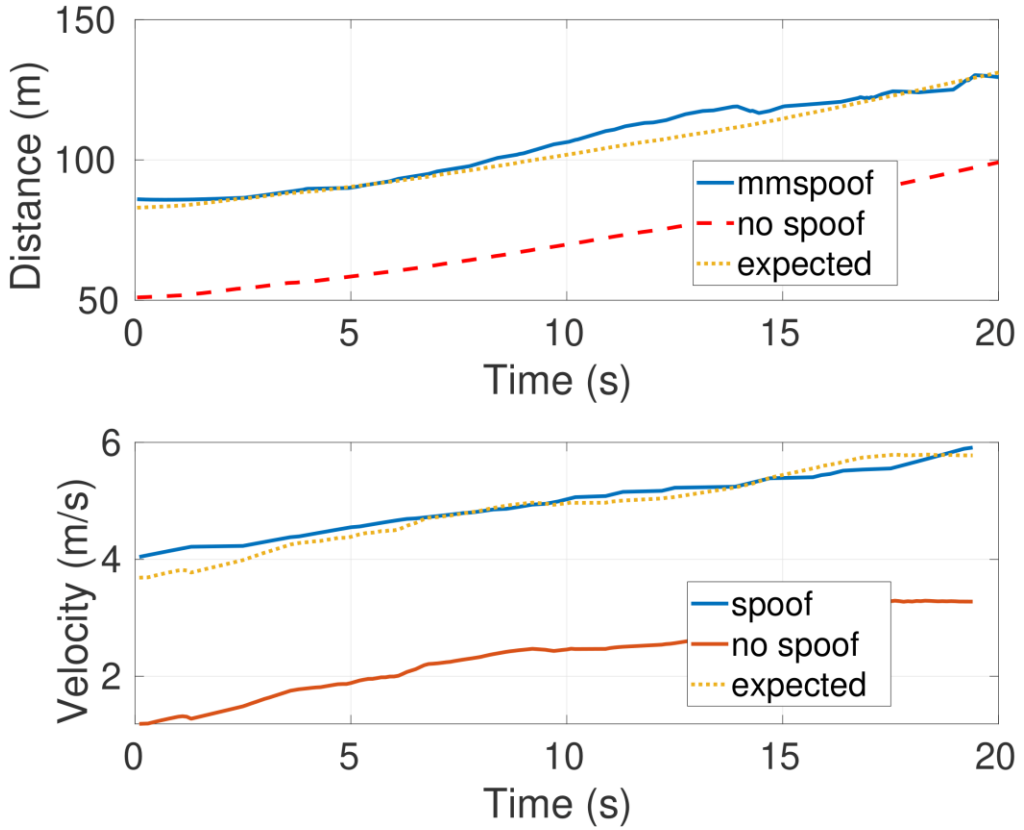
Spoofing both distance and velocity in static scenario

Attack demonstration: Moving scenario

when there is *relative velocity* between attacker and victim



Moving scenario: Evaluation setup with COTs hardware



Spoofing both distance and velocity in moving scenario (Lidar as no spoof case)

Spoofing attacks on Radar

Attack model	Independent distance & velocity spoofing	No synchronization requirement	No need-to-know victim's radar parameters	Feasibility with COTs Hardware
R. Komissarov, et. al	✓	✗	✗	✓
Nallabolu, et. al	✗	✓	✗	✗
A. Lazaro, et. al	✓	✓	✗	✗
S. Nashimoto, et. al	✗	✗	✗	✓
mmSpoof	✓	✓	✓	✓

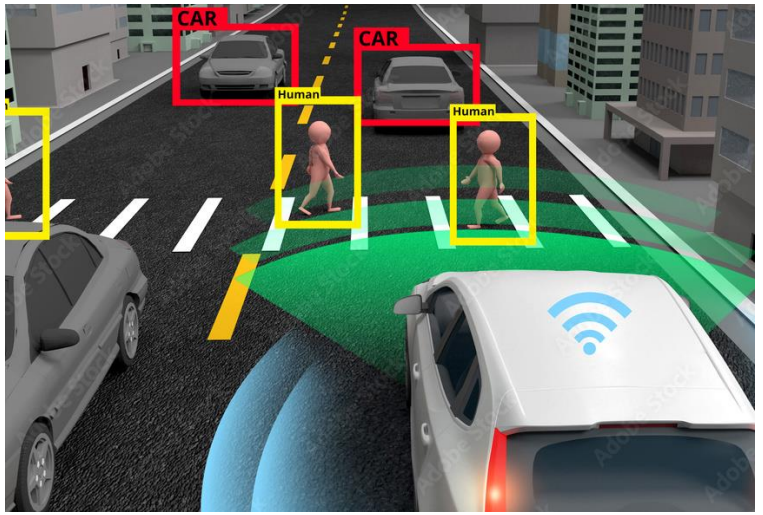
mmSpoof meets all of these requirements and has been demonstrated as a robust attack

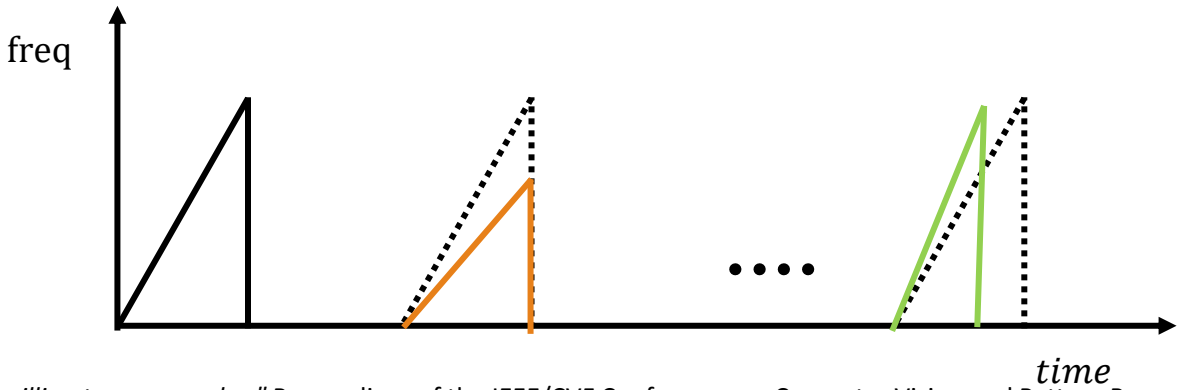
Counter measures to mmspoof

Employing High Resolution radars

Multi sensor fusion

Changing victim's params every chirp





Reference: Guan, Junfeng, et al. *"Through fog high-resolution imaging using millimeter wave radar."* Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020.

“mmSpoof: Resilient Spoofing of Automotive Millimeter-wave Radars using Reflect Array”

Scan for the project webpage
https://wcsng.ucsd.edu/mmspoof