Adversarial Attacks on mmWave Radar: A Summary of mmSpoof and MadRadar

Farris Nefissi

ECSE-4560

Agenda

- Background & Motivation
- Problem Statements
- Methodologies
- Results
- Implications
- Limitations
- Future Work
- Q&A

Background & Motivation

What is spoofing?

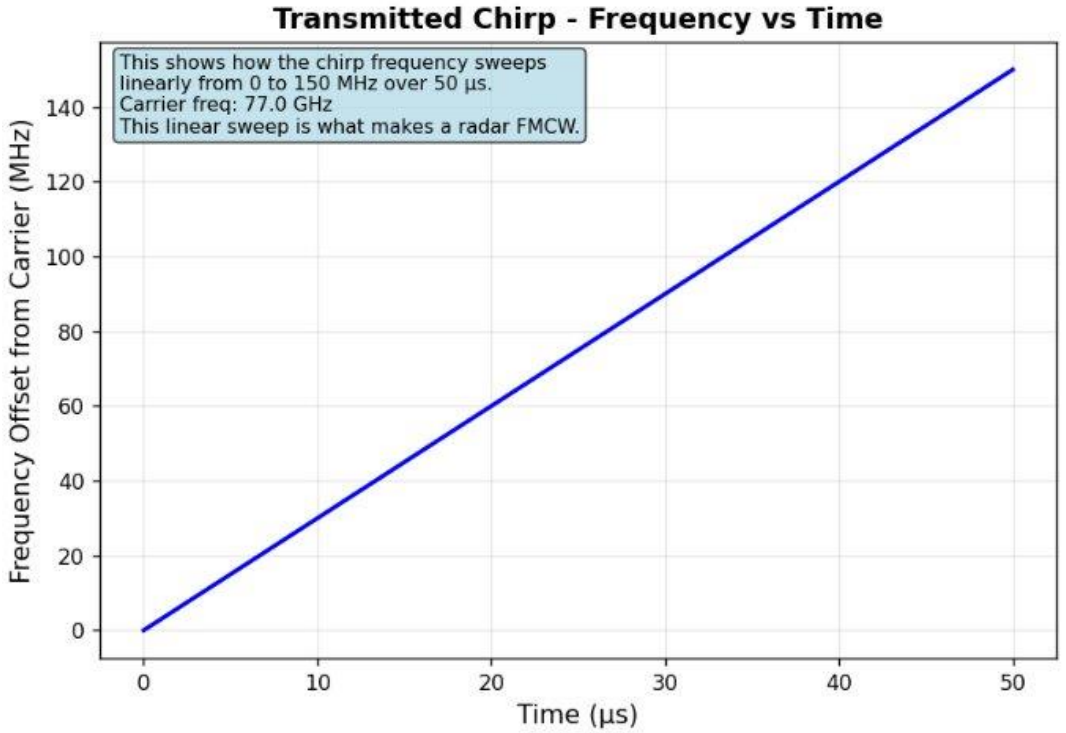
- A form of electronic attack
- Deceives a radar by injecting "ghost" targets to alter the perception of real targets

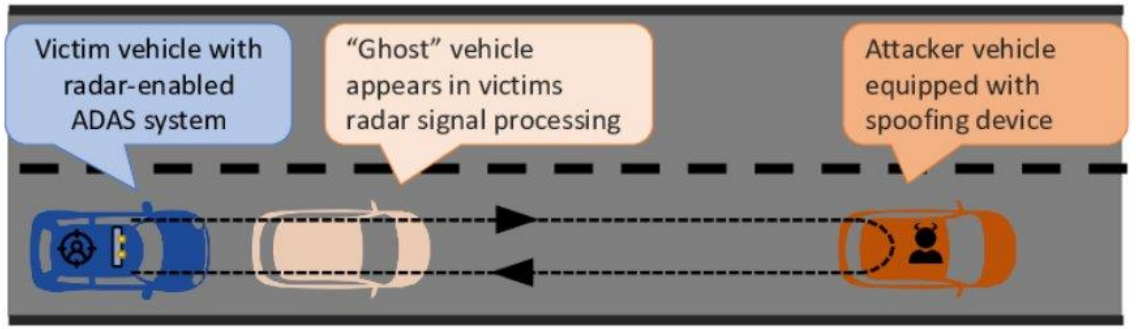
Why does this matter?

- Autonomous vehicles, aviation, military, etc.

What do these papers address?

- Radar is widely deployed but is susceptible to malicious actors





Problem Statements

mmSpoof:

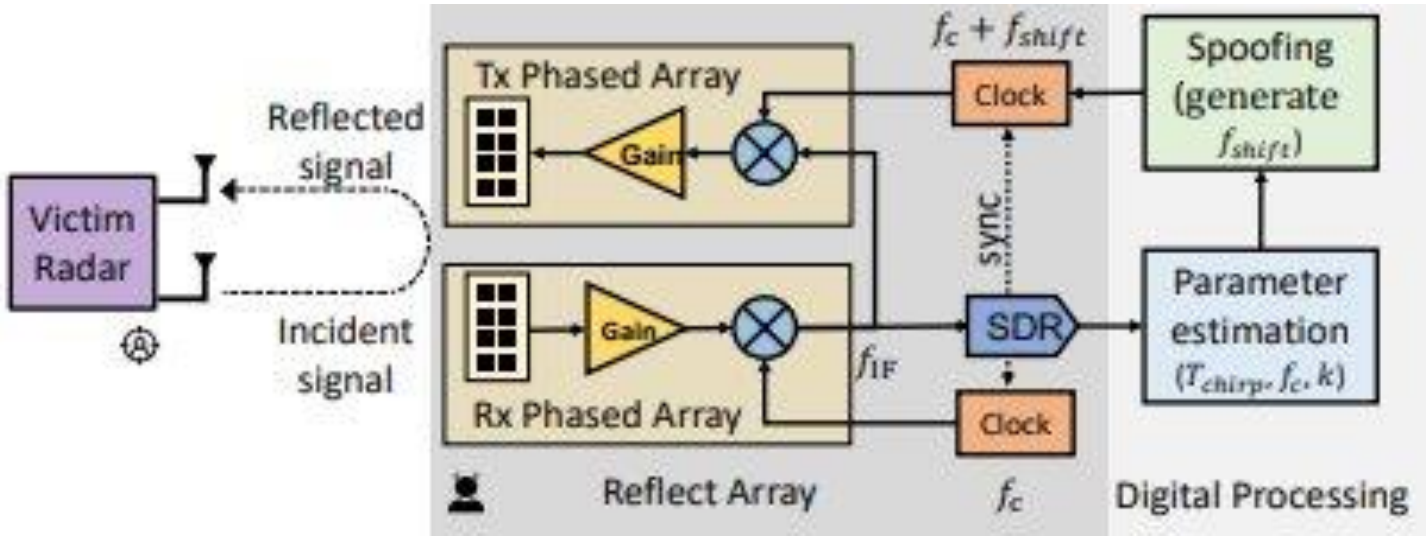
- Goal – create false targets on commercial mmWave radar through radar reflection
- What makes it different – previous attacks required perfect clock synchronization between attacker and victim

MadRadar:

- Goal: create false targets on commercial mmWave radar through general black-box attack framework
- What makes it different – can add, remove, or move objects from target detections

Methodology - mmSpoof

- Reflect array design
- Parameter Estimation
- Spoofing Mechanism



Methodology - MadRadar

- Real-time parameter estimation
- Attack signal generation
  - False positive (FP) – inserts fake object
  - False negative (FN) – removes real object
  - Translation attack – combination of FP and FN
- Physical implementation

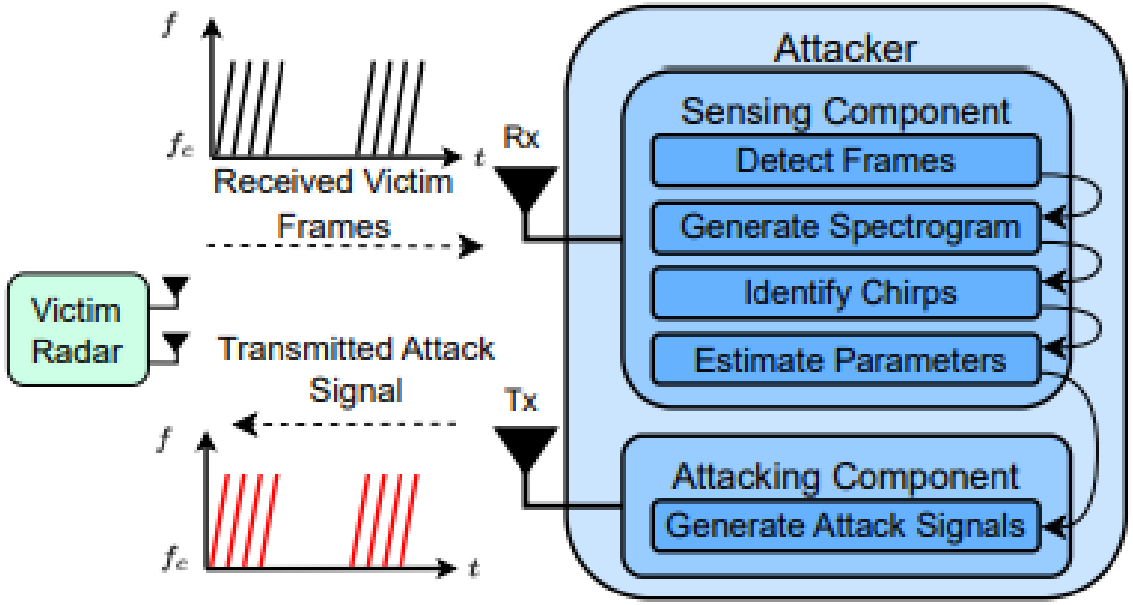
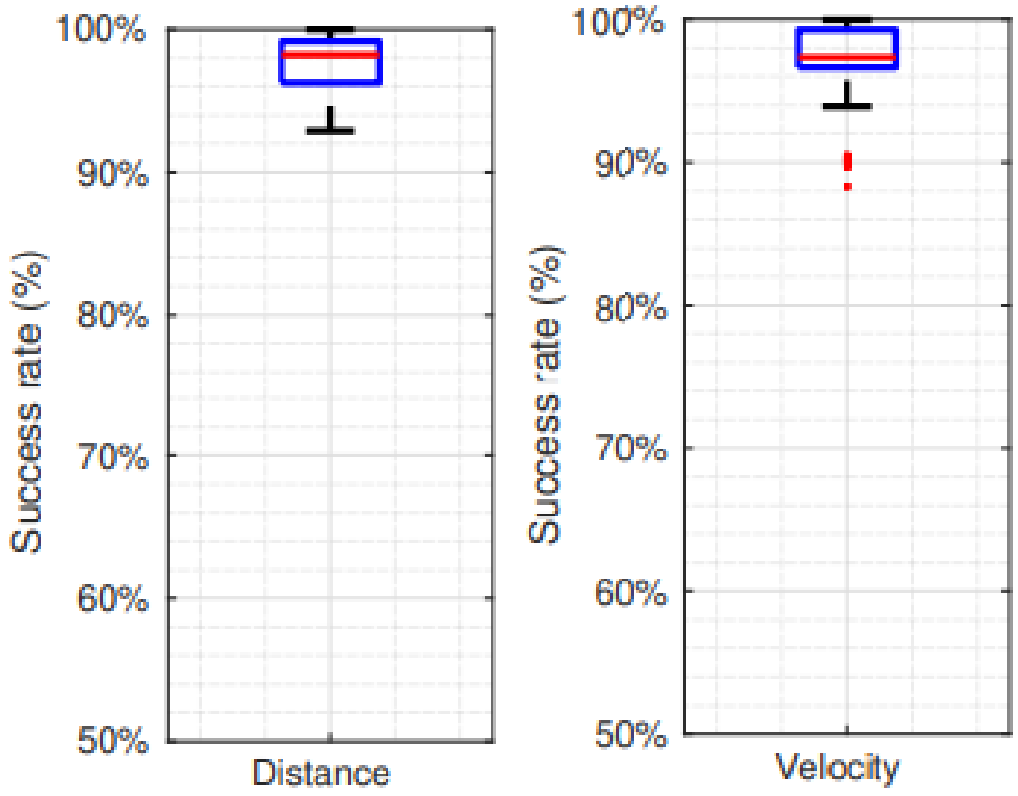


Fig. 3: MadRadar block diagram.

Results - mmSpoof

- Distance spoofing of moving car has a 98.23% median success rate
- Velocity spoofing of moving car has a 97.34% median success rate



Results - MadRadar

- High parameter estimation accuracy
- High spoofing accuracy
- 90% of attacks were successful on 100 different scenarios

TABLE I: Key parameter estimation error metrics.

Parameter	Error Type	Mean Error	95-th Percentile
Chirp Period	Absolute	0.143 ns	0.586 ns
Chirp Slope	Absolute	0.010 MHz/µs	0.0354 MHz/µs

TABLE III: Absolute error of attacker spoofing accuracy.

Configuration	Metric	Mean Absolute Error	90th Percentile
C	Range	1.49 m	1.28 m
	Velocity	0.15 m/s	0.04 m/s
D	Range	4.29 m	1.09 m
	Velocity	1.5 m/s	0.12 m/s

Implications

Implications:

- mmWave FMCW radars are vital to several applications but are vulnerable to malicious actors
- Both methods are highly practical
- Almost undetectable if no other sensor data is present

Limitations

- No angular spoofing
- Multi-sensor fusion limits spoofing strength

Future Work

- Angular spoofing attacks
- Multi-sensor spoofing
- Construct more robust defense mechanisms

Q&A

References

- https://wcsng.ucsd.edu/files/mmspoof.pdf
- https://arxiv.org/pdf/2311.16024