Analysis and Implementation of Spoofing on Automotive FMCW Radars

Farris Nefissi
Rensselaer Polytechnic Institute
nefisf@rpi.edu

Ish Jain
Rensselaer Polytechnic Institute
jaini@rpi.edu

Abstract

Millimeter-wave frequency-modulated continuous-wave (FMCW) radars are widely used in modern automotive advanced driver assistance systems (ADAS) because they provide reliable range and velocity data in conditions that camera and LiDAR cannot. However, recent research shows that these sensors can be vulnerable to spoofing attacks that can manipulate what the radar "sees", including creating false object detections, suppressing real detections, or shifting an object's apparent position. This paper will be a summary of mmSpoof and MadRadar, both demonstrating practical spoofing attacks under realistic constraints, and it connects to a small simulation we implemented that demonstrates radar spoofing in a reproducible way. The main implication of these papers is that spoofing is a real vulnerability and that when attackers exploit the chirp structure or estimate radar parameters, the resulting attacks can be devastating on systems.

1 Introduction

1.1 Motivation

Automotive mmWave FMCW radar is now the primary sensing modality for ADAS due to it being able to measure range and velocity in many different weather conditions. As vehicles rely more on radars, it can become a target for adversaries that wish to disrupt other drivers.

1.2 Problem Statement

The problem motivating this analysis and simulation is to understand how an attacker can manipulate the physical signals that the radar detects and what the victim might encounter in such a situation. However, even for the attacker, this is difficult as they must work with small changes since even small errors in timing or parameter alignment can cause large errors in range and velocity estimation. The attacker must also compete with normal radar reflections, noise, and countermeasures.

1.3 Key Contributions

The key contributions of this paper is a comparative summary of mmSpoof and MadRadar, highlighting their enabling techniques and what they solve, plus a simple simulation that we built which demonstrates the basic implementation of spoofing by injecting "ghost" targets into an FMCW radar's processing and observing the resulting peaks in a range-Doppler map.

2 Background

2.1 FMCW Radar Fundamentals

Automotive mmWave FMCW radars use waveforms to estimate target range and velocity. In FMCW systems, the transmitted chirp has a linear pattern described by the chirp slope $k = B/T_{chirp}$, where B is bandwidth and T_{chirp} is chirp time.

A target at range d introduces a round-trip delay $\tau = 2d/c$, where c is the speed of light. From this, beat frequency $f_b \approx k\tau$ can be used to determine target range $d = cf_b/2k$. The range resolution for the system is determined by $\Delta d = c/2B$.

Velocity is estimated by transmitting multiple chirps and observing the phase change across these chirps, which produces a Doppler frequency $f_D = 2v/\lambda$, where λ is wavelength. In practice, automotive radars compute a range-Doppler map using a fast-time FFT for range estimation and a slow-time FFT for Doppler estimation. Peaks in the range-Doppler map correspond to detected objects, whether real or spoofed.

2.2 Electronic Attack

Electronic attacks broadly fall into two types: jamming and spoofing. Both operate at the physical layer by manipulating the RF environment to either "blind" or "confuse" the radar. Jamming aims to degrade or deny radar sensing by overwhelming the receiver with powerful interference. This can raise the effective noise floor, reduce detection range, and cause loss of targets in the radar scene. While effective, jamming is often easy to detect given its ability to overwhelm the radar in a noticeable fashion. Spoofing, on the other hand, manipulates the radar in a controlled manner by introducing structured signals that can appear as real reflections. A successful spoofing attack can create false targets, mask real targets, or move real targets in the scene.

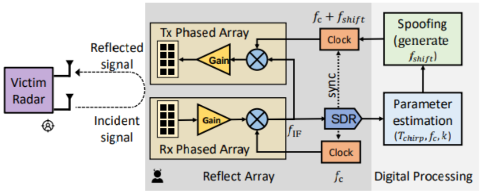


Figure 1: mmSpoof architecture design of reflect array [1]

3 Design

3.1 mmSpoof vs MadRadar

Both mmSpoof and MadRadar assume external attackers that can influence the victim's automotive radar through creation of false targets, hiding real targets, or shifting target locations. mmSpoof focuses on eliminating the need for synchronization between victim and attacker by using reflection-based modulation of the victim's own waveform. MadRadar focuses on enabling attacks when victim parameters are unknown by introducing a general black-box framework that does real-time parameter estimation [1] [2].

3.2 mmSpoof

3.2.1 System Overview

mmSpoof proposes a novel spoofing mechanism that reflects the victim radar's transmitted chirp using an attacker-controlled reflect array. The key part that makes this work novel is that prior spoofing attempts required perfect synchronization between victim and attacker. This is not only impractical, but not possible in many attacker situations. mmSpoof demonstrates that reflecting the victim waveform avoids the need for the attacker to have perfect synchronization since it is just a controlled modulation of the victim's own radar waveform. mmSpoof can be broken down into three main components: the reflect array design, the spoofing mechanism, and the parameter estimation [1].

3.2.2 Reflect Array Design

As shown in Figure 1, the reflect array is broken into an Rx phased array, Tx phased array, and software defined radio (SDR). The Rx phased array amplifies the weak received signal, downconverts it to an intermediate frequency, and then sent to the Tx phased array. The Tx phased array is similar structure to the Rx phased array except that the signal is amplified to send the desired frequency shift to the victim radar. Lastly, the SDR is the component which samples the downconverted signal for parameter estimation and generation of the configurable frequency shift [1].

3.2.3 Spoofing Mechanism

Conceptually, mmSpoof spoofs both range and velocity by applying frequency shifts f_{shift} to the reflected signal such that the victim's signal processing sees the attacker-chosen targets range and velocity. However, a constant frequency shift will couple range and velocity. mmSpoof proposes a decoupling method by using fine-grained frequency shifts which wrap around the max velocity ambiguity [1].

3.2.4 Parameter Estimation

To calculate the appropriate f_{shift}, mmSpoof estimates the victim's chirp slope k and chirp duration T_{chirp} through an SDR that captures the victim signal. To determine chirp time T_{chirp}, a spectrogram of the received signal is generated to show the energy over frequency and time. Figure 2 shows energy rows being extracted from the spectrogram and the time difference between peaks gives the chirp time T_{chirp}.

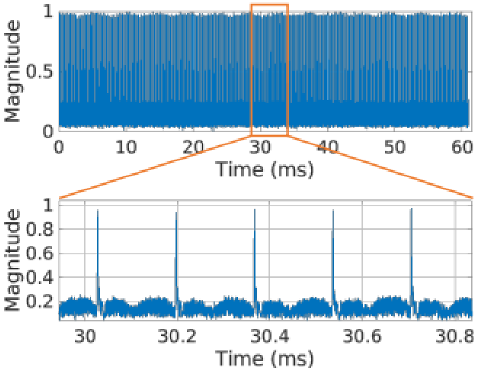


Figure 2: Extracted energy from chirps used to determine chirp time T_{chirp} [1]

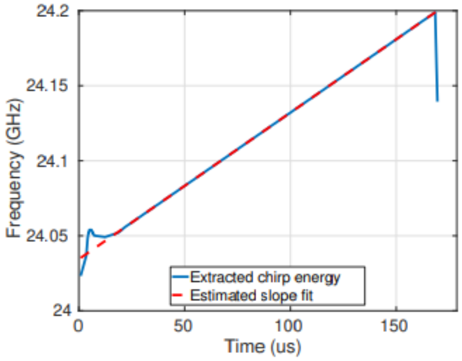


Figure 3: Extracting single chirp from received signal to estimate chirp slope k [1]

For chirp slope k, Figure 3 shows the different frequencies over one chirp time that was previously determined, which is used to estimate the slope.

This step is crucial in mmSpoof's originality since it

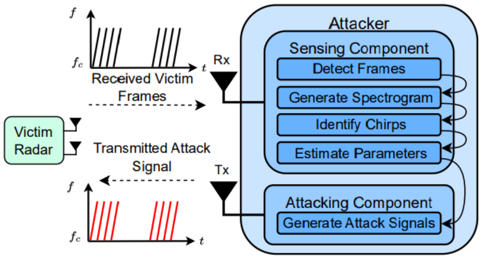


Figure 4: MadRadar Block Diagram [2]

does not assume the attacker has prior knowledge of the victim radar. The estimated parameters drive the selection of the desired f_{shift} for the attacker's spoofing choices [1].

3.3 MadRadar

3.3.1 System Overview

MadRadar is a real-time black-box FMCW radar attack framework that estimates victim radar parameters and launches three types of attacks: False Positive (FP), False Negative (FN), and Translation. FP attacks involve inserting a ghost target into the radar scene, FN attacks erase real targets from the scene, and Translation attacks move a real target to a new location. The key design of MadRadar is the ability for the black-box framework to "learn" the victim radar quickly to make attacks viable, even under randomized and unknown parameters [2].

3.3.2 Parameter Estimation

MadRadar has heavy emphasis on parameter estimation because estimation errors can directly translate to attack placement errors. The system is designed to estimate chirp time, chirp slope, and frame duration from the victim radar in real-time with no prior knowledge. MadRadar then uses these estimated parameters to schedule and create the spoofed transmissions [2].

3.3.3 False Positive Attacks

FP attacks are injections of false targets into a victim's radar scene that mimic real targets. FP attacks are the standard form of spoofing and are the baseline attack type in FMCW radar spoofing. The key idea is that an accurate parameter knowledge will allow the attacker to create ghost targets that will survive detection and not appear as typical interference [2].

3.3.4 False Negative Attacks

FN attacks aim to remove real targets from the victim's radar detection. MadRadar's design allows for FN attacks by introducing a very similar slope, which smears the real target's energy across multiple range bins, thus effectively erasing the real target from the radar's perception [2].

3.3.5 Translation Attacks

Translation attacks move an existing target to a new location in the radar's perception. This can be seen as essentially combining the methods of FP and FN to create a new "scene" for the radar [2].

3.4 My Simulation

3.4.1 System Overview

We developed a simple Python simulation to model the FMCW processing chain. The simulation shows the physical signal propagation and mixing process. In Figure 5, we can see the chirp behavior for the simulation and the propagation delay in the received chirp, modeling real channel characteristics.

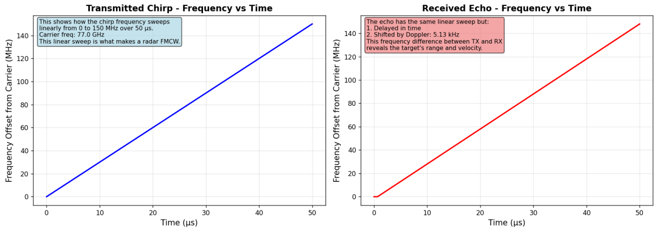


Figure 5: Radar chirp for simple Python simulation

4 Implementation

4.1 mmSpoof vs MadRadar

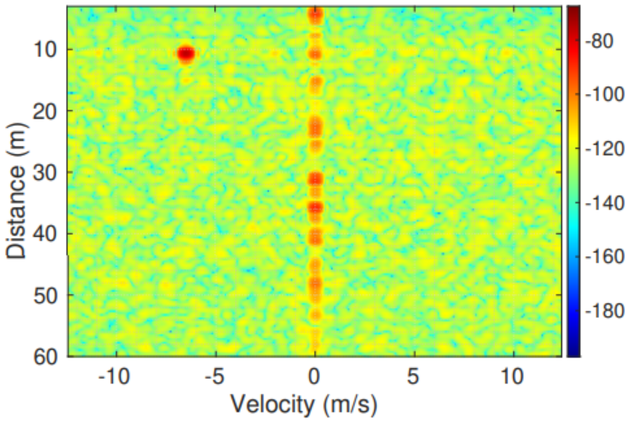


Figure 6: Range-Doppler map of mmSpoof spoofing a car originally at 35 m and 0 m/s to 10 m and 6.5 m/s [1]

mmSpoof's implementation centers around a reflect array with phased arrays and mixers, with an SDR used to digitize signals and estimate key parameters. A key implementation choice for mmSpoof is that it avoids active chirp generation, choosing to reflect the victim's waveform while imposing a controlled f_{shift}, enabling attacks without prior knowledge or victim-attacker synchronization [1]. MadRadar's implementation includes the use of a real-time parameter estimation architecture with an attack platform developed on an SDR. The SDR is used to estimation victim radar parameters and then transmit active spoofing through FP, FN, and translation attacks [2].

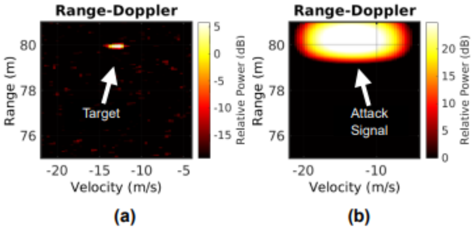


Figure 7: Example of False Negative (FN) attack: a) range-Doppler map without attack, b) range-Doppler map with attack [2]

4.1.1 Our Simulation

The key radar parameters chosen for our simulation are $f_c = 77GHz$, $B = 150MHz$, and $T_{chirp} = 50\mu s$. From these values, we can determine the chirp slope $k = B/T_{chirp} = 3MHz/s$. This slope is also seen in Figure 5.

Processing Chain:
1. Chirp generation - creates baseband transmit waveform
2. Echo generation - simulates the received chirp, spoofing is enabled and calculated in this step
3. Range-Doppler Map - performs 2D FFT to visualize the radar scene

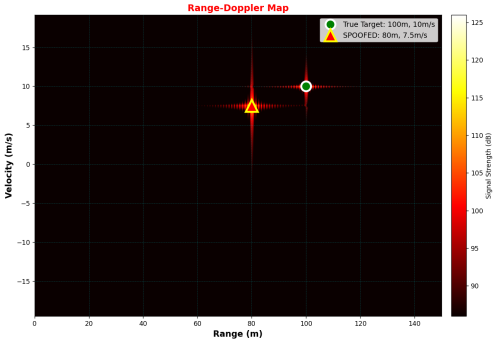


Figure 8: Range-Doppler map with real and spoofed target labeled

The range-Doppler map shown in Figure 8 represents what the simulation can accomplish by showing a labeled real and spoofed target in the scene. The real (true) target is 100 meters from the radar and is moving at 10 m/s. The spoofed target is of similar magnitude but at 80 meters and 7.5 m/s. With no countermeasures built into this simulation, it shows how easy it is to fool a radar into believing two targets are present, when only one is physically real.

5 Evaluation

5.1 mmSpoof vs MadRadar

5.1.1 Spoofing Accuracy

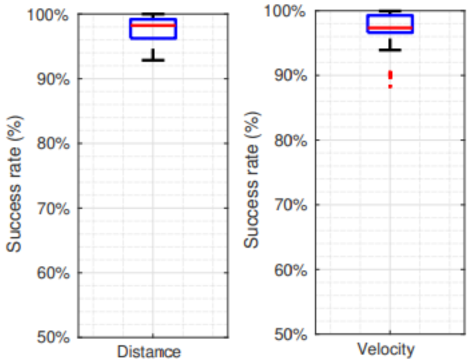
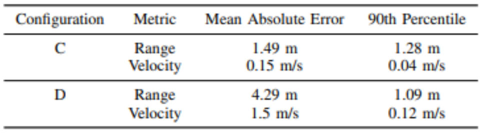


Figure 9: The left figure is the distance validation for spoofing a moving car. The right is the velocity validation for spoofing a moving car. [1]

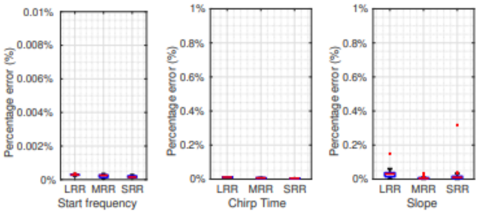
mmSpoof's use of fine-tuned frequency shifts to spoof radar has high accuracy. In Figure 9, the median success rate for distance spoofing is 98.23% and velocity spoofing is 97.34% [1].



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

Figure 10: Absolute error of attacker spoofing accuracy

MadRadar's use of parameter estimation to launch active FP, FN, and Translation attacks also boasts a fairly high spoofing accuracy. Though the results are not in the same format as mmSpoof, from Figure 10, we can extract that the average absolute error in range for a specific configuration is 1.49 meters and 0.15 m/s. The second configuration has much higher error, with 4.29 meters and 1.5 m/s being the average absolute errors [2].

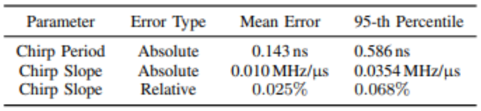


(a) Start frequency (f_0) **(b)** chirp time (T_{chirp}) **(c)** chirp slope (k)

Figure 11: Percent error for mmSpoof parameter estimation with LRR, MRR, and SRR being different radar modes [1]

5.1.2 Parameter Estimation Accuracy

As seen in Figure 11, mmSpoof has a strong parameter estimation method with start frequency (Figure 11a) having a max estimation error of 0.0005%. In Figure 11b, the median error of all radar modes for chirp time is less than 0.02%. Lastly, Figure 11c shows that the maximum median error for all modes is under 0.05% [1].



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
Chirp Slope	Relative	0.025%	0.068%

Figure 12: MadRadar key parameter estimation error metrics [2]

Figure 12 shows the absolute and relative errors for chirp period (chirp time) and chirp slope. For the 95-th percentile error for chirp time, 0.59 ns corresponds to less than 0.1 meters of spoofing error. We also see that the average error for chirp slope is less than 0.03%, meaning the MadRadar parameter estimation method is incredibly accurate and practical [2].

5.2 Our Simulation

Our simulation does not present any physical data, therefore spoofing accuracy would not be present since it is artificially injected. Parameter estimation data would also not be present since we assume that the attacker knows all relevant parameters of the victim's radar. Our code does present a configurable range resolution which is dependent on $\Delta R = c/2B \approx$ 1m, where $B = 150MHz$. This limits our range precision to around 1 meter, but is easily changeable if desired.

5.3 Limitations

5.3.1 mmSpoof

mmSpoof primarily targets range and/or velocity through reflection and frequency shifts, but focuses on creating realistic false targets rather than a broad set of perception-level outcomes like MadRadar. The main limitation of mmSpoof's method is that the attacker's angular direction cannot be spoofed, therefore the angle of spoofing is consistent [1].

5.3.2 MadRadar

MadRadar's effectiveness relies heavily on the accuracy of its black-box parameter estimation model, where any small estimation error can turn into meter-scale range errors. MadRadar also suffers from the same limitation as mmSpoof with angular spoofing not being possible [2].

5.3.3 Our Simulation

The simulation is intentionally simple and demonstrates spoofing at a fundamental level through injecting ideal frequency shifts rather than any physical modeling. This simulation assumes perfect knowledge of the victim radar and omits many physical constraints such as multipath, heavy interference, and hardware requirements. There is also no countermeasures or sensor fusion used, which is typical in automotive radar applications.

6 Conclusion

mmSpoof and MadRadar demonstrate two practical pathways to spoof FMCW radars under realistic, physical constraints. mmSpoof reflects the victim's signal and applies a controlled frequency shift that can spoof range and velocity independently without active transmission or victim-attacker synchronization. MadRadar shows that a real-time black-box parameter estimation model can not only enable false positive attacks, but also false negatives and translation attacks. MadRadar involves detailed parameter estimation and active transmission that spoof both range and velocity. Our simulation supports the core takeaway between mmSpoof and MadRadar in that FMCW radars are susceptible to spoofing attacks and that additional work must be done to ensure FMCW radars have countermeasures to stop malicious actors from manipulating these popular systems in critical applications [1] [2].

6.1 Future Work

A major focus for future work is determining how to spoof angles and choose different directions for spoofing. Another focus is multi-sensor spoofing, as many commercial applications use other modalities such as LiDAR or camera in addition to radars.

7 Acknowledgment

We are thankful to the authors of mmSpoof and MadRadar for the use of their papers to make this comparative analysis of their methods.

References

[1] Rohith Reddy Vennam, Ish Kumar Jain, Kshitiz Bansal, Joshua Orozco, Puja Shukla, Aanjhan Ranganathan, and Dinesh Bharadia. mmspoof: Resilient spoofing of automotive millimeter-wave radars using reflect array. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023.

[2] David Hunt, Kristen Angell, Zhenzhou Qi, Tingjun Chen, and Miroslav Pajic. Madradar: A black-box physical layer attack framework on mmwave automotive fmcw radars. *arXiv preprint arXiv:2311.16024*, 2023.