Toward Spoofing-Resilient & Comm.-Integrated MmWave Radar Sensing: POC Implementation & Analysis

Vedran Beganovic, *Student Member, IEEE*

***Abstract*—Radar is a powerful sensing tool used for object detection and environmental awareness. It is currently used in many applications, particularly in vehicles, such as lane keep assist and cruise control systems. Radar in vehicles will become even more important as autonomous vehicles become the norm because it can operate in rainy or foggy conditions that are difficult for camera-based systems. There exist different radars, such as continuous wave (CW) radar, moving target indication (MTI) radar, and frequency-modulated continuous wave (FMCW) radar. Vehicles typically use mmWave FMCW radars with values of 60 GHz, 77 GHz, and less common 81 GHz in order to get accurate distance, velocity, and angle measurements of objects in the environment. However, radar is vulnerable to spoofing attacks, where the backscattered signal can be manipulated to create fake or ghost targets. This is done by modulating reflections so that the erroneous values of distance, or velocity, or angle. This is especially hazardous for applications like autonomous driving. The goal is to design a spoof-resistant radar called Spoofing-Resilient and Communication-Integrated Radar (SCR) as seen in the paper by Qian and Pathak: *Toward Spoofing-Resilient and Communication-Integrated MmWave Radar Sensing.* SCR is based on two innovative approaches: chirp-splitting and frame-splitting. Chirp-splitting is dividing a chirp into two sub-chirps with different frequency bands. This allows the determination of correct and suspicious peak positions in the velocity spectrum. Frame-splitting is dividing a radar frame into two groups: uniformly sampled and nonuniformly sampled. Spoofing targets show up in the uniformly sampled set. For chirp-splitting the metric of peak-shift was examined and for frame-shifting the metric of peak magnitude difference was examined. A proof-of-concept SCR with one stationary/nonstationary target was implemented and metrics examined. SCR is an exciting approach to spoofing detection, however issues like precise chirp stability persist. Improving multi-path, spatial object detection, and scalability of modulators would enable increased SCR robustness to adversarial targets.**

***Index Terms*—FMCW, SCR, Radar, Communications**

I. Introduction

MILLIMETER (MmWave) sensing in the form of frequency-modulated continuous-wave (FMCW) radar forms an integral part of modern sensing systems along with other sensors such as cameras and LiDARs. MmWave has many useful applications, including autonomous vehicles, object localization, and health monitoring (heart-rate / breathing-rate). MmWave have many advantages over camera sensors including working in low-light/night conditions, foggy conditions, and directly measuring object velocity [1].

In the radio frequency (RF) space, there exists a possibility of performing spoofing on targets. Spoofers manipulate backscattered radar signals to generate “ghost targets” and is different than jamming, which is overpowering a certain frequency to disorient a sensor. Spoofing is a well-known phenomenon for Global Positioning System (GPS) systems: frequencies L1 (1575.42 MHz)[2] and L5 (1176.45 MHz) [3] in conflicts such as the Russia-Ukraine war [4].

The area of mmWave spoofing for attack/defense is much newer due to recent autonomous vehicle development and the higher frequencies involved (GHz vs MHz). Detecting MmWave spoofing is an developing field and an interesting paper in this field that was examined here was *Toward Spoofing-Resilient and Communication-Integrated MmWave Radar Sensing (SCR)* by Qian and Pathak (2025).

Prior work in this area involves frameworks such as mmSpoof and MadRadar [5], [6]. MmSpoof involves reflection-based spoofing, where the main advantage is that the spoofing of range and velocity is possible without having to synchronize with the targets. There is an adversarial reflector that deliberately crafts frequency shifts to create realistic ghost targets for malicious reasons, while the SCR framework assumes the modulations are inherently different for natural objects, spoofed targets, and communication tags in the environment. MadRadar focuses on "black-box" attack generality instead of "physical-layer interpretability". The black-box approach treats the radar with a probing approach and use optimizations to induce erroneous detections without knowing the radar's parameters. This general approach is less useful when even some basic adversary radar parameters are known or can be inferred.

II. Methods

A. FMCW

Mathematically, SCR is will be described below. Starting with the FMCW chirp, it is given as:

$$s(t,u) = e^{j2\pi\left(f_c t + \frac{1}{2}\gamma t^2\right)}, \quad -\tfrac{T_r}{2} \leqslant t \leqslant \tfrac{T_r}{2}, \quad u = nT_c, \quad n \in \mathcal{N} \tag{1}$$

V. Beganovic is with the Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute (RPI), Troy, NY, 12180 USA e-mail: beganv@rpi.edu

where $s(t,u)$ is a function of slow time, u and t is fast time. Slow time is the starting time for each chirp and fast time is transmit time for each sample of each chirp. Graphically, the FMCW chirp can be seen in Figure 1.

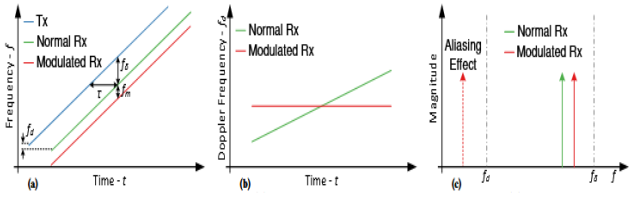


Figure 1: Frequency Modulated Continuous Wave (FMCW) waveforms, a-b: time vs frequency, c: magnitude vs frequency [7]

Additionally, slow time and fast time can be visualized in Figure 2, where one dimension is the fast time (Range) and the other dimension is the slow time.

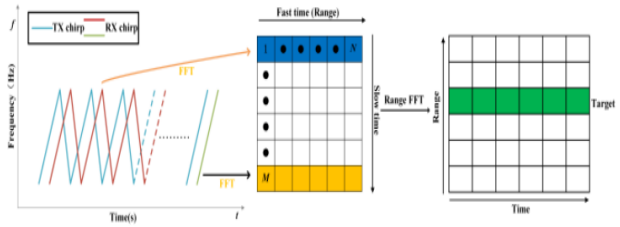


Figure 2: Slow and Fast Time FFT Representation

For a single object at a distance, d, the round-trip delay is given as $\tau = \frac{2d}{c_0}$. The received signal model is then $r(t,u) = \beta s(t-\tau, u)$, where β is a coefficient that represents the attenuation phenomena. Substituting into $s(t,u)$ and τ, the received signal

$$r(t,u) = \beta e^{j2\pi\left(f_c\left(t-\frac{2d}{c_0}\right)+\frac{1}{2}\gamma\left(t-\frac{2d}{c_0}\right)^2\right)} \tag{2}$$

Additionally, the baseband signal is given as

$$b(t,u) = s(t,u)r^*(t,u) \tag{3}$$
$$= \beta e^{j4\pi\left(f_c\frac{d}{c_0}+\gamma t\frac{d}{c_0}-\gamma\frac{d^2}{c_0^2}\right)} \tag{4}$$
$$\approx \beta e^{j\frac{4\pi}{c_0}(f_c d_0+\gamma d_0 t-\gamma v u t-f_c v u-f_c v t)} \tag{5}$$

The instantaneous frequency shifts of both the fast time t and the slow time u are given as

$$f_t' = \frac{1}{2\pi}\frac{\partial\angle b}{\partial t} \approx \frac{2\gamma\left(d_0-vu\right)}{c_0} - \frac{2f_c v}{c_0}, \tag{6}$$
$$f_u' = \frac{1}{2\pi}\frac{\partial\angle b}{\partial u} \approx -\frac{2\left(f_c+\gamma t\right)v}{c_0} \tag{7}$$
$$f_t'' = \frac{1}{2\pi}\frac{\partial\angle b}{\partial t} = f_m \tag{8}$$
$$f_u'' = \frac{1}{2\pi}\frac{\partial\angle b}{\partial u} = f_m \tag{9}$$

B. *Chirp-splitting*

Chirp-splitting is also known as velocity-modulation detection. It is possible to differentiate two types of frequency shifts by transmitting the chirp split into two pieces: The lower half of chirp has a slightly lower carrier frequency and the upper half of chirp has a slightly higher carrier frequency. For a real/natural object the Doppler plot scales with the carrier frequency so the peaks line up. For a modulated backscatterer / spoofer the Doppler response is independent of the carrier, so the peaks will misalign. The metric checked for chirp-splitting is the Peak-Shift. When examining the Doppler peak misalignment, it is shown that large shifts are more indicative of spoofing.

Mathematically, the key idea in chirp-splitting is calculating the finer-grained pseudospectrum to overcome the limitation of velocity spectrum resolution. Given N_c chirps, we can form the steering vector for any frequency shift f_d as:

$$\vec{a}\left(f_d\right) = \left(1, e^{j2\pi f_d T_c}, \cdots, e^{j2\pi f_d (N_c-1)T_c}\right)^T \tag{10}$$

C. *Frame-splitting*

Frame-splitting is also known as distance-modulation detection. The method involves grouping the chirps into two categories: Even-numbered chirps (uniform timing), mathematically written as $t_k = kT$ and odd-numbered chirps (jittered timing), mathematically written as $t_k = kT + \delta_k$. For a real/natural object, it does not depend on chirp timing, so peaks remain similar. In contrast, for a modulated backscatterer / spoofer, it relies on aliasing and collapses when timing is changed. The metric used for frame-splitting is Peak magnitude difference, $\text{magdiff}_{peak} = \frac{(|P_{uniform}-P_{jittered}|)}{P_{uniform}}$. When examining the difference between coherent peak energy under uniform vs jittered it was shown that larger reductions is more indicative of spoofing along with the splitting.

III. Results & Discussion

Initial attempts with a stationary object placed at 18 m as seen in Figure 3 was successful as seen by the large obvious signal magnitude peak at 18 m. With the object moving at $v = 1.2\,\frac{\text{m}}{\text{s}}$, accurate Doppler values were generated as seen in Figure 4 In the nonstationary case, the red line represents a strong moving target with a well-defined velocity. The yellow line is present due to the presence of sidelobes/leakage. This occurred because

even with using a Hann window compared to a simpler rectangular window, this does not completely eliminate the sidelobes. Examining the SCR implementation, for chirp-splitting in Figure 5. With the case of no spoofing, the chirp peaks line up. In the case of spoofing, the chirp peaks exhibit splitting. Similarly, examining SCR implementation, for the case of frame-splitting in Figure 6. In the case of no spoofing, the chirp peaks in each frame line up and have similar magnitude. In the case of spoofing, the chirp peaks exhibit frame splitting and show a decrease in magnitude along with splitting.

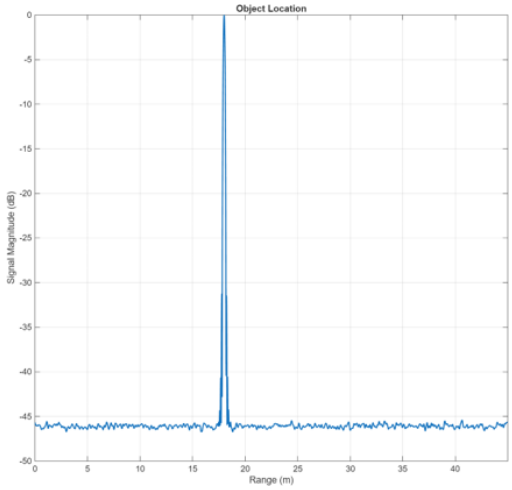


Figure 3: Peak location displays distance from the radar

IV. Conclusion

Overall, Spoofing-Resilient & Communications-Integrated MmWave Radar Sensing (SCR) was studied and implemented in a proof-of-concept with one target (stationary and nonstationary) and one spoofer. For SCR, the metrics of peak shift and peak magnitude were examined. Compared to the original paper, only a simulated MATLAB environment was developed here. Hardware verification would have interesting to implement, but it is harder due to needing to meet specific hardware specifications. Additionally, future work would be incorporating multi-frequency and multi-path approaches to more fully examine the robustness of SCR and identify areas of improvement.

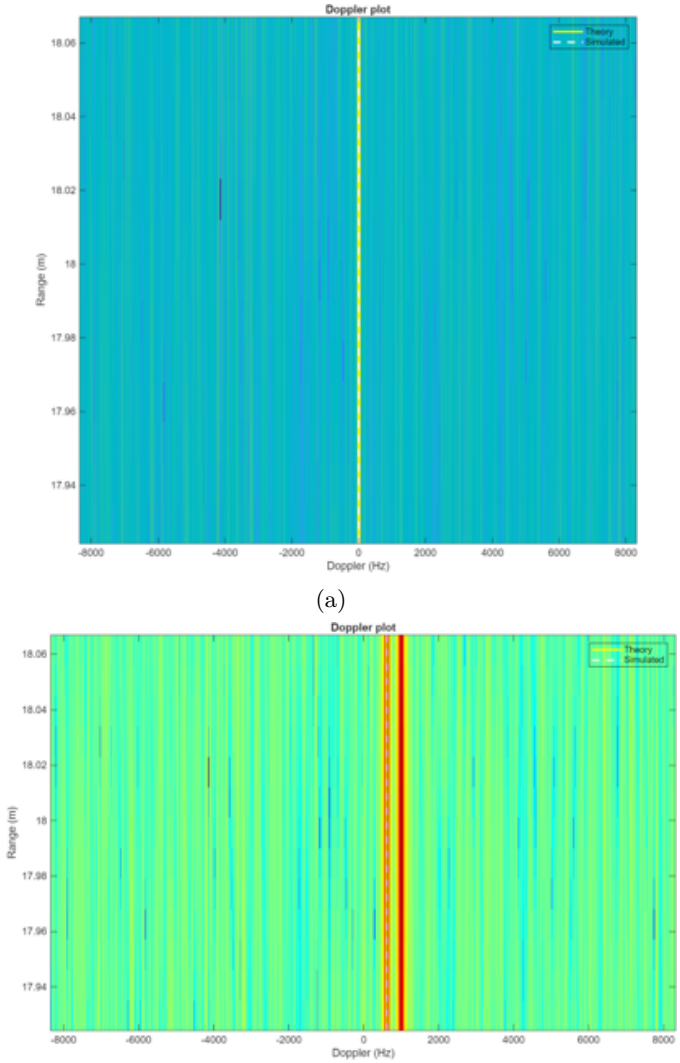


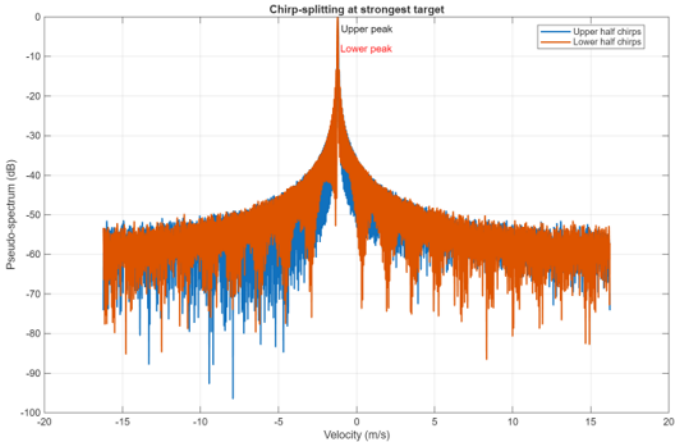
Figure 4: (a) Stationary, $d = 18\,\text{m}$, $v = 0\,\frac{\text{m}}{\text{s}}$ (b) Nonstationary, $d = 18\,\text{m}$, $v = 1.2\,\frac{\text{m}}{\text{s}}$. The red line represents the peak Doppler energy (*i.e.* the maximum magnitude) and the yellow line represents sidelobes/leakage. The theoretical red line and the simulated values overlap suggesting good agreement between theory and simulation.

References

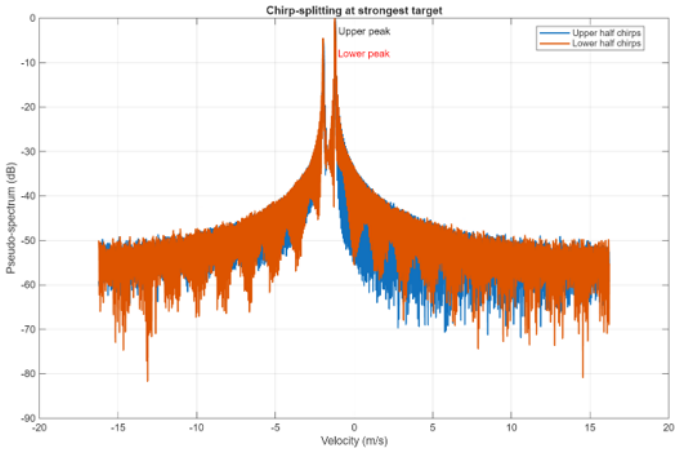
[1] A. Soumya, C. K. Mohan, L. R. Cenkeramaddi, A. Soumya, C. K. Mohan, and L. R. Cenkeramaddi, "Recent Advances in mmWave-Radar-Based Sensing, Its Applications, and Machine Learning Techniques: A Review", en, *Sensors*, vol. 23, no. 21, Oct. 2023, Company: Multidisciplinary Digital Publishing Institute Distributor: Multidisciplinary Digital Publishing Institute Institution: Multidisciplinary Digital Publishing Institute Label: Multidisciplinary Digital Publishing Institute Publisher: publisher Citations: 73 (Crossref) [2025-12-17] Citations: 74 (SemanticScholar) [2025-12-17], ISSN: 1424-8220. DOI: 10.3390/s23218901. [Online]. Available: https://www.mdpi.com/1424-8220/23/21/8901.

[2] A. R. Baziar, M. Moazedi, and M. R. Mosavi, "Analysis of Single Frequency GPS Receiver Under Delay and Combining Spoofing Algorithm", en, *Wireless Personal Communications*, vol. 83, no. 3, pp. 1955–1970, Aug. 2015, Citations: 24 (Crossref) [2025-07-08] Citations: 29 (SemanticScholar) [2025-07-08], ISSN: 1572-834X. DOI: 10.1007/s11277-015-2497-9. [Online]. Available: https://doi.org/10.1007/s11277-015-2497-9.

[3] C. M. Smitham, "GPS Program Update to Civil GPS Service Interface Committee (CGSIC)", en,

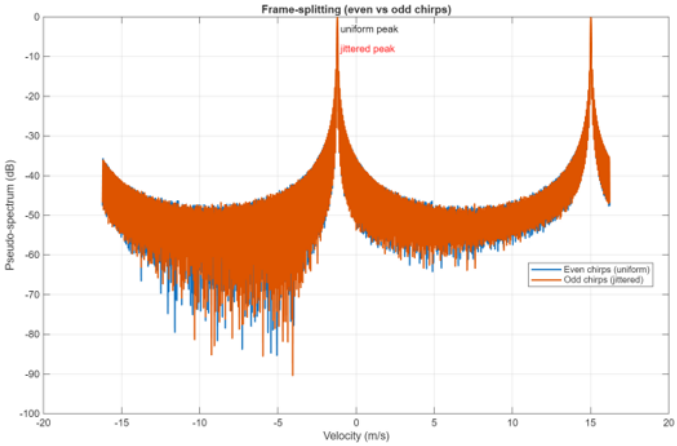


(a)

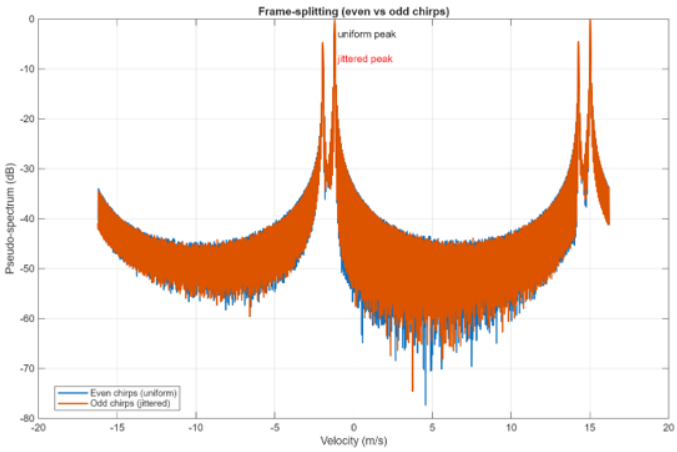


(b)

Figure 5: Chirp-splitting: (a) No spoofer, (b) Spoofer. In the case of no spoofing, the chirp peaks line up. In the case of spoofing, the chirp peaks exhibit splitting



(a)



(b)

Figure 6: Frame-splitting: (a) No spoofer, (b) Spoofer. In the case of no spoofing, the chirp peaks in each frame line up. In the case of spoofing, the chirp peaks exhibit frame splitting and show a decrease in magnitude

[4] *Russia's GPS interference is the new normal*, en-GB, Oct. 2025. [Online]. Available: https://www.politico.eu/article/russia-gps-swedish-finnish-polish-jamming-tech-risks/.

[5] R. Reddy Vennam et al., "mmSpoof: Resilient Spoofing of Automotive Millimeter-wave Radars using Reflect Array", en, in *2023 IEEE Symposium on Security and Privacy (SP)*, Citations: 15 (Crossref) [2025-07-07] Citations: 14 (SemanticScholar) [2025-07-07], San Francisco, CA, USA: IEEE, May 2023, pp. 1807–1821, ISBN: 978-1-6654-9336-9. DOI: 10.1109/SP46215.2023.10179371. [Online]. Available: https://ieeexplore.ieee.org/document/10179371/.

[6] D. Hunt, K. Angell, Z. Qi, T. Chen, and M. Pajic, "MadRadar: A Black-Box Physical Layer Attack Framework on mmWave Automotive FMCW Radars", en, in *Proceedings 2024 Network and Distributed System Security Symposium*, Citations: 10 (Crossref) [2025-07-27] Citations: 13 (SemanticScholar) [2025-07-27], San Diego, CA, USA: Internet Society, 2024, ISBN: 978-1-891562-93-8. DOI: 10.14722/ndss.2024.24153. Accessed: Jul. 27, 2025. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/ndss2024_f153_paper.pdf.

[7] K. Qian and P. Pathak, "Toward Spoofing-Resilient and Communication-Integrated MmWave Radar Sensing", en, 2025.